Cybersecurity Trends

Édition spéciale. Juin 2022

- État de la question et cas réels
- Solutions pour se défendre

Cyber-Espionnage économique et technologique : comment protéger votre entreprise et vos employés.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Embassy of Switzerland in Romania

CHAMBER OF COMMERCE
SWITZERLAND – ROMANIA

Host and support:

CYBER ESPIONAGE AWARENESS DAY FOR BUSINESS

With the support of:

Swiss Sponsors' Fund România

web for your business
swiss webacademy

Media partner:

BURSA
ZIARUL OAMENILOR DE AFACERI

In partnership with:

CMCS INTERNATIONAL

FIC Forum International de la Cybersécurité

digiVolution

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Gendarmerie nationale

Centre de recherche de l'EOGN

POLICE GENÈVE

RC3 Regional Cyber Competence Center Western Switzerland

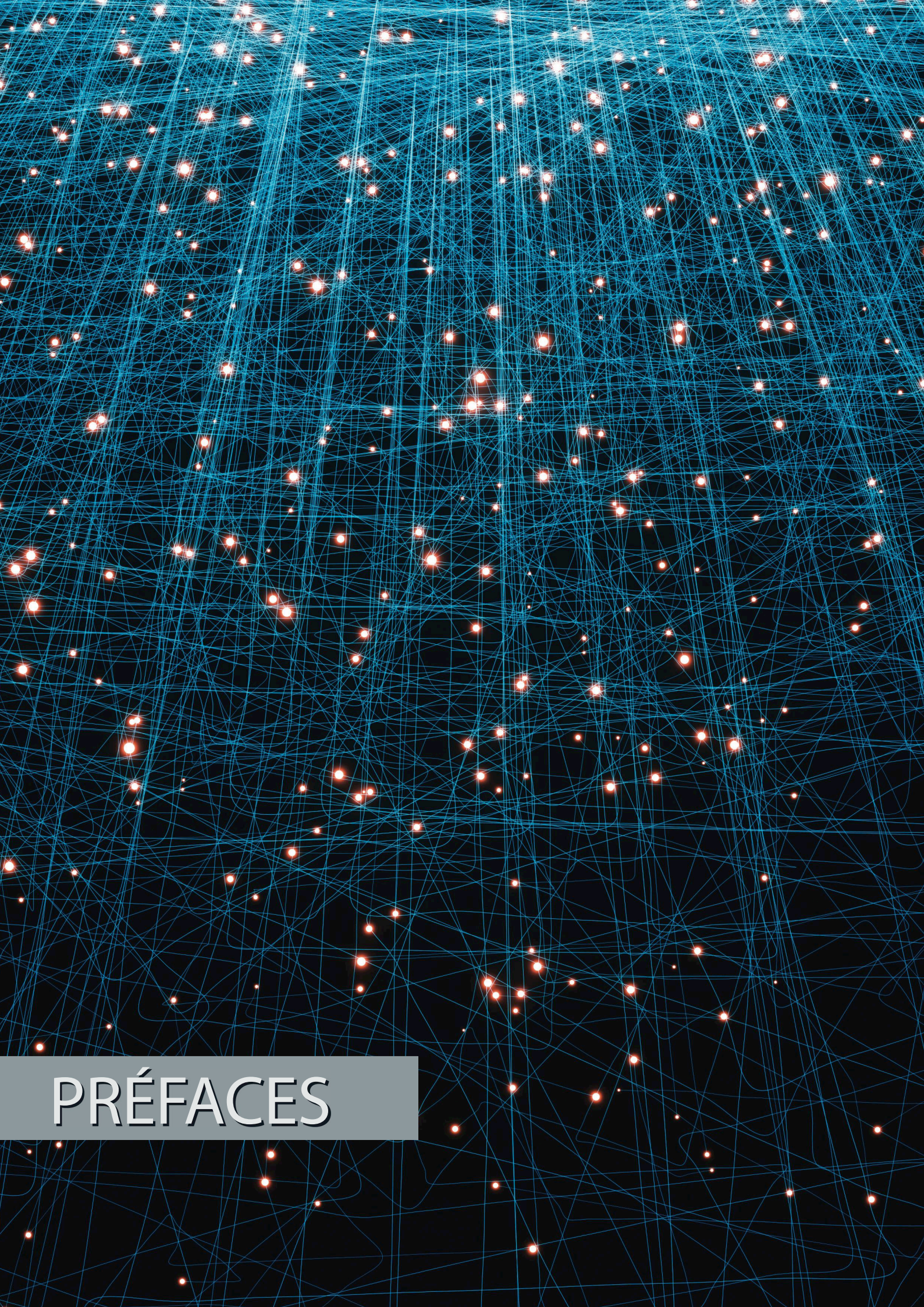
ROMANIA CYBERINT SERVICIUL ROMÂN DE INFORMAȚII

IGPR POLIȚIA ROMÂNĂ

DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ

Bucharest, June 14, 09:00-14:00, New Europe College / Swiss House, Strada Plantelor, 21
Live streaming upon inscription: www.bursa.ro

Index



PRÉFACES

Préambule.

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Ambassade de Suisse en Roumanie

Auteur : Arthur Mattli,
Ambassadeur de Suisse en Roumanie

La bataille de Talas, au 8ème siècle, fut un combat aux répercussions civilisationnelles énormes. Elle a vu se confronter la civilisation arabe (le califat Abbasside) et la civilisation chinoise (l'Empire des Tang). Suite à la défaite de l'armée des Tang, des prisonniers chinois ont négocié leur libération en échange de la livraison des secrets de la fabrication du papier.

Le papier servait alors de moteur à la civilisation : il a permis de diffuser les religions, les idéologies, l'architecture, l'ingénierie, la médecine et de cartographier le monde. De la même façon, les nombreuses formes d'échanges de données électroniques servent aujourd'hui de moteurs à la civilisation et à la société numérisées.

La quête de suprématie sur cette civilisation digitale, ou sur certaines de ses composantes, a pris de nombreuses formes. Notre utilisation de la connectivité des données s'accompagne d'un coût et d'un risque de plus en plus élevés.

S'il existe un large consensus sur le fait que l'accès et le traitement des données apportent généralement, grâce au monde digital, de grands avantages à la civilisation, l'émergence d'une utilisation critique des données peut conduire à des abus totalitaires et constituer une menace pour les réalisations d'une civilisation, d'une société et de ses libertés.

Ces périls, s'ils ne sont pas compris, détectés et combattus, peuvent entraîner des changements aussi majeurs qu'indésirables dans le monde.

Contrairement au cas de la bataille du 8ème siècle, les acteurs opérant dans le monde numérique, de même que leurs activités, sont désormais d'une telle complexité, profondeur et rapidité qu'ils deviennent de plus en plus difficiles à appréhender et à contrer, pour un seul État.

L'interopérabilité, mot clé des systèmes de défense intégrés, s'applique également dans le monde numérique et en cas de crise majeure. Les effets de la pandémie COVID-19 ont eu un impact sans précédent sur la société mondiale. Ils ont révélé la vulnérabilité des États et mis en lumière la nécessité d'une intégration plus efficace des données et d'une meilleure coordination entre les gouvernements et les entreprises.

La pandémie et la guerre en Ukraine ont montré que les *fake news*, la désinformation ou la propagande ont atteint de nouveaux sommets et que ce type de phénomène accompagnera toutes les crises majeures à venir.

La manipulation des systèmes de la société numérisée va aujourd'hui de pair avec une bonne maîtrise des contenus à utiliser, à partager et à distribuer.

L'objectif de la présente publication est de contribuer à la prise de conscience des tendances de notre cyberespace, de comprendre ses évolutions fulgurantes et d'exposer ce qui doit l'être lorsque nos acquis civilisationnels et sociaux sont en danger.

Cette publication est une invitation à rester vigilant face aux dangers qui nous guettent et nous rappelle que chaque entreprise, chaque famille, chaque utilisateur individuel doit décider lui-même comment et quoi consommer, partager et offrir en termes de données.

Je remercie chaleureusement le Prof. Laurent Chrzanovski pour avoir initié, coordonné et édité la présente publication. ■

Le Bureau du Programme sur la Cybercriminalité du Conseil de l'Europe (C-PROC).

Auteur : Virgil SPIRIDON,
Chef des opérations, C-PROC

Le Bureau du programme sur la cybercriminalité du Conseil de l'Europe (C-PROC) à Bucarest, en Roumanie, est opérationnel depuis avril 2014 et a pour mandat d'aider les pays de toutes les régions du monde à renforcer leurs capacités de justice pénale en matière de cybercriminalité et de preuves électroniques sur la base de la Convention de Budapest sur la cybercriminalité.

BIO

Virgil Spiridon est chef des opérations du Bureau du programme sur la cybercriminalité du Conseil de l'Europe (C-PROC), basé à Bucarest et responsable de la gestion des projets de renforcement des capacités en matière de cybercriminalité du Conseil de l'Europe. Avant de rejoindre le C- PROC, Virgil Spiridon a été directeur adjoint de la Police Nationale roumaine pendant trois ans, avec des responsabilités dans les domaines du crime organisé, du contre-terrorisme et des crimes financiers. Virgil Spiridon a dirigé l'Unité Nationale roumaine de lutte contre la cybercriminalité de 2003 à 2012, au sein de la Police Nationale: une unité qu'il a créé et développée et dont il a établi la stratégie de lutte contre la cybercriminalité. Il a piloté les projets EMPACT sur la cybercriminalité et la fraude par carte de crédit et a participé à la rédaction de l'étude sur les bonnes pratiques de l'unité spécialisée dans la cybercriminalité dans le cadre du projet IPA coordonné par le Conseil de l'Europe.

Le C-PROC a ainsi opéré dans un contexte défini par :

(a) l'évolution des défis posés par la cybercriminalité et les preuves électroniques aux droits de l'homme, à la démocratie et à l'état de droit,

(b) la portée et l'impact croissants de la Convention sur la cybercriminalité depuis son ouverture à la signature il y a vingt ans,

(c) la finalisation du deuxième protocole additionnel à la Convention,

(d) le début d'un processus des Nations Unies visant à un nouveau traité sur la lutte contre l'utilisation des technologies de l'information et de la communication à des fins criminelles,

(e) la pandémie COVID-19.

Le C-PROC a contribué de manière significative :

- au renforcement des capacités de la justice pénale et de la législation sur la cybercriminalité et les preuves électroniques ;
- à l'élaboration de guides et d'outils sur les questions de cybercriminalité et leur mise en œuvre;
- à l'adhésion à la Convention de Budapest et sa mise en œuvre ;
- au processus d'élaboration du deuxième protocole additionnel à la convention de Budapest;
- aux synergies avec d'autres organisations et projets.

La formule de la Convention de Budapest en tant que norme commune, soutenue par le Comité de la Convention sur la cybercriminalité (T-CY) et

le renforcement des capacités par le biais du C-PROC, a continué d'avoir un impact. Avec le deuxième protocole additionnel, la Convention de Budapest devrait rester le mécanisme international le plus pertinent pour les années à venir.

Les priorités pour l'année prochaine comprennent :

(a) le soutien à la mise en œuvre du deuxième protocole additionnel,

(b) le renforcement des garanties en matière de droits de l'homme, d'État de droit et de protection des données,

(c) l'amélioration des capacités pour la réalisation d'activités en ligne,

(d) les synergies avec d'autres instruments et mécanismes du Conseil de l'Europe ainsi qu'avec d'autres organisations,

(e) l'extension des projets actuels et la conception de nouveaux projets afin de garantir le financement du futur renforcement des capacités.

Le C-PROC est un élément clé de l'approche du Conseil de l'Europe en matière de cybercriminalité, qui comprend :

(a) la Convention de Budapest et les normes connexes,

(b) des évaluations de suivi par le Comité de la Convention sur la cybercriminalité (T-CY),

(c) le renforcement des capacités.

La pandémie de COVID-19 a rendu les individus et la société extrêmement vulnérables à tous les égards et, pendant cette période, les autorités de justice pénale ont dû s'engager dans une coopération totale pour détecter, enquêter, poursuivre et traduire en justice ceux qui exploitent la pandémie de COVID-19 à leurs propres fins criminelles.

Le C-PROC a essayé d'atténuer l'impact sur la cybercriminalité et le travail de la justice pénale en abordant les nouvelles formes de cybercriminalité et en répondant aux besoins actuels des pays. Le soutien au renforcement des capacités n'a pas été interrompu ; il a simplement été adapté et dispensé principalement à distance.

Le Bureau a maintenu sa réputation de centre d'excellence en matière de cybercriminalité et a consolidé la position du Conseil de l'Europe en tant que leader mondial pour le renforcement des capacités en matière de cybercriminalité et de preuves électroniques.

Nous tenons à féliciter les organisateurs de la première édition de la «*Journée de sensibilisation au cyberespionnage pour les entreprises*», qui s'est tenue à Bucarest en partenariat avec d'autres parties prenantes, pour avoir abordé ce sujet d'actualité.

L'événement visait à assurer des débats riches avec une large participation et des positions variées adaptées à la sensibilité du sujet.

Le C-Proc a contribué à l'événement en intervenant sur le renforcement des capacités en matière de cybercriminalité, qui constitue le cadre de la mise en œuvre au niveau mondial de la législation sur la cybercriminalité et les preuves électroniques, ainsi que des normes et des meilleures pratiques internationales.

Comme dans le monde physique, l'approche des droits de l'homme et la règle de droit devraient également s'appliquer dans le cyberespace.

La présente publication, offerte par les organisateurs et accessible gratuitement au plus grand nombre, permettra de mieux comprendre les défis auxquels sont confrontés, au niveau international, les autorités de justice pénale et les autres acteurs impliqués dans la lutte contre la cybercriminalité et la cybersécurité.

Enfin, nous exprimons notre gratitude à tous les spécialistes qui ont accepté de partager leurs connaissances lors de l'événement ainsi qu'à tous ceux qui ont participé à cette publication. ■

Cyber-espionnage - savoir le détecter pour pouvoir le contrecarrer.

Auteur : Général Anton Rog,
Directeur Général, centre CYBERINT

Le cyber-espionnage, généralement réalisé par le biais d'opérations de *type Advanced Persistent Threat* (APT), constitue la principale cyber-menace pour la sécurité nationale de la Roumanie, étant donné que ce type d'activité vise à obtenir des informations stratégiques à partir de réseaux et de systèmes d'information ayant une valeur critique pour la sécurité de notre nation.

Pour une meilleure clarification conceptuelle des opérations de cyber-espionnage, il est nécessaire de passer brièvement en revue certains éléments du cadre juridique international applicable dans le cyberespace, en se référant au Manuel de Tallinn 2.0[1], à la Convention de Vienne sur les relations diplomatiques et à la Convention de Vienne sur les relations consulaires, qui offrent des définitions claires et universellement reconnues de chaque type d'événement :

- **Cyber-opération** - une action dans le cyberespace qui peut causer des inconvénients ou des perturbations aux systèmes informatiques, mais qui ne cause pas de dommages physiques. Une telle action peut faire partie d'une cyber-attaque.
- **Cyber-attaque** - une cyber-opération défensive ou offensive capable de causer des dommages physiques et/ou humains.
- **Cyber-espionnage** - activité menée clandestinement en utilisant des capacités digitales pour obtenir des informations. Les cibles du cyber-espionnage peuvent être aussi bien des États que des entités privées.

Alors qu'une cyber-attaque cause des dommages physiques, tels que la mise hors service de réseaux et de systèmes informatiques ou la perte d'actifs financiers, les cyber-opérations du domaine de l'espionnage sont menées dans le but précis de voler des informations, généralement de valeur stratégique, dans les réseaux et systèmes gouvernementaux.

Ainsi, en fonction des objectifs visés, le cyber-espionnage peut être de deux types : politico-stratégique et économico-industriel.

En ce qui concerne le cyber-espionnage politico-stratégique, il vise principalement les grandes institutions gouvernementales afin d'obtenir des informations dans des domaines tels que la défense, les affaires étrangères, les affaires intérieures ou le renseignement.

Le cyber-espionnage espionnage économico-industriel est pratiqué pour obtenir un avantage économique en dérobant la propriété intellectuelle et les résultats d'instituts de recherche et de développement et d'entreprises privées.

Au-delà de cette différenciation, ces types de cyber-attaques impliquent des ressources financières importantes – de l'ordre de millions d'Euros – et sont caractérisées par un très haut niveau de complexité des applications et infrastructures utilisées, y compris l'exploitation de vulnérabilités de type *zero-day*.

Dans ce contexte, il convient de souligner que les opérations de cyber-espionnage visent souvent les institutions de plusieurs États, simultanément, sans être conçues spécifiquement pour un État particulier, mais plutôt pour une zone géographique dans son ensemble.

Étapes d'une opération de cyber-espionnage et éléments du modus operandi

Ciblage

Dans la première étape, appelée *ciblage*, les attaquants établissent les buts de l'opération de cyber-espionnage, en fonction des objectifs fixés et des spécificités de l'État / de l'organisation qui détient les informations qu'il cherche à extraire. Dans certaines situations, les activités réelles peuvent être menées par d'autres cyber-groupes hostiles, agissant en étroite coordination avec les attaquants.

Reconnaissance

Plus tard, au cours de la phase de *reconnaissance*, l'attaquant entame un vaste processus pour apprendre à connaître la cible, par des moyens tels que l'open source, l'interaction passive avec la cible ou l'acquisition de ces données à partir de forums spécifiques. La reconnaissance vise également à obtenir des connaissances sur l'architecture des réseaux et des systèmes de la victime.

Développement de logiciels malveillants personnalisés

Sur la base des activités précédentes, les attaquants développent un complexe de logiciels malveillants et d'autres outils techniques, chacun remplissant des fonctions spécifiques dans la future opération de cyber-espionnage. Les *exploits* sont également utilisés pour se calibrer sur la spécificité et ainsi s'adapter au système de résilience de chaque victime individuelle. C'est également à ce stade que la méthode d'infection de la victime est déterminée, la technique la plus couramment utilisée étant le *spearphishing*.

Méthodes d'extraction des données

D'après l'expérience du National CYBERINT Centre, les cyber-acteurs hostiles utilisent diverses méthodes pour extraire des données des infrastructures cibles, notamment :

- création d'un serveur/partition dédié sur lequel sont déplacées les données qui seront extraites, puis cryptées et segmentées en paquets afin d'optimiser le processus et réduire les risques d'identification.
- création des boîtes aux lettres sur le serveur dédié de l'organisation dont les noms seront familiers à ceux des employés des organisations concernées (y.c. remplacement de certaines lettres par des chiffres ou des majuscules) et extraire des paquets de données en envoyant des e-mails avec des pièces jointes.
- mise en œuvre de la *stéganographie*, c'est-à-dire l'utilisation de fichiers photographiques ou vidéo déjà présents sur le réseau ciblé dans le but d'y cacher et d'y manipuler les fichiers destinés à en être extraits.

Afin de rendre l'extraction des données d'intérêt plus efficace, les attaquants peuvent utiliser des types de *logiciels malveillants* dotés de moteurs de recherche qui indexent les éléments d'intérêt sur le serveur ciblé, qui sont généralement des noms de hauts responsables.

Détection d'opérations de cyber-espionnage :

Il est clair que la sophistication accrue de ces opérations rend souvent impossible leur détection par les solutions standard. Les technologies basées sur l'intelligence artificielle deviennent donc l'allié des experts en cyber-sécurité, permettant d'identifier les cyber-menaces en analysant les anomalies dans le comportement des réseaux.

Afin de rendre la détection plus difficile avec les solutions basées sur l'intelligence artificielle et d'assurer la persistance pendant de longues périodes, les cyber-attaquants peuvent effectuer des optimisations de la configuration du réseau de la victime. En outre, les attaquants créent de multiples chemins d'accès au réseau pour s'assurer que, même s'ils ont été détectés et retirés du réseau, ils peuvent reprendre leur activité et effectuer des déplacements latéraux au sein du réseau.

Des méthodes d'investigation spécifiques, telles que le *reverse engineering* ou l'analyse des indicateurs de compromission et/ou d'attaque, nous ont montré que les attaquants sont le plus souvent présents depuis longtemps dans le réseau de la victime, et que leur présence est souvent détectés après bien des années.

Ces cyber-opérations ont également été identifiées en temps réel par le Centre national CYBERINT, notamment grâce à l'utilisation de solutions de cyber-sécurité fondées sur l'intelligence artificielle, mais aussi en tirant parti du partage d'informations avec des organisations similaires.

Après la détection, afin d'atténuer les effets d'une opération de cyber-espionnage, il est nécessaire de mener un processus public d'attribution, dit de *blame and shame (blâme et honte)*, afin de décourager les acteurs des cyber-opérations en les poussant à abandonner ou, tout du moins, en les empêchant d'utiliser les mêmes méthodes et outils techniques.

Même si les cas où les acteurs étatiques qui abandonnent sont rares, les approches fondées sur l'approche *blame and shame* permettent de marquer une pause dans l'activité des acteurs hostiles et obligent les attaquants à investir de nouvelles sommes et à reconfigurer leurs méthodes opératives.

Nous tenons ici à saluer les responsables des deux initiatives (le congrès de Bucarest et le présent volume) ainsi qu'à adresser nos remerciements à tous les spécialistes qui ont accepté de partager leur savoir durant l'événement, de même qu'à tous les auteurs des textes constituant cette publication, qui assure la pérennité des riches débats de Bucarest, qu'elle vient approfondir, tout en en garantissant l'accessibilité auprès du plus grand nombre puisqu'éditée et offerte à tous en trois versions linguistiques. ■

BIO

Le général de brigade Anton Rog est le chef du centre national CYBERINT au sein du service de renseignement roumain (SRI). Le CYBERINT est chargé de mener des activités 24 heures sur 24 et 7 jours sur 7 pour découvrir, caractériser et contrer de manière proactive les cyber-menaces contre les systèmes et les réseaux essentiels à la sécurité nationale de la Roumanie. Anton Rog a occupé divers postes de développement technique, notamment dans la conception de logiciels et de systèmes. Il a également occupé le poste de directeur adjoint au sein du département central IT&C du SRI. Il est actif au sein de la communauté universitaire en tant que professeur associé au Centre DRESMARA, à Brasov. Anton Rog a obtenu une licence en technologie de l'information à l'Université de Bucarest en 1998 et un diplôme d'études supérieures en gestion de programmes et de projets du Centre DRESMARA en 2011. Il a été décoré Chevalier de l'Ordre de la Virilité et de la Foi en 2014 et Chevalier de l'Ordre de la Vertu Militaire en 2005 par deux présidents de la Roumanie.

L'espionnage nous cible tous : le contrer nous concerne tous.

Auteur : Colonel Monica Bonfanti,
Commandante de la Police cantonale genevoise

Le soutien accordé par la Police genevoise au Colloque international de Bucarest *«Cyber Espionage Awareness Day for Business»* ainsi qu'à la présente édition du magazine CyberSecurity Trends que j'ai le plaisir de préfacer, pourrait de prime abord sembler étranges. En effet, la lutte contre l'espionnage, coordonnée et menée par la Confédération, n'est à priori pas de la compétence d'un corps de police. Cependant, les débats du colloque, immortalisés, enrichis et approfondis par la publication que vous allez parcourir, démontrent le contraire.

BIO

Madame Monica Bonfanti est diplômée d'études de sciences forensiques à l'Institut de police scientifique et criminologie (IPSC) de l'Université de Lausanne. En 2001, elle y obtient un doctorat. Entre 1993 et 1998, elle a officié en tant qu'enseignante à l'IPSC. De septembre 1993 à janvier 2000, elle a été experte auprès des tribunaux suisses et français, plus particulièrement dans le domaine des armes à feu et des traces d'outils. De septembre 1993 à janvier 2000, elle a été responsable de l'enseignement et de la recherche dans le domaine des armes à feu, des résidus de tir, des traces d'outils ainsi que de la formation de tir avec armes de poing à l'IPSC. En février 2000 Madame Monica Bonfanti intègre le corps de police du canton de Genève, en qualité de cheffe technique de la Brigade de police technique et scientifique (BPTS). En août 2006, elle accède à la plus haute fonction de la police cantonale genevoise en devenant Commandante.

Avec l'accélération et la diversification exponentielle des moyens utilisés par les criminels dans l'espace digital, les policiers devront posséder la formation, l'expérience et les outils nécessaires pour pouvoir déceler des cybercrimes aux enjeux globaux et à l'échelle internationale derrière des phénomènes paraissant comme locaux.

La Police genevoise héberge le RC3 *(Regional Cyber Competence Center – Western Switzerland)* qui, au contact des organismes nationaux, œuvre dans le cadre de la stratégie nationale de protection de la Suisse contre les cyberrisques. La Police genevoise se retrouve ainsi en première ligne, au service des citoyens et des entreprises.

Les techniques d'attaque ainsi que les moyens de les prévenir, disséqués dans la précédente édition téléchargeable gratuitement sur le site https://swissacademy.eu/cybercovid/, sont plus que jamais d'actualité.

Cet ouvrage fourmille de conseils précieux pour se protéger. En plus de développer une prudence instinctive et de limiter une suractivité sur les réseaux sociaux, il suffit de savoir renoncer aux applications gratuites et de s'assurer de déployer les outils de défense nécessaires sur ses appareils. Comme dans le cas d'une pandémie, c'est à une immunité collective que nous devrons tenter de parvenir, tous ensemble, grâce aux «vaccins» digitaux et aux bonnes attitudes. Il en va de notre vie privée, publique et professionnelle.

Parmi tous les actes criminels expliqués dans le détail et avec clarté par les auteurs des textes qui suivent, l'exemple donné par un ancien haut responsable du FBI fait froid dans le dos par sa simplicité. Son équipe de recherche est parvenue à pénétrer au cœur des serveurs d'une entreprise grâce à huit appels téléphoniques, suivis d'un courriel infecté. Cela a été possible grâce à la connaissance du milieu corporatiste ainsi qu'à la confiance instinctive accordée à un interlocuteur qui parle le «jargon» propre à ce monde.

Cet ouvrage, auquel je souhaite plein succès, est un atout précieux pour tous : avec l'édition précédente, il continue à offrir les connaissances de base actuelles, permettant de contrer de nombreux dangers quotidiens du monde virtuel.

Pour cela, je conclurai en remerciant chaleureusement les auteurs et les éditeurs de cet ouvrage, tous bénévoles, pour leurs efforts au service d'une cause qui nous est plus prioritaire que jamais. ■

Regional Cyber Competence Center (RC3) – Western Switzerland

La Stratégie Nationale de Protection de la Suisse contre les cyberrisques (SNPC II) définit le principe des Centres de compétences cyber mis en œuvre sur le territoire de la Confédération.

Ainsi le National Cyber Security Centre (NCSC) ou Centre national pour la cybersécurité est renforcé, en ce qui concerne la poursuite pénale de la cybercriminalité, par des Centres régionaux dont celui pour la Suisse occidentale qui est basé à Genève.

Œuvrant pour l'ensemble de la Romandie, ce centre répond à un besoin de mutualisation des compétences et des infrastructures afin de lutter plus efficacement contre la cybercriminalité.

Le principe de mutualisation évite à chaque Police cantonale de devoir développer sa stratégie couvrant l'ensemble du spectre de lutte contre la criminalité informatique.

Le RC3 pour la Suisse occidentale développe des services au profit de l'ensemble des cantons Romands, qui peuvent ainsi bénéficier des prestations suivantes :

- Analyse avancée de supports numériques (IoT)
- Renseignements avancés de Sources Ouvertes (OSINT)
- Mise en œuvre de logiciels spéciaux
- Intervention sur l'informatique embarquée dans les véhicules (voitures, bateaux, avions)
- Lutte contre la pédo criminalité sur Internet
- Coordination nationale de la Plateforme Inter Cantonale pour les délits Sériels En Ligne (PICSEL)
- Coordination nationale de lutte contre les Ransomwares.

Au service de la population et des entreprises, le RC3 pour la Suisse occidentale poursuit son développement afin de détecter et répondre aux défis actuels et futurs de la cybercriminalité.

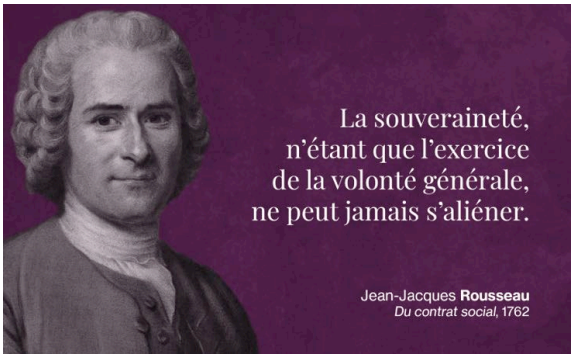
Les Polices cantonales sont les premiers partenaires privilégiés des citoyens et des entreprises pour signaler toutes infractions cyber dans le poste de police le plus proche ou au numéro de téléphone 117 en cas d'urgence.

AVANT-PROPOS

La cyber-sécurité : une condition sine qua non pour la «décennie numérique» de l'Union Européenne.

Auteur : G.al d'Armée (2S) Marc Watin-Augouard

La transformation numérique a longtemps été négligée par les Etats, à l'exception des Etats-Unis qui ont compris d'emblée quels en étaient les enjeux. Pour tous les autres, la prise en compte par le secteur privé faisait d'autant mieux l'affaire que le financement du déploiement des réseaux était hors de portée des seuls moyens publics. Ce retrait relatif n'est plus de mise depuis que le cyberespace est devenu un espace de compétition, de confrontation et même de conflictualité.

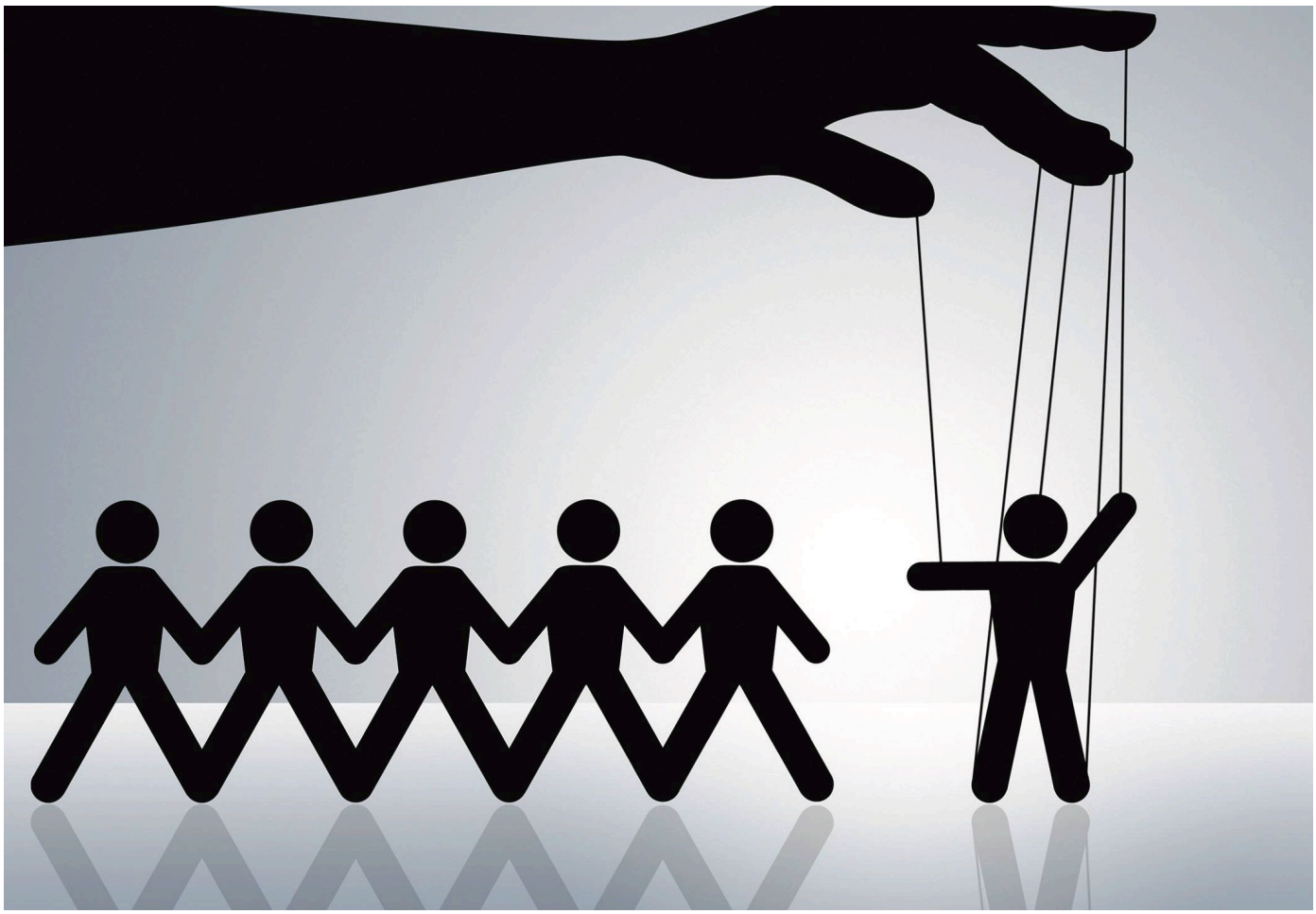


Parce qu'il est menacé dans sa souveraineté, parce que des entités privées transnationales entravent l'exercice de ses compétences, l'Etat revient sur le devant de la scène, par nécessité et, espérons-le aujourd'hui, par conviction.

Le retour de l'Etat est d'abord motivé par l'émergence de la cybercriminalité. Face au nombre croissant de victimes de prédateurs, les pouvoirs publics se voient rappeler les fondements de leur légitimité : protéger les personnes physiques et morales, les biens matériels et immatériels. Mais cette cybercriminalité, souvent inconnue, tant le «chiffre noir» est important, ne suffit pas à elle seule pour susciter un changement radical de posture de la part de l'Etat.

L'électrochoc de la cyberattaque de l'Estonie (2007) a réveillé les naïfs et les indécis. Depuis, avec plus ou moins de dynamisme, les acteurs publics développent des stratégies de cybersécurité qui conjuguent sécurité des systèmes d'information (SSI), lutte contre la cybercriminalité et cyberdéfense.

Cette dernière forme d'action, plus récente dans sa conception et sa mise en œuvre, n'est pas seulement militaire, comme le mot «défense» semble l'indiquer. Elle concerne toutes les activités essentielles à la vie de la nation. Les «pacifistes» la voulaient essentiellement défensive ; elle élargit son champ vers l'offensif, au fur et à mesure que les cyberattaques augmentent en nombre et en intensité. Face à des menaces aussi dangereuses, les Etats doivent conserver le monopole de l'action de force, sauf à admettre la légitimation du hackback, «légitime» défense reconnue aux victimes, dont les effets peuvent être particulièrement pervers.



La cyberdéfense connaît aujourd'hui un élargissement. Vers la «couche matérielle», tout d'abord : après avoir concentré les efforts sur la protection de la «couche logique» (logiciels, protocoles, etc.), il importe aujourd'hui de porter un regard sur l'infrastructure, trop souvent oubliée par ceux qui nourrissaient l'illusion d'un espace numérique virtuel.

Cette couche est vulnérable, notamment en cas d'actions de sabotage qui se multiplient depuis quelques années : inutile de monter une cyberattaque sophistiquée, dès lors qu'il suffit de brûler des relais, de couper un câble sous-marin ou de scier des fibres optiques. La «couche cognitive», celle des contenus, est devenue stratégique en raison de la démocratisation de l'accès à internet et de la viralité des réseaux sociaux.

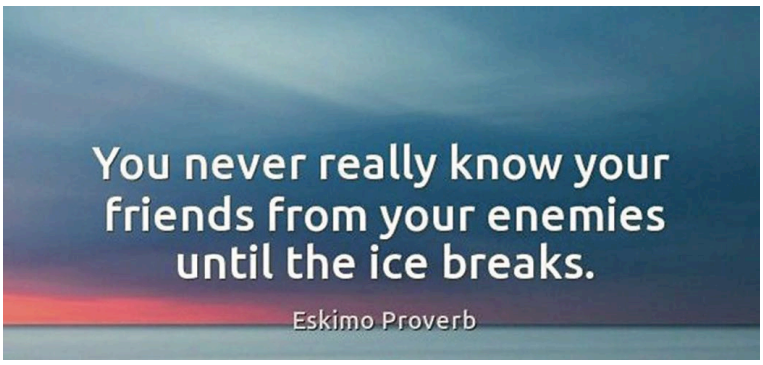
D'où l'émergence d'une «lutte informatique d'influence», nouvelle composante de la cyberdéfense, qui a pour objectif de contrer la manipulation de l'information, de déjouer les manœuvres de propagande. Le conflit en Ukraine illustre parfaitement l'impact de cette forme d'action qui relève d'abord de l'Etat.

Confrontés à l'aggravation du risque cyber, les Etats ne peuvent agir seuls. La coopération public-privé est essentielle, car nombre de solutions sont dans les mains d'entreprises, d'offreurs de sécurité. La création en France du Campus cyber, la tenue, chaque année du Forum International de la Cybersécurité (FIC), à Lille, témoignent de cette nécessaire ouverture.

Les Etats se tournent aussi vers d'autres Etats, vers des institutions internationales, espérant trouver à plusieurs les moyens de maîtriser un phénomène qui transcende les frontières et nécessite le déploiement de moyens importants. Mais la coopération internationale a ses limites. Les tentatives lancées par l'ONU ont connu des résultats «décevants», pour employer une terminologie «diplomatique».

A Dubaï, en 2012, les négociations dans le cadre de l'Union international des télécommunications (UIT) se sont conclues par un échec fondé sur une divergence relative au modèle de gouvernance. Les groupes d'experts gouvernementaux (GGE) successifs ont connu les mêmes difficultés, lorsqu'il s'est agi d'approfondir le droit international appliqué au cyberespace. Seule convention à succès, la Convention de Budapest, relative à la lutte contre la cybercriminalité (2001), a une portée parfois limitée, car elle n'a été ni signée, ni ratifiée par la Russie, la Chine, l'Iran, Cuba, etc. Aux conventions multilatérales, les Etats ajoutent des coopérations bilatérales qui permettent de construire dans la confiance.

Les alliances dans le cyberespace sont cependant fragiles, car on touche un domaine régalien. Dans le monde réel, l'alliance est une addition de forces. Dans le numérique, elle est d'abord une mise en commun des



faiblesses. Par ailleurs, l'espace numérique est devenu un territoire idéal pour l'espionnage. Tout serait «simple» si on ne devait faire face qu'aux criminels organisés, qu'aux Etats «cyber-voyous».

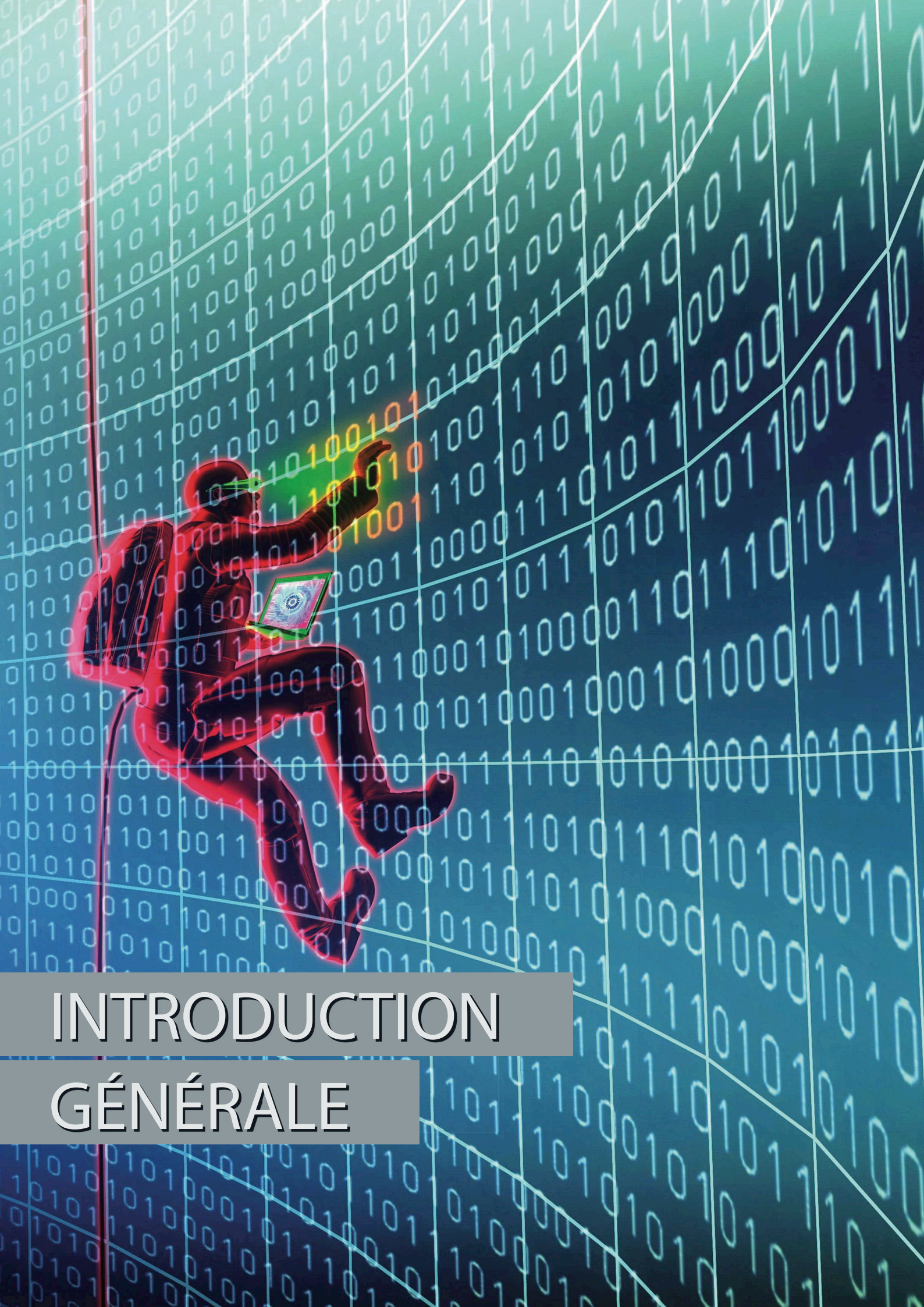
Mais le cyberespace oblige les Etats à se méfier de leurs meilleurs amis. L'espionnage n'est pas seulement le fait de ceux que l'on montre facilement du doigt. Il est aussi devenu un mode d'action mis en œuvre par des alliés. C'est dire si les alliances dans le cyberespace sont plus difficiles à sceller.

Dans ce contexte, l'Europe ne manque pas d'atouts, de talents, mais ils sont encore trop fragmentés, dispersés. Une mobilisation est essentielle, respectueuse de la souveraineté de chacun.

Mais nous savons aussi qu'il ne peut y avoir d'autonomie stratégique sans une coopération renforcée entre les Etats membres. Initialement tournée vers le Marché commun, devenu Marché Unique, l'Europe doit désormais aller plus loin, comme en témoigne son programme «pour la décennie numérique» présenté en mars 2021. Cette ambition doit être servie par une cybersécurité qui n'est pas une fin en soi mais une condition s'appuyant sur des valeurs partagées. ■

BIO

- Fondateur et Codirecteur, Forum international de la cybersecurité – FIC
- Responsable de la formation majeure « souveraineté numérique et cybersécurité » de l'IHEDN (Institut des Hautes Études de Défense Nationale)
- Ancien Directeur, Centre de Recherche de l'École des Officiers de la Gendarmerie Nationale (CREOGN) (2012-2020)
- Ancien inspecteur général des armées-gendarmerie
- Général d'armée (2008)
- Général de corps d'armée (2007)
- Général de division (2006)
- Commandant, Gendarmerie pour la zone de défense Nord (2005 – 2008)
- Commandant, Région de gendarmerie du Nord-Pas-de-Calais
- Conseiller pour la gendarmerie, Cabinet de Dominique de Villepin (2004 – 2005)
- Général de brigade (2003)
- Conseiller pour la sécurité, Cabinet de Nicolas Sarkozy (2002 – 2004)
- Commandant de la légion de gendarmerie départementale de Champagne-Ardenne (2000 - 2002)
- ENSEIGNEMENT : Chargé de cours en droit, Universités Panthéon-Assas (Paris II), René Descartes (Paris V) et Aix-Marseille III-Méditerranée.



INTRODUCTION GÉNÉRALE

De James BOND 007 à OSS365…

Auteur : Didier SPELLA

De James Bond 007… (d'une définition à un personnage type)

Un espion, ou encore un agent secret, est un individu qui pratique l'espionnage ou, de manière plus générale, une activité relative à la collecte clandestine de renseignements ou d'informations classifiées secrètes, le plus souvent pour les livrer à un État.

Par extension, on appelle aussi espion ou agent secret, toute personne exerçant une activité clandestine au service d'un État, comme le sabotage, la destruction, la capture de matériel, l'assassinat, l'enlèvement ou encore l'exfiltration de personnes.

Le personnage culte qui répond bien sûr à ces critères est le plus célèbre des espions, nous avons nommé James BOND.

Comment pourrions-nous le caractériser ? Sportif accompli, rompu à toutes les disciplines qui lui permettent ainsi de se sortir de toutes les situations dangereuses. C'est aussi un homme cultivé et élégant, maîtrisant plusieurs langues et bien sûr, pour compléter le personnage, à l'aise dans tous les environnements sociaux dans lesquels il est amené à évoluer afin de réussir sa mission.

Ses outils sont assez classiques : armes diverses, gadgets, voitures et véhicules spéciaux, etc. Déjà, il a recours à des outils connectés comme le guidage de sa voiture au travers de son téléphone. Mais il reste avant tout un personnage hors du commun.

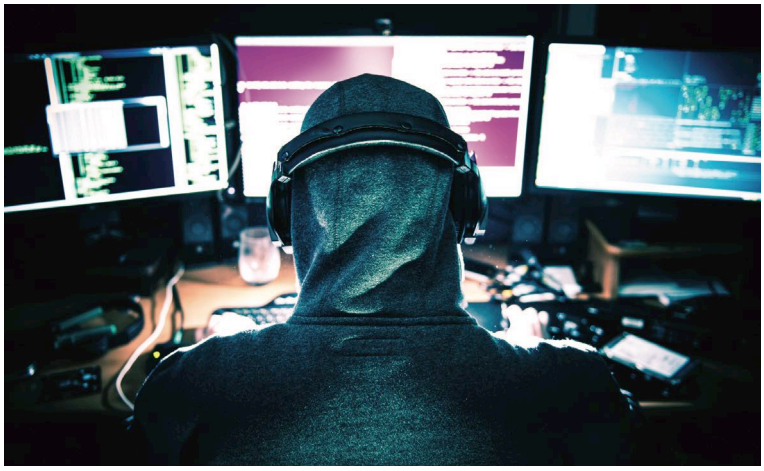
Il est fier de citer son nom et son appartenance aux services secrets et ses modes d'actions sont assez simples à décrire :

- Repérer le personnage qui traite et/ou les lieux dans lesquels les documents sont stockés ;
- Procéder à la neutralisation du personnage visé et pénétration dans les locaux identifiés ;
- Enfin, exfiltrer les documents d'une manière discrète (ou pas) afin de les ramener aux services compétents.

… À OSS365

Aujourd'hui, notre espion est d'un tout autre genre.

Il est déjà beaucoup plus discret et peu connu en tant qu'individu, car bien souvent, ce sont des «équipes» ou groupes structurés qui opèrent.



Grâce au cybermonde, les attaques sont très ciblées et ont recours à des technologies numériques sophistiquées.

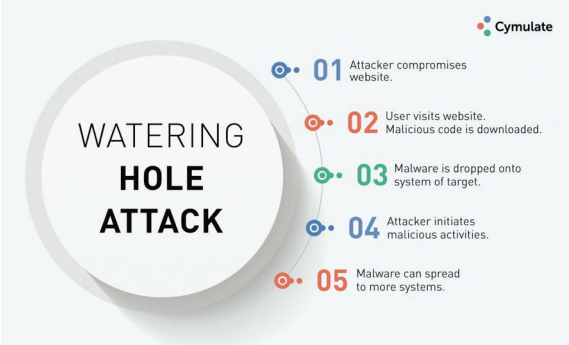
Comme pour notre espion, ces attaques ont pour but d'amener de lourdes conséquences pour les intérêts nationaux des pays qui se sont fait espionner.

La discrétion de ces attaques a pour conséquence qu'il faut parfois un certain temps à une organisation pour s'apercevoir qu'elle a été victime d'espionnage. Il sera donc quasi impossible d'en évaluer le préjudice.

Les outils utilisés par l'attaquant lui permettent de maintenir discrètement son accès le plus longtemps possible afin de capter l'information stratégique quand il veut.

Les différentes attaques peuvent être décrites de la manière suivante :

▸ *La technique du «point d'eau» consiste à piéger un site en ligne légitime afin d'infecter les équipements des visiteurs du secteur d'activité visé par l'attaquant.*



Objectif : infiltrer discrètement les ordinateurs de personnels œuvrant dans un secteur d'activité ou une organisation ciblée pour récupérer des données. Notre espion exploite une vulnérabilité du site et y dépose un logiciel malveillant (malware). Le site qui sert d'appât est choisi spécifiquement pour attirer la victime ciblée par l'attaque in fine.

Notre espion pourra avoir recours aux réseaux sociaux afin de «profiler» sa victime. Ainsi celle-ci est incitée à se rendre ou est redirigée automatiquement sur le site contaminé. Son navigateur exécute alors le malware qui est installé à son insu sur ses appareils (ordinateur, téléphone). Notre espion dispose ainsi d'un accès total ou partiel à l'appareil infecté. Il restera discret afin de capter le plus longtemps possible des données.

▸ *L'attaque par hameçonnage ciblé ou spearphishing repose généralement sur une usurpation de l'identité de l'expéditeur et procède par ingénierie sociale forte afin de lier l'objet du courriel et le corps du message à l'activité de la personne ou de l'organisation ciblée.*

Objectif : infiltrer le système d'information d'une organisation d'un secteur d'activité ciblé. Pour cela, il usurpe l'identité d'une personne morale (établissement financier, service public, concurrent…) ou d'une personne physique (collègue de travail, famille, ami…). Le destinataire est invité à ouvrir une pièce jointe malveillante ou à suivre un lien vers un site malveillant. Une première machine est ainsi contaminée.

Notre espion en prend le contrôle pour naviguer dans le système d'information de l'organisation qui est la véritable cible. Il va chercher à obtenir des droits «d'administrateur» pour pouvoir rebondir et s'implanter sur les postes de travail et les serveurs de l'organisation où sont stockées les informations visées («propagation latérale»). Enfin, comme pour James BOND, il vole le plus discrètement possible des données soit en une seule fois, en profitant d'une période de moindre surveillance (la nuit, durant les vacances scolaires, lors d'un pont…), soit de manière progressive plus insidieuse. Il prendra soin d'effacer derrière lui toute trace de son activité malveillante.

Notre OSS365 n'est plus du tout le personnage que nous avons décrit précédemment. Sa discrétion est son premier atout. Aucune action physique n'est nécessaire. C'est avant tout un brillant technicien.

Nous avons donc à faire à un autre personnage souvent caricaturé mangeant des pizzas et buvant de la bière devant ses écrans. C'est un personnage très discret.

Des recommandations

Comme toujours, les recommandations « habituelles » sont à mettre en œuvre :

- Mettez à jour régulièrement tous vos principaux logiciels, notamment ceux en charge du filtrage.
- Effectuez des sauvegardes régulières sur des périphériques externes (ex : disque dur).

N'ayez pas une confiance spontanée dans le nom de l'expéditeur.

- Méfiez-vous des pièces jointes et des liens dans des messages dont la provenance est douteuse.

Nous vous conseillons de respecter les 2 règles suivantes qui sont essentielles :

R1 : prenez le temps au niveau de votre organisation de définir les niveaux de connaissances nécessaires à vos utilisateurs.

R2 : mettez en place la règle du moindre privilège.

Dans tous les cas, une analyse de risques formelle vous permettra d'identifier vos informations sensibles et les chemins que peut emprunter l'espion pour y parvenir.

Il faudra mettre aussi en place une bonne administration de vos systèmes, notamment par l'utilisation d'une journalisation (suivi régulier des événements constatés) et ainsi identifier très vite tout fonctionnement erratique de vos systèmes qui, s'ils ne sont pas liés à un problème identifié, ne peuvent correspondre qu'à un début d'attaque.

Enfin d'une manière plus «générique» les réseaux sociaux sont souvent la première source d'informations. Soyez donc vigilants à ce que vous y publiez. ■

BIO

Directeur Général de l'Institut National de la Cyber sécurité et de la Résilience des Territoires (INCRT), Didier Spella est un expert en stratégie des entreprises et en cybercriminalité. Il est le président de MIRAT DI NERIDE, société de consultance en cyber-sécurité. Il est co-fondateur de CMCS (Charente-Maritime Cyber Sécurité) dont la deuxième édition en 2019 a réuni près de 450 participants et plus de 60 intervenants pendant 3 jours à La Rochelle. En 2021, ce sont 4 jours de colloque où ont été traités des sujets relatifs aux sports, l'agro-alimentaire, le tourisme et les collectivités territoriales. Didier est également Responsable du Bureau CLUSIR - Nouvelle Aquitaine Ouest (La Rochelle – Niort – Cognac), Référent CyberMalveillance et réserviste Civique (Cyber) de la Police Nationale.
Ancien Officier Supérieur de l'Armée de l'Air, expert en réseau et continuité des Affaires dans une multinationale américaine, il a toujours été passionné par la problématique de la cyber sécurité et notamment le conflit qui peut exister entre le cybermonde et la sécurité. Comment pouvons-nous positionner l'être humain confronté au dilemme liberté-sécurité ?

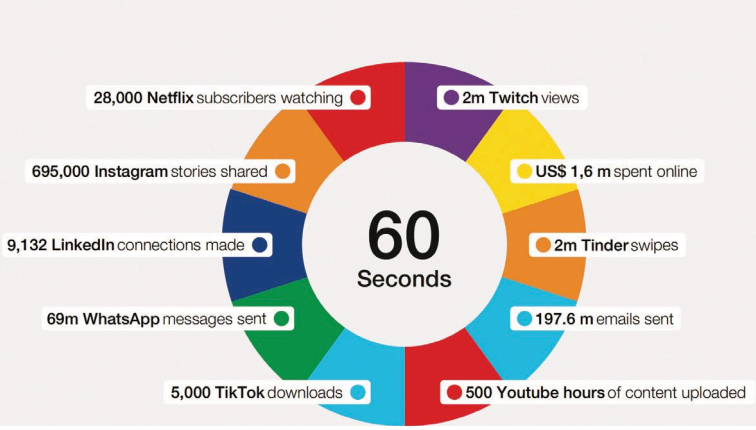
Notre mémoire est-elle en train de devenir un melting-pot de *«connaissances inconnues»* ?

Auteur : Laurent Chrzanovski

L'année dernière, dans un essai socio-psychologique à la mémoire de Donald Rumsfeld, le célèbre philosophe Slavoj Zizek a rappelé le discours prononcé en 2002 par le défunt Secrétaire américain à la Défense, peu avant la guerre en Irak. Dans ce discours, intentionnellement ou non, Rumsfeld a mentionné des concepts essentiels de la philosophie ancienne, à savoir les *inconnus inconnus*, les *inconnus connus* et les *connus connus*. Pourtant, il manquait un concept né très récemment : les ***inconnus connus***.

Comme l'a souligné le philosophe allemand Jürgen Habermas (2) depuis 2020, notre cerveau est tellement saturé d'informations que notre mémoire est pleine de savoirs que nous avons... oublié. Ce phénomène est profondément ancré chez les *«individus connectés aux médias»*, c'est-à-dire la plupart d'entre nous dans les pays développés. La quantité de «nouvelles fraîches» absorbées quotidiennement envahit notre esprit critique et pousse aux oubliettes des informations plus anciennes, souvent vitales, surtout si l'on n'a pas eu besoin d'appliquer dans la vie réelle toutes ces connaissances, pourtant «assimilées».

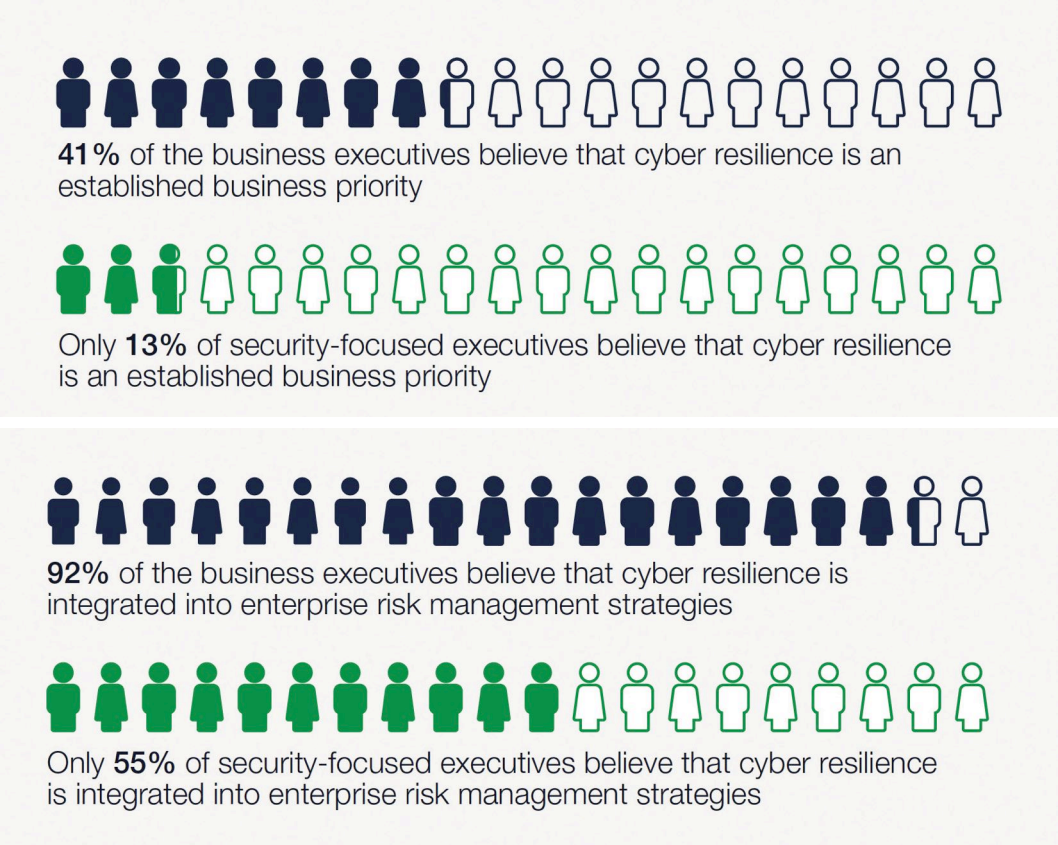
Dans le domaine de la cybersécurité, la racine profonde du problème qui génère les comportements humains décrits par les philosophes est devenue une véritable préoccupation. Le problème de la *«surinformation»* (mesuré par la quantité de documents chargés et ensuite téléchargés/lus sur le web chaque minute, dans le monde entier) fait l'objet de pas moins d'un chapitre entier dans le *Global Cybersecurity Outlook 2022* (3) publié il y a trois mois par le Forum économique mondial de Davos (WEF).



Nouvelles données créées en une minute.
© WEF, Global Cybersecurity Outlook 2022, p. 12, figure 3

Du haut vers le bas : experts métier contre experts en sécurité

Le rapport du WEF souligne, parmi les «inconnues», que l'écart moyen entre la confiance des membres du conseil d'administration (les «dirigeants d'entreprise») dans les politiques de résilience et, par conséquent, dans les systèmes de sécurité utilisés au sein de leur société, et les craintes des équipes de sécurité (les «dirigeants des départements de sécurité») est plus



Confiance dans la priorité et l'intégration de la cyber-résilience, chefs d'entreprise versus spécialistes de la sécurité.
© Global Cybersecurity Outlook 2022, p. 19-20

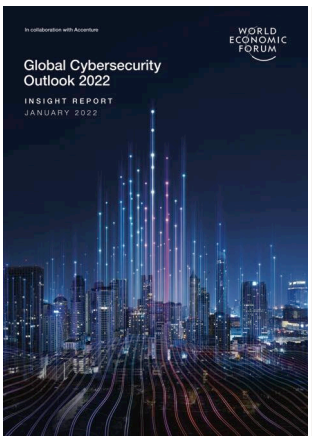
grand que jamais. Un long chapitre du rapport du WEF est, à ce titre, rédigé sur cette différence majeure de perception : «*Les cyber-dirigeants se trouvent de plus en plus dans une position précaire à mesure que l'écart entre les dirigeants d'entreprise et les responsables des départements de sécurité se creuse*».

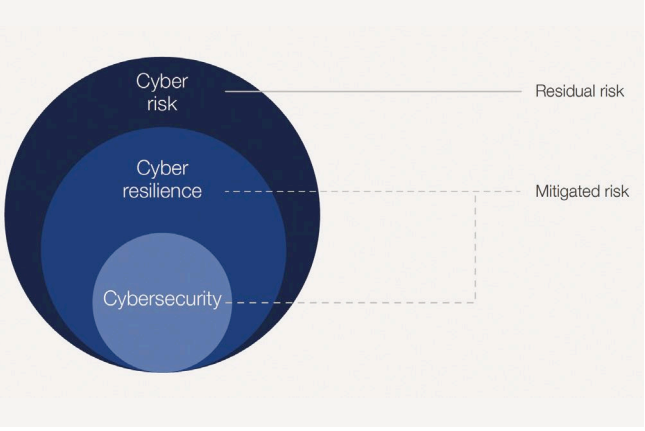
Les perspectives soulignent une série de mesures très importantes à prendre immédiatement dans tous les secteurs d'activité, afin de combler ce fossé qui, comme de nombreuses recherches l'indiquent, est l'une des principales raisons de la faiblesse générale observée par le succès de formes très primitives de cyberattaques durant la pandémie (phishing, escroqueries de base, etc.).

Une fois encore, la faille, croissante, concerne exactement l'un des faits que nous avons abordé depuis longtemps : l'absence d'inclusion des RSSI et/ou des CSO au sein des membres du conseil d'administration / l'absence de leur présence obligatoire lors de réunions décisionnelles. Cette décision a, a elle seule, des conséquences graves sur la cyber-sécurité de l'entreprise.

En outre, la plus grande différence de *modus cogitandi* entre les chefs d'entreprise et les spécialistes de la sécurité, et la source de nombreux problèmes, est l'incompréhension croissante des entrepreneurs sur la différence de ce que couvrent les concepts de cyber-sécurité et de cyber-résilience : la plupart des chefs d'entreprise considèrent les deux domaines comme un tout et ne mettent pas en corrélation les différences, les spécificités et les besoins de chacun d'entre eux.

Le nombre record de cyberattaques réussies en 2021 et durant le premier semestre de 2022 trouve son origine, selon tous les rapports, dans une multitude de





Relations entre le cyberrisque, la cyberrésilience et la cybersécurité.
© Global Cybersecurity Outlook 2022, p. 16

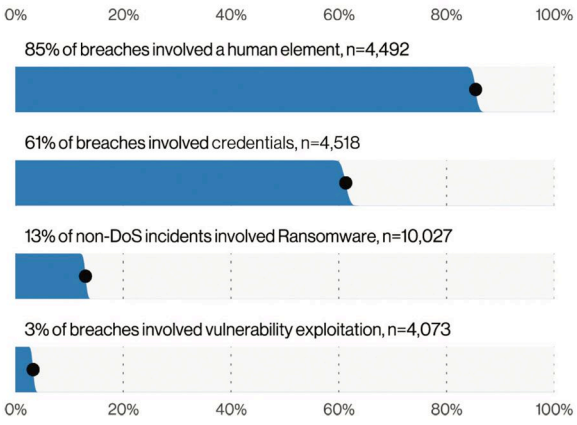
décisions inappropriées prises durant les périodes de «lockdown» lors des pics de la COVID, auxquelles s'ajoute la transformation, pensée comme provisoire mais qui est désormais devenue une réalité à long terme : celle des nombreux emplois qui sont passés du bureau au travail à domicile, sans aucun changement radical de l'architecture de sécurité de l'entreprise.

Les perspectives du WEF et les autres rapports mentionnent également que nous avons atteint un point critique de pénurie d'emplois dans le domaine de la cyber-sécurité, qui pourrait être réduite en suivant les indications données par de nombreux experts du domaine de la formation. En effet, à ce sujet, nous devrions atténuer un peu les chiffres donnés par Forbes, le WEF et d'autres, car ils reflètent surtout l'incapacité de trop d'institutions d'enseignement à fournir des formations à spectre large. Plus concrètement, en admettant que la cyber-sécurité a sept piliers – selon la définition des spécialistes –, la nouvelle génération d'experts en cyber-sécurité devrait être en mesure de maîtriser au moins deux, sinon trois d'entre eux, aidés par les nouvelles technologies disponibles sur le marché.

Tous les facteurs susmentionnés ont de graves conséquences sur les coûts d'assurance, à tel point que les primes d›assurances constituent le troisième des 10 principaux défis de la cyber-sécurité pour l›année en cours selon les prédictions annuelles publiées par Forbes et rédigées par E. Saygeh (4). De nombreuses assurances, dont les primes de couverture ont explosé en 2021, refusent désormais d›accepter les entreprises qui ne disposent pas d›une politique de cyber-sécurité stricte et complète, aussi bien technologique qu›humaine, à commencer par une formation continue de sensibilisation délivrée à chaque employé, du dernier venu au directeur général.

De la base au sommet : un manque constant de formation de sensibilisation à tous les niveaux

Les coûts des incidents pour les entreprises, pendant les années de pandémie, ont atteint des records. Comme l'a souligné le *Data Breach Investigations Report 2021* (5) de Verizon, 85 % des brèches impliquaient le *«maillon faible humain»*.



Verizon, Data Breach Investigations Report 2021, fig. 7, p.7.

Bien qu'il s'agisse d'une préoccupation majeure pour tous les secteurs d'activité, très peu d'entreprises, à l'exception des sociétés de sécurité, des secteurs de la haute technologie ou du luxe, ont entrepris le travail de longue haleine consistant à sensibiliser régulièrement l'ensemble du personnel, de la femme de ménage au PDG.

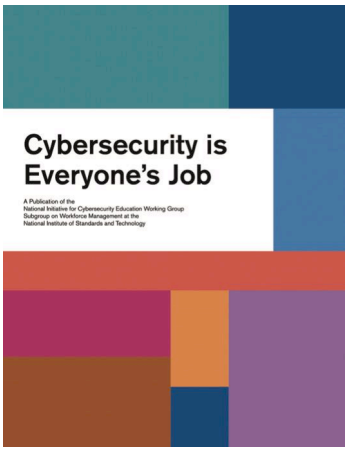
Comme l'a récemment souligné Clive Madders (6), ce n'est qu'en cultivant une culture de sensibilisation à la cyber-sécurité qu'une entreprise peut réellement devenir résiliente. Outre les technologies nécessaires, l'auteur insiste sur le fait que *«Fortifier la ligne de front (lire : les employés) est souvent la meilleure méthode de défense»,* rappelant le mauvais usage fait par trop d'entreprises des directives essentielles publiées par le NIST en 2018 déjà, *«La cyber-sécurité est l'affaire de tous»* (7).

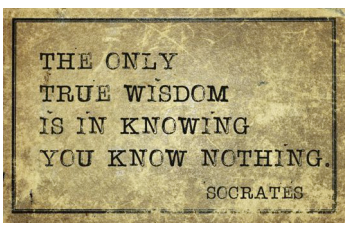
Les conséquences d'années de sensibilisation à la sécurité mal distribuée, sous forme de documents en format pdf ou de publicités d'une page, ont été largement dévoilées lors des pandémies. Ces «connaissances» ont été

largement oubliées par trop d'employés travaillant à distance. Ceux-ci ont échangé avec des collègues leurs mots de passe, leurs identifiants, cliqué sur des liens malveillants et ouvert tout type de courrier de hameçonnage. Le stress et l'ignorance, comme le souligne l'étude *«Why employees violate cybersecurity policies» (Pourquoi les employés violent les politiques de cyber-sécurité)* que vient de publier l'Université de Harvard (8), en sont les principaux responsables. Dans un contexte de stress, les trois principales raisons, avouées par les employés qui ont contourné les politiques de sécurité, sont les suivantes : chacun a enfreint les règlements :

- «pour mieux accomplir les tâches de mon travail»
- «pour obtenir quelque chose dont j'avais besoin»
- «pour aider les autres à faire leur travail»

Pour mieux comprendre la recherche de Harvard, il faut lire une recherche psychologique plus approfondie intitulée *«The Role of User Behaviour in Improving Cyber Security Management»* (9). Elle permet de comprendre, en décortiquant «le danger intérieur» : les différentes catégories d'ego que peut avoir chaque employé, conduisant à des erreurs majeures et donc à des comportements non sécurisés, allant de l'excès de confiance à l'impulsivité et à un désir toujours plus grand d'être proactif (i.e. *«future thinking»*) pour mieux faire face au stress lié à la quantité de demandes reçues quotidiennement par un supérieur direct. Tous ces facteurs conduisent à oublier les bases acquises et à ne pas appliquer les politiques de sécurité qui sont trop souvent mal expliquées et donc mal comprises et ce dès le jour de leur mise en place.





Pour terminer là où nous avons commencé, il est désormais inutile d' essayer de se souvenir des *«inconnus connus»*. Pour faire face à la quantité toujours croissante de nouvelles technologies que nous utilisons, ainsi qu'au mode d'utilisation spécifique de chaque produit, à ses forces et, bien sûr, à ses faiblesses, il est nécessaire d'adopter une nouvelle stratégie (même en ayant recours à des jeux de rôle, i.e. la *gamification*) afin de sensibiliser tous les employés, en commençant par une utilisation correcte de l'outil le plus vulnérable, le smartphone.

Les employés, s'ils sont bien encadrés, devraient ainsi trouver satisfaction en ayant le sentiment d'apprendre quelque chose de très utile. Si l'on part du paradoxe socratique décrit par Platon : **« ἔν οἶδα ὅτι οὐδὲν οἶδα » (tout ce que je sais, c›est que je ne sais rien)**, c'est-à-dire d'une attitude d'humilité couplée à une ouverture d'esprit, ces mêmes employés réaliseront que ces formations leur sont utiles pour évoluer et se sentir en sécurité non seulement dans leur travail, mais aussi dans leur vie personnelle, grâce aux connaissances de base sur la cyber-sécurité.

Bien entendu, le comportement des chefs d'entreprise devra également changer: il s'agira de récompenser leurs équipes et leurs employés non seulement pour leur productivité mais aussi pour la bonne application des politiques de sécurité. ■

BIO

Titulaire d'un doctorat en archéologie romaine de l'Université de Lausanne, d'un diplôme de recherche postdoctorale en histoire et en sociologie de l'Académie roumaine et d'une habilitation de l'UE à diriger des doctorats en histoire et en sciences connexes, Laurent Chrzanovski est professeur à l'école doctorale de l'Université «Lucian Blaga» de Sibiu, et professeur invité auprès des écoles doctorales des Universités de Genève, Lyon II et Varsovie ; il donne chaque année des cours postdoctoraux dans plusieurs universités de l'UE (top-200 uniquement). Il est l'auteur/éditeur de 42 livres, de plus de 150 articles scientifiques et d'autant d'articles destinés au grand public.
Dans le domaine de la cybersécurité, Laurent Chrzanovski est membre et consultant contractuel du groupe d'experts de l'UIT (ONU-Genève). Il a fondé et dirige les congrès annuels de partenariat public-privé «Cybersecurity Dialogues» (Roumanie, Italie, Suisse). Dans le même esprit de partenariat public-privé, il est cofondateur et rédacteur en chef du seul magazine trimestriel gratuit de sensibilisation à la cybersécurité, Cybersecurity Trends, publié en roumain, français, anglais et italien. Ses principaux domaines d'étude portent sur la relation humaine avec le monde digital, ainsi que les comportements à risque qu'entraine la méconnaissance des dangers du monde virtue; il travaille aussi sur la recherche d'un juste équilibre entre la sécurité et la vie privée des citoyens «numériques».

(1) Slavoj Zizek :»How Donald Rumsfeld's catastrophic 'unknown unknowns' approach on Iraq can help us deal with Covid crisis», RT, 04.07.2021 (https://www.rt.com/op-ed/528359-donald-rumsfeld-iraq-covid/)
(2) Jürgen Habermas :: «So viel Wissen über unser Nichtwissen gab es noch nie», Frankfurter Rundschau 10.04.2020 https://www.fr.de/kultur/gesellschaft/juergen-habermas-coronavirus-krise-covid19-interview-13642491.html
(3) World Economic Forum, Global Cybersecurity Outlook 2022, janvier 2022. https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf
(4) E. Saygeh, Predicting What 2022 Holds For Cybersecurity, Forbes, 6 janvier 2022. https://www.forbes.com/sites/emilsayegh/2022/01/06/predicting-what-2022-holds-for-cybersecurity/
(5) Verizon, Data Breach Investigations Report 2021. DBIR, automne 2021 https://www.researchgate.net/publication/351637233_2021_Verizon_Data_Breach_Investigations_Report
(6) Clive Madders : «Protect Your Organization by Cultivating a Culture of Cybersecurity Awareness» (Protégez votre organisation en cultivant une culture de cyber-sécurité), 28 décembre 2021. https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/protect-your-organization-by-cultivating-a-culture-of-cybersecurity-awareness/
(7) NIST, Cybersecurity is Everyone's Job, 2018. https://www.nist.gov/news-events/news/2018/10/cybersecurity-everyones-job
(8) C. Posey, M. Schoss, Research : Why Employees Violate Cybersecurity Policies, Harvard Business Review, 20 janvier 2022. https://hbr.org/2022/01/research-why-employees-violate-cybersecurity-policies
(9) A.A. Moustafa, A. Bello et A. Maurushat, The Role of User Behaviour in Improving Cyber Security Management, Frontiers in Psychology 12 (2021), https://www.frontiersin.org/article/10.3389/fpsyg.2021.561011

Le cyber-espionnage, le pire des risques possibles pour une entreprise. Comment le prévenir au mieux ?

Auteur : Laurent Chrzanovski

Les coûts de l'espionnage industriel et commercial ainsi que ceux des fraudes par internet sont les deux principaux éléments, pourtant vitaux, qui nous manquent pour nous permettre d'évaluer aussi bien les bénéfices des organisations cybercriminelles que les pertes subies par les entreprises. Le secret qui enveloppe la première catégorie d'incidents (qui ne sont médiatisés que lorsqu'ils sont «commandités» par un État) est évidemment motivé, pour les entreprises, par le souci d'éviter des dommages supplémentaires, liés à leur réputation tandis que leur non-divulgation, de la part de l'État, vise à éviter une perte d'emplois par la reconnaissance explicite du niveau de faiblesse réelle de l'écosystème national des entreprises actives sur son sol.

Du point de vue des dirigeants d'entreprise, nous entendons hélas toujours les mêmes propos génériques tenus en ce qui concerne l'amélioration de la sécurité afin de parer – si ce n'est les techniques de piratage les plus sophistiquées – tout au moins les méthodes les plus communément utilisées par les cyber-criminels : «*Mon entreprise est trop petite*». «*Mon activité est banale et sans intérêt*». «*Mon entreprise ne vaut pas les coûts d'une telle attaque*».

Loin de nous l'idée de blâmer les PDG et les conseils d'administration : depuis cinq ans, tous les efforts des États de l'UE, dans les domaines de la prévention et de la sensibilisation des entreprises à la cybercriminalité, se concentrent sur les données personnelles, une initiative logiquement motivée pour aider les entreprises à comprendre les dommages causés par une attaque et surtout les amendes qu'elles risquent de subir et ce non seulement en raison de la mise en œuvre du RGPD de l'UE et des sanctions prévues, mais aussi de celles, exponentiellement plus lourdes, prévues par le Cloud Act américain.

Malheureusement, chaque année la surabondance de matériel de sensibilisation à la protection des données dites «personnelles» a tendance à devenir une sorte d'énorme soleil aveuglant, empêchant les chefs d'entreprise d'ouvrir les yeux sur la protection vitale de l'ensemble des données de leur propre société, celles, justement, qui constituent ce que l'on nomme communément «les joyaux de la couronne». Cette triste réalité règne dans la plupart des pays de l'UE, et en particulier dans les nations de l'Est et du Sud-Est de l'Union, où la plupart des entreprises les plus importantes sont aujourd'hui des filiales de multinationales des pays de l'Ouest : la sensibilisation aux dangers de l'espionnage y est ainsi presque totalement absente des documents de prévention fournis par l'État.

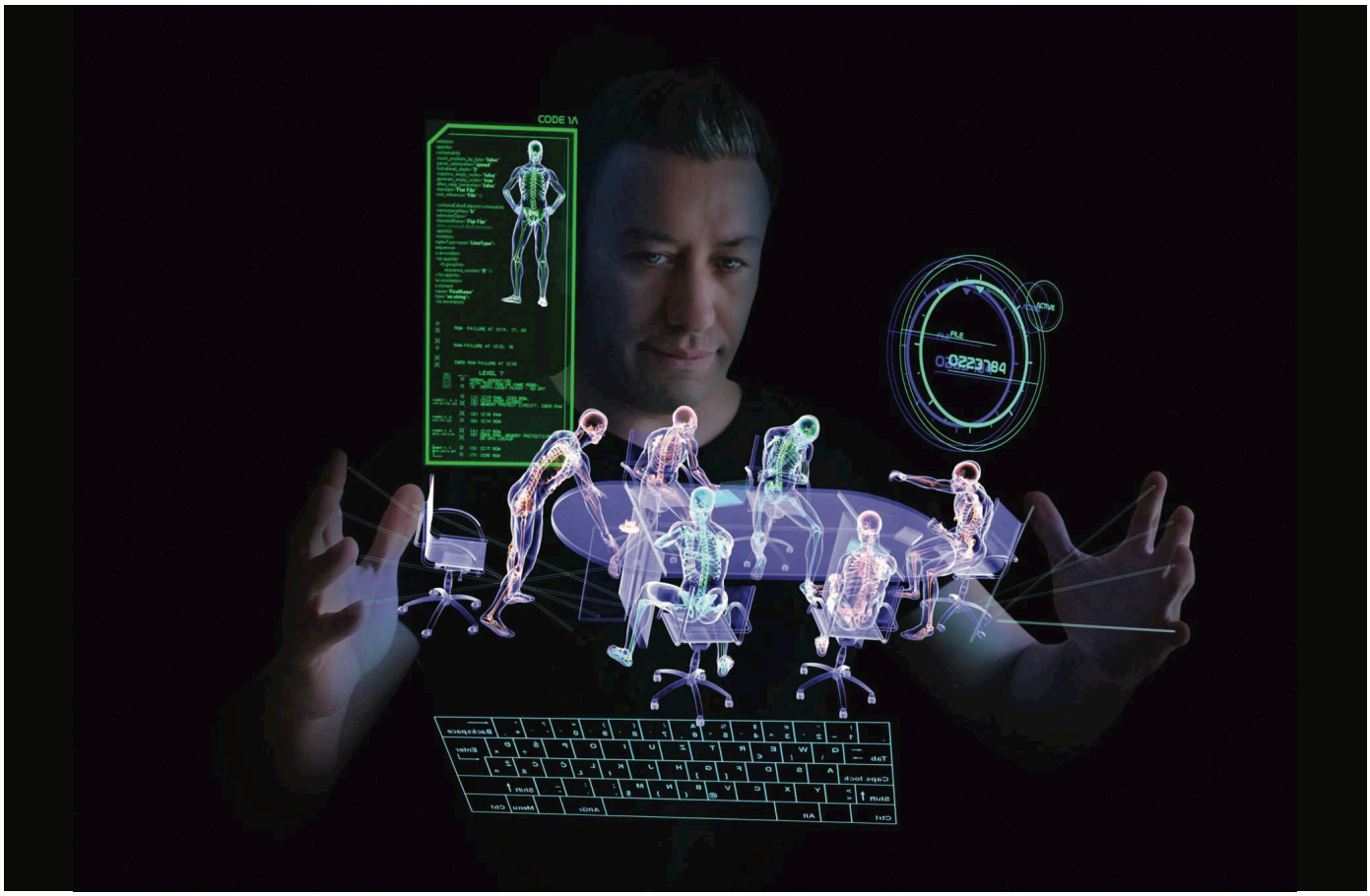
Ce numéro spécial de Cybersecurity Trends a été voulu, en trois versions linguistiques, pour pallier ce besoin d'informations et pour être diffusé en accompagnement à la *1ère journée annuelle de sensibilisation des entreprises au cyber-espionnage* (Bucarest, 14 juin 2022), une initiative placée sous l'égide et en collaboration avec l'Ambassade de Suisse en Roumanie ainsi qu'avec la Chambre de Commerce Suisse-Roumanie.

En effet, les autorités suisses figurent parmi les leaders mondiaux en matière de sensibilisation à l'espionnage, avec les États-Unis, Israël, la Corée du Sud et le Japon. C'est une conséquence logique, bien prise en compte par les organismes compétents de l'État, dans des pays où une très grande partie de l'économie repose sur des entreprises innovantes, actives sur le marché global et disposant d'énormes budgets de recherche et de développement. De plus, le cœur de leur métier est concentré dans certains des domaines économiques les plus importants, de surcroît les plus sensibles dans le contexte mondial actuel: systèmes militaires, chimie, pharmacie, haute précision et luxe sans oublier les entreprises livrant des outils numériques sécurisés d'avant-garde ou encore les leaders mondiaux en matière de produits agroalimentaires.

1. Quels sont les objectifs de l'espionnage pour tout type d'entreprise ?

Chaque entreprise, dans le contexte actuel qui combine une situation post-pandémique et une donnée nouvelle - une guerre sur le continent Européen, est désormais intéressante. L'espionnage, lorsqu'il ne vise pas les résultats d'une longue période de recherche et de développement qui ne sont pas encore brevetés, se concentre sur la collecte d'informations complètes sur chaque partie vitale d'une entreprise : sa comptabilité intégrale, y compris les coûts individuels de chaque fournisseur, de sa production propre et de ses revendeurs, sa stratégie commerciale à court et moyen terme, son bénéfice annuel réel ainsi que les nouveaux produits qui seront lancées sur le marché, ou encore les stratégies de fusions/acquisitions prévues: bref, un diagnostic complet de la santé réelle de l'entreprise et de ses plans pour l'avenir.

L'objectif, pour le bénéficiaire des informations obtenues par ce biais est, bien entendu, de savoir quand acheter ou détruire un concurrent. Hélas, les activités d'espionnage fleurissent dans un monde où des sociétés parfaitement légales, y compris dans les pays de l'UE. De nombreuses 'entreprises' proposent à leurs clients d'obtenir toutes les données qu'ils désirent, tout en les exonérant par contrat de toute responsabilité légale en ce qui concerne les moyens que ces sociétés utiliseront pour recueillir les informations que demandées. Cette clause est due, en premier lieu, au recours fréquent, de la part de ces 'entreprises', aux services payants faisant partie de la vaste panoplie de l'offre des grands groupes cybercriminels. Tout n'est donc qu'une question du montant à payer, établi en fonction de la difficulté d'accéder à ces données pour les dérober.



2. Quels sont les chiffres de l'espionnage industriel et commercial ?

Dans son chef-d'œuvre «*Managing Cyber Risk*», Ariel Evans, en analysant les coûts de l'interruption des activités et de l'exfiltration des données (le premier type d'attaques permettant le second) nous présente des chiffres réels qui font peur. Il a basé ses calculs sur une très grande entreprise, mais pas sur une multinationale. L'objet de la recherche reflète ainsi parfaitement la réalité de la plupart des grandes entreprises d'un pays de l'UE, à savoir toutes celles qui se situent à la fois en dessous des fleurons nationaux (de 60 ou 10 en fonction de la taille de l'économie du pays concerné, à l'instar, pour la France, des entreprises dites «du CAC 40») et au-dessus des entreprises de taille moyenne ou des start-ups.

Tout d'abord, l'auteur montre **l'impact de l'interruption des activités**, comme suit :

Affectation des joyaux de la couronne	Perte d'exploitation
Gestion des brevets	$0
Gestion des essais R&D	$0
Gestion de la chaîne logistique	$0
Gestion de la chaîne d'approvisionnement	$100,000
RH	$25,000
Mouvements financiers	$20,000,000
Gestion des clients	$20,000,000
Total	$40,125,000

Fig. 1 : Evans 2019, Tableau 3.1, Pertes potentielles liées à l'interruption des activités, p. 61

Vient ensuite l'impact de l'exfiltration des données, où, comme on peut le voir, la compromission des brevets, à elle seule, fait doubler la perte finale :

Affectation des joyaux de la couronne	Perte par exfiltration de données
Gestion des brevets	$50,000,000
Gestion des essais R&D	$25,000,000
Gestion de la chaîne logistique	$5,000,000
Gestion de la chaîne d'approvisionnement	$2,000,000
RH	$1,000,000
Mouvements financiers	$5,000,000
Gestion des clients	$4,000,000
Total	$92,000,000

Fig. 2 : Evans 2019, Tableau 3.2, Pertes potentielles liées à l'interruption des activités, p. 62

Hélas, pour une entreprise incapable de faire face à une telle attaque, les dommages financiers ne s'arrêtent pas là, car les actions en justice des clients ainsi que les amendes réglementaires vont pleuvoir (l'auteur a fait une moyenne pondérée des amendes cumulées et des poursuites individuelles permises par le RGPD + le Cloud Act) :

Affectation des joyaux de la couronne	Perte réglementaire
Gestion des brevets	$0
Gestion des essais R&D	$0
Gestion de la chaîne logistique	$0
Gestion de la chaîne d'approvisionnement	$0
RH	$25,000,000
Mouvements financiers	$0
Gestion des clients	$400,000,000
Total	$425,000,000

Fig. 3 : Evans 2019, Tableau 3.4, Pertes réglementaires potentielles aux États-Unis et dans l'UE, p. 64

Ce schéma complet avec des montants réalistes nous permet de revenir au top 10 des défis de la cyber-sécuritaire définis par Forbes pour l'année en cours, où l'on trouve, en 3ème position, les coûts d'assurance (2). En effet, de nombreuses assurances américaines, dont les primes de couverture ont explosé en 2021, refusent déjà d'accepter les entreprises qui ne disposent pas d'une politique stricte et complète en matière de cyber-sécurité - aussi bien technologique qu'humaine, à commencer par une formation continue de sensibilisation dispensée à chaque employé.

Les coûts à supporter par l'assurance deviennent, dans l'exemple de d'Evans, cas astronomiques, atteignant plus d'un demi-milliard de dollars, comme illustré ci-dessous :

Joyaux de la couronne	Perte d'exploitation	Perte par exfiltration de données	Perte réglementaire	Total
Gestion des brevets	$0	$50,000,000	$0	$50,000,000
Gestion des essais R&D	$0	$25,000,000	$0	$25,000,000
Gestion de la chaîne logistique	$0	$5,000,000	$0	$5,000,000
Gestion de la chaîne d'approvisionnement	$100,000	$2,000,000	$0	$2,100,000
RH	$25,000	$1,000,000	$25,000,000	$26,025,000
Finances	$20,000,000	$5,000,000	$0	$25,000,000
Gestion de la relation client	$20,000,000	$4,000,000	$400,000,000	$424,000,000
Total	$40,125,000	$92,000,000	$425,000,000	$557,125,000

Fig. 4 : Evans 2019, Tableau 3.7, Quantification des coûts pour la cyber assurance, p. 67

Les coûts à supporter par l'assurance deviennent, dans l'exemple de d'Evans, cas astronomiques, atteignant plus d'un demi-milliard de dollars, comme illustré ci-dessous :

3. Mon entreprise n'est pas si importante, quels seraient mes coûts ?

Tout d'abord, il faut souligner que dans l'UE, la plupart des assurances sont bien conscientes que la cyber-sécurité n'est pas une priorité pour une grande partie des entreprises. Les meilleures d'entre elles, celles qui répondent à tous les critères de sécurité humaine et technologique, sont ainsi assurées aux Etats-Unis ou au Royaume-Uni, tandis que les autres seront remboursées par les assureurs de l'UE à hauteur de 10% maximum de leurs bénéfices annuels (et non de leur chiffre d'affaires !), donc une somme quasi-inutile lorsqu'il s'agit de couvrir les coûts d'une attaque d'espionnage.

Mais pour rendre tout cela de façon plus lisible, prenons deux cas précis:

a. pour une entreprise européenne de taille moyenne, les dommages pourraient atteindre 1/1000 du cas d'Evans, c'est-à-dire 5 millions d'Euros.

b. pour une PME ou une start-up européenne, les dommages pourraient atteindre 1/10'000 du montant, c'est-à-dire 500'000 Euros.

Dans les deux cas, sur notre continent, une faillite de l'entreprise est la conséquence la plus probable, un fait principalement causé par le faible remboursement des assurances et surtout par l'énorme réticence des banques à offrir des prêts supplémentaires pouvant permettre à l'entreprise de se remettre de l'attaque.

4. Comment réduire au maximum les risques d'être victime d'un espionnage ?

I. Prenez certaines parties des exemples des «meilleurs des meilleurs» :

En Suisse, la tentative d'intrusion dans le département R&D de l'une des entreprises de systèmes militaires de pointe du pays a eu un impact sismique sur toutes les autres entreprises fournissant des produits issus de processus

de R&D longs et coûteux (entreprises pharmaceutiques et chimiques, etc.) ou fabriquant des articles à très haute valeur ajoutée (horlogers de luxe, fabricants de composants industriels haut de gamme, etc.).

Le meilleur exemple est celui d'une entreprise de luxe de renommée mondiale. Elle a choisi les meilleures sociétés d'informatique et de cyber-sécurité pour construire sa propre architecture informatique, la segmenter avec des règles d'accès très strictes et très restreintes et la faire tester par les meilleurs anciens «black hats» disponibles. Dans le même temps, elle a construit un siège social flambant neuf avec un département de R&D et ses propres serveurs dans des bunkers à l'épreuve des bombes atomiques. Insatisfaite de tout cela, elle a engagé les meilleurs anciens voleurs, des cascadeurs capables d'escalader un mur les mains libres, un véritable ancien commando d'élite et, à nouveau, d'anciens pirates informatiques pour effectuer un test de résistance à une attaque à grande échelle, qui a échoué.

Bien entendu, aucune trace d'IoT à l'intérieur du bâtiment, la surveillance extérieure et intérieure est assurée par des caméras câblées de premier ordre, et tous les outils nécessaires composés, y compris la climatisation, les ascenseurs, les systèmes de détection et d'extinction d'incendie sont constamment surveillés

par l'équipe SOC de la société doublée d'employés de la sécurité physique (et non du personnel d'une société de sécurité sous-traitante), la plupart d'entre eux étant titulaires d'un permis de port d'arme à feu.

Ensuite, les règles : aucune réunion sans une vérification totale que les participants ont laissé derrière eux tous les appareils IoT/IT, des réunions spéciales traitées dans des salles anti-G, et des règles draconiennes pour chaque employé : laisser son bureau ou son ordinateur portable ouvert ou donner un mot de passe à un collègue entraîne le licenciement sur le champ. En outre, même le PDG n'a pas accès à plus de 2 % d'une base de données.

Si vous atteignez un tel niveau de sécurité, l'espionnage ne peut avoir lieu que sous sa forme «*néolithique*», en soudoyant un employé bien placé.

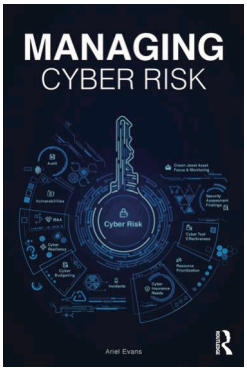
L'exemple de l'échec de la proposition d'accord-cadre, faite il y a plus de deux décennies par la Suisse à l'Allemagne illustre parfaitement la menace du «danger intérieur». Cet accord visait à taxer avec un taux fixe tout citoyen allemand détenteur d'un compte bancaire suisse et à remettre aux autorités allemandes le montant annuel collecté. Pourtant, les Länder les plus riches ont refusé la proposition, obligeant le gouvernement fédéral allemand à la décliner.

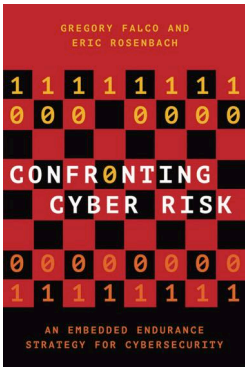
Pourquoi ? Parce qu'à l'époque (c'est-à-dire avant que la Suisse ne rejoigne le système de coopération bancaire de l'UE), la plupart de ces régions ont réussi, par l'intermédiaire de diverses agences privées, à corrompre, parfois à hauteur de 10 millions d'euros ou plus, plusieurs responsables informatiques des deux plus grandes banques suisses, recevant en échange un DVD ou un dispositif USB contenant les informations complètes sur chacun de leurs citoyens ayant un compte - et surtout le montant figurant sur ce compte - dans les banques mentionnées, ce qui a permis aux forces de l'ordre de traduire en justice et de punir les coupables d'évasion fiscale, avec toute la sévérité de la loi allemande, récupérant ainsi des montants bien supérieurs à l'impôt forfaitaire proposé par la Suisse.

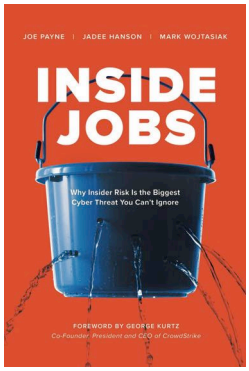
Mais comme nous n'écrivons pas sur les banques ou les multinationales, résumons simplement les risques auxquels une moyenne ou petite entreprise devra faire face, et comment atténuer, voire effacer certains d'entre eux.

II. Essayez d'adopter les politiques et règles suivantes :

Avant toute chose, le PDG et le conseil d'administration doivent être convaincus que la réduction drastique des zones de risque est la meilleure garantie pour mener une activité sans problème, sans interruption, sans







amende et, pire, sans exfiltration de données. Dans ce contexte, «*Confronting Cyber Risk*», de Gregory Falco & Eric Rosenbach (3), et «*Inside Jobs : Why Insider Risk Is the Biggest Cyber Threat You Can't Ignore*» par les collaborateurs de Code42 (4) constituent une lecture intéressante.

La première vulnérabilité provient d'une mauvaise architecture de stockage et de gestion des accès aux systèmes informatiques. Chaque CISO et CSO devrait examiner attentivement l'architecture actuelle et, en utilisant des solutions comme le multi-cloud, limiter drastiquement le nombre de personnes ayant accès aux données les plus critiques.

Un examen et une évaluation minutieux des clauses de sécurité et des points forts mentionnés dans le contrat avec chaque fournisseur informatique - matériel, logiciel, transmission (câble ou wifi) et cloud(s) - doivent être effectués en priorité par le CISO et l'équipe CSO, et les entreprises dont les niveaux de sécurité sont faibles doivent être remplacées par des entreprises fiables. Dans l'idéal, la meilleure solution pour atténuer les dangers possibles lors du chargement, du téléchargement et du transfert de données vers des nuages ou vers des serveurs distants d'une autre filiale consisterait à confier à des «chapeaux blancs» la gestion d'un système de cryptage complet, propre à l'entreprise et dont les sources sont codées.

Il en va de même pour les caméras de surveillance extérieures et intérieures, en remplaçant les webcams par des caméras câblées et en engageant du personnel de sécurité physique dirigé par un ancien policier ou militaire au lieu de confier la sécurité des bâtiments et des entrées à des sociétés externes bon marché.

Ensuite, chaque entreprise devrait disposer d'un inventaire exhaustif de ses moyens informatiques, et cette liste devrait être mise à la disposition du CSO. Dans trop d'entreprises, des serveurs de différentes générations et des ordinateurs portables avec des versions différentes d'OS et de logiciels fonctionnent en même temps.

Je me souviens encore d'une discussion avec le CSO du siège d'une grande banque italienne en Europe de l'Est pendant la crise «non Petya». Il a plaisanté en disant : «*Aujourd'hui, c'est moi l'archéologue, pas vous ! J'ai découvert à l'étage 7 un serveur Windows XP encore connecté et personne dans le département informatique n'a pu me dire pourquoi il était là et surtout pourquoi il est encore actif*».

Dans le même domaine, la vérification quotidienne obligatoire, par votre SOC, des vulnérabilités sur les organisations de confiance (comme la page d'alertes du CerT de Singapour) (5), ce qui permet de connaître les problèmes avant qu'un correctif ne soit livré par le producteur du logiciel/matériel vulnérable.

Les mêmes imprimantes multitâches connectées en Wifi, facilement piratables, ainsi que les autres appareils partagés connectés en Wifi devraient idéalement être interdits et remplacés/réinitialisés sur le bon vieux mode câble.

D'autres politiques obligatoires, qui doivent être précédées d'entretiens de sensibilisation, devraient inclure :

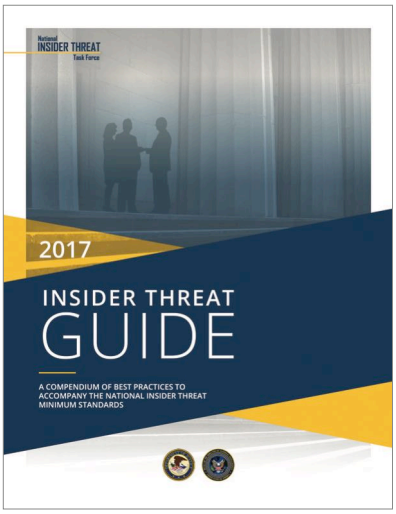
A. **Interdiction de surfer sur Internet via les outils informatiques fournis par l'entreprise** - au moins pour chaque décideur de chaque département de l'entreprise, en plus du PDG et des membres du conseil d'administration. Il s'agit d'une question particulièrement sensible qui ne peut être appliquée de manière réaliste à tous les employés car des études ont démontré que l'interdiction d'accéder aux réseaux sociaux est un facteur qui peut, à lui seul, motiver une démission immédiate et un changement d'emploi en faveur d'une entreprise autorisant cette pratique.

B. **Vérification constante par le SOC des informations d'identification de tous les employés et des données auxquelles ils ont accès. Bien entendu, la révocation immédiate des informations d'identification d'un employé qui quitte l'entreprise est essentielle**. De nombreuses entreprises oublient cette pratique et des études ont révélé que d'anciens employés conservaient leurs privilèges d'accès pendant 3 à 6 mois après avoir quitté une entreprise !

C. **Interdiction de pénétrer dans des zones ou des départements bien établis de l'entreprise avec tout**

dispositif personnel IoT ou Smart. Surtout, pas de smartphone, pas d'IoT, pas d'informatique pendant les réunions stratégiques/de comptabilité/de R&D. Cette solution simple permet d'éviter l'outil d'espionnage le plus basique, car des études récentes estiment que jusqu'à 2 smartphones sur 10 des employés essentiels dans les entreprises intéressantes ont un logiciel espion vocal installé, permettant aux pirates d'entendre tout ce qui est dit par tout le monde autour de la personne portant le smartphone infecté.

D. Si la loi du pays le permet, une **vérification constante de tous les courriers des employés envoyés via l'adresse de leur entreprise** ainsi que (toujours si la loi le permet) une **surveillance constante de leurs connaissances ainsi que de leurs publications sur les médias sociaux,** en particulier sur LinkedIn.



Une étude réalisée par Bitdefender il y a douze ans, sur un échantillon de 2000 employés du secteur des TI et de la sécurité informatique acceptant un nouvel «ami» sur ce média, a montré qu'après une demi-heure de conversation, 10 % d'entre eux divulguaient des informations personnelles sensibles et, pire encore, deux heures plus tard, 73 % d'entre eux siphonnaient ce qui semble être des informations confidentielles de leur lieu de travail, telles que des stratégies et des plans futurs, ainsi que des technologies/logiciels inédits. Loin d'être arrêté, ce phénomène se produit maintenant aussi sur Facebook, Google+ et, cerise sur le gâteau, des études récentes montrent que la plupart des faux emplois «sur mesure» proposés sur LinkedIn contiennent des liens vers certains des malwares et spywares les plus sophistiqués du moment.

E. **L'analyse comportementale des employés ayant accès aux documents sensibles devrait être effectuée de manière régulière**. Hélas, dans un monde où la plupart des employés et même des PDG travailleront pour au moins dix entreprises différentes jusqu'à leur retraite, en **plus des employés grassement payés par un tiers** (comme dans l'exemple bancaire susmentionné), **la plupart des menaces intérieures** et des actions nuisibles directes (voler des informations confidentielles et les partager partout) **sont perpétrées par des employés dans le seul but de se venger de relations conflictuelles avec des collègues ou des supérieurs directs au sein même de l'entreprise**. Pour ce sujet précis et crucial, les Etats-Unis ont créé un outil extrêmement important pour les entreprises : le National Insider Threat Task Force (NITTF) (6), qui fournit en permanence des analyses, des outils, des tutoriels vidéo et web ainsi que des rapports extrêmement pertinents.

Si une entreprise parvient à adopter toutes ces recommandations de base et à mettre en œuvre les politiques correctes mentionnées, elle sera à l'abri de 90 % des actes d'espionnage les plus courants, ne restant vulnérable qu'aux attaques par force brute de type «zero day», conçues sur mesure pour le système informatique central, extrêmement coûteuses à réaliser et donc réservées à des objectifs de très grande valeur.

En outre, les entreprises devraient être prêtes, moyennant quelques actions supplémentaires, à obtenir les certifications ISO/NIST/BSI leur permettant d'être éligibles à une assurance américaine ou britannique couvrant tous les coûts en cas d'attaque sans faute, erreur ou trahison d'un employé. ■

(1) Ariel Evans, Managing Cyber Risk, Londres-New York : Routledge, 2019
(3) Gregory Falco, Eric Rosenbach, Confronting Cyber Risk. An Embedded Endurance Strategy for Cybersecurity, New York, NY : Oxford University Press, 2022
(4) Joe Payne, Jadee Hanson, Mark Wojtasiak, George Kurtz, Inside Jobs : Why Insider Risk Is the Biggest Cyber Threat You Can't Ignore, New-York : Skyhorse, 2020
(5) https://www.csa.gov.sg/singcert/Alerts
(6) https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf

Sécurité économique et cybersécurité, de la confusion à l'intrication.

Auteur : Stéphane Mortier

Une cyberattaque… ?

Les chercheurs de Proofpoint ont identifié une campagne visant des entités françaises dans le secteur de la construction, de l'immobilier et de l'industrie. D'après l'entreprise de cybersécurité, les attaquants ont utilisé un document Word

malveillant portant sur le RGPD (Règlement général sur la protection des données). L'activation des macros permettant de requêter une URL contenant un script PowerShell caché via des techniques de stéganographie dans une image. Ce script conduit au téléchargement du gestionnaire de paquets Chocolatey. Enfin, la chaîne de compromission se poursuit pour déployer la charge utile finale, la porte dérobée « Serpent ». Les chercheurs n'ont pas identifié les objectifs finaux des attaquants. Toutefois, d'après les techniques, tactiques et procédures employées, Proofpoint émet l'hypothèse qu'il s'agisse d'un mode opératoire avancé.

Voici une brève communiquée dans la newsletter de l'ANNSI le mardi 23 mars 2022, résumant un article de Proofpoint[1]. Une brève analyse peut nous donner les informations suivantes :

- les secteurs de la construction, de l'immobilier et de l'industrie, en France, sont visés ;
- l'argument de la conformité au RGPD est avancé par l'attaquant ;
- un lien permet l'installation d'un gestionnaire de paquets ;
- l'effet final recherché n'est pas connu mais le mode opératoire avancé laisse penser à une attaque ciblée.

En matière de sécurité économique, la tendance actuelle tend à montrer que la cyberattaque est généralement le vecteur d'une attaque plus complexe en vue de fragiliser ou désorganiser un acteur économique. Par exemple pour atteindre à la réputation, pour capter des données, pour entraver une mesure de sûreté, pour désorganiser une chaîne de production,... Peut-on alors dissocier, au travers de cette attaque, le risque cyber des autres risques ? La réponse est probablement non bien que des attaques purement cyber peuvent coexister avec des attaques plus élaborées.

La sécurité économique peut aujourd'hui être considérée comme un paradigme a part entière, tant en management stratégique qu'en management public. Au travers de l'attaque susmentionnée nous proposons une ébauche d'analyse au travers de ce paradigme.

La sécurité économique comme paradigme

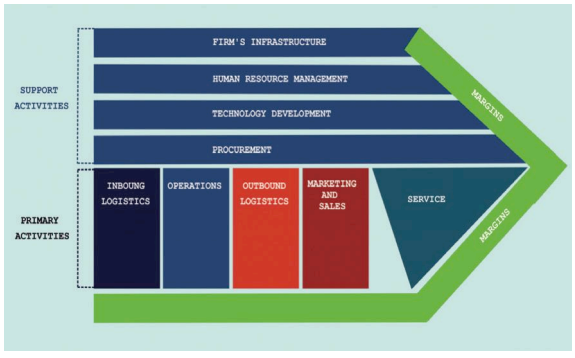
Toute entreprise répond à plusieurs objectifs : économiques, sociétaux et réputationnels (management stratégique). La création de valeur impliquant la compétitivité de l'entreprise répond aux objectifs économiques ; la contribution à la vie de la société (emploi, fiscalité, responsabilité sociale de l'entreprise) aux objectifs sociétaux ; la recherche de notoriété, la conformité, le développement et l'accroissement de la taille de l'entreprise aux objectifs réputationnels.

Les entreprises, à l'instar de tout acteur économique, évoluent alors dans un écosystème, dans un environnement (concurrentiel, normatif, technologique, social, sécuritaire, politique, informationnel,...) qui leur est

propre et qu'elles doivent maîtriser pour réaliser leurs objectifs. Au sein de cet environnement global se situe la chaîne de valeur.

Cette dernière, contient les différentes activités de l'entreprise utiles à la création de valeur. Il convient d'ajouter à ces activités la logistique entrante et la logistique sortante, c'est-à-dire toutes les étapes reliant les fournisseurs de biens ou services à l'entreprise ainsi que toutes les étapes reliant l'entreprise aux clients, sans omettre les prestataires, y compris les banques, assurances et même les pouvoirs publics.

La chaîne de valeur ainsi entendue constitue une cartographie utile à toutes les parties prenantes de la création de valeur, mais aussi à tout acteur malveillant qui souhaiterait nuire à une entreprise. En effet, que ce soit au niveau de la logistique entrante, des activités internes ou de soutien, de la logistique sortante, une multitude d'atteintes sont possibles.



La prédation économique est aujourd'hui une réalité qu'il n'est plus à démontrer. Dans un contexte de guerre économique, aucune entreprise n'est à l'abri ni de la prédation, ni de la déstabilisation. Acteurs économiques, société civile, puissances étrangères, cybercriminels, sont autant de prédateurs éventuels, quelles que soient leurs motivations.

Les conséquences d'une atteinte à la sécurité économique sont systématiquement un affaiblissement de l'entreprise et donc une exposition plus grande à la prédation. Ces atteintes emportent souvent des conséquences sur la trésorerie des entreprises, point névralgique de leur stabilité et de leur capacité de résilience.

Dans le cadre de la politique publique d'intelligence économique française (management public), ces atteintes ont été catégorisées en huit familles. Ces familles d'atteintes constituent un véritable référentiel en matière de sécurité économique. En voici les principales caractéristiques :

- Les **atteintes physiques** qui vont essentiellement concerner les intrusions, destructions, vols de matériels et de matériaux. Un intrusion informatique pourra aider l'intrusion physique par exemple ;
- Les **désorganisations et fragilisations** sont des actions venant de l'extérieur. Au moyen d'une cyberattaque il est possible de ralentir l'activité d'une entreprise par exemple ;
- Les **risques cyber** eux-mêmes sont bien entendu un risque considérable pour les entreprises (attaque DdoS, vol de données, ransomware,…) ;
- Les **risques financiers** ne constituent généralement pas d'infraction au sens du droit pénal mais sont des outils de prédation par excellence. Les flux financiers étant dématérialisés, le risque cyber y est particulièrement important ;
- Les **atteintes aux savoir-faire** sont relatives essentiellement aux questions de propriété intellectuelle et par conséquent à la contrefaçon, mais aussi aux compétences et à l'espionnage industriel...
- Les **atteintes à la réputation** ont pris une dimension considérable avec le développement des moyens de communication au premier titre desquels les réseaux sociaux.
- Les **fragilités humaines** ne sont bien évidement pas à écarter du spectre des atteintes à la sécurité économique. L'humain étant l'utilisateur (et le concepteur) des moyens numériques.
- Les **intrusions consenties** enfin sont des facteurs de risques très importants. Tout prestataire extérieur constitue un risque en matière d'intrusion consentie, y compris les prestataires informatiques (stockage de données, maintenance,…).

Il s'agit ici d'une grille de lecture au sein de laquelle le risque cyber est omniprésent. Du paradigme à l'outil, la sécurité économique et le référentiel des atteintes apportent une vision particulièrement large des risques liés à l'environnement d'une activité et une clé pour l'anticipation de ces risques.

Analyse d'une cyberattaque au prisme de la sécurité économique

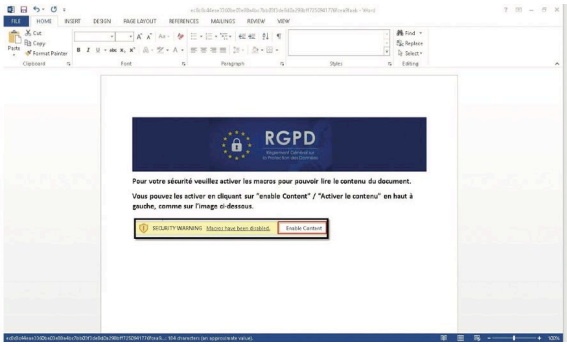
Revenons brièvement sur la brève citée en introduction pour analyser la cyberattaque dont il est question avec la grille de lecture de la sécurité économique.

Premièrement, ce sont les secteurs de la construction, de l'immobilier et de l'industrie, en France, qui ont été visés. Pourquoi ces trois secteurs en particulier ? En sortie de crise de la COVID 19 (*a priori* à la date de rédaction du présent article), les secteurs ayant été particulièrement impactés sont ceux qui n'étaient pas ou peu « télé-travaillables ». En d'autres termes les secteurs d'activité pour lesquels soit la chaîne de production ne peut se passer d'une présence physique des travailleurs : production industrielle, construction et restauration/hôtellerie. Ces secteurs se trouvent actuellement en difficulté et n'ont pu être tenus à flots que par des aides publiques (prêt garanti par l'État, chômage partiel,…). La cyberattaque en question vise donc des secteurs déjà en position de difficulté (industrie, construction et immobilier).

Le prédateur s'attaque plus facilement à une proie affaiblie ou blessée, ce qui augmente ses chances de réussite.

Deuxièmement, l'argument de la conformité au RGPD est avancé par l'attaquant. L'arrivée du Règlement général sur la protection des données personnelles (RGPD) en 2018 à imposer une mise en conformité des acteurs économiques. Ce règlement n'avait été que très peu anticipé et de nombreuses PME/TPE peinent encore à se conformer.

De plus, dès 2018, de nombreuses escroqueries « à la mise en conformité RDPD » ont visé les entreprises, souvent sous forme de phishing comme point de départ. Au regard des sanctions prévues en cas de manquement à la protection des données personnelles, ce sujet est généralement pris au sérieux. Par l'argument RGPD, le cyberattaquant peut convaincre plus facilement sa victime.



Une entreprise déjà fragilisée par la crise ne prendra pas le risque d'être également sanctionnée en matière de gestion des données personnelles. L'argumentaire de l'attaquant semble ici être particulièrement bien construit et pousse à clicker sur le lien qui installera une logiciel malveillant sur le réseau ou le poste de l'utilisateur.

BIO

Stéphane Mortier est actuellement adjoint au chef du Centre de Sécurité Economique et de Protection des Entreprises (CSECOPE) au sein de la Direction Générale de la Gendarmerie Française et membre de la Communauté de Recherche de la Gendarmerie Nationale (CREOGN). Il est maître de conférences à l'Université Gustave Eiffel. Il est diplômé en sciences politiques, sociologie et relations internationales de l'Université libre de Bruxelles (ULB), en management stratégique et intelligence économique de l'École de Guerre Économique, et docteur en gestion à Paris 1 Panthéon-Sorbonne. Il est également le représentant des sections étrangères de l'Union des anciens de l'ULB et préside la section française (UAEF). Dans ce cadre, il développe des projets de coopération en Afrique. Il est chargé de cours à l'Ecole de Guerre Économique (lutte contre le blanchiment d'argent), à l'Université de Likasi - RDC (stratégie, droit des affaires). Il est membre fondateur du Cercle K2 et membre actif de l'Association pour l'Unification du Droit en Afrique (UNIDA). Il est l'auteur de plusieurs publications sur l'intelligence économique.

Troisièmement, un lien permet l'installation d'un gestionnaire de paquets, c'est-à-dire un système permettant d'installer des logiciels, de les maintenir à jour et de les désinstaller. Le paquet contient les fichiers informatiques, les informations et procédures nécessaires à l'installation d'un logiciel sur un système d'exploitation au sein d'un agrégat logiciel, en s'assurant de la cohérence fonctionnelle du système ainsi modifié.

Cela constitue un mode opératoire avancé et ne peut être l'œuvre d'un simple escroc. De plus, une porte dérobée est également installée, donnant ainsi un accès à distance à l'ordinateur infecté. Il s'agit là des aspects techniques de l'attaque. Ces outils vont permettre la captation de données, l'accès à l'ensemble des fichiers de la victime,…

Enfin, l'effet final recherché n'est pas connu mais le mode opératoire avancé laisse penser à une attaque ciblée : secteurs d'activité fragilisés, argument du RGPD et utilisation de techniques assez complexes.

Conclusion

Quel peut être l'objectif d'une cyberattaque sur des entreprises de secteurs d'activité fragilisés ? Au regard de la gille de lecture proposée ci-dessus, le mode opératoire laisse à penser que l'appropriation de données pourrait être le motif de la cyberattaque. Mais alors pourquoi dans le secteur de la construction, de l'immobilier et de l'industrie ?

La forte augmentation des prix des matériaux de construction et un marché de l'immobilier qui continue de croître (valeur refuge notamment) induit des intérêts financiers particulièrement importants. Recueillir des données précises sur les activités de construction et les projets immobiliers revêt alors une valeur stratégique pour la concurrence mais également pour les fabricants de matériaux de construction, voire pour les logisticiens qui exerceront le transport de ces matériaux.

Également, la construction étant un secteur ayant un recours important à la sous-traitance, les enjeux de positionnement sur des projets futurs peuvent s'avérer très lucratifs si anticipés et donc acquis. Quant au secteur de la production industrielle, il est soumis à une hausse importante du coût des matières premières (rappelons que, par exemple, le cours du cuivre a atteint son record historique en mars 2022).

Obtenir de l'information sur les carnets de commande, la santé financière, l'état des stocks,... permet d'analyser les besoins futurs et donc de se positionner sur la fourniture de matière première. Il semblerait donc, par cette analyse rapide et sans entrer dans le détail, que l'objectif de la cyberattaque est de capter l'information nécessaire à une analyse des besoins en matières premières ou de matériaux pour les secteurs visés.

Une telle analyse, sur le marché français en l'occurrence, permettrait au commanditaire d'établir un plan stratégique sur la fourniture de ces besoins. On serait par conséquent ici confronté à une opération d'espionnage économique que seule une analyse au prisme du paradigme de la sécurité économique puisse mettre au jour. Au-delà de la cyberattaque, une opération de positionnement sur un marché, voire de prédation économique est peut-être en train de se jouer... ■

1 https://www.proofpoint.com/us/blog/threat-insight/serpent-no-swiping-new-backdoor-targets-french-entities-unique-attack-chain

Par quel moyens serons-nous «espionnés» ou, au contraire, plus protégés demain: anciennes et nouvelles «normalités» des télécoms.

Auteur : **Mika Lauhde**

Début 2020, l'hypothèse était que la pandémie de la Covid-19 aurait généré une brève perturbation de l'économie et des affaires mondiales, mais qu'il y aurait ensuite un retour rapide à la «bonne vielle normalité».

Aujourd'hui, en 2022, tout le monde a compris que ce ne sera pas le cas, notamment en raison de la guerre en Ukraine, mais qu'il n'y aura qu'une «nouvelle normalité». À ce stade, nous sommes déjà en mesure de proposer quelques prédictions sur la façon dont cette «nouvelle normalité» pourrait se réaliser et sur les impacts qu'elle aura sur notre infrastructure de télécommunications et sur les fondements même de la cyber-sécurité.

La Covid-19 a ouvert les yeux de tous les décideurs du monde sur des problèmes particulièrement sensibles: le soutien nécessaire aux soins de santé nationaux en cas de pandémie (avec en tête d'affiche le «vaccin») et l'assurance de garantir une bonne fonctionnalité des services de télécommunications, facteurs de continuité des activités en cas de pandémie ou de guerre/ guerre technologique (à savoir tout ce que comprend le terme «connectivité»).

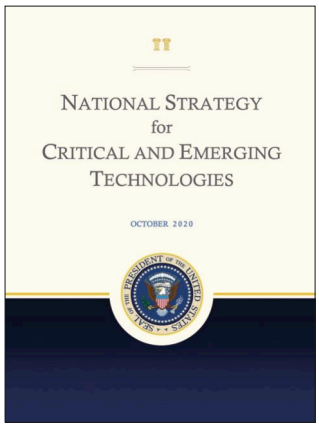
Cela signifie que pratiquement tous les pays planifient actuellement la manière de surmonter ces problèmes dans un avenir proche et, dans le meilleur des cas, prennent un avantage politique certain avec des mesures viables.

Le dernier point est que la réponse à la question «comment ?» ne doit pas être logique, ni suivre les règles commerciales normales «d'avant». En d'autres termes, quoi qu'il en coûte, il faut que ces changements se produisent !

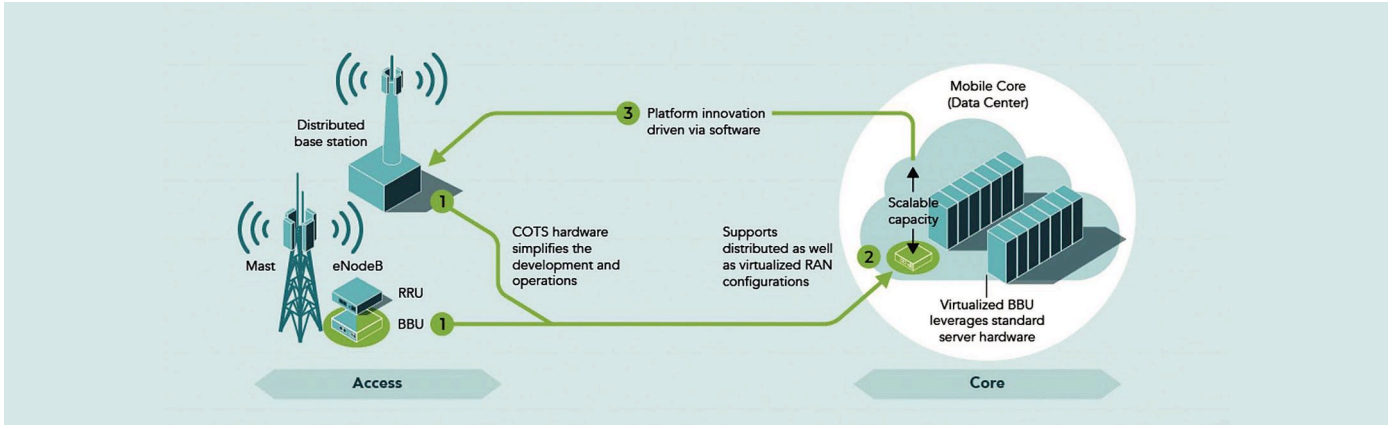
L'outil, le «comment» pour que ce prochain miracle des télécommunications se produise sur un territoire national, s'appelle OpenRAN ou Open Radio Access Network (O-RAN). Ce concept repose sur l'interopérabilité et la normalisation des éléments du RAN, y compris une norme d'interconnexion unifiée pour des éléments hardware construits à partir de composantes diverses et munis de logiciels à code source ouvert, le tout étant garanti par différents fournisseurs.

En d'autres termes, il s'agit de créer une solution de télécommunications qui n'est pas contrôlée ou développée par un seul fournisseur, mais qui est le fruit d'un effort mondial conjoint, incluant à la fois les logiciels et le hardware. Il y a aujourd'hui plusieurs compagnies industrielles d'«OpenRAN», en compétition, dans l'attente de savoir laquelle d'entre elles parviendra à proposer la solution OpenRAN gagnante. Ces compagnies, pour en donner la dimension, englobent des entités de tailles diverses, du puissant Ministère américain de la Défense en passant par les opérateurs de télécommunications actuels et en aboutissant à une pléthore de PME et de start-ups.

Les pays qui envisagent de jouer un rôle actif adoptent également différentes approches pour atteindre ces objectifs : techniques et commerciales. Cela va de la création d'une chaîne d'approvisionnement nationale à un durcissement des réglementations nationales concernant les droits de propriété intellectuelle.



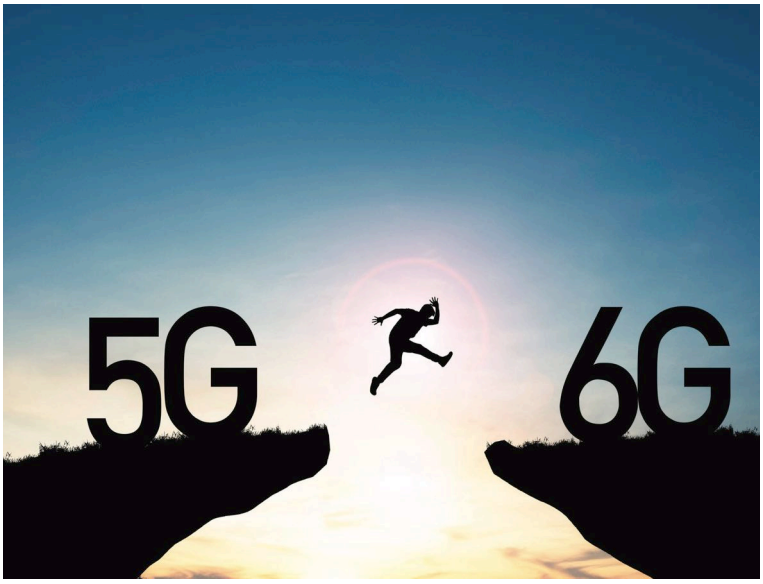
Les États-Unis ont publié leur «*National Strategy for Critical and Emerging Technologies*» en octobre 2020. Dans ce document, la manière dont le leadership en matière de télécommunications doit être construit est clairement définie. Les États-Unis bénéficient clairement de nombreux avantages, parmi lesquels on citera une énorme part du marché mondial dans le domaine des systèmes d'exploitation (PC et appareils mobiles) doublé des écosystèmes qui les produisent et en assurent le fonctionnement. Dans le cadre



de cette stratégie, le Sénat américain a également demandé aux fournisseurs de télécommunications européens de soutenir ce développement, mais sur le sol américain, et ce afin de maintenir les activités sur le marché américain actuel des télécommunications. L'un des moyens d'atteindre cet objectif est d'investir massivement dans des technologies comme celle de l'OpenRAN aux États-Unis. Après tout, les États-Unis ont un avantage mondial en matière de compétences logicielles.

L'Inde a également pris des mesures audacieuses pour assurer ses télécommunications nationales. Le ministère indien des télécommunications a déclaré qu'en janvier 2021, le cœur des télécommunications indiennes devrait être indien. Les subventions que les entreprises indiennes reçoivent actuellement sont bien supérieures à celles que les fournisseurs chinois ou européens reçoivent de leurs gouvernements respectifs. Mais le gouvernement indien pense de la même manière que les États-Unis, à savoir que les fournisseurs doivent déplacer leur département de R&D, leur fabrication, leurs propriétés intellectuelles, etc. sur le sol indien pour pouvoir continuer à vendre leurs produits dès maintenant, tout en soutenant progressivement le développement des compétences nationales indiennes. Et, dès à présent, certaines entreprises indiennes déclarent qu'elles possèdent déjà la technologie OpenRan et qu'elles sont à la disposition des opérateurs indiens.

Le gouvernement japonais, quant à lui, vient de publier un rapport sur l'objectif à plus long terme du Japon : celui de devenir le leader mondial de la 6G. Il investira donc près de 500 millions de dollars en 2022 et des sommes considérables dans les années à venir pour le développement des télécommunications locales. Selon le plan, le but du Japon devrait être atteint en 2025, soit dans trois ans seulement ! Ce projet devrait être réalisé par des entreprises privées japonaises, par plusieurs universités ainsi que par

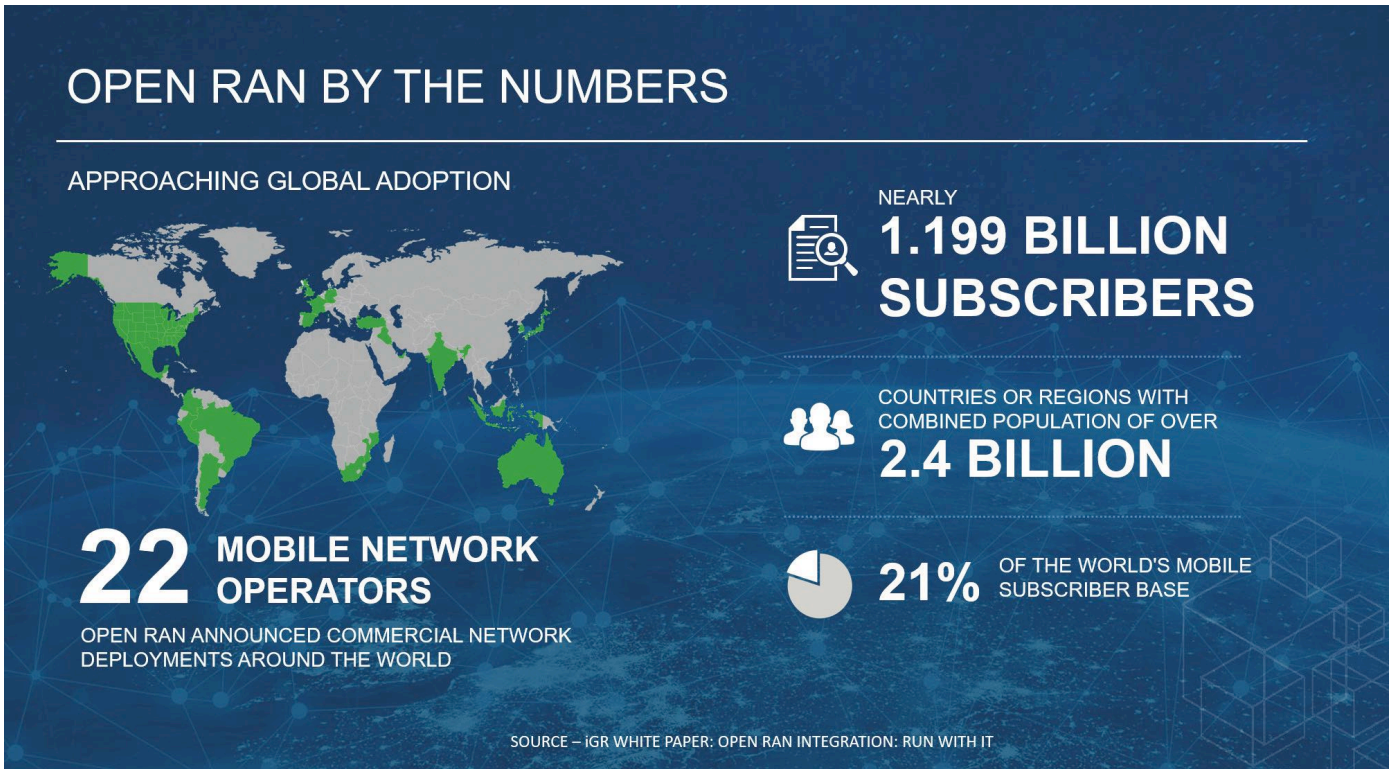


l'Institut national des technologies de l'information et des communications, qui dépend du ministère des télécommunications. Déjà aujourd'hui, la radio 5G américano-japonaise de Fujitsu intègre désormais la technologie nécessaire aux macro-sites OpenRAn et aux nouveaux réseaux.

La Commission européenne pense un peu de la même manière. L'UE vient de prendre la décision de stimuler la création d'une souveraineté numérique qui se fera par le biais de contrôles financiers, de la création

BIO

Mika Lauhde a plus de 30 ans d'expérience dans ces domaines. Il a dirigé les dépatrtenments de sécurité de plusieurs des plus grandes entreprises de télécommunications du monde, travaillant dans l'UE et en dehors de l'UE dans postes-clés, définissant l'avenir des directives, des règlements et des stratégies pour les fonctions critiques de la cybersécurité et de la protection de la vie privée. En tant que directeur de la sécurité et de la continuité des affaires, Mika a été responsable des efforts mondiaux en matière de cybersécurité auprès de Nokia Telecommunication.
Chez Nokia, il s'est notamment occupé des relations gouvernementales liées à la cybercriminalité mais aussi de la gestion de crise, ainsi que de la sécurité liée aux appareils de communication ainsi que de leurs opérations de fabrication dans le monde entier. En tant que vice-président mondial de la cybersécurité et de la protection de la vie privée chez Huawei Technologies, Mika Lauhde a conseillé les cadres supérieurs de l'entreprise sur les politiques, les lois, les réglementations, les technologies et les grandes tendances en matière de cybersécurité et a dirigé les relations avec les gouvernements et les grandes multinationales dans le monde entier. Avant de rejoindre Huawei, il a été vice-président des relations gouvernementales et du développement commercial chez SSH Communications Security (inventeur du protocole SSH), où il conseillait les gouvernements et autres partenaires du groupe sur les questions de sécurité et de confidentialité, notamment la protection des infrastructures critiques, la conformité, l'assurance logicielle et la gestion des risques et des identités à l'échelle mondiale.
Mika a été pendant 11 ans membre de l'ENISA (l'Agence européenne chargée de la sécurité des réseaux et de l'information) et conseille Europol dans les domaines relatifs à la cybersécurité et la à la vie privée. De 2005 à 2009, il a été membre du CPNI, le groupe de protection des infrastructures critiques du gouvernement britannique. Il est actuellement Senior Fellow au Centre de protection des données et de cybersécurité de la faculté de droit de l'université de Maastricht et Fellow de l'Institution of Engineering and Technology (FIET) du Royaume-Uni.



d'écosystèmes, du développement technologique et de la protection des entreprises européennes et de leurs droits de propriété intellectuelle afin d'empêcher des rachats hostiles.

Naturellement, Ericsson et Nokia y gagneront, mais l'intention est de faire en sorte que les PME européennes participent également à l'effort collectif. Il s'agit aussi et surtout d'éviter que les financements garantis soient utilisés en dehors de l'UE, comme cela s'est souvent produit jusqu'à présent. La «loi sur les puces électroniques» fait également partie de ces mesures. Elle devrait ramener la fabrication des puces en Europe et permettre de réduire la taille des puces de 22 nm à 2 nm en 8 ans seulement !

Et la liste ne s'arrête pas là. L'Allemagne a réservé 2 milliards d'euros de fonds de stimulation économique pour l'OpenRAN, tandis que la stratégie de diversité des réseaux du Royaume-Uni dispose de 250 millions d'euros pour soutenir l'OpenRAN en partenariat avec la Corée du Sud.

Savoir aujourd'hui si ces «bonnes intentions» seront commercialement ou techniquement réalisables n'est pas la question. À l'heure actuelle, ces mesures desservent à merveille l'ordre du jour politique, celui de dissimuler le manque d'action des gouvernements en ce qui concerne le manque de toutes sortes de vaccins et de médicaments pour les hôpitaux, les déficits des investissements et des engagements nationaux en matière de largeur de la bande passante servant les réseaux de télécommunications, mais aussi leur contrôle et leur cyber-sécurité.

Les fournisseurs d'équipements de télécommunications traditionnels comme Huawei, Nokia, Ericsson et Cisco ne sont pas encore prêts à affirmer que des technologies comme OpenRAN sont capables de changer le monde. Après tout, il y a plusieurs domaines dans lesquels OpenRAN n'est pas très bon : la sécurité, l'interopérabilité, l'évolutivité, l'augmentation de la complexité opérationnelle, le coût total d'exploitation, etc.

Et quelqu'un doit résoudre ces problèmes. Mais qui ?

Le problème, c'est que même si la technologie n'est pas nécessairement en mesure de fournir ce qu'elle promet, il est bon de se rappeler que des technologies moins bonnes ont parfois gagné, uniquement pour des raisons commerciales ou purement politiques.

Et la Chine, que fait la Chine avec OpenRAN ? La Chine surveille ce que fait le reste du monde. Après tout, Huawei, ZTE et de nombreux autres

fournisseurs de télécommunications se portent très bien, tant sur le plan technique que commercial. Ils dépensent un peu d'argent pour le développement d'OpenRAN, mais pas de manière significative. La Chine a la patience d'attendre et de voir. Et entre-temps, elle a construit le réseau national 5G le plus avancé de la planète pour soutenir sa croissance économique future.

Et la fin du jeu de l'OpenRAN ?

Le jeu de l'OpenRAN pourrait naturellement se terminer de différentes manières, mais il y a des similitudes avec un événement historique antérieur : le projet «Starwars» annoncé en 1983 par le président Reagan. Il s'agissait d'une initiative stratégique dont les promesses étaient techniquement quasi impossibles à tenir et qui entraînait de lourdes dépenses économiques, principalement pour les États-Unis et l'URSS / la Russie. Mais elle ne générait aucune valeur ajoutée réelle pour qui que ce soit.

Cette fois, l'impact économique pourrait frapper d'autres pays (ceux qui investissent lourdement dans leur OpenRAN national) et, au cas par cas, si un pays ne parvient pas à réaliser son projet OpenRAN national et à le fragmenter pour qu'il puisse servir des solutions normalisées et certifiées au niveau mondial (comme dans le cadre du 3GPP), le vainqueur final pourrait, contre toute attente, être un OpenRAN qui sera basé sur l'OPS-5G (dirigé par la DARPA - *Defense Advanced Research Projects Agency* - la toute puissante agence placée sous le commandement du Département de la Défense des États-Unis), même si, actuellement, son impact sur l'industrie est considéré comme le plus faible parmi les projets cités ci-dessus.

Tout cela pourrait conduire à une nouvelle partition de l'écosystème des fournisseurs de télécommunications mondiaux dans les pays occidentaux, un cas où l'Europe pourrait se retrouver exactement dans la même situation avec les télécommunications qu'avec la technologie des chipsets. Une technologie qui n'existe plus nulle part. ■

Espionnage économique et industriel et cyberespace.

Auteur : Olivier Kempf

La révolution cyber dure depuis maintenant près de quarante ans. L'informatique avait commencé avec de puissants ordinateurs mais restait une affaire de grosses structures professionnelles. Tout changea à partir des années 1980 avec une révolution qui connut plusieurs phases :

- Années 1980 : arrivée de l'ordinateur individuel (le PC, *personal computer*, sous ses versions DOS-Windows et Mac) ;
- Années 1990 : irruption d'Internet : les ordinateurs communiquent entre eux. Une toile se met en place ;
- Années 2000 : Arrivée du net 2.0 avec la multiplication des blogs et autre sites personnels. Désormais, l'individu n'est plus un consommateur d'information, il devient un producteur. Son trafic est analysé par les algorithmes de données massives *(Big Data)*. Les GAFA prennent leur essor.
- Années 2010 : généralisation des ordiphones *(smartphones)*. La connectivité devient ultra mobile. Les nouvelles techniques d'intelligence artificielle (par réseaux de neurones et apprentissage machine) se généralisent. L'infonuagique *(cloud computing)* devient la norme.
- Années 2020 : La vague en cours devrait prendre appui sur la mise en place de la 5G et la massification des objets connectés, de plus en plus autonomes.

Ces vagues successives ont suscité une véritable révolution anthropologique. Nos sociétés fonctionnent désormais entièrement

appuyées sur le cyberespace et ses couches multiples (physique, logicielle et informationnelle). Ce qui affecte le citoyen a également bouleversé le monde de l'entreprise.

Auparavant, la modernisation informatique venait du monde de l'entreprise vers celui de l'individu. Désormais, l'entreprise est obligée de conduire deux activités simultanées : d'une part une montée en puissance de son équipement et la numérisation de ses procédures.

Aujourd'hui, une entreprise de taille moyenne utilise plusieurs dizaines de logiciels professionnels et des centaines de machines, serveurs et services infonuagiques : tout ceci est destiné à son fonctionnement interne.

Elle doit simultanément modifier en profondeur ses procédures pour tenir compte de la décentralisation radicale des comportements : relations avec les employés qui doivent être de plus en plus mobiles, tendance accentuée avec le télétravail ; mais aussi relation avec les clients, de plus en plus d'activités commerciales B to C se déroulant désormais en ligne. Cette explosion des usages informatiques entraîne des contraintes évidentes de cybersécurité.

La plupart des entreprises ont pris des mesures de sécurité et les responsables de sécurité des systèmes d'information (RSSI) sont devenus des maillons essentiels dans les organisations professionnelles, même si leur rôle

BIO

Après une carrière militaire où , outre des opérations, il s'est occupé d'affaires internationales et de transformation, le général (2S) Olivier Kempf est consultant indépendant et chercheur associé à la FRS). Auteur de «Introduction à la cyberstratégie» ainsi que «Gagner le cyberconflit, comment lutter dans l'espace sémantique» (Economica), il est directeur de publication de La Vigie, cabinet de synthèse stratégique qu'il a fondé en 2014 qui publie une lettre bimensuelle et rédige diverses études pour ses clients.

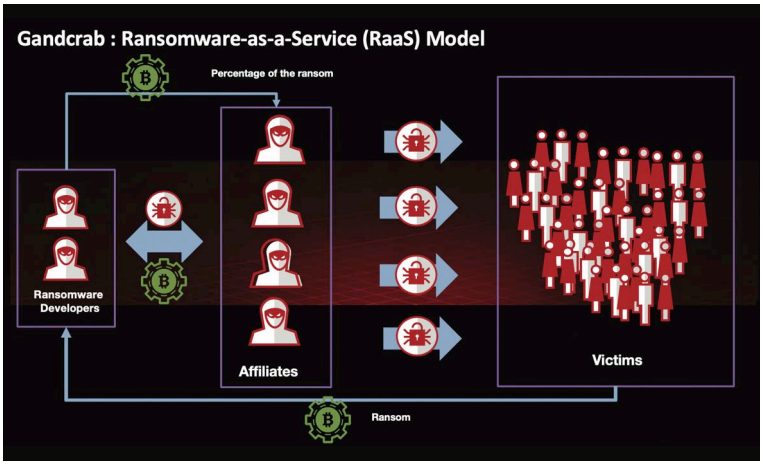
n'est pas toujours reconnu à sa juste place. Il reste que la plupart du temps, leur action se concentre sur les deux couches primaires du cyberespace, la couche physique et la couche logicielle. La couche informationnelle est généralement moins couverte.

Or l'information, au cœur de la troisième couche, devient un facteur de production essentiel de l'entreprise contemporaine. Elle revêt de multiples formes. Ainsi, l'analyse des données de ses clients via du Big data *(know your customer)* utilise des microdonnées recueillies en nombre et traitées de façon à fournir de la valeur.

Mais des informations particulières, plus élaborées, sont également essentielles à l'entreprise : il peut s'agir de la structure de prix d'une offre au moment d'une négociation commerciale, ou encore des projets de recherche et développement, ou enfin du plan stratégique de l'entreprise. Finalement, la gamme des informations traitées par l'entreprise est énorme.

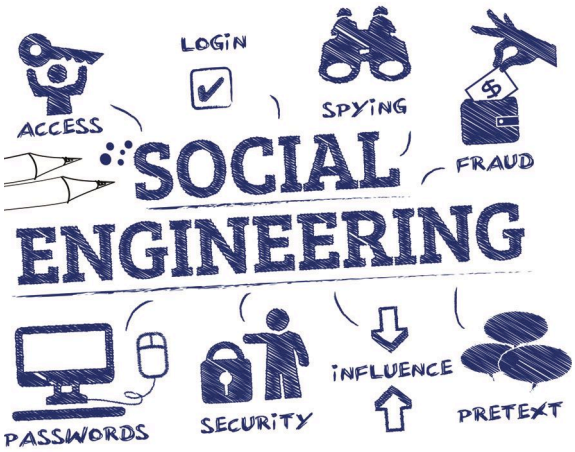
Elles ne sont évidemment pas toutes du même pied mais fondamentalement, elles intéressent autrui : aussi bien les concurrents que les bandits. Dans le deuxième cas, il s'agit de les voler afin de se faire rétribuer : soit en les revendant à un acteur tiers, soit en rançonnant directement l'entreprise avec un dispositif de codage (technique du rançonnage, *ransomware*).

Dans ce cas, l'agresseur vise à prendre en otage un maximum de données, sensibles ou non, mais essentielles à l'entreprise pour son fonctionnement. Ce risque pèse sur toutes les entreprises, quelle que soit leurs tailles. En effet, on observe depuis quelques années une industrialisation de cette technique *(ransomware as a service)* et désormais, toutes les organisations peuvent être ciblées.



Penser que sa faible taille permet de passer en dessous du radar est une stratégie fatale : Il n'y a qu'à observer le nombre de collectivités territoriales de faible taille qui ont été prises en otage ces trois dernières années. Le phénomène s'est d'ailleurs accentué avec la pandémie, qui a forcé la majorité des organisations à passer en télétravail sans avoir anticipé non seulement les aspects techniques de cette transition, mais surtout les aspects de sécurité et de protection des données qui lui sont liées.

Mais derrière ces activités criminelles, force est de constater que las concurrents peuvent également espionner les organisations : il ne s'agit pas ici de bloquer l'activité de l'entreprise, mais de connaître son capital informationnel (où en est tel projet de recherche ? quelle est sa position tarifaire ? quelle ambition a-t-elle auprès de ce client ?) afin d'ajuster sa propre stratégie.

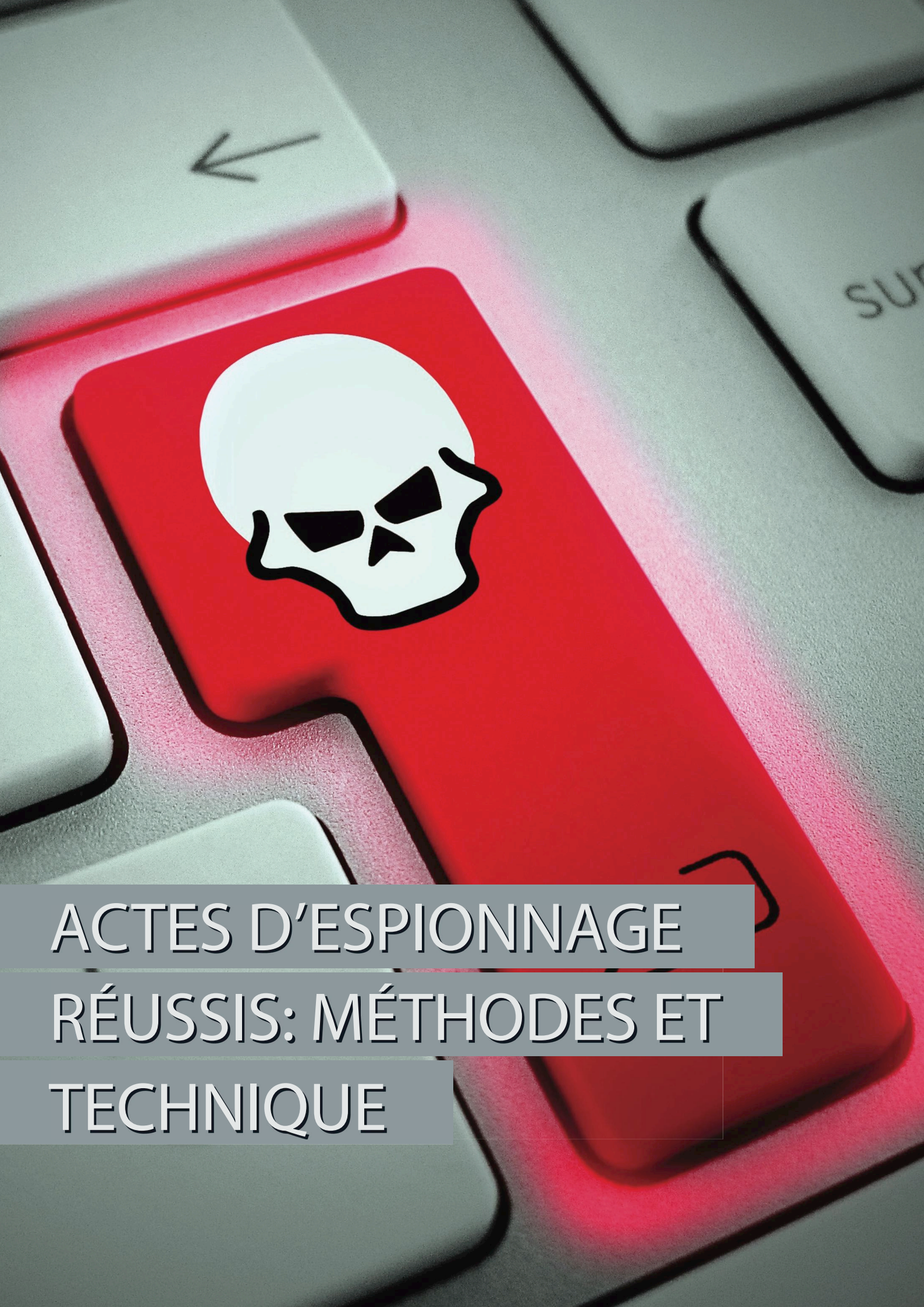


Plusieurs techniques existent : beaucoup d'informations sont décelables par de l'ingénierie sociale ou ce qu'on appelle du renseignement en source ouverte : ainsi, nombreux sont les collaborateurs de l'entreprise qui s'expriment sur les réseaux sociaux sans se rendre compte des données qu'ils communiquent. Mais également, la concurrence peut utiliser des méthodes d'espionnage, ce qui est frauduleux.

Il n'en reste pas moins que beaucoup d'entreprises n'ont pas conscience de ces risques et ne voient pas que la dilapidation de leur capital informationnel les entrave fortement. Avant même de penser à prendre des mesures, il y a un travail de conviction à faire pour que le management prenne conscience de ce risque.

Ce risque est en effet à la fois hautement probable et en même temps avec des effets maximaux. Or, toute cartographie du risque devrait traiter en priorité ces risques-là. La protection du capital informationnel doit donc devenir une priorité des directions d'entreprise.

Ce n'est malheureusement pas le cas. ■



ACTES D'ESPIONNAGE RÉUSSIS: MÉTHODES ET TECHNIQUE

Le cas de l'attaque cyber contre l'entreprise RUAG Holding SA en 2016.

Auteur : Marc-André Ryter

Le 4 mai 2016, l'entreprise d'armements RUAG a annoncé avoir subi une attaque cyber très élaborée et a pu retrouver des traces qui permettent de dire que l'attaque se déroulait depuis au moins septembre 2014.

Together ahead. RUAG

Page 1 / 2

Communiqué de presse

RUAG visé par une cyberattaque: les dommages ont pu être limités

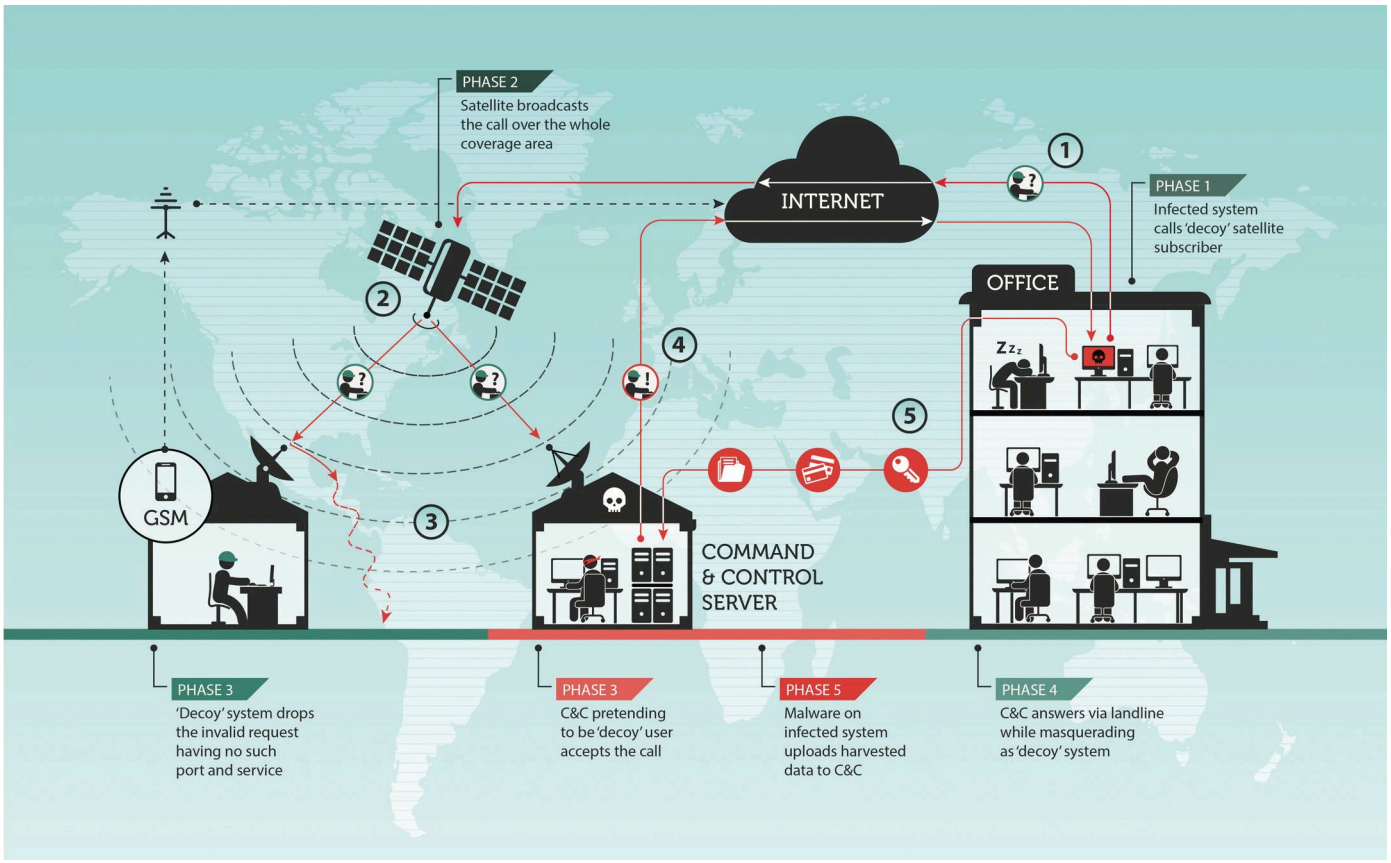
Berne, le 12.05.2016. La cybercriminalité ne s'arrête pas aux frontières de la Suisse: RUAG est spécialisé en informatique et intervient avec succès dans le domaine de la sécurité depuis de nombreuses années. Cependant, la sécurité à 100% n'existe pas – une attaque visant RUAG a pu être détectée et stoppée grâce au soutien des instances fédérales compétentes. Et tout autre préjudice a ainsi pu être évité.

Cette annonce faisait suite à l'information interne donnée en janvier 2016 par le Département de la Défense, de la Protection de la Population et des Sports (DDPS) à la Délégation des Commissions de gestion des Chambres fédérales (DélCdG) *«qu'un incident grave avait compromis la sécurité informatique au sein du groupe d'armement suisse RUAG, aux mains de la Confédération»*[1]. Un rapport détaillé, qui constitue la principale source de cet article, a été par la suite publié afin de fournir aux membres de la communauté cyber des informations leur permettant d'améliorer la protection de leurs systèmes[2].

L'objectif principal de cet article n'est pas l'analyse technique de cette attaque ni même l'analyse du débat

politique qui a suivi l'attaque, mais bien la mise en évidence des moyens engagés et des possibilités de se protéger. Il est intéressant de constater que de très nombreuses informations ont pu être réunies à propos de cette attaque, et que la mise à disposition du rapport technique montre une haute disponibilité à partager ces informations. Ce partage est de manière générale considéré comme une des clés essentielles pour la lutte contre les attaques cyber, et le cas de RUAG représente en ce sens aussi un très bon exemple. L'effort principal a été mis sur les informations concernant les indicateurs de compromission (IoC) et le Modus Operandi de l'attaquant, surtout en raison du fait que l'attaquant a été identifié comme ayant infiltré de nombreuses organisations gouvernementales et compagnies privées lors de la dernière décennie[3].

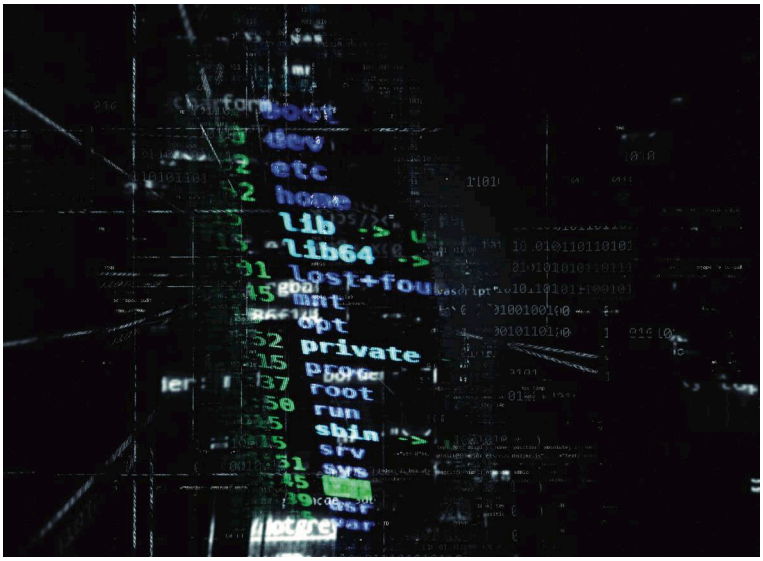
Le malware utilisé dans le cas de l'attaque contre RUAG faisait partie de la famille Turla[4], qui est une famille de malware destinée à l'espionnage. Selon l'expert Matthieu Faou, chercheur en logiciels malveillants, ces malwares sont parmi les plus complexes et utilisent des fonctions cachées



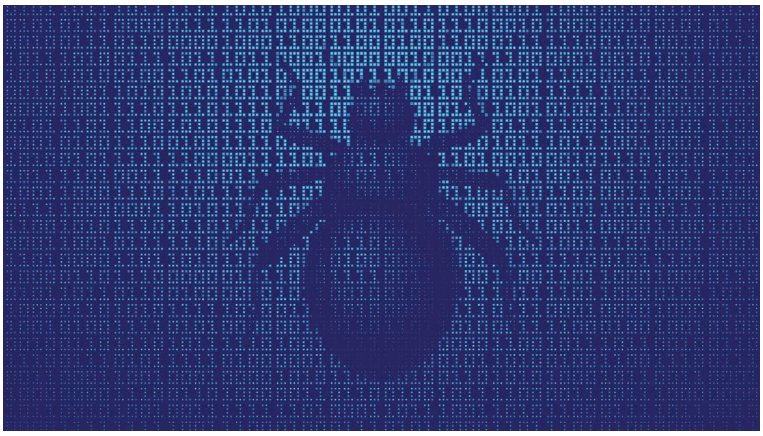
de Windows[5]. Bien que datant de plusieurs années, ses spécificités le rendent toujours difficile à détecter. Les spécialistes de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI/GovCert) du Département fédéral des Finances (DFF) ont en effet mis près de un mois et demi afin d'établir sa présence dans le système de RUAG[6].

Il est particulièrement intéressant de noter que selon toute vraisemblance, l'attaquant a agi sur une longue durée et a fait preuve d'une grande patience avant d'extraire les données visées. Il a aussi fait preuve d'une grande prudence durant toute la phase d'infiltration, de fingerprinting et d'exploration par des mouvements latéraux, ce qui lui a permis par la suite d'agir sur les cibles spécifiques visées. Les mouvements latéraux peuvent se répéter sur plusieurs mois, afin de continuellement vérifier les informations à disposition et le cas échéant les mettre à jour[7].

RUAG a aussi mis en évidence un processus d'attaque progressif, avec une infection d'appareils supplémentaires et le gain de privilèges de plus en plus élevés au sein du système. L'attaquant a créé un réseau interne de communication entre les appareils infectés, et établi différentes fonctions visant à limiter le nombre d'appareils et de voies utilisées afin d'extraire les données. De plus, l'intensité des activités d'espionnage a été très irrégulière afin de compliquer l'identification de la fuite.



Le déroulement de l'attaque délivre de précieux enseignements. Trois phases principales ont ainsi été identifiées. La première phase a été une phase de préparation. La cible a été évaluée en détail et il s'est agi pour l'attaquant de récolter le maximum possible d'informations et de placer les malwares qui lui ont servi par la suite. Il est possible que l'attaquant, dans le cas de RUAG, ait eu une idée du genre d'informations potentiellement disponible au sein du système de l'entreprise. L'utilisation d'ingénierie sociale a peut-être eu lieu durant cette phase, mais n'est pas confirmée. L'attaquant a utilisé des malwares de reconnaissance, qui lui ont permis de confirmer l'intérêt de la cible.



La deuxième phase a consisté à préparer et effectuer l'infection de la cible. La première phase ayant confirmé le potentiel de la cible, des malwares plus performants ont été installé, également en vue d'acquérir une plus grande persistance[8]. Ces malwares ont eu accès à des privilèges d'administrateur du système. Un des obstacles rencontrés par RUAG était que les malwares de reconnaissances ainsi que ceux installés durant la deuxième phase utilisaient les processus déjà existants, sans que cela n'affecte les opérations courantes. RUAG n'aurait ainsi durant près d'une année pas remarqué que son système était infecté[9]. En plus, des outils de dissimulation d'activité (rootkit) très évolués à ce moment-là ont aussi été engagés[10], de même que des processus qui évitent d'utiliser des fichiers cachés qui peuvent devenir visibles (Carbon DLL)[11]. Les malwares installés à ce stade contenaient les instructions sur les opérations à effectuer par le système attaqué au moment choisi.

Enfin, durant la troisième phase, l'attaquant était pleinement présent au sein de la cible et a commencé son exploitation. Cette phase d'exploitation a continué à se dérouler de façon quasi indétectable pour la victime. L'attaquant a pu, durant une période prolongée, continuer son exploration du système, compléter son arsenal, mettre en place un réseau au sein du système attaqué et obtenir plus de privilèges en utilisant des mouvements latéraux. Le rapport mentionne que des mouvements latéraux ont eu lieu durant les 8 premiers mois de l'attaque[12]. L'attaquant s'est ainsi créé les chemins vers les informations recherchées, et a mis en place le système nécessaire pour les exfiltrer. Durant la reconnaissance approfondie du système, très peu de données ont été exfiltrées. Ce n'est que lorsque que l'attaquant a été satisfait du niveau atteint, et qu'il a pensé qu'il disposait de tous les éléments nécessaires, qu'il a mis en œuvre l'exfiltration de données en grandes quantités.

Cette phase fût la plus délicate, car c'est le moment au cours duquel la victime est la plus à même de se rendre compte de l'attaque en raison du trafic de données non ordonné de sa part, voire du volume soudain de ce trafic. Lorsque le malware envoie les données extraites en utilisant des processus qui utilisent de façon normale une connexion à internet, comme dans le cas de l'attaque sur RUAG, la détection est très difficile. En plus, l'attaquant avait pris soin de découpler les différentes phases de l'exécution des tâches, ce qui rendait tout le processus d'extraction plus sûr[13]. Ainsi, les données étaient collectées par des drones au sein du système, sans communication avec l'extérieur, puis des drones spécifiques de communication utilisaient internet pour l'exfiltration des données[14]. L'attaquant a aussi utilisé des outils disponibles sur internet, comme Mimikatz, afin d'obtenir des mots de passe[15].

Il est aussi possible que la RUAG ait elle-même durant les 3 phases négligé de procéder aux investissements nécessaires dans le domaine de la cybersécurité afin de protéger ses propres systèmes, ce qui aurait facilité la tâche de l'attaquant[16].

Leçons à retenir et recommandations

RUAG mentionne que au total près de 23 GB de données ont été extraites, tout en indiquant que certaines données ont été extraites plusieurs fois. Par contre, il a été impossible de définir si les données extraites avaient un caractère confidentiel et quelle était leur valeur[17]. D'autres sources mentionnent des attaques gravissimes, même si les dommages sont difficiles à estimer[18].

Il se pourrait aussi qu'en raison des interfaces informatiques entre RUAG et le DDPS, des données issues des annuaires de messagerie de la Confédération aient été touchés[19]. Le rapport mentionne que le rythme

BIO

Diplômé en politiques de sécurité, après avoir obtenu une licence en sciences politiques, le colonel Marc-André Ryter est actuellement chef d'état-major à la division des constructions militaires au sein de l'état-major des armées. Dans le cadre de ses fonctions, il suit et étudie les évolutions technologiques qui peuvent s'avérer pertinentes pour les Forces Armées et pour les différents champs d'opération, notamment dans le but d'adapter la doctrine militaire.

d'extraction a été très irrégulier, et que certains jours, près de 1 GB a été extrait, et que d'autres périodes, parfois assez longues, n'ont connus que très peu d'activités. En tout, la phase d'extraction principale a duré 4 mois, de septembre à décembre 2015[20].

Sur la base des expériences faites et des informations engrangées lors de travaux subséquents à l'attaque, RUAG

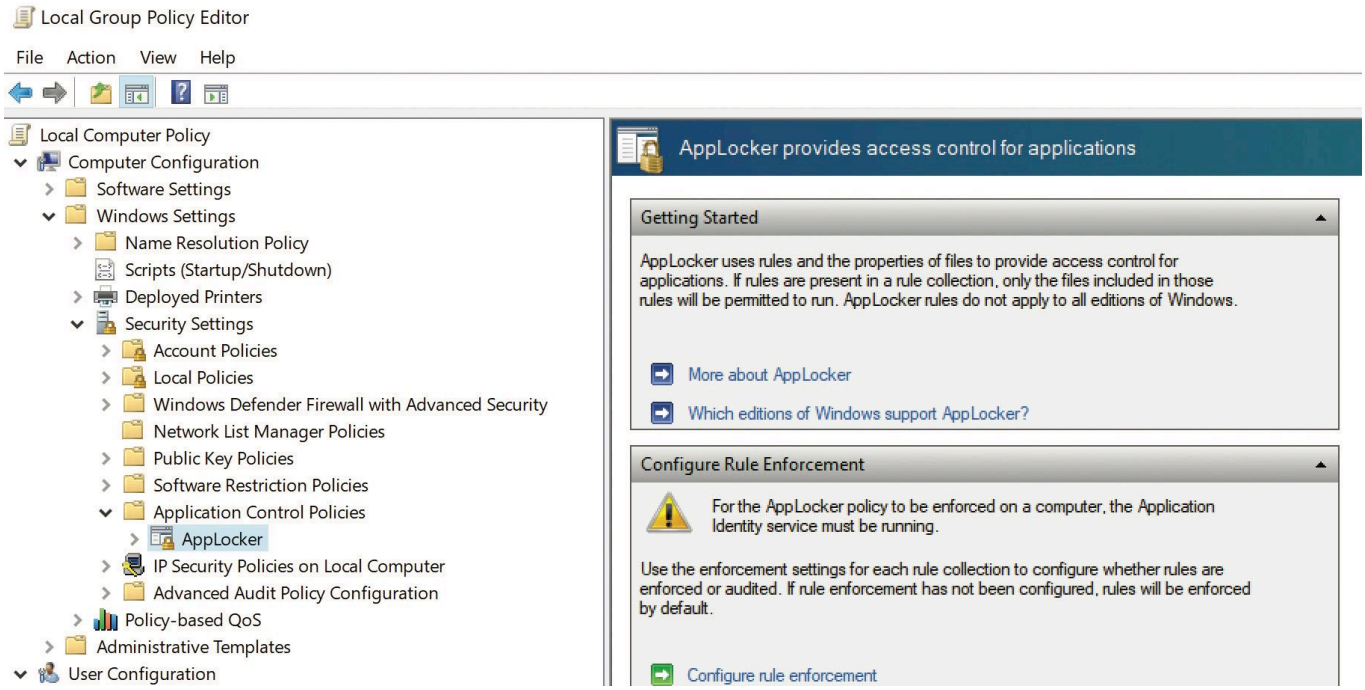
émet dans son rapport une série de recommandations afin de compliquer la tâche d'éventuels attaquants. Ces recommandations consistent en différentes contre-mesures qui devraient être mises en œuvre à différents niveaux. Nous nous limiterons ici à la mise en évidence de certaines recommandations qui nous semblent particulièrement importantes[21].

Au niveau du système, la mise en place de Applocker (Microsoft) est recommandée. Ceci permet de créer des règles qui limitent les applications autorisées pour les utilisateurs et par là même rendent l'installation de malwares plus difficile. De même, la limitation des privilèges des utilisateurs normaux constitue aussi un obstacle efficace. D'autres mesures concernant le système semblent évidentes, mais ne sont pas encore assez répandues. RUAG mentionne en particulier la nécessité de superviser les systèmes en permanence, de s'assurer de leur mise à jour régulière et d'éliminer toutes les applications inutiles qui élargissent la surface d'attaque possible.

Des mesures sont aussi possibles au niveau de l'annuaire actif (Active Directory). RUAG recommande de superviser les demandes qui parviennent à l'annuaire, en particulier afin d'identifier des demandes de grandes quantités d'information, ainsi que d'utiliser une identification à deux niveaux. En ce qui concerne les réseaux, il s'agit d'augmenter la résilience et les capacités de détection en créant un point de passage (choke point) qui permet une meilleure supervision de ce qui part en direction d'internet. La sauvegarde des fichiers journal du serveur devrait aussi être d'une durée minimale de deux ans et la gestion du système devrait s'effectuer à partir d'un réseau séparé du trafic des affaires courantes.

Ces quelques recommandations assez basiques, parfois même qualifiées de simples et peu coûteuses[22], ajoutées aux mesures plus techniques telles que recommandées, devraient permettre d'accroître massivement la sécurité contre les attaques cyber, même si elles sont techniquement élaborées et complexes.

Le rapport de RUAG sur cette attaque rappelle que le but n'est pas d'éviter toutes les attaques, mais bien de rendre celles-ci aussi difficiles que possible, respectivement de créer le plus d'obstacles possibles pour in fine dissuader



l'attaquant. Le point d'entrée doit être difficile à trouver et les attaques qui échouent doivent pouvoir être identifiées, permettant ainsi de gagner du temps et de développer de nouvelles défenses.

RUAG répète que le partage d'informations concernant de telles attaques, y compris à l'échelon international, est la meilleure des contre-mesures. Sans préciser les sources, RUAG mentionne que l'attaque qui l'a touché a précisément été découverte grâce au partage d'information. Selon la Aargauer Zeiutung, c'est le Service de Renseignement de la Confédération qui en décembre 2015 a prévenu la RUAG[23], celui-ci ayant lui-même été informé par un service de renseignement étranger[24].

D'une manière générale, les utilisateurs du cyberespace doivent être conscients de leurs responsabilités, maintenir leurs réseaux et données sûres et s'assurer que leurs serveurs ne peuvent pas être utilisés afin d'attaquer d'autres cibles. RUAG elle-même ne donne aucune indication sur la source de l'attaque dont elle a été victime. Cependant, la «Handelzeitung», qui cite le président de la DélCdG Alex Kuprecht, mentionne clairement la Russie comme attaquant dans ce cas[25]. Ces certitudes viennent du fait que l'origine du software, qui avait déjà été utilisé dans une attaque antérieure contre le Département des Affaires Etrangères, est connue, et qu'une attaque tellement sophistiquée ne peut venir que d'un acteur étatique[26].

Cette attaque a aussi eu des conséquences au sein de l'administration fédérale. Le Conseil fédéral avait en effet pris, dès le 23 mai 2016, 14 mesures à court et moyen-terme visant à éliminer le risque de vols de données[27]. Ces mesures ne peuvent cependant être décrites et commentées car elles n'ont pas été publiées. L'information divulguée mentionne cependant des mesures portant «essentiellement sur des procédures et des vérifications internes»[28] ainsi que des mesures organisationnelles entre RUAG et la Confédération, comme le désenchevêtrèrent des réseaux[29].

De même, une Task Force spécifique, dénommée RHINO, a été instituée «en vue de prendre les mesures d'urgences nécessaires et d'évaluer les dommages causés»[30]. De manière générale, il est intéressant de constater que cette attaque a servi de sonnerie d'alarme. Elle a démontré l'importance de la cybersécurité et la nécessité absolue et urgente pour l'administration fédérale et les entreprises de la Confédération d'améliorer la protection de leurs systèmes. ■

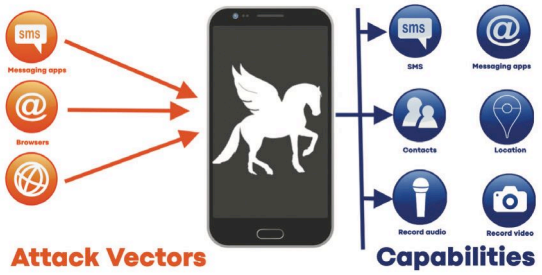
---

1 Selon le Rapport de la Commission de gestion du Conseil national: «Bilan de la gestion de la cyberattaque menée contre RUAG» du 8 mai 2018, disponible sous https://www.parlement.ch, consulté le 27.05.2022.
2 APT Case RUAG: Technical Report, by MELANIGovCert, 23.05.2016, disponible sous https://www.govcert.ch/whitepapers/apt-case-ruag-technical-report-govcert-ch/.
3 APT Case RUAG: Technical Report, p. 2.
4 APT Case RUAG: Technical Report, p.1.
5 Voir sous https://www.01net.com/actualites/les-malwares-les-plus-sophistiques-au-monde-sont-ceux-du-groupe-turla-2052740.html, consulté le 24.05.2022.
6 Rapport de la Commission de gestion du Conseil national: «Bilan de la gestion de la cyberattaque menée contre RUAG» du 8 mai 2018, disponible sous https://www.parlement.ch, consulté le 27.05.2022, p. 6.
7 APT Case RUAG: Technical Report, p. 21.
8 APT Case RUAG: Technical Report, p. 8.
9 https://www.handelszeitung.ch/politik/ruag-hackerangriff-es-war-russland-1071536, consulté le 25.05.2022
10 APT Case RUAG: Technical Report, p. 13.
11 APT Case RUAG: Technical Report, p. 15.
12 APT Case RUAG: Technical Report, p. 25.
13 APT Case RUAG: Technical Report, p. 15.
14 APT Case RUAG: Technical Report, p. 23.
15 APT Case RUAG: Technical Report, p. 21.
16 https://www.aargauerzeitung.ch/schweiz/verteidigung-wie-die-ruag-warnungen-ihrer-experten-ignorierte-und-die-cybersicherheit-verschlampte-ld.2093294, consulté le 25.05.2022.
17 APT Case RUAG: Technical Report, p. 25.
18 https://www.handelszeitung.ch/politik/ruag-hackerangriff-es-war-russland-1071536,consulté le 25.05.2022.
19 https://www.letemps.ch/monde/cyberattaque-ruag-reveille-suisse, consulté le 27.05.2022.
20 APT Case RUAG: Technical Report, p. 25.
21 Toutes les mesures sont décrites en détails dans le rapport, APT Case RUAG: Technical Report, pp. 27-29.
22 https://www.letemps.ch/monde/cyberattaque-ruag-reveille-suisse,consulté le 27.05.2022.
23 https://www.aargauerzeitung.ch/schweiz/verteidigung-wie-die-ruag-warnungen-ihrer-experten-ignorierte-und-die-cybersicherheit-verschlampte-ld.2093294, consulté le 25.05.2022.
24 https://www.letemps.ch/monde/cyberattaque-ruag-reveille-suisse, consulté le 27.05.2022.
25 https://www.handelszeitung.ch/politik/ruag-hackerangriff-es-war-russland-1071536, consulté le 25.05.2022.
26 https://www.swisscybersecurity.net/news/2018-08-27/ruag-hacker-kommen-davon, consulté le 25.05.2022.
27 https://www.handelszeitung.ch/politik/ruag-hackerangriff-es-war-russland-1071536,consulté le 25.05.2022.
28 Rapport de la Commission de gestion du Conseil national: «Bilan de la gestion de la cyberattaque menée contre RUAG» du 8 mai 2018, disponible sous https://www.parlement.ch, consulté le 27.05.2022, p. 7.
29 Rapport de la Commission de gestion du Conseil national: «Bilan de la gestion de la cyberattaque menée contre RUAG» du 8 mai 2018, disponible sous https://www.parlement.ch, consulté le 27.05.2022, p. 11.
30 Rapport de la Commission de gestion du Conseil national: «Bilan de la gestion de la cyberattaque menée contre RUAG» du 8 mai 2018, disponible sous https://www.parlement.ch, consulté le 27.05.2022, p. 7.

«Pegasus», le logiciel-espion pour smartphones. Comment fonctionne-t-il et comment s'en protéger ?

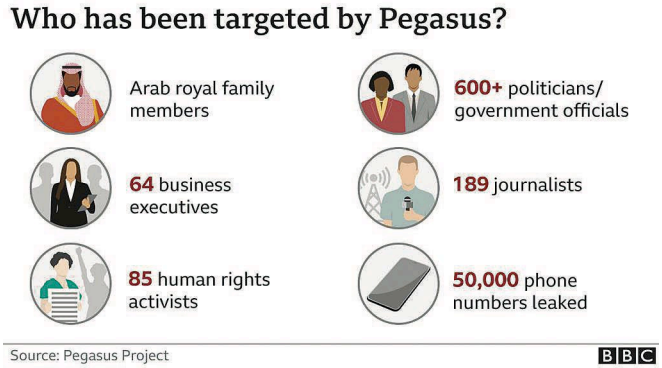
Auteur : Costin G. Raiu

L'un des plus importants événements du monde «cyber», en 2021, est constitué par les résultats d'une enquête menée par The Guardian et 16 autres organisations médiatiques, dont les conclusions estiment que plus de 30 000 militants des droits de l'homme, journalistes et avocats à travers le monde pourraient avoir été ciblés à l'aide du logiciel espion Pegasus (Pegasus est un soi-disant «*logiciel de surveillance légale*» développé par la société israélienne NSO).



Le rapport publié en juillet 2021, intitulé «Pegasus Project» (1), affirme que le logiciel malveillant a été déployé à grande échelle par le biais de divers exploits, dont plusieurs zero-days ciblant les systèmes iOS. Sur la base de l'analyse forensique de nombreux appareils mobiles, le laboratoire de sécurité d'Amnesty International a en fait constaté que le logiciel était utilisé à plusieurs reprises de manière abusive à des fins de surveillance.

La liste des personnes visées comprend 14 dirigeants mondiaux et de très nombreux militants, défenseurs des droits de l'homme, dissidents et figures de l'opposition. Plus tard, au courant du même mois qui a vu la publication du Guardian et du rapport d'Amnesty, des représentants du gouvernement israélien ont visité les bureaux de NSO dans le cadre d'une enquête sur ces allégations (2).



En octobre 2021, la Cour suprême de l'Inde a chargé un comité technique d'enquêter sur l'utilisation de Pegasus pour espionner ses concitoyens (3). En novembre, Apple a annoncé qu'elle engageait une action en justice contre NSO Group pour avoir développé un logiciel qui cible ses utilisateurs avec des «*logiciels malveillants et des logiciels espions*»(4).

Enfin, en décembre 2021, Reuters a publié que les téléphones du département d'État américain, alerté par Apple, ont été piratés avec le logiciel malveillant Pegasus de NSO (5).

En 2022, les divulgations se sont poursuivies - le 2 mai 2022, le gouvernement espagnol a annoncé que le premier ministre, Pedro Sánchez,

et la ministre de la défense, Margarita Robles, étaient tous deux surveillés par Pegasus (6). À la suite de ces révélations, le gouvernement espagnol a immédiatement limogé le chef des services secrets du pays, Paz Esteban.

La détection des traces d'infection de Pegasus et d'autres logiciels malveillants mobiles avancés est très délicate et est rendue encore plus compliquée par les fonctions de sécurité des systèmes d'exploitation modernes tels qu'iOS et Android.

D'après nos observations, leur analyse est rendue encore plus difficile car il s'agit du déploiement de logiciels malveillants non persistants, qui ne laissent pratiquement aucune trace après un redémarrage de l'appareil infecté.

Étant donné que de nombreux outils de criminalistique nécessitent un *jailbreak* (intrusion totale, ici consentie) de l'appareil, le logiciel malveillant est supprimé de la mémoire lors du redémarrage, nécessaire à cette opération. Heureusement, à ce jour, plusieurs méthodes peuvent être utilisées pour la détection de Pegasus et d'autres logiciels malveillants mobiles. Par exemple, le MVT *(Mobile Verification Toolkit)* d'Amnesty International est gratuit (7), en open source et permet aux techniciens et aux enquêteurs d'inspecter les téléphones mobiles à la recherche de signes d'infection. MVT est renforcé par une liste d'IoC *(indicateurs de compromission)* constituée suite à des cas très médiatisés de violations des droits de l'homme, elle aussi mise à disposition par Amnesty International.

En ces temps incertains, de nombreux utilisateurs inquiets dans le monde entier se demandent comment protéger leurs appareils mobiles de Pegasus et d'autres outils et logiciels malveillants similaires.

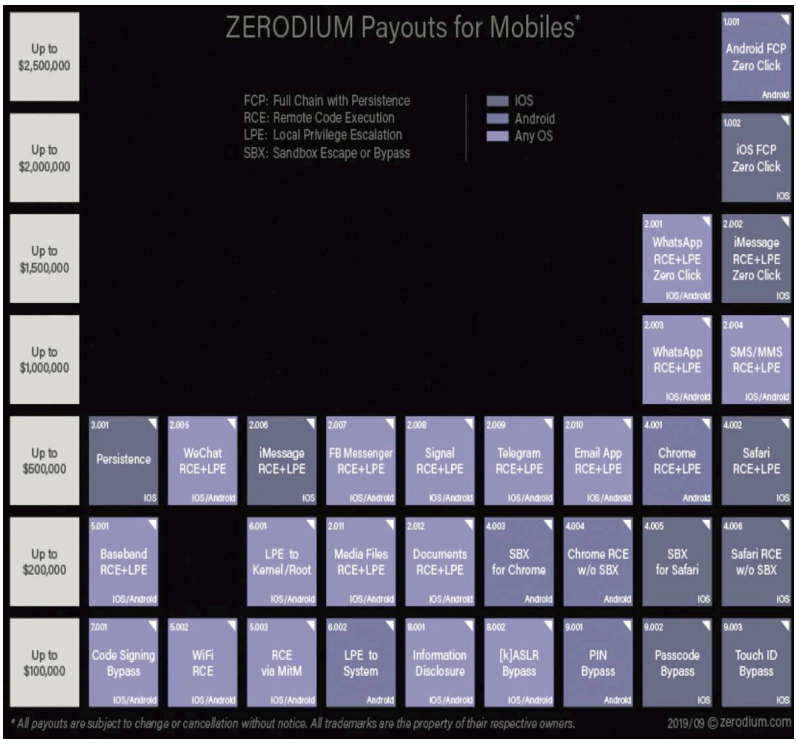
De même, les gouvernements tentent d'évaluer leurs faiblesses et de mettre au point des stratégies pour identifier de telles failles, ou du moins pour empêcher qu'elles ne se produisent à l'avenir. Dans ce texte, nous nous proposons d'examiner les dernières techniques d'attaque utilisées pour déployer des logiciels malveillants sur les téléphones portables ainsi que la manière de s'en défendre, tout en tenant compte qu'une liste de techniques de défense ne saurait être exhaustive. De plus, comme les attaquants changent leur modus operandi, les techniques de défense existantes doivent également être très fréquemment adaptées.

Comment rester à l'abri des logiciels malveillants mobiles les plus sophistiqués ?

Tout d'abord, il faut dire que Pegasus est une boîte à outils vendue à des prix relativement élevés. Le coût d'un déploiement complet peut facilement atteindre des millions de dollars américains. De même, d'autres logiciels malveillants mobiles peuvent être déployés par le biais d'exploits 0-clic 0-day. Ceux-ci sont extrêmement coûteux - à titre d'exemple, Zerodium, une société de courtage en «*exploits*», demande jusqu'à 2,5 millions USD pour une chaîne d'infection Android 0-click avec degré de persistance avancé:

BIO

Directeur du Global Research and Analysis Team (GReAT) de Kaspersky, Costin est spécialisé dans l'analyse des menaces persistantes avancées, des exploits de type «zero-day» et des logiciels malveillants complexes. Il dirige l'équipe de recherche et d'analyse mondiale (GReAT), connue dans le monde entier, qui a étudié les rouages de nombreuses attaques très médiatisées, notamment RedOctober, WannaCry, ShadowPad et ShadowHammer et Moonlight Maze. Son travail actuel est axé sur le développement de technologies et de systèmes de similarité de code pour enrichir le renseignement sur les menaces. Costin a plus de 28 ans d'expérience dans les technologies antivirus et la recherche en sécurité. Il est membre du comité consultatif technique du Virus Bulletin, membre de la Computer AntiVirus Researchers' Organization (CARO) et reporter pour la Wildlist Organization International. Avant de rejoindre Kaspersky Lab, Costin a travaillé pour GeCad en tant que chercheur en chef et en tant qu'expert en sécurité des données au sein du groupe de développeurs d'antivirus RAV. Costin est ceinture bleue de Taekwondo. Parmi ses loisirs figurent les échecs, la photographie et la littérature de science-fiction.



D'emblée, on peut en tirer une conclusion importante: le cyber-espionnage sophistiqué est une entreprise qui nécessite des ressources considérables. Lorsqu'un commanditaire peut se permettre de dépenser des millions, voire des dizaines de millions ou des centaines de millions de dollars américains pour se procurer des programmes offensifs, il est très peu probable qu'une cible puisse éviter d'être infectée. En pratique, plus prosaïquement, la question n'est pas de savoir *«si vous pouvez être infecté»*, mais quand et comment : ce n'est, en fait, qu'une question de temps et avant que vous ne soyez infecté, grâce aux ressources correspondantes à vos outils et à leur niveau de sécurité.

La bonne nouvelle, c'est que le développement d'exploits et la cyber-guerre offensive sont souvent plus un art qu'une science exacte. Les exploits doivent être adaptés à des versions de systèmes d'exploitation et à des matériels spécifiques et peuvent être facilement contrecarrés par de nouveaux systèmes d'exploitation, de nouvelles techniques d'atténuation ou même de petites choses comme des événements aléatoires.

Dans cette optique, l'infection et le ciblage sont également une question de coût et de difficulté pour les attaquants. Bien que nous ne soyons pas toujours en mesure d'empêcher l'exploitation et l'infection d'un appareil mobile, nous pouvons essayer de rendre les choses aussi difficiles que possible pour les attaquants.

Comment s'y prendre en pratique ? Voici une liste de contrôle simple :

1. Sur iOS :

a) Redémarrez quotidiennement.

Selon les recherches d'Amnesty et de CitizenLab, la chaîne d'infection de Pegasus repose souvent sur des 0-clic journaliers sans persistance, de sorte qu'un redémarrage régulier permet de nettoyer l'appareil.

Si l'appareil est redémarré quotidiennement, les attaquants devront le réinfecter encore et encore.
À terme, cela augmente les chances de détection ; un crash peut se produire ou de simples apps peuvent être installées pour révéler une infection de nature furtive.

En fait, ce n'est pas seulement de la théorie, c'est de la pratique - nous avons analysé un cas dans lequel un appareil mobile a été ciblé par un exploit 0-clic (probablement FORCEDENTRY). Le propriétaire de l'appareil a redémarré son appareil régulièrement et l'a fait dans les 24 heures qui ont suivi l'attaque. Les attaquants ont essayé de le cibler à plusieurs reprises, mais ont fini par abandonner après s'être fait botter le train à plusieurs reprises lors des redémarrages.

b) Désactiver iMessage.

iMessage est intégré à iOS et est activé par défaut, ce qui en fait un vecteur d'exploitation intéressant. Parce qu'il est activé par défaut, il s'agit d'un mécanisme de livraison de premier ordre pour les chaînes 0-clic.

Pendant de nombreuses années, les exploits iMessage étaient très demandés, avec des gains importants pour les sociétés de courtage en «exploits». *«Au cours des derniers mois, nous avons observé une augmentation du nombre d'exploits iOS, principalement des chaînes Safari et iMessage, développés et vendus par des hackers du monde entier. Le marché des zero-day est tellement inondé d'exploits iOS que nous avons récemment commencé à refuser certains (d'entre eux)»*, a écrit Chaouki Bekrar, fondateur de Zerodium, en 2019 à WIRED (8).

Nous sommes conscients que cela peut être très difficile pour certains (plus tard), mais si Pegasus et d'autres malwares mobiles APT haut de gamme font partie des modèles de menace qui vous concernent, c'est un compromis qui vaut la peine de prendre.

c) Désactiver Facetime.

Même chose que ci-dessus.

d) Maintenez l'appareil mobile à jour ; installez les derniers correctifs iOS dès qu'ils sont disponibles.

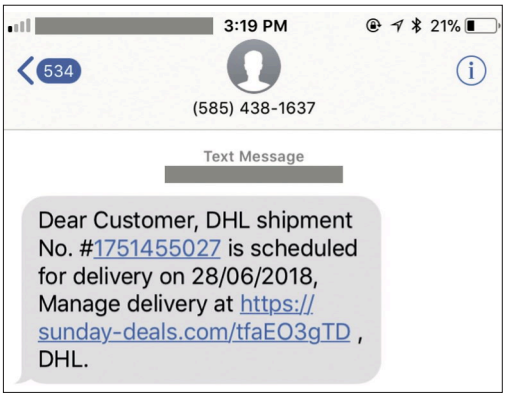
Tout le monde ne peut pas se permettre d'utiliser des «0-day». En fait, la plupart des kits d'exploitation iOS que nous connaissons visent des vulnérabilités déjà corrigées. Néanmoins, de nombreuses personnes utilisent des téléphones plus anciens et reportent les mises à jour pour diverses raisons.

Si vous voulez avoir une longueur d'avance sur (certains) hackers dits «state-sponsored», mettez à jour dès que possible votre système d'opération et apprenez à ne pas avoir besoin d'émojis pour installer les correctifs (9).

e) Ne cliquez jamais sur les liens reçus dans les SMS.

C'est un conseil simple mais efficace. Tous les clients de Pegasus ne peuvent pas se permettre d'acheter des chaînes 0-day à plusieurs millions d'euros, ils s'appuient donc sur des exploits 1-clic.

Ceux-ci arrivent sous la forme d'un message, parfois par SMS, mais peuvent aussi être via d'autres messageries ou même par e-mail. Si vous recevez un SMS intéressant (ou un message par tout autre service de chat) avec un lien, ouvrez-le sur un ordinateur de bureau, de préférence en utilisant TOR Browser, ou en utilisant un OS non persistant sécurisé comme Tails.



SMS contenant un lien malveillant utilisé pour cibler un activiste politique - crédit : Citizenlab

```
detect_os()

return {
       mobile: (typeof window.orientation !== "undefined") || (navigator.userAgent.indexOf('IEMobile') !== -1),
       webkit: parseFloat(/AppleWebKit\/([\d.]+)/.exec(navigator.userAgent)[1]) || 0,
       safari: window.navigator.userAgent.indexOf('Safari') > -1,
       version: function()
       {
              var match = (navigator.appVersion).match(/OS (\d+)_(\d+)_?(\d+)?/);
       if(match) {
              var version = [
                  parseInt(match[1], 10),
                  parseInt(match[2], 10),
                  parseInt(match[3] || 0, 10)
                      ];
                      return parseFloat(version[0]+'.'+version[1]+version[2]);
           } else {
               return "unknown";
```

Le kit d'exploitation LightRiver vérifie la présence de «Safari» dans la chaîne de l'agent utilisateur.

f) Naviguez sur Internet avec un navigateur non-natif, tel que Firefox Focus, au lieu de Safari ou Chrome.

Bien que tous les navigateurs sur iOS utilisent à peu près le même moteur de recherche, Webkit, certains exploits ne fonctionnent pas bien (voir le cas APT LightRighter / TwoSailJunk) (10)) sur certains navigateurs alternatifs :

Chaînes d'agent utilisateur sur iOS provenant de Chrome (gauche) / Firefox (droite) :

Chaîne d'agent utilisateur de Chrome sur iOS	La chaîne d'agent utilisateur de Firefox Focus sur iOS
Mozilla/5.0 (iPhone ; CPU iPhone OS 15_1 comme Mac OS X) AppleWebKit/605.1.15 (KHTML, comme Gecko) CriOS/96.0.4664.53 Mobile/15E148 Safari/604.1	Mozilla/5.0 (iPhone ; CPU iPhone OS 15_1 comme Mac OS X) AppleWebKit/605.1.15 (KHTML, comme Gecko) FxiOS/39 Mobile/15E148 Version/15.0

g) Utilisez toujours un VPN qui masque votre adresse IP et votre trafic de données.

Certains exploits sont transmis par des attaques MitM via votre opérateur GSM, lors de la navigation sur des sites HTTP ou par un détournement de DNS. En utilisant un VPN pour masquer votre adresse IP et votre trafic de données, il est difficile pour votre opérateur GSM de vous cibler directement sur Internet.

Cela complique également le processus de ciblage si les attaquants ont le contrôle de votre flux de données, par exemple en cas d'itinérance (roaming).

Sachez que tous les VPN ne sont pas identiques et que tous les VPN ne sont pas bons à utiliser. Sans privilégier un VPN en particulier, voici quelques éléments à prendre en compte lors de l'achat d'un abonnement VPN :L'achat signifie exactement cela - pas de VPN «gratuits».

- Recherchez des services qui acceptent les paiements en crypto-monnaies.
- Recherchez des services qui ne vous demandent pas de fournir des informations d'enregistrement.
- Essayez d'éviter les applications VPN - utilisez plutôt des outils open source tels que WireGuard et OpenVPN et des profils VPN.
- Évitez les nouveaux services VPN et recherchez des services bien connus qui existent depuis un certain temps.

h) Installez une application de sécurité qui vérifie et prévient si votre appareil est "jailbreaké".

Frustrés de se faire botter l'arrière-train encore et encore, les attaquants finiront par déployer un mécanisme de persistance et par «jailbreaker» votre appareil (accéder illégalement à tout son contenu). C'est là que les chances de surprendre les malfaiteurs sont décuplées et que nous pouvons tirer parti du fait que l'appareil a été jailbreaké.

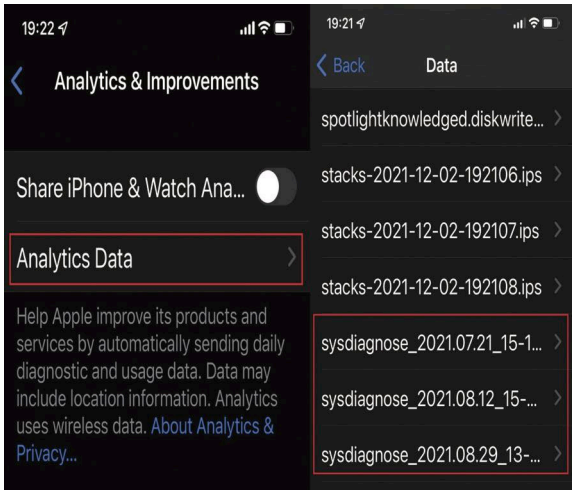
i) Faites des sauvegardes d'iTunes une fois par mois.

Cela permet de diagnostiquer et de trouver des infections plus tard, grâce à l'utilisation du merveilleux paquet MVT d'Amnesty.

j) Déclenchez souvent des sysdiags et enregistrez-les dans des sauvegardes externes.

Les outils forensiques peuvent vous aider à déterminer ultérieurement si vous avez été ciblé. Le déclenchement d'un *sysdiag* (application permettant un diagnostic complet du système et des contenus) dépend du modèle de téléphone.

Par exemple, sur certains iPhone, il suffit d'appuyer



simultanément sur les touches VOL Up + Down + Power. Il se peut que vous deviez jouer avec ces touches plusieurs fois, jusqu'à ce que le téléphone émette un signal sonore.

Une fois le *sysdiag* créé, il apparaîtra dans les diagnostics de la section «données analytiques» :

2. Sur Android

a) Redémarrez quotidiennement.

La persistance sur les dernières versions d'Android est difficile, de nombreux APT et vendeurs d'exploits évitent toute persistance !

b) Maintenir le téléphone à jour ; installer les derniers correctifs.

c) Ne cliquez jamais sur les liens reçus dans les SMS.

d) Naviguez sur l'internet avec un autre navigateur tel que Firefox Focus au lieu de Chrome.

e) Utilisez toujours un VPN qui masque votre adresse IT et votre trafic de données.

Certains exploits sont diffusés par des attaques MitM d'opérateurs GSM, lors de la navigation sur des sites HTTP ou par détournement de DNS.

f) Installez une suite de sécurité qui recherche les logiciels malveillants et vérifie et prévient si l'appareil est «jailbreaké».

À un niveau plus sophistiqué, vérifiez toujours le trafic de votre réseau en utilisant des IOC en direct. Une bonne configuration pourrait inclure un VPN Wireguard toujours actif vers un serveur sous votre contrôle, qui utilise *pihole* pour filtrer les mauvais éléments et enregistre tout le trafic pour une inspection ultérieure (11).

Un jeu à résultat nul ?

Ryan Naraine, célèbre commentateur en matière de sécurité, a déclaré : *«iMessage et FaceTime - sont les raisons pour lesquelles les gens utilisent des iPhones !»* Et il a raison : iMessage et FaceTime sont deux des meilleures additifs qu'Apple ait ajoutées à son écosystème.

Heureusement, Apple a considérablement amélioré la *sandbox* de sécurité protégeant iMessage avec BlastDoor dans iOS 14 (12). Néanmoins, l'exploit FORCEDENTRY utilisé par NSO pour livrer Pegasus a contourné BlastDoor et, bien sûr, aucune fonction de sécurité n'est jamais à l'abri d'un piratage à 100% (13).

Alors, quel est le meilleur des deux mondes, vous demanderez-vous ?

Certaines personnes, dont je fais partie, possèdent plusieurs téléphones - un où iMessage est désactivé, et un iPhone *«pot de miel»* où iMessage est activé. Les deux sont bien sûr associés au même identifiant Apple et au même numéro de téléphone. Si quelqu'un décide de me cibler de cette manière, il y a de fortes chances pour qu'il aboutisse dans le téléphone *«pot de miel»*.

Ne vous taisez pas si vous êtes surveillé ...

Bien sûr, on peut suivre ces recommandations à la lettre et être quand même infecté. Malheureusement, c'est la réalité dans laquelle nous vivons aujourd'hui. Lorsque quelqu'un nous dit qu'il a été ciblé par un logiciel espion mobile, nous lui répondons de réfléchir à ces questions :

- Qui vous a ciblé et pourquoi ?
- Essayez de comprendre ce qui a attiré l'attention des gros bonnets sur vous. Pouvez-vous éviter cela à l'avenir en adoptant un comportement plus discret ?
- Pouvez-vous en parler ?

Ce qui a fini par faire tomber de nombreuses sociétés de surveillance, par la mauvaise publicité que ce genre de cas leur a crée, comme lorsque de nombreux reporters et journalistes relatent les abus et exposent les mensonges et les méfaits générés par un acteur de ce domaine.

Si vous avez été pris pour cible, essayez de trouver un journaliste et racontez-lui votre histoire.

Changez d'appareil

Si vous étiez sur iOS, essayez de passer à Android pendant un certain temps. Si vous étiez sur Android, passez à iOS. Cela peut désorienter les attaquants pendant un certain temps ; par exemple, certains acteurs de la menace sont connus pour avoir acheté des systèmes d'exploitation qui ne fonctionnent que sur une certaine marque de téléphone et d'OS.

Achetez un appareil secondaire, de préférence sous GrapheneOS, pour des communications sécurisées. Utilisez-le avec une carte prépayée ou connectez-vous uniquement par Wifi et TOR en mode avion.

Évitez les messageries où vous devez fournir votre numéro de téléphone à vos contacts. Une fois qu'un attaquant a votre numéro de téléphone, il peut facilement vous cibler à travers de nombreuses messageries différentes - iMessage, WhatsApp, Signal, Telegram, car elles sont toutes liées à votre numéro de téléphone.

Un nouveau choix intéressant est Session, qui achemine automatiquement vos messages via un réseau de type Onion et ne dépend pas des numéros de téléphone.

Essayez d'entrer en contact avec un chercheur en sécurité dans votre région et discutez constamment des meilleures pratiques à suivre. Partagez avec eux les données, les messages suspects ou les logins dès que vous pensez que quelque chose est bizarre.

La sécurité n'est jamais une solution instantanée unique qui offre une garantie à 100 % ; considérez-la comme un cours d'eau, dans lequel vous devez adapter votre navigation en fonction de la vitesse, des courants et des obstacles.

A la fin de ceci, j'aimerais vous quitter avec une pensée. Si vous êtes pris pour cible par des acteurs servant des États-nations, cela signifie que vous êtes important.

Souvenez-vous : c'est bien d'être important, mais c'est plus important d'être gentil.

Seuls, nous sommes faibles, ensemble, nous sommes forts.

Le monde est peut-être brisé, mais je crois que nous vivons à un moment où nous pouvons encore changer les choses.

Selon un rapport du Comité pour la protection des journalistes (CPJ), 293 journalistes ont été emprisonnés en 2021, le chiffre le plus élevé jamais enregistré par le CPJ depuis qu'il a commencé à le recenser, en 1992 (14).

C'est à nous de façonner ce à quoi le monde ressemblera pour nous dans 10 ans, pour nos enfants et les enfants de nos enfants. ■

(1) https://www.amnesty.org/en/latest/news/2021/07/the-pegasus-project/
(2) https://www.theguardian.com/news/2021/jul/29/israeli-authorities-inspect-nso-group-offices-after-pegasus-revelations
(3) https://www.theregister.com/2021/10/29/india_nso_pegasus_probe/
(4) https://www.theguardian.com/technology/2021/nov/23/apple-sues-israeli-cyber-firm-nso-group
(5) https://www.reuters.com/technology/exclusive-us-state-department-phones-hacked-with-israeli-company-spyware-sources-2021-12-03/
(6) https://www.theguardian.com/world/2022/may/02/spain-prime-minister-pedro-sanchez-phone-pegasus-spyware
(7) https://github.com/mvt-project/mvt
(8) https://www.wired.com/story/android-zero-day-more-than-ios-zerodium/
(9) https://twitter.com/ryanaraine/status/1324445133668974592
(10) https://securelist.com/ios-exploit-chain-deploys-lightspy-malware/96407/
(11) https://pi-hole.net
(12) https://googleprojectzero.blogspot.com/2021/01/a-look-at-imessage-in-ios-14.html
(13) https://citizenlab.ca/2021/09/forcedentry-nso-group-imessage-zero-click-exploit-captured-in-the-wild/
(14) https://edition.cnn.com/2021/12/09/media/journalists-imprisoned-cpj-census/index.html

Vous, le peuple, {vous} avez le pouvoir : le pouvoir de créer les machines, le pouvoir de créer le bonheur. Vous, le peuple, en avez le pouvoir : le pouvoir de rendre la vie belle et libre, le pouvoir de faire de cette vie une merveilleuse aventure.

Alors au nom même de la Démocratie, utilisons ce pouvoir. Il faut nous unir, il faut nous battre pour un monde nouveau, décent et humain qui donnera à chacun l'occasion de travailler, qui apportera un avenir à la jeunesse et à la vieillesse la sécurité.

Ces brutes vous ont promis toutes ces choses pour que vous leur donniez le pouvoir - ils mentent. Ils ne tiennent pas leurs promesses - jamais ils ne le feront. Les dictateurs s'affranchissent en prenant le pouvoir mais réduisent en esclavage le peuple.

Alors, battons-nous pour accomplir cette promesse ! Il faut nous battre pour libérer le monde, pour abolir les frontières et les barrières raciales, pour en finir avec l'avidité, la haine et l'intolérance.

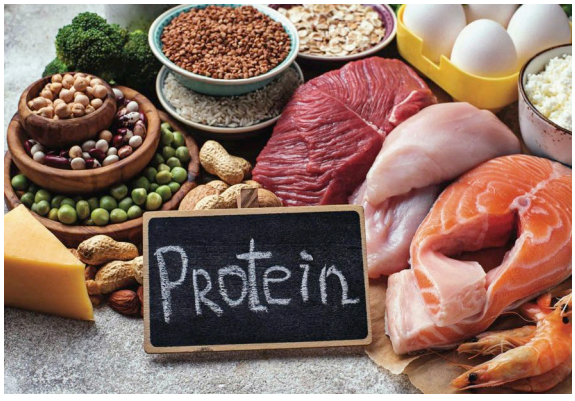
Il faut nous battre pour construire un monde de raison, un monde où la science et le progrès mèneront vers le bonheur de tous. Soldats, au nom de la Démocratie, unissons-nous !

Discours final du film «Dictateur» (Charlie Chaplin)

2020-2022, vague de cyber-attaques contre les coopératives et industries agricoles : le début d'un séisme mondial autour de la protéine végétale ?

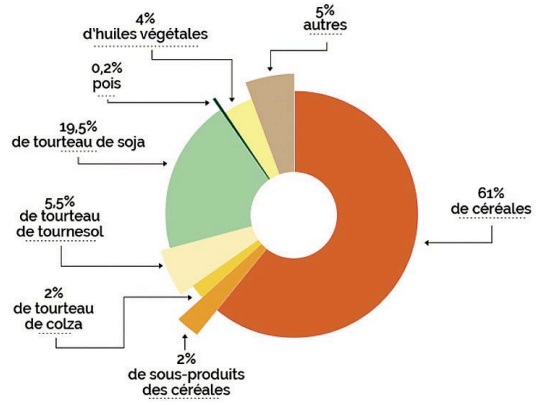
Auteur : **Stéphane Mortier**

La période 2020-2022 est marquée par de nombreuses cyberattaques visant les coopératives et industries agricoles, partout dans le monde. Au-delà de l'attaque elle-même, souvent par ransomware, que peuvent chercher les attaquants ? Y aurait-il une volonté de déstructuration de filières agricoles ? Dans l'affirmative, avec quels objectifs *in fine* ?



La base de l'alimentation humaine repose sur les protéines végétales, ce qui en fait une matière particulièrement stratégique. L'être humain consomme en moyenne 2/3 de protéines animales et 1/3 de protéines végétales. Or les protéines végétales composent l'essentiel de l'alimentation des animaux produisant ainsi les protéines animales.

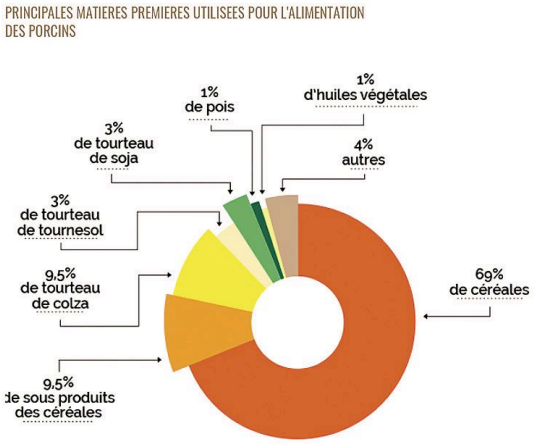
PRINCIPALES MATIERES PREMIERES UTILISEES POUR L'ALIMENTATION DES VOLAILLES



L'être humain est donc totalement dépendant des protéines végétales ! Dans un contexte de croissance de la population mondiale, qui maîtrisera la production de protéines végétales, maîtrisera le monde !

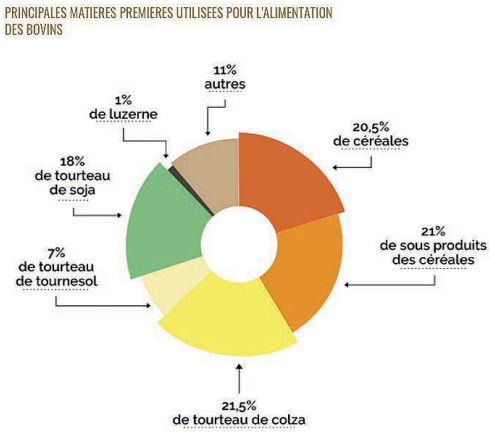
Face à ce constat, la France, depuis fin 2020, a mis en place une stratégie nationale en faveur du développement des protéines végétales. Elle ne produit actuellement que 50 % de ses besoins et vise par conséquent une

augmentation (40%) dans les trois prochaines années. Les objectifs sont les suivants :



- réduire la dépendance aux importations et sécuriser les approvisionnements ;
- améliorer la situation économique des éleveurs ;
- répondre aux enjeux climatiques et environnementaux ;
- développer une offre de produits locaux.

Intérêt stratégique, stratégie nationale,...de quoi attiser les velléités de prédation. C'est ici qu'à la fois l'espionnage et le cyber entrent en jeu.



L'espionnage, en l'occurrence l'espionnage économique en ce qui nous concerne, est le fait de rechercher, dans un but économique, de manière illégitime des informations techniques ou de toute nature lorsque ces informations présentent une valeur, même potentielle, dont la divulgation serait de nature à nuire aux intérêts essentiels de la victime[1]. Qu'en est-il lorsque l'auteur, pour obtenir un avantage stratégique ou concurrentiel peut, en lieu et place de s'approprier l'information recherchée, se contenter de la détruire ou de la rendre inaccessible ? Si l'effet final recherché est atteint (nuire à la cible et amoindrir sa compétitivité sur un marché donné), par extension, cela relèverait alors d'un acte d'espionnage. En effet, c'est bien l'information qui est visée et non les infrastructures. Au-delà, si l'action de nuire vient d'une puissance étatique, il pourrait s'agir d'un acte de guerre économique.

Quant au cyberespionnage, il s'agit, comme indiqué dans un document de l'ENISA en 2020[2], de l'utilisation des réseaux informatiques pour obtenir l'accès illicite à des informations confidentielles, généralement détenues par un gouvernement ou une autre organisation. Les cyberattaques menées par des groupes de menaces ciblées avancées (APT - Advanced Persistant Threat) indiquent que les attaques financières sont souvent motivées par l'espionnage. Mais qu'en est-il des attaques par ransomware ? Ces dernières rendent les informations de la victime indisponibles, ce qui implique des difficultés dans le fonctionnement de la structure visée voir l'empêchement total de fonctionner. La notion de «nuisance» est donc avérée. De plus, certains groupes cybercriminels utilisant des ransomware sont également connus pour des vols de données.

Par exemple, le groupe Lockbit connu pour mener des attaques au ransomware mais qui a revendiqué à plusieurs reprises des vols de données (notamment lors d'une attaque contre THALES et contre le Ministère français de la Justice). Espionnage (recherche d'informations dans le but de nuire) et fragilisation (empêchement de fonctionner, blocage de l'activité) par accès et/ou blocage des informations d'une entreprise font donc bon ménage.

Revenons aux cyberattaques qui ont émaillé les coopératives et industries agricoles en 2020-2021. La plupart sont des attaques de type ransomware et touchent tous les secteurs agroalimentaires. Le tableau ci-dessous donne un aperçu des coopératives et industries les plus impactées sur la période considérée. A l'exception de JBS Foods (Brésil), toutes sont des entreprises dont le siège social se situe dans des États occidentaux. Toutefois, les sites de JBS Foods impactés par l'attaque de mai 2021 se situent essentiellement dans des démocraties occidentales. Est-ce une coïncidence ? Il semblerait que l'origine géographique des attaques soit concentrée en Russie et en Ukraine. En sachant qu'il est extrêmement complexe d'attribuer une origine géographique certaine à une cyberattaque, il faut prendre ce constat avec un maximum de circonspection.

Entreprise	Nationalité	Activité	Type d'attaque	Origine supposée de l'attaque	Date
Lion	Australie/Nouvelle-Zélande	Boissons/Lait	Ransomware	Chine (?)	2020/06
Campari Group	Italie	Boissons	Ransomware	Ukraine	2020/11
Cérésia	France	Semences/Viticulture/ Alimentation animale	Ransomware	Russie	2020/11
Sollio	Canada	Intrants agricoles/ Céréales/Viande	Ransomware	Ukraine	2020/11
Lactalis	France	Produits laitiers	Intrusion	?	2021/03
Molson Coors	USA/Canada/Grande-Bretagne	Boissons/Bière	Ransomware	?	2021/03
JBS Foods	Brésil/Australie/USA/ Canada	Viande	Ransomware	Russie	2021/05
Cristal Valley	USA	Céréales/Semences	Ransomware	Europe de l'Est(?)	2021/06
La Martiniquaise-Bardinet	France	Vins et spiritueux	Vol de données	Russie	2021/09
New cooperative	USA	Semences	Ransomware	Russie	2021/09
Avril	France	Transformation animale/ Agroalimentaire	Ransomware	?	2021/11
Jean Floc'h	France	Viande/Agroalimentaire	Ransomware	Russie	2021/11
Eureden	France	Alimentation animale, viande, œuf, légumes	Ransomware	?	2022/03
AGCO	USA/Allemagne/Chine/ France/Finlande	Matériels agricoles	Ransomware	Russie (?)	2022/05

Parmi ces attaques, très peu, a priori, concerneraient du vol de données. Cela n'implique cependant pas que ces attaques ne relèvent pas de l'espionnage, comme indiqué supra, mais dans un contexte plus large que la simple captation d'informations ou de données stratégiques. De telles attaques peuvent alors dissimuler trois stratégies distinctes :

- Prédation économique (rachat, prise du pouvoir décisionnel) ;
- Désorganisation/Affaiblissement (mise en difficulté sur le marché concerné) ;
- Destruction (disparition de l'acteur visé) ;

Ces stratégies s'inscrivent pleinement dans une guerre économique systémique. Celle-ci est un mode de domination qui évite de recourir à l'usage de la puissance militaire pour imposer une suprématie durable. Il ne s'agit plus de soumettre l'autre par la force mais de le rendre dépendant par la technologie, ou encore par la chaîne d'approvisionnement. La maîtrise de la *supply chain* est une condition inéluctable d'indépendance stratégique tant pour les acteurs économiques que pour les États. L'intérêt stratégique des protéines végétales pourrait-il être la source d'un tel conflit ?

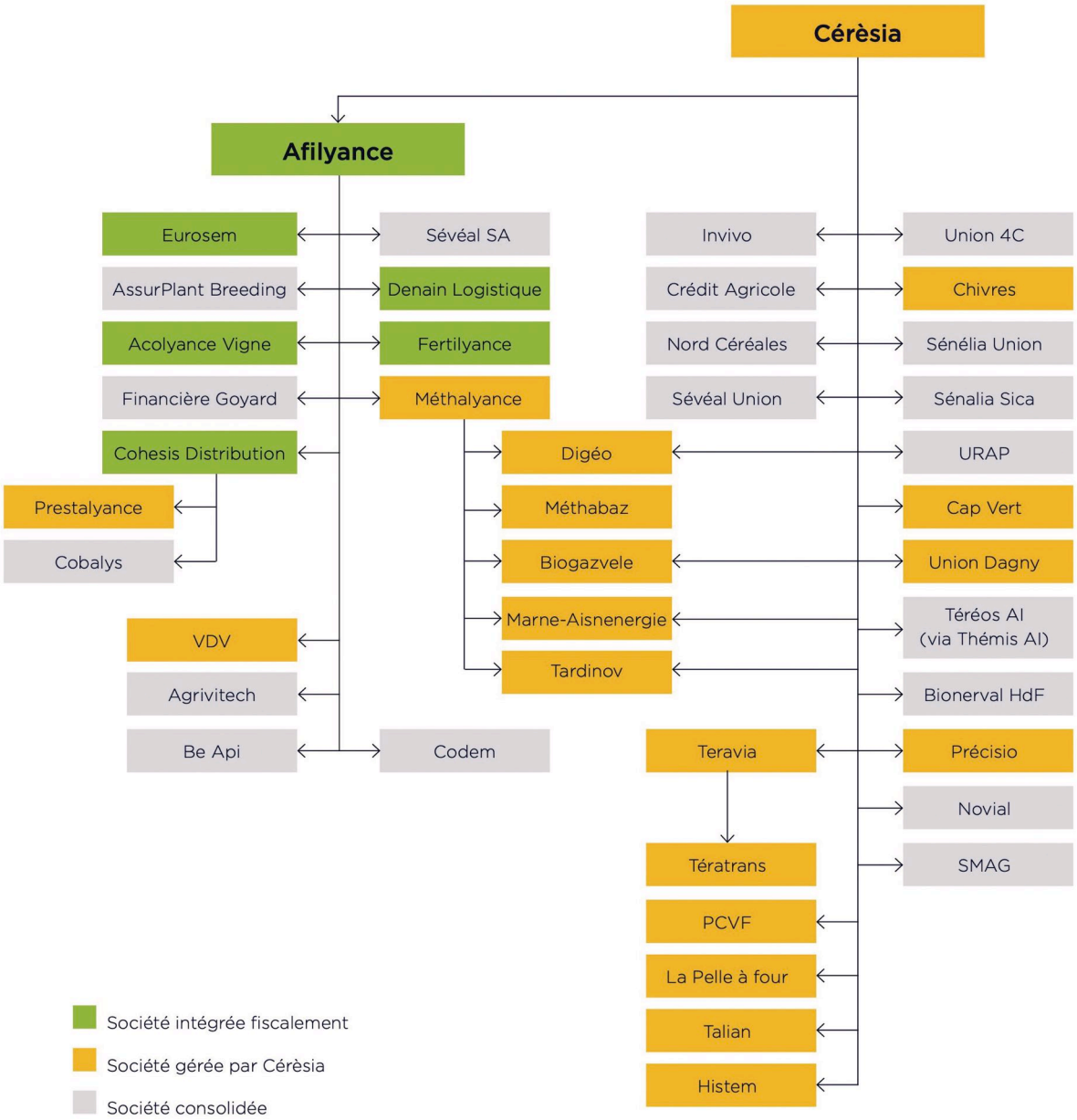
Sur les treize coopératives ou industries agricoles et agroalimentaires attaquées entre 2020 et 2022, neuf

ont une activité centrée autour des protéines végétales dont trois sont également positionnées sur les protéines animales, et quatre exclusivement sur les protéines animales. Comme déjà indiqué, la production de protéines animales n'est possible que par l'utilisation de protéines végétales dans l'alimentation animale. La clé de voûte du système alimentaire repose donc sur la production de protéines végétales. Par conséquent, quelle que soit la coopérative ou l'entreprise visée, l'impact sur la production de protéines végétales est inéluctable (de la production à l'utilisation en fin de chaîne).

L'impact est direct sur des coopératives comme Eureden, Cérésia, Sollio, Cristal Valley par exemple puisque les céréales sont au cœur de leurs activités. L'impact sera par contre plus diffus auprès d'autres acteurs comme par exemple, pour Molson Coors, la production de bière demande des céréales ; pour Lactalis, la production de lait demande de l'alimentation animale à base de protéines végétales ; pour La Martiniquaise-Bardinet,

l'alcool est fabriqué à partir de végétaux (céréales, betteraves,…) ;… Si l'on reprend ces trois exemples, pour Molson Coors, l'impact sur la filière végétale peut se faire ressentir par un sur-stock en raison de l'arrêt ou du ralentissement d'activité, voir un arrêt des commandes auprès des fournisseurs. Pour Lactalis, un ralentissement ou un arrêt de production impacte les élevages de vaches laitières qui ne peuvent écouler leurs stocks de lait et ainsi les fragiliser et, par rebond, impacter la filière de l'alimentation animale. Dans le cas de la Martiniquaise-Bardinet, l'impact de la cyberattaque peut avoir une incidence sur la production d'alcool, à base de...protéines végétales.

Il est intéressant de s'arrêter sur une des attaques en particulier. Le cas de Cérésia montre à quel point les conséquences sur les victimes peuvent être conséquentes. Cérésia est une coopérative française dont les activités sont multiples : solutions agricoles et approvisionnements (semences, engrais, produits phytopharmaceutiques, collecte), viticulture (solutions



BIO

Stéphane Mortier est actuellement adjoint au chef du Centre de Sécurité Economique et de Protection des Entreprises (CSECOPE) au sein de la Direction Générale de la Gendarmerie Française et membre de la Communauté de Recherche de la Gendarmerie Nationale (CREOGN). Il est maître de conférences à l'Université Gustave Eiffel. Il est diplômé en sciences politiques, sociologie et relations internationales de l'Université libre de Bruxelles (ULB), en management stratégique et intelligence économique de l'École de Guerre Économique, et docteur en gestion à Paris 1 Panthéon-Sorbonne. Il est également le représentant des sections étrangères de l'Union des anciens de l'ULB et préside la section française (UAEF). Dans ce cadre, il développe des projets de coopération en Afrique. Il est chargé de cours à l'Ecole de Guerre Économique (lutte contre le blanchiment d'argent), à l'Université de Likasi - RDC (stratégie, droit des affaires). Il est membre fondateur du Cercle K2 et membre actif de l'Association pour l'Unification du Droit en Afrique (UNIDA). Il est l'auteur de plusieurs publications sur l'intelligence économique.

viticoles, approvisionnements, fournitures, prestations), logistique (stockage de productions végétales), élevage (fournitures agricoles et aliments pour animaux), énergie (méthanisation, photovoltaïque), distribution (jardineries, bricolage). Il s'agit donc d'un véritable écosystème agricole représentant plus de 4.400 agriculteurs et plus de 620 employés.

«L'attaque a eu lieu le 20 novembre 2020, un vendredi soir. Les premières alertes ont été données le samedi matin quand plusieurs salariés n'ont pas réussi, depuis leur téléphone portable, à se connecter à l'intranet de l'entreprise, se souvient Olivier Bacon, directeur des opérations chez Cérèsia. Les informaticiens se sont très vite rendus au siège et ont constaté que l'entreprise faisait l'objet d'une cyberattaque. Tout notre système, interne et externe, était paralysé. Pas de demande de rançon clairement affichée mais un message, en russe, "Bon courage à vous".»[3] Près d'un an après l'attaque la coopérative n'avait toujours par retrouvé son rythme d'activité normal. Au-delà de l'attaque elle-même, des tentatives de récupération des données, de la remise en fonction du système,...des conséquences financières et humaines ont ralenti la reprise d'activité. Un véritable traumatisme psychologique s'est fait ressentir chez les personnels et les coopérateurs. Cérésia et tout son écosystème ont évité la destruction totale et donc la disparition mais se sont retrouvés en position de faiblesse, de fragilité pendant plus d'une année.

Le 05 mai 2022, AGCO, fabricant et distributeur mondial d'équipements agricoles a annoncé dans un communiqué que l'entreprise a fait l'objet d'une attaque par ransomware qui a affecté certaines de ses installations de production. Il est possible que l'engagement de l'entreprise en soutien aux agriculteurs ukrainiens soit à l'origine de l'attaque. En effet, l'AGCO Agriculture Foundation a lancé un programme d'aide humanitaire à l'Ukraine en mars 2022 (financement de l'ONG ukrainienne BORSCH)[4].

Il pourrait s'agir ici d'un prolongement du conflit armé dans le cyberespace mais avec pour cible, une fois encore le secteur agroalimentaire (au travers de la fourniture de matériels agricoles). C'est donc toute la *supply chain* (de la culture au produit fini en passant par l'outil de production) qui est visée et toutes les vulnérabilités potentielles sont exploitées.

Les secteurs agricole et agroalimentaire, dépendant des protéines végétales, sont-ils face à un séisme mondial ? Les quelques éléments d'analyse présentés ici laissent à penser qu'une véritable guerre économique se joue face à de telles matières stratégiques. Renforcé par un conflit entre deux puissances agricoles depuis le 20 février 2022, l'enjeu stratégique des protéines végétales est placé au devant de la scène médiatique. Cependant, cela fait plus de deux années que les grands acteurs du secteur sont victimes de cyberattaques d'ampleur, paralysant leurs activités et les fragilisant. Faut-il y voir une simple coïncidence ou plutôt une succession d'actes de guerre économique visant une restructuration mondiale de la production de protéines végétales ?

Dans un tel cas, les grands équilibres géo-économiques actuels pourraient être largement modifiés. Le vecteur utilisé est ici la cyberattaque de type ransomware… La grille de lecture par la sécurité économique montre une dimension cachée du ransomware qui, au-delà et au même titre que l'espionnage, est une véritable arme de guerre économique et est en mesure de répondre à des objectifs stratégiques à dimension mondiale. ■

1 Jérôme DUPRE (2001), «Espionnage économique et droit : l'inutile création d'un bien informationnel», LexElectronica, Vol.7, n°1. http://hdl.handle.net/1866/9506
2 https://www.enisa.europa.eu/publications/report-files/ETL-translations/fr/etl2020-cyber-espionage-ebook-en-fr.pdf
3 https://www.reference-agro.fr/sept-mois-apres-ceresia-nous-raconte-sa-cyberattaque/
4 https://www.businesswire.com/news/home/20220427005230/en/AGCO-Agriculture-Foundation-Donates-to-Farmer-Focused-Initiative-BORSCH-in-Ukraine

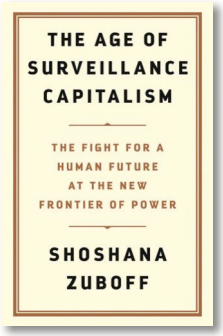

0 1 0 0 1 0 0 1 1 0 1 1
0 1 1 1 0 1 0 1 0 0 1 0

LA MENACE INTÉRIEURE, TOUJOURS NÉGLIGÉE

Le renseignement est de plus en plus important dans la cyber-stratégie des entreprises.

Auteur : Nicola Sotira

Nous vivons dans une période qui se caractérise de plus en plus par un développement exponentiel de la technologie.



Une technologie qui comporte également des menaces potentielles pour nous tous, qui vivons sous le spectre d'une architecture de surveillance omniprésente, active 24 heures sur 24 et 365 jours par an. Cette architecture, nous l'avons vu, sert les intérêts des grands OTT *(Over the Top)*, c'est-à-dire les colosses qui gèrent l'achat et la vente de nos données personnelles et, surtout, acquièrent la partie prédictive de nos habitudes et de nos comportements.

Dans ce scénario, Facebook est désormais l'une des sources faisant autorité en matière de modèles comportementaux. Ce modèle économique est dénommé, dans le livre homonyme de Shoshana Zuboff, le *«capitalisme de la surveillance»;* il s'agit d'un scénario dans lequel les données servent de base à de véritables guerres et à des mouvements de pouvoir qui défient même les démocraties.

Ce scénario s'est également compliqué par le conflit russo-ukrainien, qui a des répercussions majeures sur les pays de l'OTAN en termes de cyber-guerre. Au moment où nous rédigeons cet article, les journaux font état d'attaques menées par des groupes pro-russes contre de nombreuses organisations gouvernementales et des institutions financières.

BIO

Chef du CERT du groupe Poste Italiane, Nicola travaille dans le domaine de la sécurité informatique et des réseaux depuis plus de vingt ans, avec une expérience acquise dans des environnements internationaux. Les contextes desquels il s'est occupé couvrent la cryptographie, la sécurité des infrastructures, mais également les réseaux mobiles et la 3G. Il a collaboré avec plusieurs magazines du secteur informatique en tant que journaliste, contribuant à la diffusion de connaissances liées à la sécurité ainsi qu'à ses aspects techniques et juridiques. Membre de l'*Association for Computing Machinery* (ACM) depuis 2004, Nicola a collaboré avec plusieurs start-ups en Italie et à l'étranger. Dans ce domaine, il a participé avec plusieurs entreprises à la conception et au développement de services mobiles ; il est co-éditeur de la version italienne de *Cybersecurity Trends* (www.cybertrends.it) et a fait partie du conseil d'administration de la fondation Global Cyber Security (GCSEC).

Ces développements ont remodelé le rôle du renseignement en l'insérant puissamment dans les stratégies de cyber-sécurité des organisations, publiques comme privées.

Mais de quoi parle-t-on ? Quelle est la signification des acronymes que nous lisons dans les journaux ? De la relation entre le renseignement dans le monde physique et celui mis en œuvre dans le monde numérique ?

Activité de renseignement

L'activité de renseignement est le produit résultant de la collecte, de l'évaluation, de l'analyse et de l'interprétation des informations recueillies.

L'élaboration d'un produit de renseignement nécessite la collecte d'informations auprès de diverses sources, sources qui doivent être sélectionnées en fonction des objectifs requis par l'organisation.

Le produit du renseignement, dans ce cadre, fournit aux États les informations dont ils ont besoin pour promouvoir leurs intérêts nationaux. Les organisations de renseignement recherchent généralement des informations concernant les capacités militaires, les problèmes qui menacent la sécurité nationale, les programmes économiques et les positions diplomatiques.

Dans le scénario numérique/cyber, des scénarios similaires sont utilisés dans le but de prévenir les menaces ou de recueillir des informations stratégiques. Des programmes de plus en plus sophistiqués font désormais partie de la stratégie de cyber-protection défensive/offensive, tant au niveau des gouvernements que des entreprises faisant partie du secteur des «infrastructures critiques», ces dernières se limitant cependant à la partie défensive de la stratégie.

L'activité de renseignement se divise en deux catégories : stratégique et opérationnelle. La première fournit les informations nécessaires aux décideurs pour faire des choix ou prendre des décisions de longue durée. Normalement, ces données doivent ensuite être complétées par des informations sur la politique, l'économie, les interactions sociales et les développements technologiques. Le renseignement opérationnel, quant à lui, concerne des événements actuels ou à court terme et n'implique pas de projections sur le long terme.

Techniques de collecte d'informations

Il existe plusieurs disciplines utilisées pour la collecte d'informations. Ces disciplines comprennent le renseignement humain (HUMINT), le renseignement dérivé des signaux (SIGINT), le renseignement dérivé des images (IMINT), le renseignement dérivé des détections de radiofréquences et d'émissions radioactives (MASINT), et enfin le renseignement obtenu par la recherche de sources disponibles sur le *deep web* (OSINT).

En ce qui concerne le renseignement de type OSINT, il convient de souligner que plus une organisation ou un État expose ouvertement ses

données, plus ce type d'activité a du succès. Les journaux, les sites, les bases de données en ligne, les réseaux sociaux deviennent ainsi, souvent, des sources d'information à forte valeur ajoutée, surtout en ce qui concerne nombre d'activités gouvernementales et commerciales.

Les activités de renseignement humain, HUMINT, sont synonymes d'espionnage et d'activités clandestines telles que celles décrites dans le livre de Fabrizio Gatti *(Educazione Americana)*, mais il ne faut pas non plus négliger les activités menées par les diplomates et les attachés militaires.

Cette discipline représente la plus ancienne méthode de collecte d'informations et était, jusqu'à la fin du 20e siècle, la principale source de renseignements pour les gouvernements aussi bien que pour les organisations privées.

L'activité HUMINT comprend des activités subversives, sensibles et clandestines ciblant les personnes qui contrôlent, supervisent et ont accès aux sources visées. Les activités subversives peuvent être traitées ouvertement: dans ce cas, les personnes qui recueillent les informations

peuvent être des diplomates, des attachés militaires, des membres de délégations officielles participant ou gèrant des publications ou des conférences non classifiées.

Les activités clandestines, en revanche, nécessitent des agents infiltrés dans des pays/organisations, sous couverture. La gestion de cette variante d'HUMINT nécessite un nombre important de personnes, aussi bien parmi celles qui recueillent les informations que celles qui soutiennent et coordonnent les différentes activités menées sur le terrain.

HUMINT dans Onlife

Aujourd'hui, aussi bien les acteurs malveillants que les professionnels de la cyber-sécurité ont à leur disposition des technologies de plus en plus efficaces et meurtrières, dans le sens digital aussi bien que, potentiellement, dans le sens physique. Parallèlement aux technologies, nous disposons d'outils que l'on peut considérer comme les plus utiles de tous, à savoir la connaissance et l'expérience humaines.

Pour ces raisons, il est facile de voir comment l'utilisation de l'HUMINT est un élément vital à la fois pour ceux qui travaillent à la détection des actions des cybercriminels que pour ceux qui sont impliqués dans la gestion et la prévention des menaces.

Comprendre les motivations, les tendances et les raisons des adversaires est essentiel pour tout type de guerre, y compris la cyberguerre. Comme le confirme l'abondante littérature sur le sujet, il faut connaître son ennemi en «se mettant dans la peau de son ennemi»; il faut toujours garder à l'esprit que l'ennemi, dans cette cyberguerre, peut être virtuel, anonyme mais jamais invisible.

La technique utilisée dans le monde numérique est identique à celle utilisée dans le monde physique: un chasseur de menaces, pour réussir à mener ses activités HUMINT avec succès, doit apprendre à penser comme les acteurs qui mettent en œuvre les menaces: il doit en identifier les outils, les techniques utilisées et en comprendre les objectifs.

Tout cela exige de bonnes compétences et une bonne capacité à infiltrer les acteurs de la cyber-menace, à gagner leur confiance et à apprendre leur mode de fonctionnement. Un effort équivalent à celui déployé par les agences de renseignement lorsqu'elles insèrent un agent sous couverture pour infiltrer une organisation criminelle.

C'est un travail minutieux, qui met nos nerfs à rude épreuve : identifier les lieux numériques où les acteurs de la menace se réunissent pour partager des informations, les forums du dark web, les chats IRC, les salles virtuelles et les marchés noirs.

Une activité tout aussi dangereuse que celle qui se déroule dans le monde physique, quelles que soient l'expérience et les compétences de chacun. Lorsque vous pénétrez dans le côté le plus obscur du web, où l'on trouve des acteurs de toutes les régions du monde, qui sont souvent aussi en conflit les uns avec les autres, vous êtes constamment scruté.

Dans ces forums, les administrateurs ou les modérateurs examinent tout ce qui vous concerne dans le but de déterminer si vous êtes un infiltré. Au minimum, un simple soupçon suffit pour vous en bannir l'accès.

Bien sûr, avant de commencer cette activité, il est important de se prémunir en gérant très bien sa propre sécurité. Les chasseurs de menaces ont besoin d'outils qui cachent leur véritable identité ; en partant d' outils aussi simples que la connexion par VPN et la maîtrise de TOR, la liste s'étend jusqu'à la mise en œuvre de proxys et à l'utilisation de machines virtuelles.

Être démasqué peut constituer une menace sérieuse pour soi-même et pour l'organisation pour laquelle on

travaille. Dans le cadre de ces activités, la prudence est de mise et la connaissance des limites à ne pas franchir dans le *dark web* est obligatoire. Si on les dépasse, il est en effet possible d'être poursuivi par les forces de l'ordre, ou même, en fonction de la spécificité des activités qu'on effectue, d'être passible de conflits avec le service juridique sa propre entreprise.

La collecte de données par le biais de techniques HUMINT peut prendre beaucoup de temps: il est donc nécessaire de s'appuyer sur des technologies de pointe tout en ayant toujours à l'esprit quels peuvent être les objectifs et les cibles, pour les criminels, au sein sa propre organisation, c'est-à-dire *in primis* l'infrastructure et les processus opérationnels critiques.

Pour gérer les initiatives HUMINT, il ne faut pas seulement compter sur soi-même: nous suggérons fortement de travailler en équipe avec des sociétés de cyber-sécurité qui ont une bonne réputation car, en général, plus on recueille d'informations, meilleure est la qualité du travail accompli.

Les informations provenant de sources multiples, du *dark web* aux réseaux sociaux, etc., il est donc essentiel de créer le bon mélange d'analystes, internes et externes. Le travail effectué ne peut pas être basé sur une recherche aléatoire des acteurs du *dark web*, il faut y identifier ceux qui ont les accès aux sources et aux ressources spécialisées nécessaires pour atteindre les actifs que nous devons défendre.

Par exemple, il peut être utile, dans le secteur financier, d'avoir des sources parmi les développeurs qui échangent et achètent des informations sur les cartes de crédit ou les codes PIN ainsi que les modérateurs de forums sur le sujet.

Il existe des listes sur Jabber et, sur ce système de messagerie décentralisé, on pose des questions, ou on cherche des indices pour enquêter. Durant cette activité, il faut aussi gérer et entretenir plusieurs avatars, chacun ayant sa propre liste de personnes qu'il sait pouvoir contacter sur Jabber.

Il est évident qu'il faut veiller à ne rien faire d'illégal, à ne rien acheter et encore moins manipuler du matériel illégal.

Un autre point qui doit être résolu est celui des horaires, si vous voulez maintenir la crédibilité de vos avatars, vous devez sortir du paradigme 09:00-17:00 et de celui de la semaine de travail des employés classiques, car l'absence de votre avatar en dehors de ce créneau horaire attirerait certainement la suspicion de vos sources.

Pour être crédible, vous avez besoin d'une présence en ligne constante, vous devrez assurer la présence des avatars bien au-delà des heures de bureau et accéder aux forums même les samedis et dimanches.

Conclusions

Les logiciels, les outils et les technologies évoluent rapidement, mais même dans ce scénario complexe, on retrouve toujours le facteur humain ; toutes les cyber-attaques sont pilotées par des humains. C'est précisément la raison pour laquelle la connaissance des motivations des adversaires et des tendances sous-jacentes aux campagnes de malveillance et aux attaques peut vous aider à définir des décisions stratégiques et à cibler les investissements qui protègent le mieux nos infrastructures.

Comme nous l'avons décrit, l'activité HUMINT peut être une pièce essentielle de votre stratégie de cyberdéfense, mais elle peut aussi être incroyablement dangereuse. Il faut prendre soin de dissimuler son identité et ses objectifs.

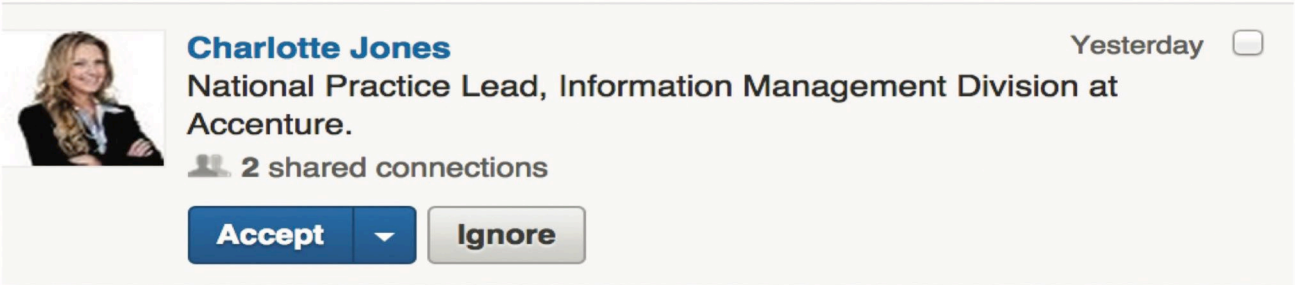
Pour commencer, on peut certainement s'appuyer sur des plateformes de renseignement qui intègrent ce service ou encore faire appel à des entreprises qui proposent spécifiquement ce type de service. Les outils traditionnels et les tactiques HUMINT combinés donnent la capacité d'identifier les comportements criminels et permettent de passer à une approche plus proactive de la cyber-sécurité, une approche qui se concentre sur la prévention des attaques, car la meilleure forme de résilience et d'adaptation réussie est bel et bien celle qui permet d'arrêter les menaces avant qu'elles n'affectent nos infrastructures et nos processus critiques. ■

Bonjour Charlotte! Un exemple de social engineering sur Linkedin.

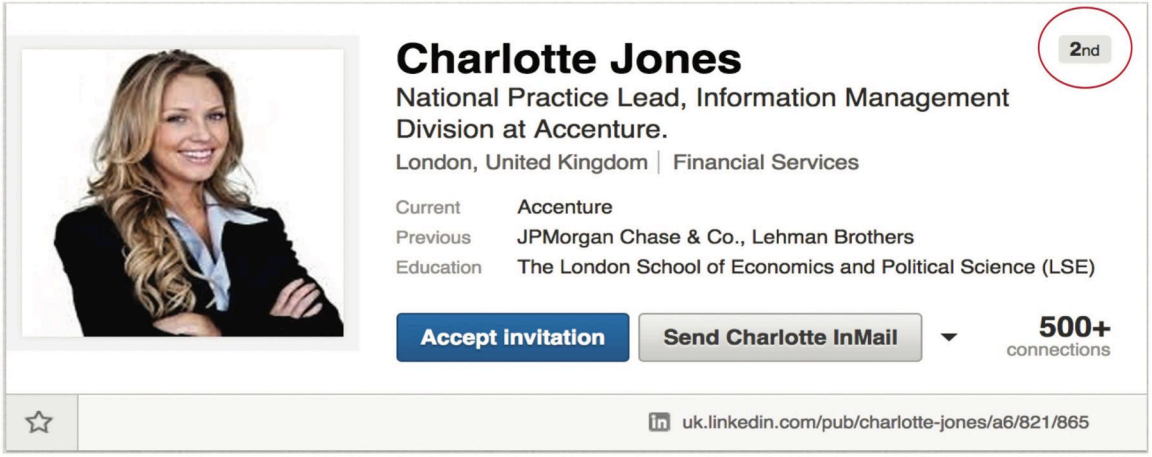
Auteur : Battista Cagnoni

«*Charlotte*» est un cas parmi d'autres, qui a fait l'objet d'une petite investigation que j'ai mené récemment.

Tout part de l'image, à cause de son fort composant émotionnel. L'exemple que nous observons ici est un cas réel : Charlotte, une belle femme blonde souriante, qui m'a demandé de rejoindre mon cercle Linkedin, une invitation de deuxième niveau, c'est-à-dire que quelqu'un de mon réseau de contacts a accepté Charlotte, ce qui «en principe» voudrait dire qu'il la connaît.



Charlotte is in my network



Experience

National Practice Lead, Information Management Division.
Accenture
October 2014 – Present (1 month) | London, United Kingdom

Accenture plc is a multinational management consulting, technology services, and outsourcing company. Its incorporated headquarters are in Dublin, Republic of Ireland. It is the world's largest consulting firm as measured by revenue and is a Fortune Global 500 company. As of 2014, the company reported net revenues of $30.0 billion with approximately 305,000 employees, serving clients in more than 200 cities in 56 countries. Accenture has more employees in India than any other country; in the US, it has about 40,000 employees and 35,000 located in the Philippines. Accenture's current clients include 96 of the Fortune Global 100 and more than three-quarters of the Fortune Global 500. Since September 1, 2009 the company has been incorporated in Ireland.

Director, Enterprise Technology
JPMorgan Chase & Co.
September 2011 – September 2014 (3 years 1 month) | London, United Kingdom

JPMorgan Chase is a global investment bank with expertise in mergers and acquisitions, capital markets, financial restructuring, and valuation.

As strategist and enterprise architect, defining and advancing technology vision of enterprise systems aligned with the firm's vision for growth and service innovation, supporting entire investment banking business of Corporate Finance, Financial Restructuring, Financial Advisory Services, Capital Markets, Private Equity / Financial Sponsors Coverage and corporate departments. Constructed business case for various sized technology investments and highly successful selling concepts and solutions to business and IT.

Supported application landscape of CRM, ERP, data warehouse, web sites & applications, document management, collaboration portal, SaaS, and industry data services. Responsible for technology fit assessment, selection and execution of new technologies. Chief evangelist on enterprise CRM to accelerate conversion of prospects to clients, contacts to relationships to closed deals. Constructed Workday user stories to articulate value of streamlined investment bank talent management. Executed quick pilots / proof of concepts (POC) to introduce new technology as IT capability. Product manager of Salesforce.com, leading cross functional team in business process streamlining and technology platform implementation.

Business Intelligence Lead, Financial Planning & Analysis
Lehman Brothers
January 2006 – March 2008 (2 years 3 months) | London, United Kingdom

Lead advisor in FP&A supporting executive decision making process with data, metrics and analytics of Lehman Brothers' mortgage banking statistics and capital market trends. Managed team of data analysts and programmer analysts, responsible for corporate finance data architecture, data analysis, financial reporting, management reporting, systems integration and scorecard / dashboard design and development. Established data management best practices in taxonomy, data cleansing, migration and governance. Designed and implemented data marts to facilitate budget, forecast and metrics driven reporting and analysis. Developed integration to Cognos Planning and Hyperion / Essbase monthly consolidation and closing process.

Developer / Database Architect
Lehman Brothers
November 2003 – January 2006 (2 years 3 months) | London, United Kingdom

Architecture and design of large transactional databases, financial data marts, data warehouse, integration to Cognos Planning and enterprise/financial reporting of the origination and servicing businesses of Lehman Brothers Mortgage Capital, supporting field operations and corporate functions in finance, accounting, treasury, legal, compliance, risk management and Lehman Brothers corporate finance.

Volunteer Experience & Causes

Opportunities Charlotte is looking for:
- Joining a nonprofit board

Languages

French (fluent) Spanish (basic)
Germany (basic)

Education

The London School of Economics and Political Science (LSE)
2000 – 2003

Additional Info

Interests
Fiction, International Affairs, Opera, Horseriding, Fine Food

Je reçois donc un email de Charlotte via Linkedin, me demandant de se connecter avec moi. Je regarde son profil, qui est impressionnant. Riche en compétences et en expériences professionnelles. Il n'y a apparemment rien de suspect dans son curriculum, qui a tout pour inciter à l'accepter dans son cercle de relations.

En tant que «victime» potentielle mais ayant des connaissances en sécurité en réseaux sociaux, j'observe d'emblée que le profil est presque trop riche, presque trop beau pour être réel. Un détail attire mon attention : ce profil, si parfait, n'est complété par aucune recommandation, ni écrite, ni sur la liste des compétences précises.

Summary

I bring common sense and a human touch to enterprise problem solving. My passion intersects market, industry, business, customer and technology. I speak expressively across these disciplines, advising clients on strategic vision of user centric technology and organizational behavior change.

I'm passionate about boosting competitiveness and value creation enabled by technology, cultivating trust based relationships, creating win win opportunities and giving back to community.

Specialties:
- IT Strategy, technology enablement, enterprise architecture, cross functional change leadership, strategic transformation
- Consultative sales & marketing, business / alliance / partnership development
- M&A due diligence, management consulting, technology competitive analysis
- Financial services vertical - investment banking, mortgage banking, capital markets - front office, across business lines, and with regulators
- Enterprise software / solutions, product management, user experience
- Platform / service architecture, governance, outsourcing, program management, agile delivery
- SaaS, business intelligence / analytics, ERP, CRM, content management, collaboration
- Building high performance / virtual / global teams, developing capability, teaching / coaching

Lately my interest is CRM / marketing automation, data and analytics, content management, business development and financial services marketing. I enjoy product ideation and evaluate software from small niche companies.

Connect with me @ jonescharlotte947@gmail.com

Je me demande donc si ce profil correspond ou non à une personne réelle ou s'il s'agit d'un profil créé expressément pour faire des opérations de social engineering, pour gagner la confiance des victimes, en premier lieu pour les inciter, une fois l'invitation acceptée, à ne pas mettre en doute les futurs emails que «Charlotte» va leur envoyer, et surtout cliquer sur les liens qu'elle va leur recommander.

Cor dos cabelos e bronzeado fazem mulheres sentirem-se ...
www.portalrcr.com.br/.../45878-cor-dos-c... ▾ Oversæt denne side
574 × 430 - 01/11/2012 - Longos **cabelos** loiros, bronzeado e unhas tipo francesinha. Assim as mulheres sentem-se atraentes, segundo pesquisa realizada pela rede ...

Cor dos cabelos e bronzeado fazem mulheres sentirem-se ...
www.portalrcr.com.br/.../45878-cor-dos-c... ▾ Oversæt denne side
574 × 430 - 01/11/2012 - Longos **cabelos** loiros, bronzeado e unhas tipo francesinha. Assim as mulheres sentem-se atraentes, segundo pesquisa realizada pela rede ...

Cor dos cabelos e bronzeado fazem mulheres sentirem-se ...
www.portalrcr.com.br/.../45878-cor-dos-c... ▾ Oversæt denne side
574 × 430 - 01/11/2012 - Longos **cabelos** loiros, bronzeado e unhas tipo francesinha. Assim as mulheres sentem-se atraentes, segundo pesquisa realizada pela rede ...

Aprenda simpatias para crescer na profissão - Terra Brasil
vidaeestilo.terra.com.br/.../aprenda-simpat... ▾ Oversæt denne side
407 × 305 - 09/09/2013 - Beleza · **Cabelos** e Salão · **Cabelo** do dia · Dicas Profissionais · Faça você mesma · Quero esse **cabelo** · Tratamento e tintura · Salão em Casa.

Cor dos cabelos fazem mulheres sentirem-se atraentes; veja
www.meionorte.com/.../cor-dos-cabelos-e... ▾ Oversæt denne side
600 × 449 - 27/10/2012 - Longos **cabelos** loiros, bronzeado e unhas tipo francesinha. Assim as mulheres sentem-se atraentes, segundo pesquisa realizada pela rede ...

Professional Image | The Work at Home Woman
www.theworkathomewoman.com/.../profe... ▾ Oversæt denne side
507 × 338 - How to Dress for an Interview – Styling Tips for Women. Tags: Business ... A smart and professional image will say that you are a smart and **professional woman**.

How to Dress for Success - The Work at Home Woman
www.theworkathomewoman.com/dress-fo... ▾ Oversæt denne side
507 × 338 - How to Dress for an Interview – Styling Tips for Women. Tags: Business ... A smart and professional image will say that you are a smart and **professional woman**.

Job Seekers | The Work at Home Woman
www.theworkathomewoman.com/.../job-s... ▾ Oversæt denne side
507 × 338 - Upcoming Events for Entrepreneurial Women, Career Bloggers and Job Seekers ... professional image will say that you are a smart and **professional woman**.

Woman | The Work at Home Woman
www.theworkathomewoman.com/.../wom... ▾ Oversæt denne side
507 × 338 - How to Dress for an Interview – Styling Tips for Women. Tags: Business ... A smart and professional image will say that you are a smart and **professional woman**.

Michaela Quinn | The Work at Home Woman
www.theworkathomewoman.com/.../mich... ▾ Oversæt denne side
507 × 338 - How to Dress for an Interview – Styling Tips for Women. Tags: Business ... A smart and professional image will say that you are a smart and

Mulher

Quinta-feira, 1 de novembro de 2012 - 21h44

Cor dos cabelos e bronzeado fazem mulheres sentirem-se atraentes

A- A+

Longos cabelos loiros, bronzeado e unhas tipo francesinha. Assim as mulheres sentem-se atraentes, segundo pesquisa realizada pela rede inglesa de lojas de produtos de beleza, Superdrug. As informações são do site Female First.

Woman

Thursday, November 1, 2012 - 21h44

Hair color and tan make women feel attractive

A- The

Long blond hair, tan and nails French girl type. So women feel attractive, according to a survey by the British chain of beauty product stores, Superdrug. The information is the site Female First.

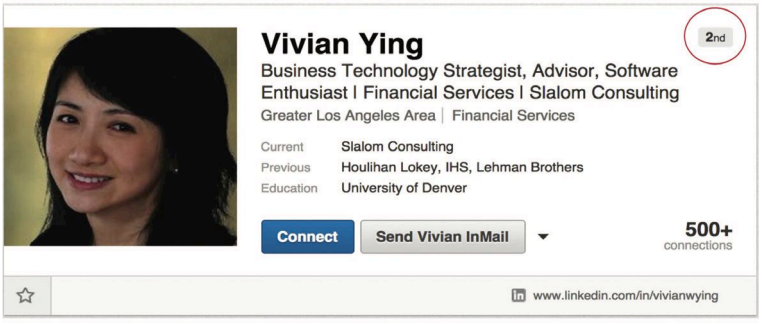
La première étape de mon rôle d'enquêteur, est très simple : je vais insérer la photo de Charlotte dans le moteur de recherches d'images de Google. Et là, première surprise : la photo de «Charlotte» apparaît sur de très nombreux sites, certains brésiliens, d'autres anglais, proposant toutes sortes de services pour des femmes qui veulent réussir.

L'image a donc été soigneusement choisie pour son caractère purement émotionnel, pour cibler spécifiquement des hommes : une belle femme, blonde, jeune, à laquelle on a ajouté, dans le profil Linkedin, plusieurs éléments soulignant son intelligence et ses multiples talents, qui se traduisent par sa réussite professionnelle incontestable, selon le curriculum mis en ligne.

Toujours en utilisant Google, je vais copier des parties de ce curriculum, en les mettant entre guillemets. Avec trois simples recherches, j'observe que «Charlotte» a emprunté des phrases existantes : depuis Wikipédia en ce qui concerne la description de l'entreprise où elle travaille, mais surtout depuis le profil d'une certaine Vivian Ying en ce qui concerne le parcours et les compétences professionnelles.

Il s'agit désormais de déterminer qui, de Charlotte ou de Vivian, est une personne réelle. Je me penche alors sur le profil de Vivian.

Je découvre tout d'abord que le profil de Vivian est déjà dans mon réseau, ce qui implique que ceux qui ont créé Charlotte ont fait des



Experience

National Practice Lead, Information Management Division.
Accenture
October 2014 – Present (1 month) | London, United Kingdom

Accenture plc is a multinational management consulting, technology services, and outsourcing company. Its incorporated headquarters are in Dublin, Republic of Ireland. It is the world's largest consulting firm as measured by revenue and is a Fortune Global 500 company. As of 2014, the company reported net revenues of $30.0 billion with approximately 305,000 employees, serving clients in more than 200 cities in 56 countries. Accenture has more employees in India than any other country; in the US, it has about 40,000 employees and 35,000 located in the Philippines. Accenture's current clients include 96 of the Fortune Global 100 and more than three-quarters of the Fortune Global 500. Since September 1, 2009 the company has been incorporated in Ireland.

Director, Enterprise Technology
JPMorgan Chase & Co.
September 2011 – September 2014 (3 years 1 month) | London, United Kingdom

JPMorgan Chase is a global investment bank with expertise in mergers and acquisitions, capital markets, financial restructuring, and valuation.

As strategist and enterprise architect, defining and advancing technology vision of enterprise systems aligned with the firm's vision for growth and service innovation, supporting entire investment banking business of Corporate Finance, Financial Restructuring, Financial Advisory Services, Capital Markets, Private Equity / Financial Sponsors Coverage and corporate departments. Constructed business case for various sized technology investments and highly successful selling concepts and solutions to business and IT.

Supported application landscape of CRM, ERP, data warehouse, web sites & applications, document management, collaboration portal, SaaS, and industry data services. Responsible for technology fit assessment, selection and execution of new technologies. Chief evangelist on enterprise CRM to accelerate conversion of prospects to clients, contacts to relationships to closed deals. Constructed Workday user stories to articulate value of streamlined investment bank talent management. Executed quick pilots / proof of concepts (POC) to introduce new technology as IT capability. Product manager of Salesforce.com, leading cross functional team in business process streamlining and technology platform implementation.

Business Intelligence Lead, Financial Planning & Analysis
Lehman Brothers
January 2006 – March 2008 (2 years 3 months) | London, United Kingdom

Lead advisor in FP&A supporting executive decision making process with data, metrics and analytics of Lehman Brothers' mortgage banking statistics and capital market trends. Managed team of data analysts and programmer analysts, responsible for corporate finance data architecture, data analysis, financial reporting, management reporting, systems integration and scorecard / dashboard design and development. Established data management best practices in taxonomy, data cleansing, migration and governance. Designed and implemented data marts to facilitate budget, forecast and metrics driven reporting and analysis. Developed integration to Cognos Planning and Hyperion / Essbase monthly consolidation and closing process.

Accenture - Wikipedia, the free encyclopedia
en.wikipedia.org/wiki/Accenture ▾ Oversæt denne side
Accenture plc is a multinational management consulting, technology services, and outsourcing company. Its incorporated headquarters are in Dublin, Republic ...
Pierre Nanterme - HealthCare.gov - Accenture top 50 business ... - Consulting firm

Vivian Ying | LinkedIn
www.linkedin.com/in/vivianwying ▾ Oversæt denne side
Greater Los Angeles Area - Business Technology Strategist, Advisor | Financial Services | Slalom Consulting
As strategist and enterprise architect, defining and advancing technology vision of enterprise systems aligned with the firm's vision for growth and service ...

Vivian Ying | LinkedIn
www.linkedin.com/in/vivianwying ▾ Oversæt denne side
Greater Los Angeles Area - Business Technology Strategist, Advisor | Financial Services | Slalom Consulting
Lead advisor in FP&A supporting executive decision making process with data, metrics and analytics of Lehman Brothers' mortgage banking statistics and ...

• Charlotte

Summary

I bring common sense and a human touch to enterprise problem solving. My passion intersects market, industry, business, customer and technology. I speak expressively across these disciplines, advising clients on strategic vision of user centric technology and organizational behavior change.

I'm passionate about boosting competitiveness and value creation enabled by technology, cultivating trust based relationships, creating win win opportunities and giving back to community.

Specialties:
• IT Strategy, technology enablement, enterprise architecture, cross functional change leadership, strategic transformation
• Consultative sales & marketing, business / alliance / partnership development
• M&A due diligence, management consulting, technology competitive analysis
• Financial services vertical - investment banking, mortgage banking, capital markets - front office, across business lines, and with regulators
• Enterprise software / solutions, product management, user experience
• Platform / service architecture, governance, outsourcing, program management, agile delivery
• SaaS, business intelligence / analytics, ERP, CRM, content management, collaboration
• Building high performance / virtual / global teams, developing capability, teaching / coaching

Lately my interest is CRM / marketing automation, data and analytics, content management, business development and financial services marketing. I enjoy product ideation and evaluate software from small niche companies.

Connect with me @ jonescharlotte947@gmail.com

• Vivian

Summary

I bring common sense and a human touch to enterprise problem solving. My passion intersects market, industry, business, customer and technology. I speak expressively across these disciplines, advising clients on strategic vision of user centric technology and organizational behavior change.

I'm passionate about boosting competitiveness and value creation enabled by technology, cultivating trust based relationships, creating win win opportunities and giving back to community.

Specialties:
• IT Strategy, technology enablement, enterprise architecture, cross functional change leadership, strategic transformation
• Consultative sales & marketing, business / alliance / partnership development
• M&A due diligence, management consulting, technology competitive analysis
• Financial services vertical - investment banking, mortgage banking, capital markets - front office, across business lines, and with regulators
• Enterprise software / solutions, product management, user experience
• Platform / service architecture, governance, outsourcing, program management, agile delivery
• SaaS, business intelligence / analytics, ERP, CRM, content management, collaboration
• Building high performance / virtual / global teams, developing capability, teaching / coaching

Lately my interest is CRM / marketing automation, data and analytics, content management, business development and financial services marketing. I enjoy product ideation and evaluate software from small niche companies.

Connect with me - viviany at slalom.com (email), @vivianwying (Twitter).

recherches sur les personnes qui font partie de mon cercle professionnel étendu, pour mieux étudier les intérêts communs qui me lient à elles.

Le CV de Charlotte est identique à celui de Vivian! Seule la dernière ligne, qui comprend l'adresse email, a changé.

Pour mieux comprendre les détails du «piège-Charlotte», comparons maintenant les deux profils. Nous avons déterminé que «Charlotte» a un profil constitué d'une fausse photo, d'un parcours copié et d'un CV intégralement plagié. Il y a en outre quelques erreurs d'orthographe, les descriptions de son travail actuel sont très génériques et elle n'est, rappelons-le, recommandée par personne.

Vivian, de son côté, a une photo réelle, est active sur twitter, a des dizaines de recommandations et, surtout, possède un historique professionnel dont les éléments sont confirmés puisque conformes aux informations fournies par les sites internet des entreprises où elle travaille et où elle a travaillé dans le passé.

Une fois que nous avons définitivement établi, sans l'ombre d'un doute, que Charlotte n'est pas une personne réelle, nous refusons évidemment sa demande d'intégrer notre réseau.

Who is real?

Charlotte	Vivian
▪ "Cheated" with her profile picture	▪ Seems to be a real picture
▪ Spelling mistakes	▪ She is active on twitter
▪ Generic description of her current work	▪ She have endorsements and recommendations
▪ No endorsements or recommendations	▪ She have a searchable work history which match her LinkedIn profile

Pourquoi existe-t-il autant de «Charlottes» sur Linkedin ? Il y a plusieurs raisons complémentaires entre elles. Par ce site destiné aux échanges professionnelles, ceux qui se cachent derrière des «Charlottes» le font, au mieux, pour découvrir les compétences de la victime et les revendre à des recruteurs ou à des chasseurs de tête d'entreprises. Mais souvent, ces attaquant utilisent cette méthode pour collecter des informations et surtout la liste des contacts de la victime pour leur envoyer des spam aux contenus de plus en plus dangereux sans éveiller les soupçons, ou encore faire du *profiling* de cibles potentielles pour des attaques précises, par exemple dans le cercle professionnel interne aux contacts de la victime dans sa propre entreprise.

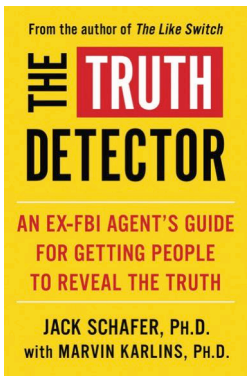
En conclusion

En conclusion, il faut être de plus en plus vigilant lorsque l'on se connecte sur des réseaux sociaux. L'idéal lors de la réception d'une invitation de la part d'une personne inconnue est de faire les recherches simples que nous avons expliqué ci-dessus («sanitychecking») pour vérifier que la personne est bien réelle. N'oubliez pas que vous pouvez toujours demander à la personne qui vous invite quelles sont les raisons qui l'ont poussée à désirer vous connaître : c'est l'une des meilleures méthodes, car les «scammers», en principe, ne répondent jamais. Enfin, par mesure de prudence, n'acceptez aucune invitation de personnes que vous ne connaissez pas et qui ont desprofils par trop «génériques». ■

BIO

Battista Cagnoni, Senior Consultant, Advisory Services, EMEA auprès de Vectra, est un expert en sécurité, bénéficiant d'une longue expérience dans des domaines différents de l'industrie, où il a assuré les postes de Security engineer, Security Analyst ou encore SOC Lead. Il est passionné de la culture de la cyber-sécurité, de la prise de conscience dans ce domaine et de la compréhension des méthodologies à suivre pour faire face aux problèmes de sécurité. Il partage constamment ses connaissances, offrant des conseils et des processus au plus haut niveau, aidant les CISO qui réfléchissent à la manière de renforcer et d'atteindre un haut degré de maturité dans le cadre des opérations de sécurité. Battista détient les certification GIAC de Forensic Analyst et d'Incident Handler ainsi que les certificats d'Expert CISSP, GCFA, GCIH.

Taillés en bits et en pièces. Que pouvons-nous apprendre d'un exemple d'espionnage d'entreprise?



Cet article est reproduit et traduit grâce à l'aimable autorisation des auteurs. Sa version originale a d'abord été publiée sous la forme d'un court exemple dans Schafer, J. et Karlins, M. (2020) ,The Truth Detector. An Ex-FBI Agent's Guide for getting people to reveal the truth, Simon & Schuster, New York, 144-150 (version epub) puis comme article complet : Schafer, J. et Karlins, M. (2021), Hacked by Bits and Pieces : What Can We Learn from an Example of Corporate Espionage ? Journal of Information Security, 12:3, 224-231. (https://doi.org/10.4236/jis.2021.123012)

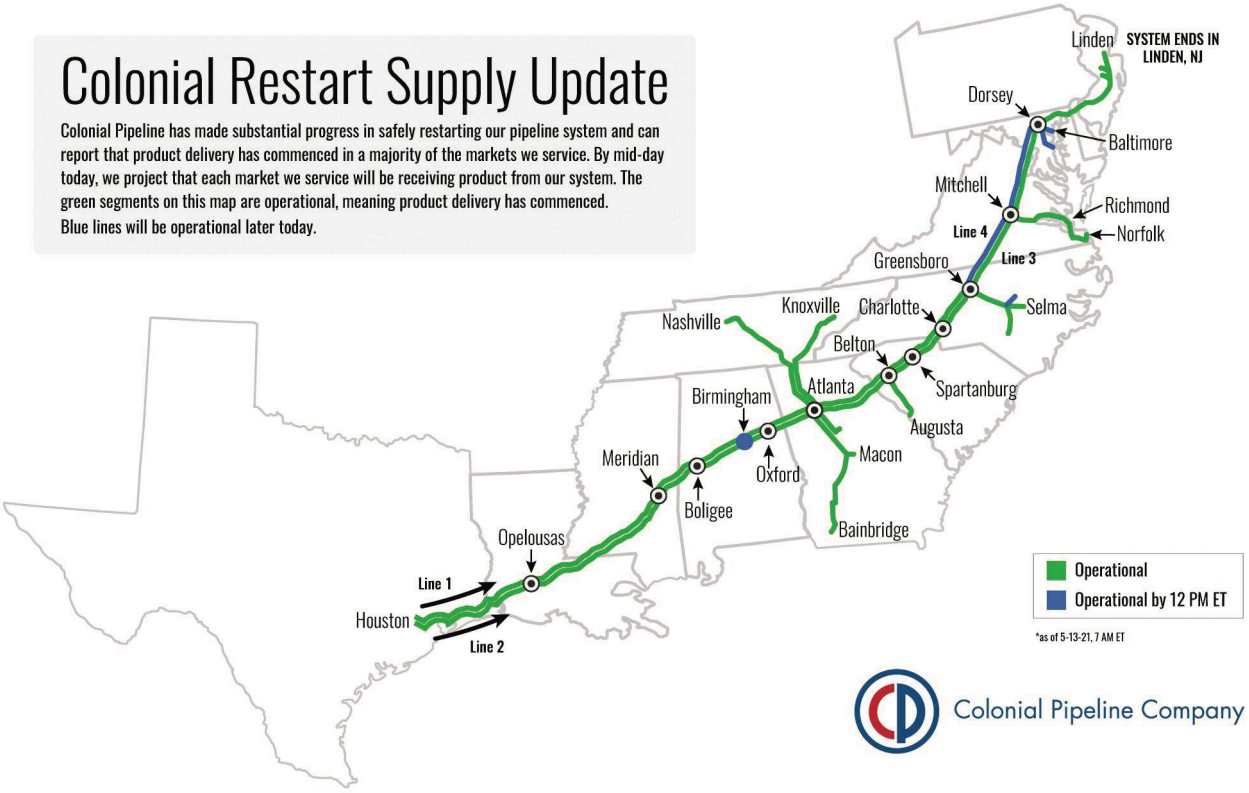
Auteurs : Jack Schafer, Marvin Karlins

1. Introduction

Alors que le stockage d'informations exclusives et confidentielles sur les ordinateurs des estreprised devient une pratique commerciale courante, le besoin de cybersécurité devient de plus en plus important [1] [2].

Ce besoin a été mis en évidence par les nombreuses failles de sécurité impliquant des multinationales bien connues du public, notamment Adobe, eBay, Equifax, LinkedIn et Yahoo [3] [4].

Lorsque des cas d'espionnage industriel dans de grandes entreprises américaines sont portés à la connaissance du public, la plupart des gens évoquent des images inspirées des films de Hollywood: des super-techno-geeks du darknet avec des dizaines d'ordinateurs et des dispositifs de piratage 'de type James Bond' et qui utilisent leurs connaissances supérieures et leurs inventions de pointe pour faire sauter les pare-feu et extraire les données qu'ils veulent.



Bien que ce moyen d'espionnage très sophistiqué existe, comme dans le cas de la récente attaque par ransomware contre Colonial Pipeline (le plus grand pipeline pétrolier des États-Unis), les mêmes résultats peuvent souvent être obtenus par des moyens beaucoup plus simples.

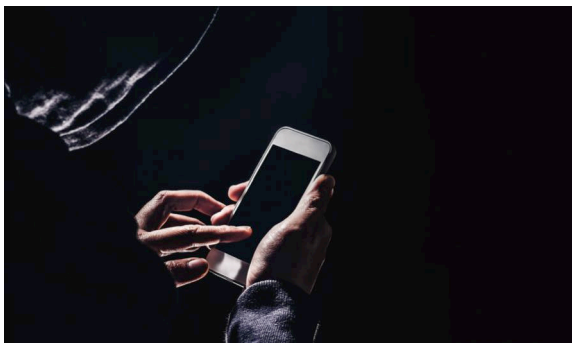
En fait, il suffit d'une personne, d'un téléphone portable, d'un logiciel facilement disponible et d'un plan d'action pour franchir les barrières de sécurité les plus avancées des entreprises et obtenir des informations commerciales exclusives.

Le but de cet article est de mettre en évidence, à travers un exemple concret,

1. l'importance de réaliser et de reconnaître que chaque individu dans une organisation peut être un portail pour une cyber-intrusion
2.
3. la nécessité de former correctement les individus pour qu'ils soient vigilants face aux cyber-escroqueries et se méfient de toute demande d'accès à un ordinateur.

2. Procédure

Pour montrer à quel point il est facile pour un pirate informatique malin d'accéder à des informations digitales, même lorsque ces données sont protégées par des mesures de cybersécurité avancées, nous fournissons ici un exemple de violation de données. Nous remercions Nathan House, expert en cybersécurité, de nous avoir fourni cet exemple révélateur d'espionnage d'entreprise. Son défi - en tant que pirate informatique en puissance - a été de s'introduire dans un réseau informatique sécurisé en utilisant uniquement son intelligence et un téléphone portable.



3. Résultats

L'objectif de Nathan est d'accéder à l'ordinateur d'une entreprise spécifique afin d'en extraire des informations auxquelles il n'aurait pas accès autrement. Il explique ci-dessous, étape par étape, ce qu'il fait et pourquoi il le fait (quelles informations il essaie d'obtenir).

Appel #1 : Au standard principal de l'entreprise

NATHAN : Bonjour, j'ai un problème avec mon téléphone de bureau. Pouvez-vous me passer quelqu'un qui pourrait me dépanner ?

STANDARDISTE : Je vous connecte.

SERVICE IT : Salut.

Bonjour. J'ai un problème avec mon téléphone de bureau. Désolé, je suis nouveau ici. Y a-t-il un moyen de savoir qui m'appelle quand on

appelle mon téléphone de bureau ? Y a-t-il une identification de l'appelant ?

SERVICE IT : Pas vraiment, car nous utilisons des hot desks ici. [Un hot desk est un bureau partagé par plus d'une personne, parfois plusieurs personnes durant les trois tours de travail quotidiens.] Comme les gens utilisent généralement leur téléphone portable, l'identification de l'appelant n'est pas souvent liée à un nom. Cela vous pose-t-il un problème ?

NATHAN : Non, c'est bon maintenant. Je comprends. Merci. Au revoir.

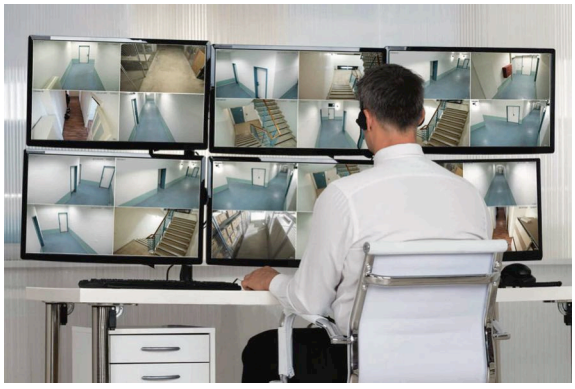
Je sais maintenant que l'entreprise utilise des hot-desks et que l'identification de l'appelant n'est pas toujours requise. Par conséquent, ce n'est pas un problème si j'appelle de l'extérieur de l'entreprise. Si l'identification était requise, je pourrais de toute façon la contourner.

Appel n°2 : vers le standard principal de l'entreprise

NATHAN : Bonjour, pouvez-vous me passer la sécurité du bâtiment ?

RÉCEPTIONNISTE : Ok.

BUILDING SECURITY : Bonjour, comment puis-je vous aider ?



NATHAN : Bonjour, je ne sais pas si cela vous intéressera, mais j'ai trouvé une carte d'accès à l'extérieur du bâtiment que quelqu'un a dû laisser tomber.

BUILDING SECURITY : Il suffit de nous le rendre. Nous sommes dans le bâtiment 3.

NATHAN : Ok, pas de problème. Puis-je demander à qui je parle ?

BUILDING SECURITY :: Mon nom est Eric Wood. Si je ne suis pas là, donnez-le à Neil.

NATHAN : Ok, c'est super. Je vais le faire. Etes-vous le chef de la sécurité du bâtiment ?

BUILDING SECURITY : Il s'agit en fait de la Sécurité des Installations, et son responsable est Peter Reed.

NATHAN : Ok, merci beaucoup. Bye.

Cet échange m'a permis de connaître le nom de quelques personnes du service de sécurité, le nom exact du département et du chef de la sécurité, et de savoir que ce sont eux qui s'occupent des cartes d'accès physique.

Appel n° 3 : vers le standard principal de l'entreprise

NATHAN : Bonjour, j'appelle de la part de Agency Group Associates et je me demande si vous pouvez m'aider. J'ai eu une réunion il y a environ un mois avec certains de vos employés des ressources humaines, mais malheureusement mon ordinateur est tombé en panne et j'ai totalement perdu leurs noms.

STANDARDISTE : Bien sûr, pas de problème. Laissez-moi regarder ce département. Avez-vous la moindre idée de leurs noms ?

NATHAN : Je sais que l'un d'entre eux était le chef des RH. Il y avait un certain nombre de personnes à la réunion, cependant.

STANDARDISTE : [Pause.] Ok, nous y sommes. Le chef des RH est Mary Killmister. XXX-XXXX.

NATHAN : Oui, ça me dit quelque chose. Quels sont les autres noms en RH ?»

STANDARDISTE : En RH, Jane Ross, Emma Jones...

NATHAN : Oui, définitivement Jane et Emma. Pourrais-je avoir leurs numéros, s'il vous plaît.»

STANDARDISTE : Bien sûr. Jane Ross est le XXX-XXXX et Emma Jones est le XXX- XXXX. Voulez-vous que je vous passe l'une d'entre elles ?

NATHAN : Oui. Pouvez-vous me passer Emma, s'il vous plaît ?

Je connais maintenant les noms des trois personnes des RH, y compris le chef de service.

Appel n°4 : Au département des ressources humaines de l'entreprise

RESSOURCES HUMAINES : Bonjour, Emma Jones.

NATHAN : Salut, Emma. C'est Eric de la sécurité des installations dans le bâtiment 3. Je me demandais si vous pouviez m'aider. Nous avons eu un problème ici avec l'ordinateur de la base de données des cartes d'accès. Il a planté la nuit dernière, et certaines des données des nouveaux employés ont été perdues. Savez-vous qui pourrait

nous dire qui étaient les nouveaux employés au cours des deux dernières semaines, car leurs cartes d'accès ne fonctionnent plus ? Nous devons les contacter et leur faire savoir dès que possible.

EMMA : Je peux vous aider avec ça. Je vais chercher les noms et vous les envoyer par e-mail si ça vous va. Pour les deux dernières semaines, avez-vous dit ?

NATHAN : Pour les deux dernières semaines, oui. C'est super, merci, mais est-ce que ça serait

Il n'a pas été possible de le faxer, car nous partageons un ordinateur pour le courrier électronique et celui-ci a également été affecté par la panne d'ordinateur.

EMMA : Oui, ok. Quel est votre numéro de fax ? Oh, et quel est votre nom déjà ?

Notez-le à l'attention d'Eric. Je vais devoir trouver le numéro de fax pour vous et vous rappeler.

EMMA : Ok.

NATHAN : Savez-vous combien de temps il vous faudra pour trouver l'information ?

EMMA : Ça ne devrait pas me prendre plus de trente minutes.

Pourrez-vous commencer à travailler dessus tout de suite ? C'est assez urgent.

EMMA : J'ai quelques choses à faire ce matin, mais je devrais avoir les noms cet après-midi.

NATHAN : C'est génial, Emma. Merci. Quand vous aurez terminé, pourriez-vous m'appeler tout de suite pour que je puisse commencer à réactiver leurs cartes ?

EMMA : Oui, bien sûr. Quel est votre numéro ?

NATHAN : Je vais vous donner mon numéro de portable. Comme ça tu seras sûre de me joindre. XXX-XXX-XXXX.

EMMA : Ok, bien sûr. Je vous appellerai quand j'aurai la liste.

NATHAN : Excellent. Merci. J'apprécie vraiment cela.

Appel n°5 : Au standard principal de l'entreprise

NATHAN : Bonjour. Pouvez-vous me passer le support informatique ?

RECEPTIONNISTE : Vous connecter... [Longue attente dans la file d'attente].

SUPPORT IT : Bonjour, puis-je avoir votre numéro d'identification ou la référence de votre dossier ?

NATHAN : J'ai juste une petite question. C'est bon ?

SUPPORT IT: Qu'est-ce que c'est ?

NATHAN : Un type de Reuters essaie de m'envoyer une présentation et me demande quelle est la taille maximale des pièces jointes.

SUPPORT IT: C'est 5 mégaoctets, monsieur.

NATHAN : C'est génial, merci. Oh, une dernière chose. Il a dit que c'était un fichier .exe et parfois ils sont bloqués ou quelque chose comme ça.

SUPPORT IT: Il ne pourra pas envoyer un fichier exécutable, car les scanners de virus l'arrêteront. Pourquoi faut-il que ce soit un fichier .exe ?

NATHAN : Je ne sais pas. Comment peut-il me l'envoyer, alors ? Il pourrait le zipper ou quelque chose comme ça ?

SUPPORT IT : Les fichiers Zip sont autorisés, monsieur.

NATHAN : Ok. Oh, une dernière chose : je n'arrive pas à voir l'icône de mon Norton Antivirus dans ma barre d'état système. Au dernier endroit où je travaillais, il y avait une petite icône.

SUPPORT IT: Nous utilisons McAfee ici. C'est juste une icône différente, la bleue.

NATHAN : Ça explique tout, alors. Merci. Au revoir.

Je sais maintenant que pour envoyer un exécutable par courrier électronique, il devra d'abord être zippé et peser moins de 5 Mo. Je sais également qu'ils utilisent l'antivirus McAfee.

Appel n°6 : Quelques heures plus tard, un appel d'Emma aux ressources humaines.

EMMA : Salut, c'est Eric ?

NATHAN : Oui, salut.

EMMA : J'ai la liste des nouveaux employés pour vous. Voulez-vous que je vous la faxe ?

NATHAN : Oui, s'il vous plaît. Ce serait génial. Combien y en a-t-il ?

EMMA : Environ dix personnes.

Je ne suis pas sûr que le fax fonctionne correctement ici. Pourriez-vous éventuellement

me les lire à haute voix ? Je pense que ça serait plus rapide.

EMMA : Ok. Vous avez un stylo ?

NATHAN : Oui, allez-y.

EMMA : Sarah Jones, Département des ventes. Le directeur est Roger Weaks... [lit le reste de la liste].

NATHAN : Ok, merci. Vous avez été d'une grande aide. Au revoir.

J'ai maintenant une liste des nouveaux employés des deux dernières semaines. J'ai également les départements auxquels ils appartiennent et les noms de leurs responsables. Les nouveaux employés sont beaucoup plus sensibles à l'ingénierie sociale (influence ou contrôle par une source extérieure) que les employés de longue date.

Appel n° 7 : Au standard principal de l'entreprise

NATHAN : Bonjour, j'essaie d'envoyer un e-mail à Sarah Jones mais je ne suis pas sûr du format de vos adresses e-mail. Est-ce que vous le savez ?

STANDARDISTE : Oui. Ce serait sarah.jones@targetcompany.com.

NATHAN : Merci.

Email d'ingénierie sociale

Quelques minutes plus tard, un courriel usurpé [message électronique avec une fausse adresse d'expéditeur] est envoyé.

De : itsecurity@targetcompany.com.
À : sar.jones@targetcompany.com.
Sujet : Sécurité informatique.

Chère Sarah,

En tant que nouvel employé de l'entreprise, vous devrez être informée des politiques et procédures de sécurité informatique de l'entreprise et, plus particulièrement, de la «Politique d'utilisation raisonnable» à appliquer par tout employé.

L'objectif de cette politique est de définir une utilisation raisonnable de l'équipement informatique de [l'entreprise cible]. Ces règles sont en place pour protéger l'employé et [l'entreprise cible]. Une utilisation inappropriée présente des risques, notamment des attaques de virus, la compromission des systèmes et services du réseau et des problèmes juridiques.

Cette politique s'applique aux employés, contractants, consultants, intérimaires et autres travailleurs de [société cible], y compris tout le personnel affilié à des tiers. Cette politique s'applique à tous les équipements détenus ou loués par la société cible].

Quelqu'un vous contactera prochainement pour en discuter avec vous.

Salutations, Sécurité informatique

Appel n°8 : Quelques heures plus tard, un appel au standard principal de l'entreprise.

Bonjour. Pourriez-vous me passer Sarah Jones, s'il vous plaît ?

STANDARDISTE : Je vous connecte.

SARAH : Bonjour. Département des ventes. En quoi puis-je vous aider ?

NATHAN : Salut, Sarah. J'appelle de la part de la sécurité informatique pour vous informer des meilleures pratiques en matière de sécurité informatique. Vous devriez avoir reçu un e-mail à ce sujet.

SARAH : Oui, j'ai reçu un courriel à ce sujet aujourd'hui.

NATHAN : Ok, excellent. C'est juste une procédure standard pour tous les nouveaux employés et ça ne prend que 5 minutes. Comment trouvez-vous les choses ici ? Tout le monde vous aide ?

SARAH : Oui, merci. C'est génial. C'est un peu intimidant de commencer quelque chose de nouveau, cependant.

NATHAN : Oui, et c'est toujours difficile de se souvenir du nom de chacun. Roger vous a-t-il présenté ? [Le bavardage est destiné à établir une relation entrecoupée de confiance]. Emma Jones est très gentille aux RH si vous avez besoin d'aide de ce côté-là.

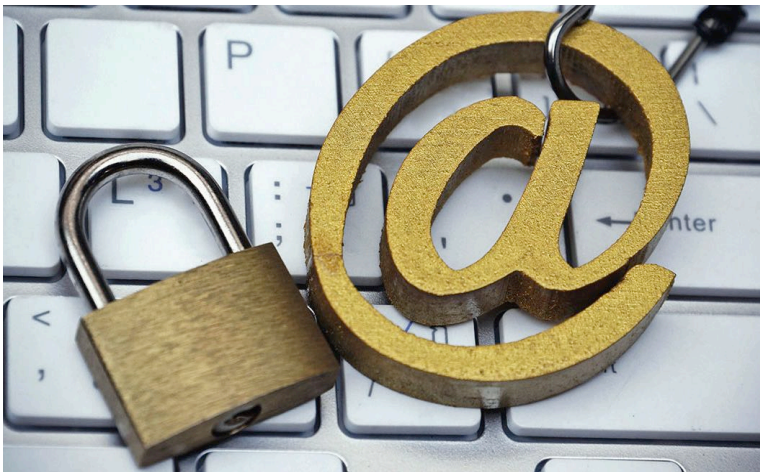
SARAH : Oui, Emma a fait mon entretien avec les RH pour le poste.

NATHAN : Bien, je ferais mieux de parcourir la présentation de la sécurité avec toi. Est-ce que tu as ton email ouvert ? Je vais t'envoyer la présentation de la sécurité maintenant et je pourrai t'en parler.

SARAH : Ok, je vois l'email.
NATHAN : Ok, il suffit de double-cliquer sur la pièce jointe .zip de la présentation sur la sécurité.
SARAH : Okay....

L'exécutable qu'elle a exécuté est, en fait, une série de scripts et d'outils astucieusement emballés, créés par notre programme d'encapsulation, qui comprend le RAT (programme malveillant d'accès à distance utilisé pour prendre le contrôle d'un ordinateur), un rootkit (qui permet d'accéder à un ordinateur tout en cachant son existence), un keylogger (qui enregistre les frappes sur le clavier de l'ordinateur) et tout ce que je pourrais vouloir ajouter.

Lorsque Sarah clique sur le fichier, la présentation démarre immédiatement. Il s'agit simplement d'une série de diapositives PowerPoint lui indiquant de ne pas exécuter les exécutables qu'on lui envoie, etc. et d'autres bonnes pratiques de sécurité.



La présentation est marquée de tous les logos de l'entreprise qui ont été commodément copiés depuis leur serveur web public, juste pour ajouter un peu plus de confiance. Quelques secondes plus tard, alors qu'elle suit la présentation, des scripts contenus dans le paquet commencent à essayer de désactiver McAfee et toute autre sécurité informatique susceptible de protéger l'utilisateur. Ensuite, le rootkit s'installe, cachant toutes les actions futures du système d'exploitation ou de toute personne effectuant une enquête médico-légale.

Ensuite, le RAT est caché et installé. On fait en sorte que le RAT démarre à chaque fois que la machine redémarre, et ces actions sont toutes cachées par le rootkit.

Le RAT recherche ensuite les paramètres de proxy et d'autres informations utiles et tente de sortir du réseau et de se connecter à Internet, prêt à recevoir les commandes de son maître. Évidemment, tous les processus et toutes les connexions TCP (Transmission Control Protocol) sont cachés et même l'exécution d'éléments tels que netstar (statistiques réseau) et le gestionnaire de tâches (procédures qui peuvent être utilisées pour détecter les manipulations informatiques non autorisées) ne les révélera pas.

Le RAT se connecte au maître. Je possède maintenant le PC et il est temps de commencer à regarder autour de moi et de vraiment commencer à pirater ! Le travail est terminé.

BIO

Le Dr John R. «Jack» Schafer est un agent spécial du FBI à la retraite, actuellement professeur associé à la Western Illinois University. Le Jack Schafer a été analyste comportemental, détaché au programme d'analyse comportementale de sécurité nationale du FBI, où il a développé bon nombre des idées présentées dans son livre "The truth detector". Le Dr Schafer a obtenu un doctorat en psychologie à la Fielding Graduate University de Santa Barbara, en Californie. Il possède sa propre société de conseil et donne des conférences et des consultations en Amérique et à l'étranger. Il est l'auteur d'un livre intitulé Psychological Narrative Analysis : A Professional Method to Detect Deception in Written and Oral Communications. Il a également coécrit le volume Advanced Interviewing Techniques : Proven Strategies for Law Enforcement, Military, and Security Personnel. Il a publié de nombreux articles sur un large éventail de sujets, notamment la psychopathologie de la haine, l'éthique dans l'application de la loi, la détection de la tromperie et les principes universels du comportement criminel. Le dernier livre coécrit par M. Schafer est le best-seller The Like Switch : An Ex-FBI Agent's Guide to Influencing, Attracting, and Winning People Over.

BIO

Le Dr Marvin Karlins a obtenu son doctorat en psychologie sociale à l'université de Princeton. Il est actuellement professeur titulaire de gestion au Muma College of Business de l'université de Floride du Sud. Le Dr Karlins consulte dans le monde entier et, pendant vingt ans, il a formé tout le personnel opérationnel de Singapore Airlines. Il a publié 30 livres et plus de 150 articles dans des revues professionnelles, universitaires et populaires. Plusieurs de ses livres coécrits sont devenus des best-sellers internationaux, notamment What Every BODY Is Saying : An Ex-FBI Agent's Guide to Speed-Reading People et The Like Switch : An Ex-FBI Agent's Guide to Influencing, Attracting, and Winning People Over. Son dernier livre, coécrit avec Tony March, s'intitule Paying It Backward : How a Childhood of Poverty and Abuse Fueled a Life of Gratitude and Philanthropy, et a été publié en 2020. M. Karlins est membre de la Guilde des auteurs et de la Fédération internationale des journalistes.

4. Discussion

Les auteurs espèrent qu'en lisant l'exemple qui vient d'être fourni, décrivant la prise de contrôle calculée, étape par étape, du système informatique d'une entreprise cible, les employés à tous les niveaux de la hiérarchie d'une organisation seront plus conscients (et reconnaîtront) comment

1. des morceaux d'informations apparemment inoffensives et faciles à obtenir peuvent être utilisés à des fins malveillantes ;
2. l'établissement d'un rapport de confiance avec une personne peut la rendre plus susceptible de devenir un co-conspirateur à son insu dans une entreprise d'espionnage ; et
3. il faut être constamment vigilant pour ne pas donner des informations sans examiner soigneusement l'authenticité et la justification de la source qui les demande.

Lorsque nous enseignons à nos étudiants - que ce soit à l'Académie du FBI ou à l'École de commerce - nous leur présentons toujours une citation qui leur rappelle le rôle qu'ils jouent dans la protection des informations nationales et/ou d'entreprise : «*Les informations confidentielles peuvent être protégées dans des coffres verrouillés, derrière une série de barrières physiques et électroniques. Le maillon le plus faible de toute chaîne de sécurité est l'homme. Une fois qu'une serrure est verrouillée, elle ne se déverrouille pas d'elle-même... mais une langue liée se dénoue facilement.*» Ce commentaire est suivi de cette observation : «*Chaque fois que quelqu'un vous fait participer à une conversation - en particulier lorsqu'il cherche à obtenir des informations - ne passez pas en mode «réponse automatique» ! Réfléchissez à tout motif caché que la personne qui vous parle pourrait avoir au fur et à mesure que le dialogue se déroule. Soyez prudent lorsque vous donnez des informations, en particulier les types de données qui pourraient être utilisées pour le vol d'identité ou l'espionnage d'entreprise, et rappelez-vous que l'élément d'information que vous donnez peut sembler insignifiant, mais que, combiné à d'autres éléments, il peut être la pièce essentielle qui permet de reconstituer l'ensemble du puzzle*» [5].

5. Conclusion

Les informations présentées dans cet article illustrent comment des bribes d'informations, soigneusement et astucieusement collectées, peuvent conduire à une violation majeure de la sécurité du réseau informatique d'une organisation. Il vise à donner au lecteur un éclaircissement préalable sur le fonctionnement d'un tel processus, afin de réduire le risque qu'il se produise à l'avenir. ■

[1] Brooks, C.J., Grow, C., Craig, P. et Short, D.D. (2018) Cybersecurity Essentials. Sybex, Hoboken. https://doi.org/10.1002/9781119369141
[2] Sai, H. (2019) Next Level Cyber Security. Leader's Press, Santa Barbara.
[3] Swinhoe, D. (2021) The 15 Biggest Data Breaches of the 21st Century. https://www.csoonline.com/
[4] Daswani, N. et Elbayadi, M. (2021) Big Breaches : Leçons de cybersécurité pour tous. Apress, New York, États-Unis. https://doi.org/10.1007/978-1-4842-6655-7
[5] Schafer, J. et Karlins, M. (2020) The Truth Detector. Simon & Schuster, New York, États-Unis.

Menaces intérieures : profilage et détection.

Auteur : Battista Cagnoni

«Tout est question de confiance» pourrait-on dire. La majorité des activités et des interactions humaines sont basées sur la confiance.

Nous faisons confiance à ceux qui ont construit et mis en place le système des sémaphores routiers. Nous ne pouvons pas vérifier que lorsque nous voyons du vert sur notre chemin en roulant à 80 km/h, tous les autres ont du rouge et ne bougent pas. De même, nous faisons confiance au chef du restaurant qui prépare notre repas en utilisant de bons ingrédients et rien de nuisible pour notre santé. Nous ne pouvons pas nous introduire dans la cuisine et inspecter personnellement ce qui s'y passe.

BIO

Battista Cagnoni, Senior Consultant, Advisory Services, EMEA auprès de Vectra, est un expert en sécurité, bénéficiant d'une longue expérience dans des domaines différents de l'industrie, où il a assuré les postes de Security engineer, Security Analyst ou encore SOC Lead. Il est passionné de la culture de la cyber-sécurité, de la prise de conscience dans ce domaine et de la compréhension des méthodologies à suivre pour faire face aux problèmes de sécurité. Il partage constamment ses connaissances, offrant des conseils et des processus au plus haut niveau, aidant les CISO qui réfléchissent à la manière de renforcer et d'atteindre un haut degré de maturité dans le cadre des opérations de sécurité. Battista détient les certification GIAC de Forensic Analyst et d'Incident Handler ainsi que les certificats d'Expert CISSP, GCFA, GCIH.

De la même manière, nous faisons confiance aux membres de notre entourage professionnel, nous faisons confiance à ceux que nous embauchons en leur donnant accès à des informations confidentielles et à la propriété intellectuelle, si essentielle pour l'entreprise.

Cela représente un risque commercial et les organisations qui ont rejoint un haut degré de maturité savent très bien où le bât blesse, mais en même temps, qu'il s'agit là d'un des problèmes les plus difficiles à résoudre.

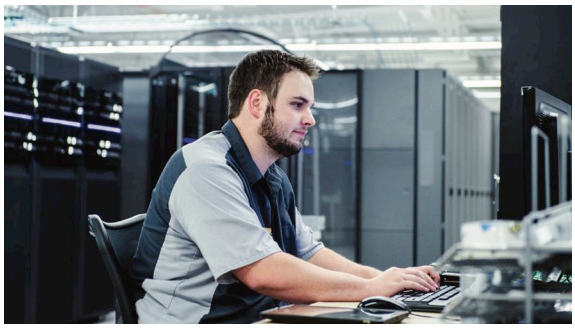
Les opérations de sécurité articulent leurs activités autour des personnes, des processus et de la technologie et, si un bon équilibre entre ces trois composantes est judicieux, efficace et nécessaire en ce qui concerne les menaces externes, il est encore plus nécessaire et doit être poussé à la limite des ses capacités pour ce qui relève de la détection des menaces internes.

Mais qui est une menace interne ?

Si l'on consulte l'un des meilleurs ouvrages à ce jour, le livre Blanc d'Eric D. Shaw et Harley V. Stock[1], on soulignera ici les conclusions les plus intéressantes de cette étude :

À l'interne, Les voleurs de propriété intellectuelle occupent plus souvent des postes techniques.

La majorité des vols de propriété intellectuelle sont majoritairement commis par des employés de sexe masculin, avec une moyenne d'âge de 37 ans, occupant principalement des postes techniques, notamment des ingénieurs ou des scientifiques, des gestionnaires, des vendeurs et des programmeurs. La majorité des voleurs de propriété intellectuelle avaient signé des accords de propriété intellectuelle, ce qui indique que des règles seules, sans une bonne compréhension de la part des employés et une bonne mise en application, se révèlent inefficaces.



À l'interne, généralement, les voleurs de propriété intellectuelle ont déjà trouvé un nouveau travail.

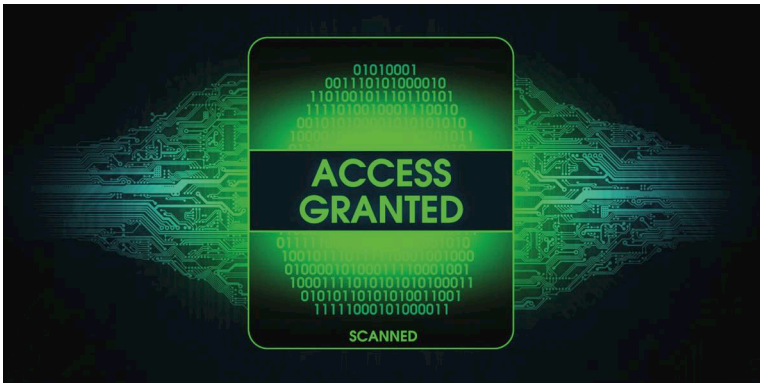
Environ 65 % des employés qui commettent un vol de propriété intellectuelle ou un délit d'initié ont déjà accepté un poste dans une entreprise concurrente ou ont créé leur propre entreprise au moment du vol. Environ 25% ont été recrutés par une personne extérieure qui avait ciblé les données qu'elle désirait obtenir d'eux et environ 20% des vols impliquent une collaboration avec un autre «ennemi intérieur».

À l'interne, les voleurs de propriété intellectuelle volent le plus souvent ce à quoi ils sont autorisés à accéder.

Les sujets s'emparent des données qu'ils connaissent, avec lesquelles ils travaillent et auxquelles ils ont souvent l'autorisation d'accès. En fait, 75 % d'entre eux ont volé du matériel auquel ils avaient un accès dûment autorisé. Cela complique la capacité d'une organisation à protéger sa propriété intellectuelle par des contrôles techniques et confirme la nécessité d'accords contraignants avec les employés sur quelles parties de la «propriété intellectuelle» leur revient ou non s'ils quittent leur poste.

À l'interne, les secrets commerciaux sont le type de propriété intellectuelle le plus souvent dérobé.

Les secrets commerciaux constituent 52% des cas de vols. Dans 30 % des cas, il s'agit d'informations commerciales telles que les données de facturation, listes de prix et autres données administratives; dans 20 % des cas, les code source, dans 14 % des cas, les logiciels propriété de l'entreprise, dans 12 % des cas,



les informations sur les clients et enfin, dans 6% des cas, les stratégies d'affaires.

À l'interne, les voleurs utilisent des moyens techniques pour voler la propriété intellectuelle, mais ils sont découverts par des employés non techniques.

La majorité des voleurs (54 %) ont utilisé un courrier électronique du réseau de l'entreprise, un canal d'accès à distance au réseau ou encore un transfert de fichiers partant de ce même réseau pour exfiltrer les données volées. Cependant, la plupart des vols de propriété intellectuelle commis

par des employés ont été découverts par des collègues appartenant aux services non techniques plutôt que par ceux qui travaillent dans le secteur IT de l'entreprise.

Les échecs professionnels peuvent inciter les initiés à envisager de voler la propriété intellectuelle de l'entreprise.

Dans le cadre des vols commis à l'interne, on remarque une accélération vers le passage à l'acte lorsque l'employé en a assez d'y «penser» et décide d'agir ou est sollicité par d'autres pour ce faire. Cette démarche intervient souvent à la suite d'un événement perçu comme un échec professionnel ou dans le cas d'attentes non satisfaites. Cette démarcation entre l'intention et l'action explique pourquoi certains vols d'initiés semblent être spontanés, alors qu'ils ne le sont pas.

Après avoir dressé le profil de la menace interne typique, examinons comment aborder ce risque et les mesures d'atténuation possibles. Le CISA propose une approche intéressante. Dans la section de son site Web consacrée à la sécurité des infrastructures[2], on trouve la description du concept de «*People as Sensor*».

«Le personnel d'une organisation constitue la composante humaine de la détection et de l'identification d'une menace interne. Les collègues de travail, les pairs, les amis, les voisins, les membres de la famille ou les observateurs occasionnels sont souvent en mesure de comprendre et de connaître les prédispositions, les facteurs de stress et les comportements d'un employé qui pourrait envisager des actes malveillants. Lorsque l'on observe le comportement humain, il faut garder à l'esprit deux qualités importantes :

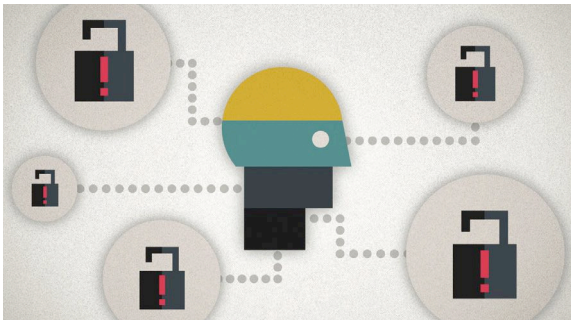
Savoir écouter l'autre personne à travers l'ensemble de ses critères de référence, pas les vôtres. Ne pas supposer que quelqu'un va demander de l'aide ou demander à être stoppé, ou qu'il va parler de ses intentions de la même manière que vous pourriez le faire.

Savoir écouter l'autre personne avec vos yeux. Les gens révèlent souvent leurs intentions par des moyens non verbaux.»

Il existe également une série d'indicateurs qui méritent d'être mentionnés car ils approfondissent le contexte et indiquent de précieux détails qui permettent de déceler des signes qu'il existe une menace interne.

- **Les indicateurs personnels** sont constitués par une combinaison de prédispositions et de facteurs de stress personnels qui affectent, à un moment précis, un employé qui peut devenir une menace ou passer à l'acte.
- **Les indicateurs de parcours professionnels** sont constitués par des événements qui se sont produits avant qu'une personne ne soit embauchée par une organisation ou avant qu'elle n'obtienne l'accès au réseau de l'organisation.
- **Les indicateurs comportementaux** sont des actions directement observables par les pairs, le personnel des ressources humaines, les supérieurs directs et la technologie. Au fil du temps, les comportements constituent un fil rouge d'activités à partir du quel certains changements peuvent être considérés comme un indicateur de menace.
- **Les indicateurs techniques** impliquent une activité du réseau et de l'utilisateur et nécessitent une application directe de systèmes et d'outils informatiques pour être détectés.
- **Indicateurs organisationnels/environnementaux :**
  - Les politiques de l'entreprise et les pratiques culturelles peuvent jouer un rôle important dans la création ou la gestion d'une menace interne.
  - Les facteurs environnementaux peuvent intensifier ou atténuer les facteurs de stress susceptibles de contribuer aux changements de comportement et à la progression d'un individu de l'état d'employé de confiance à celui de menace interne. Ces facteurs sont souvent liés aux politiques organisationnelles et aux pratiques culturelles.
- **Les indicateurs de violence** sont des comportements spécifiques ou des ensembles de comportements susceptibles d'inspirer la peur ou de susciter l'inquiétude faisant qu'une personne puisse passer à l'acte ; ces comportements comprennent, entre autres, l'intimidation, le harcèlement et les brimades.

Enfin, il est important de mentionner qu'avec l'évolution des technologies d'intelligence artificielle, comme le *machine learning,* il est possible de combiner l'approche comportementale avec des outils techniques comme

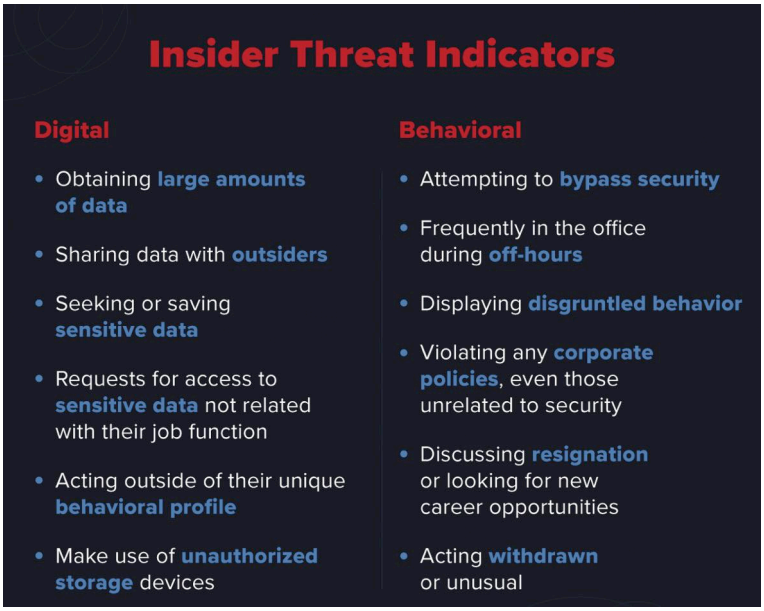


les métadonnées du réseau ou de l'utilisateur. Cela permet d'accélérer le processus de détection selon plusieurs ordres de grandeur.

Qu'il s'agisse d'un comportement de type *«Smash and Grab»* ou *«Slow bleeding»,* l'intelligence artificielle sera capable de générer des indicateurs utiles à partir du *«noise»* (ensemble des données) du flux du réseau de l'entreprise.

La combinaison de différents types d'indicateurs peut également créer une valeur ajoutée et améliorer ainsi la préparation d'une entreprise contre les menaces internes.

Un exemple que nous avons vu récemment est celui d'un employé qui démissionne et qui, pendant la période de préavis, commence à collecter et à exfiltrer des données. Dans ce scénario spécifique, la combinaison d'indicateurs non techniques - la démission - avec une approche de chasse aux menaces - recherche d'anomalies dans les métadonnées du réseau - peut être très bénéfique. ■



1 Eric D. Shaw, Harley V. Stock, BehavioralRiskIndicators of MaliciousInsider Theft of IntellectualProperty: Misreading the Writing on the Wall, Symantec 2011 (https://static1.squarespace.com/static/596a623ba5790afcec9c024e/t/59c9e063a803bb62117213c0/1506402404657/Symantec+Malicious+Insider+Whitepaper+FINAL2.pdf)
2 https://www.cisa.gov/detecting-and-identifying-insider-threats

SOLUTIONS

Rénover la cybersécurité.

Auteur : Gérald Vernez

Les défis de la mutation digitale[1], en particulier les risques liés, augmentent sans cesse. L'ampleur de cette évolution pour la société réclame un changement de posture et d'instruments, une action en profondeur où chacun est conscient de ses responsabilités et en mesure de les assumer à son échelon. L'approche proposée dans cette courte contribution repose sur trois méthodes, holistique, systémique et en réseau et trois piliers, l'anticipation, la responsabilité et l'action. Il s'agit ainsi de mutualiser les capacités et de réellement rendre la cybersécurité accessible aux petites structures.

Même si on ferme les yeux, le temps est à l'orage

Consulter un dictionnaire au sujet du mot *«paix»* en dit long sur l'humanité: *«absence de guerre»*. En tout cas, depuis le 24 février, ceux qui avaient rêvé d'une Europe pacifiée après la chute du mur de Berlin ont été contraints de réviser leurs attentes. Oui, l'espèce humaine est incapable de penser en dehors du prisme de la compétition, de la conquête et de la destruction et il y aura toujours quelqu'un pour s'approprier ce que vous possédez ou pour essayer de vous dépasser.

Le cyberespace ne fait pas exception et les délits contre ou au moyen de celui-ci, affranchis de la contrainte des formes classiques de la criminalité (distances, temps, risques, etc.) progressent rapidement et permettent des gains substantiels à leurs auteurs. En face des activistes, criminels, espions, saboteurs… acteurs agiles, collaboratifs et opportunistes, on trouve des dispositifs de sécurité souvent inexistants (au niveau des petites structures), inadaptés, inefficaces et compartimentés ou encore soumis à un contrôle démocratique et juridique étroit.

Ainsi, le score du match entre la société et la face obscure du cyber penche largement en faveur de cette dernière ainsi que des nations[2] qui ont par exemple inscrit le vol de propriété intellectuelle dans leur stratégie ou qui n'hésitent plus à y faire également la guerre. Tous ces acteurs ont fort bien compris que la digitalisation fait du monde une cible facile et un gigantesque self-service[3]. Malgré le coût des dommages[4] et les nombreux avis de tempête et la guerre en Ukraine, il faut malheureusement constater que nous n'avons pas encore réussi à cesser de faire semblant et de nous mentir.

Corriger la posture et élargir la focale

Lorsque les patrons de l'ANSSI en France[5] ou du NCSC en Suisse[6] informent certaines entités exposées aux cyberrisques, leur comportement indifférent et irresponsable – alors qu'ils sont assis sur des bombes – laisse songeur.

Récemment, un entrepreneur alerté à deux reprises pour sa vulnérabilité a ainsi répondu: *«je n'ai pas le temps pour ça»*. La troisième fois c'est lui qui appelait au secours…! Frustrant lorsque des incidents appartiennent à la catégorie apparemment plutôt nombreuse des *«aurait pu facilement être évité»*.

BIO

Gérald Vernez a étudié la géologie, la météorologie et la politique de sécurité. Après une première carrière d'ingénieur et de gestionnaire de risques dans l'industrie, il a rejoint l'état-major général de l'armée suisse en 1996. Il a préparé et entraîné l'état-major de crise de la Confédération pour le passage à l'an 2000 (Y2K), planifié l'organisation du commandement (Command & Control) de l'armée, puis développé le domaine des opérations d'information. Chef d'état-major de l'état-major de conduite de l'armée de 2009 à fin 2010 il a ensuite été directeur adjoint pour l'élaboration de la première stratégie nationale pour la protection de la Suisse contre les cyberrisques avant de devenir en 2013 Délégué du chef de l'armée pour la cyberdéfense puis, dès 2016, Délégué pour la cyberdéfense du Département fédéral de la Défense (DDPS). Depuis 2021 Gérald Vernez dirige la Fondation digiVolution (www.digivolution.swiss), une nouvelle force de réflexion et d'action stratégique.

En Suisse, les entreprises du secteur de l'électricité annonçaient même en 2021 une maturité moyenne de cybersécurité en dessous de 1[7] sur une échelle de 0 à 4. Si le 42ème rang[8] attribué à la Suisse par l'UIT dans son index global 2020 est certainement en partie immérité et dû à l'absence de réponse de la Suisse à son enquête, il apparaît que malgré ses talents de premier plan et ses importants moyens, à maints endroits notre pays peine encore à saisir les enjeux et a besoin d'un vigoureux changement de posture.

Depuis une quinzaine d'années, avec la cyberattaque contre l'Estonie (2007), celle subie par le secteur nucléaire iranien (Stuxnet, 2010), les révélations de Snowden (2013) ou encore les attaques contre les infrastructures électriques ukrainiennes (2015, 2016), la cybersécurité a considérablement gagné en importance.

Pour l'OTAN et l'Union Européenne un événement grave serait même susceptible de justifier le déclenchement des mécanismes ultimes de défense. Après la terre, la mer, le ciel, les domaines électromagnétique et informationnel et enfin l'espace exo-atmosphérique, les armées rivalisent désormais dans le cyberespace et les commandements cybernétiques se multiplient.

Un développement logique, mais entre toutes ces sphères d'opération, il y a un «*mais*» de taille. En effet, le cyber est la seule dimension présente au cœur de toutes les autres dès leur conception. Considérer donc le cyber sous le seul angle technique, des menaces et

des geeks est à l'évidence réducteur. Sa focale doit être considérablement élargir.

Il est simple de dire «*je veux une cyberdéfense*», mais de quoi dépend une telle capacité pour être installée et exploitée durablement? De personnel, de matériel, d'infrastructures, de textes de lois, de finances, etc. qui proviennent tous d'une chaîne complexe de capacités, compétences, procédures, etc.

Avec le COVID, la guerre en Ukraine, la dispute américano-chinoise sur les terres rares, les avertissements du ministre suisse de l'Économie quant aux prochaines pénuries d'électricité et les nombreux événements observés durant les 18 derniers mois[9], il est désormais clair que la liste des domaines à prendre en considération pour appréhender correctement et à temps la mutation digitale, ses défis et les mesures pour les maîtriser doit impérativement être élargie.

Le kaléidoscope de la mutation digitale et trois recommandations clés

Les constats qui précèdent (pas de pause chez les malveillants, besoin d'un changement de posture chez les défenseurs et élargir la focale) ont présidé à la création de la fondation *digi*Volution[10] en 2020. Fondée par les membres de l'ancien groupe d'experts qui a forgé la cyberdéfense suisse, cette nouvelle institution à but non lucratif[11] inscrit son action stratégique dans une vision d'idéal et de neutralité au service des décideurs à tous les niveaux. Ainsi est né un observatoire chargé de cartographier tous les éléments de «*l'équation digitale*» de notre monde VUCA[12] et de comprendre

Cartographie © digiVolution

la nature et les interactions complexes de l'ensemble des «*tuiles*» de la figure ci-après, dans une approche holistique, systémique et en réseau.

La méthode de digiVolution se voit aussi dans les petites phrases qui jalonnent son message: «*prepare for the next*», «*quel est le prix de l'inaction et du manque d'anticipation*» ou encore «*notre ambition: des effets sur le terrain. Et vite !*». Derrière ces énoncés se cachent trois recommandations très claires:

- **Anticipation** – Ne pas être prêt à temps alors que toutes les données sont disponibles n'est pas une attitude acceptable; c'est tout simplement de la négligence et en droit suisse[13], c'est d'ordre pénal.
- **Responsabilité** – Dans un monde interdépendant, les risques qu'une entité accepte peuvent entraîner des conséquences pour d'autres; ainsi, une entreprise qui ne se protège pas s'expose à la faillite et à mettre ses employés au chômage.
- **Action** – Les plans et stratégies sont bien entendu nécessaires, mais il s'agit d'abord de mettre en œuvre des mesures de cyberhygiène – simples, disponibles auprès des autorités et des prestataires spécialisés et applicables de suite – et ainsi de créer sans délai des effets mesurables pour la sécurité de tous.

Conclusion

Les États et les grandes entreprises disposent généralement de moyens conséquents pour maîtriser les défis de la mutation digitale, mais ce n'est pas le cas des microentreprises (moins de 10 employés, 90% des entreprises et 25% des emplois en Suisse) et des individus.

Ces catégories ne disposent que rarement du temps, de l'argent et des compétences pour, en plus de tout le reste, s'occuper aussi de cette dimension.

C'est donc aux solutions d'aller à leur rencontre et de leur offrir, vite et à un coût négligeable, l'*empowerment* dont ils ont un urgent besoin. Les «*je n'ai pas le temps pour ça*» doivent disparaître.

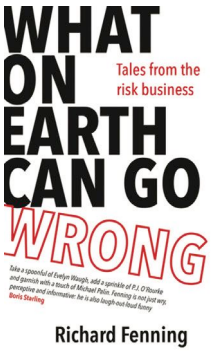
Veillons cependant à ce que cela ne se fasse pas via la plateformisation à outrance promue par les géants technologiques et ainsi, de manière irréversible, au détriment des questions cruciales de souveraineté, de l'individu à l'État. ■

1 Ce terme signifie une modification en profondeur et irréversible, comme en biologie lorsque des poissons sont sortis des premiers océans il y a des milliards d'années et changé leurs branchies en poumons pour vivre grâce aux différents gaz qui composent l'atmosphère.
2 https://www.csis.org/analysis/put-chinas-intellectual-property-theft-larger-context
3 https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/
4 https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-220-Milliarden-Euro-Schaden-pro-Jahr
5 https://www.lemagit.fr/actualites/252503454/Anssi-trop-dorganisations-ignorent-les-alertes-qui-leurs-sont-adressees
6 https://www.ncsc.admin.ch/ncsc/en/home/aktuell/im-fokus/2022/schwachstelle-exchange-server-5.html
7 https://pubdb.bfe.admin.ch/fr/publication/download/10524
8 https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf
9 digiVolution a constamment assuré un suivi de situation et son analyse. Ces travaux sont disponibles sous https://www.digivolution.swiss/dv-blog/
10 La Fondation (institution sans but lucratif) est un observatoire de l'espace digital au service des décideurs politiques, économiques et académiques, auxquels elle propose analyses, conseils et formations. Elle contribue au dialogue public et politique en Suisse sur le sens et la sécurité de la société digitale.
11 Qui on l'espère fera des émules dans de nombreux pays.
12 https://hbr.org/2014/01/what-vuca-really-means-for-you
13 https://www.fedlex.admin.ch/eli/cc/54/757_781_799/en

Les racines de la résilience sont dans les gênes de la famille.

Auteur : **Luca Tenzi**

Au cours de la dernière décennie, de nombreux articles ont été écrits sur la résilience et sur la manière dont les entreprises ont appris à gérer, ou à surfer sur la crise et à rebondir. L'empreinte mondiale des entreprises s'est étendue, tout comme les risques auxquels elles sont confrontées quotidiennement.



En référence au livre de Richard Fenning, *«What on earth can go wrong ?»*, nous pouvons faire allusion aux disruptions prolongéees de chaînes d'approvisionnement, aux interdépendances technologiques, aux vulnérabilités informatiques, aux virus mutants, aux turbulences géopolitiques, à l'anémie économique mondiale et même aux phénomènes météorologiques ou terrestres, à savoir un ensemble d'évenements combinés qui constitue un environnement d'affaires de type VUCA *(volatilité, incertitude, complexité et ambiguïté)*.

Mais la résilience n'est pas une invention de la nouvelle économie, ni de l'industrie 4.0 ou de la culture des start-up. La résilience est dans le gène unique, les racines solides des familles d'entrepreneurs et de fabricants qui, génération après génération, ont su transmettre les clés du royaume à la génération suivante.

Des entreprises comme la Fabbrica d'Armi Pietro Beretta S.p.A., dont le siège se trouve à Gardone Val Trompia, une petite vallée du nord de l'Italie, est si éloignée du bruit de n'importe quelle ville métropolitaine qu'elle fait oublier au visiteur sa présence mondiale et sa réputation renommée. Fondée en 1526, couvrant 500 ans d'histoire, dirigée par les 16 générations de la même famille, cette entreprise a été témoin de l'histoire du monde. Un exemple primordial de résilience et d'adaptabilité dans cinq siècles d'histoire mondiale.

Pietro Beretta (1870-1957), l'homme qui a fait de Beretta un des leaders mondiaux dans son domaine et de la Fabbrica d'Armi en 1960 © Beretta.com

Si 500 ans avec la même famille est peut-être un record mondial, il existe des milliers d'entreprises dans le monde, créées il y a deux, trois ou quatre générations, qui sont toujours gérées par la famille. La résilience, c'est la capacité inégalée des anciens d'une famille de savoir transmettre l'entreprise à la génération suivante, tout en laissant aux jeunes une faculté enracinée d'adaptation, propre à affronter les changements specifiques à leur époque, et ce qu'il s'agisse d'un restaurant, d'une usine de motos ou d'une manufacture de montres de luxe. La résilience est donc une affaire de famille.

BERETTA
500 YEARS. ONE PASSION.

Mais les dirigeants de l'entreprise 4.0 ont perdu ce concept générationnel, la résilience 4.0 étant en quelque sorte une capacité plus prosaïque de l'entreprise à affronter la tempête et à passer à autre chose. Selon Raphäel De Vittoris, c'est la capacité à faire face à tout et n'importe quand qui rendra l'entreprise durable dans l'environnement VUCA actuel. Un contexte durable étant prospère pour les investisseurs après la dernière crise et avant la prochaine.

Par conséquent, la résilience 4.0 face à l'augmentation des risques et des perturbations, qui se résume à la capacité d'éviter, de dissuader, de protéger, de répondre et de s'adapter aux perturbations du marché, de la technologie et des opérations, devient un élément essentiel de la rentabilité, de la valeur actionnariale et de la compétitivité, et non un legs à la prochaine génération.

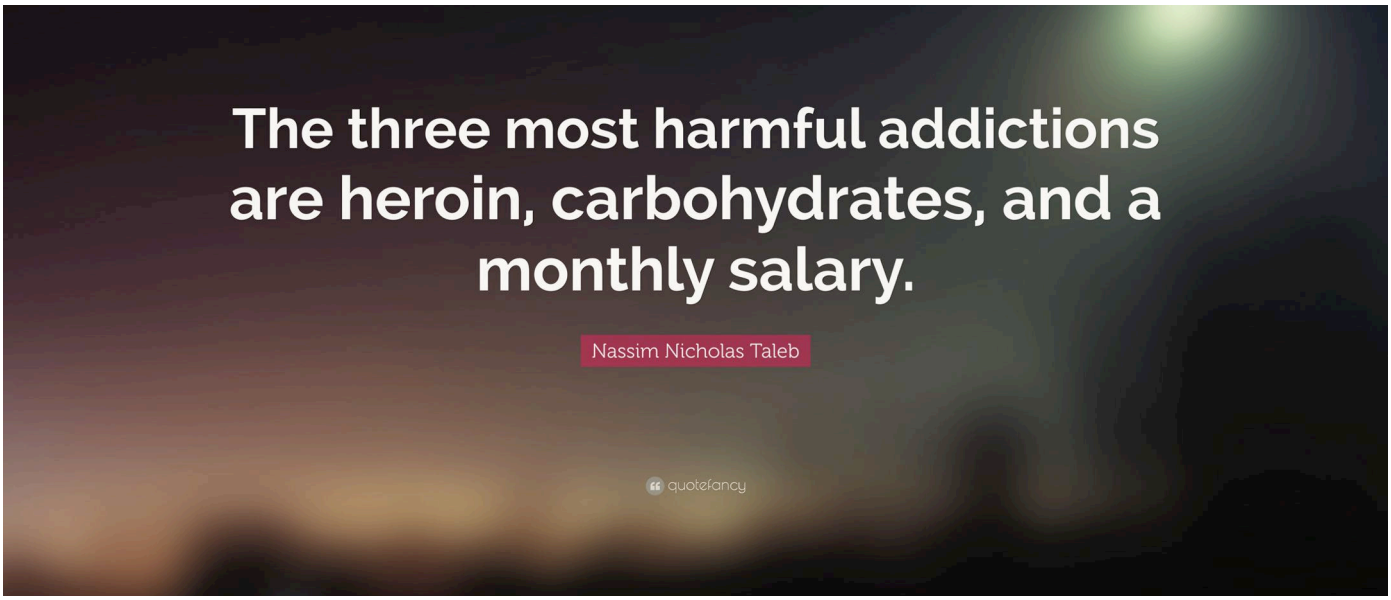
L'économie des start-up a créé plusieurs nouveaux entrepreneurs, de jeunes talents, qui considèrent la richesse comme la mesure de la réussite et négligent la longévité comme élément clé de la réalisation. Ce modèle économique crée des entreprises qui ne durent pas une décennie dans les mêmes mains, des entreprises qui peuvent traverser la tempête pour être vendues ou dissoutes avant la prochaine.

Le legs que ces jeunes professionnels laissent à la génération suivante n'est qu'un amoncellement de richesses sans histoire.

En tant que moment évolutif ou révolutionnaire de l'histoire, chaque génération incarne des aspects de la perturbation des affaires qui transformeront les sociétés, en bien ou en mal. Nous pouvons donc nous rapprocher des vues extrémistes et médiocratiques de Nassim Taleb et accepter que les perturbations soient des facteurs génétiques de l'activité économique, tandis que la résilience se trouve dans les racines de ceux qui sont capables de transmettre leur entreprise à la génération suivante. ■

BIO

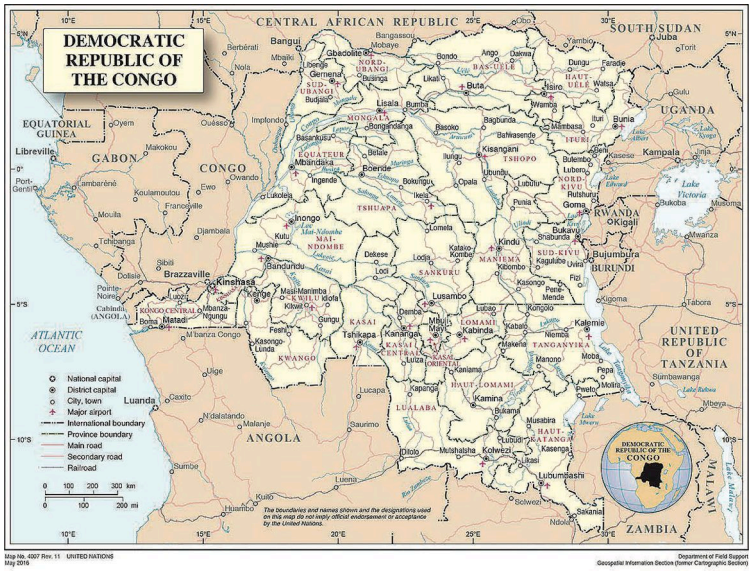
Luca est actuellement expert senior contractuel à l'AIEA (Agence internationale de l'énergie atomique, ONU-Vienne). Expert en sécurité d'entreprise avec près de 25 ans d'expérience dans des sociétés cotées en bourse - il a dirigé des opérations de sécurité dans divers environnements. Son expérience couvre de nombreux secteurs, notamment l'industrie manufacturière, l'industrie pharmaceutique, les technologies de l'information et de la communication, les institutions financières et toutes les sociétés Fortune 100 et 500. Elle est complétée par une expérience au sein d'agences spécialisées des Nations unies, dont l'agence principale pour les technologies de l'information et de la communication. Fervent défenseur de la convergence entre la sécurité physique et la sécurité des TIC. Penseur stratégique innovant ayant fait ses preuves en matière de coopération, il travaille actuellement sur des projets de convergence et d'intégration technologiques. Il a publié des articles sur la sécurité physique, organisationnelle et des TIC, et a été invité à présenter des remarques dans des revues industrielles ou géopolitiques et des séminaires internationaux présentant les risques émergents ou latents en matière de sécurité des entreprises exposant de nouvelles menaces asymétriques. Il est titulaire d'un diplôme post-grade en gestion de la sécurité et des urgences de l'Université Bocconi, d'un Master en gestion du crime et des risques de l'Université de Leicester et d'un DAS en gestion des risques d'entreprise de la HEG-SO (Genève).



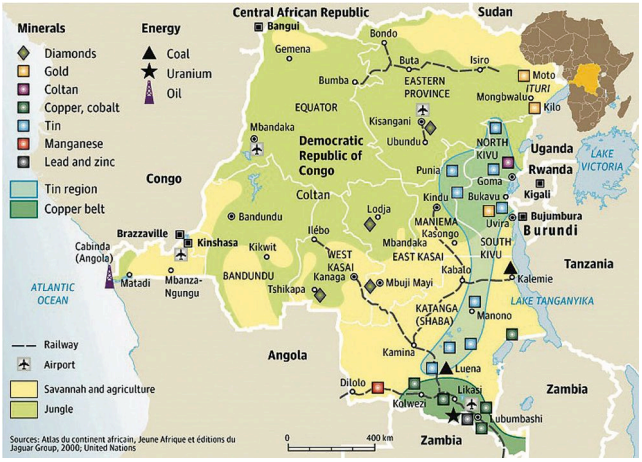
Donner les gages de la confiance : l'exemple de la République Démocratique du Congo.

Auteur : **Mauro Vignati**

La République Démocratique du Congo (RD Congo) est un immense pays, d'une superficie de 2.345000 km2, avec une population estimée à environ 86,73 millions d'habitants, se classant ainsi parmi les vingt premières nations du monde. Sa population est jeune (70 % du total) et environ 40 % vit dans des zones urbaines.



C'est un pays divisé en 26 provinces, auxquelles la constitution de 2006 donne une large indépendance dans la gestion politique et administrative. Le pays est riche en ressources naturelles ; les forêts occupent la moitié du territoire. Mais outre les 80 millions d'hectares de terres arables, la RD Congo est connue pour avoir plus de 1100 minéraux et métaux précieux dans son sous-sol.



On y trouve d'importantes quantités de diamants, cuivre, cobalt, étain, or, uranium, zinc, argent, germanium, tantale, niobium, manganèse, fer et bien d'autres encore. Ces ressources se présentent sous la forme d'indices miniers ou de réserves économiquement exploitables. La contribution du secteur à l'économie nationale est essentielle. En effet, il représente près de 90% des exportations du pays, plus de 15% du produit intérieur brut et près de 20% du budget national de l'Etat.

Le secteur minier est clairement le principal moteur du pays, générant une dépendance écrasante en termes d'exportations, de recettes publiques et de croissance du PIB.

Malgré cette richesse, la RD Congo est confrontée de manière quasi permanente à l'instabilité financière et aux récessions économiques. Des politiques nationales brutales et une mauvaise gestion des affaires publiques, la guerre et l'insécurité ont généré un climat de profonde méfiance à l'égard de la gestion de l'État, créant un système parasitaire désormais solidement ancré dans le tissu social et économique, dégradant les entreprises minières d'État, et jetant généralement la population dans une pauvreté persistante.

Une fiscalité arbitraire et discriminatoire, des infrastructures physiques médiocres, une application marginale des droits de propriété et un état de droit approximatif ont entraîné une mutation progressive d'une puissance industrielle minière formelle et mécanisée vers un marché informel, illégal et rudimentaire. Dans plusieurs régions du pays, le parallélisme et les conflits de pouvoir entre les autorités coutumières et administratives finissent par influencer les activités minières. Le commerce de l'or congolais est largement informel, orienté vers les pays voisins de l'Est. Le niveau élevé des taxes constitue un obstacle majeur à la commercialisation formelle de l'or, et plus généralement de l'ensemble du secteur minier national.

Lorsqu'on examine la production artisanale d'or en RD Congo, l'aspect informel semble prévaloir dans toutes les provinces. De récentes études de terrain[1] nous apprennent que dans les cinq provinces de l'est du pays - Haut-Uele, Ituri, Sud-Kivu, Tanganyka, Tshopo - environ 80 % de tout l'or congolais est extrait, avec 230 000 à 250 000 prospecteurs d'or fournissant entre 8,1 et 12,5 tonnes par an, avec une pureté moyenne de 22 carats.

Un chercheur d'or serait capable d'extraire 0,93 gramme par jour en période de production. L'organisation hiérarchique commence par les patrons de mine, suivis des patrons de fosse, puis des transporteurs et enfin d'une main d'œuvre d'appoint.

Les conditions de vie et d'hygiène sont extrêmement difficiles, souvent des femmes et des enfants y travaillent. D'énormes quantités de mercure et de cyanure sont déversées dans les eaux. Une grande partie de l'or artisanal finit dans les pays voisins, en Ouganda, au Rwanda, au Burundi, en Tanzanie, en passant par des routes difficiles avec une forte présence de personnes armées. Mais cette voie est préférable à celle du gouvernement central, qui est lourde en termes d'administration, de taxes et de manque général de volonté de formaliser le secteur.

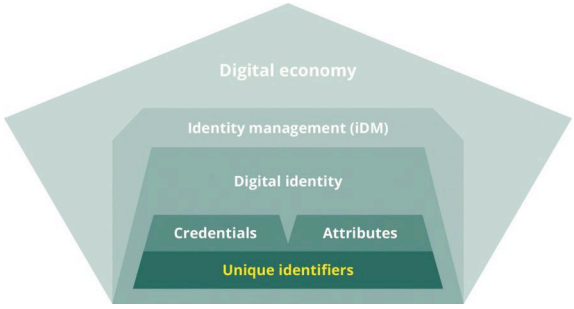
Au cours de l'année 2020, j'ai été approché par un groupe de personnes, congolaises et européennes, expertes en économie, numérique et finance,

BIO

Mauro Vignati est Conseiller en matière de nouvelles technologies numériques de guerre auprès du CICR (Comité International de la Croix-Rouge). Depuis plus de 18 ans, Mauro travaille dans le domaine du renseignement, sur les cyber-menaces et la cyber-sécurité. Il a travaillé à KOBIK, la première unité du gouvernement suisse consacrée à la lutte contre la cyber-criminalité, puis à MELANI, l'organisme gouvernemental fédéral chargé de protéger les infrastructures critiques nationales contre les cyberattaques. Par la suite, il a travaillé pour le Département de la Défense, dans le Centre national de Cybersécurité (NCSC.ch). Mauro a une longue expérience dans la prévention, l'identification et l'analyse des cyber-crimes et des menaces persistantes avancées (APT). Il consacre également son temps à la recherche dans le domaine de l'innovation des technologies de communication dans différents environnements politiques et économiques. Il est titulaire d'une Licence et d'un Master en littérature et d'un Executive Master en criminologie. Il a enseigné aux Universités de Berne, de Genève et de Lugano.

qui entendaient accélérer la formalisation du secteur par la technologie blockchain. Le projet comportait plusieurs aspects.

Fournir un identifiant numérique unique : Le nouvel identifiant national aurait été basé sur les certificats de naissance ou d'autres documents pouvant prouver l'identité des habitants du pays. Il aurait été associé à un élément biométrique, tel qu'un scan de l'iris. Une carte d'identité numérique certifiée par le gouvernement aurait empêché les mineurs d'être employés dans les mines, leur fréquentation des établissements d'enseignement aurait pu être enregistrée, ce qui aurait renforcé l'éducation et diminué l'exploitation. En outre, l'identification numérique aurait permis d'associer l'or extrait au mineur, au transporteur et aux aides responsables.



Émettre un nouveau stablecoin national : le (C-GBS) serait émis, adossé à des réserves d'or comme garantie. L'or extrait des mines serait enregistré sur la blockchain, accumulé dans les réserves nationales, et vendu à l'extérieur par le gouvernement. La nouvelle monnaie, une monnaie numérique de la banque centrale (CBDC) aurait eu l'avantage d'être une monnaie stable, évitant des taux d'inflation de 30 à 40 %. L'augmentation ou la diminution des réserves d'or aurait permis de maintenir la stabilité de la CBDC. Une augmentation des réserves aurait mis plus de C-GBS en circulation, une diminution des réserves aurait brûlé les C-GBS. Le gouvernement central aurait ainsi endigué la fuite de l'or vers les pays voisins, un trafic incontrôlé entraînant des pertes énormes pour l'économie du pays. En augmentant les profits pour le gouvernement, les taxes auraient diminué, incitant les mineurs à travailler dans ce nouveau processus formel.

Générer un porte-monnaie pour chaque habitant : chaque habitant de la RD Congo se verrait attribuer un porte-monnaie, afin de pouvoir utiliser le C-GBS. Les participants à la chaîne minière auraient été payés en C-GBS : à la livraison de l'or extrait, ils auraient été récompensés en déposant du C-GBS dans leur portefeuille. Cela aurait évité aux mineurs d'être agressés le jour de la collecte de leur salaire en espèces. Et il aurait été possible de vérifier que l'or extrait correspondait aux paiements effectués en C-GBS. Cela aurait créé une économie basée sur le C-GBS, puisque les jetons auraient circulé des mineurs vers l'ensemble du secteur économique du pays.

Grâce à ces mesures, un "commerce équitable" aurait été garanti, sans exploitation des mineurs et une juste rémunération des travailleurs. L'or extrait aurait été de l'"or vert" (or traçable) et le pays aurait pu enfin disposer d'une monnaie stable, contrôlant l'inflation, stimulant

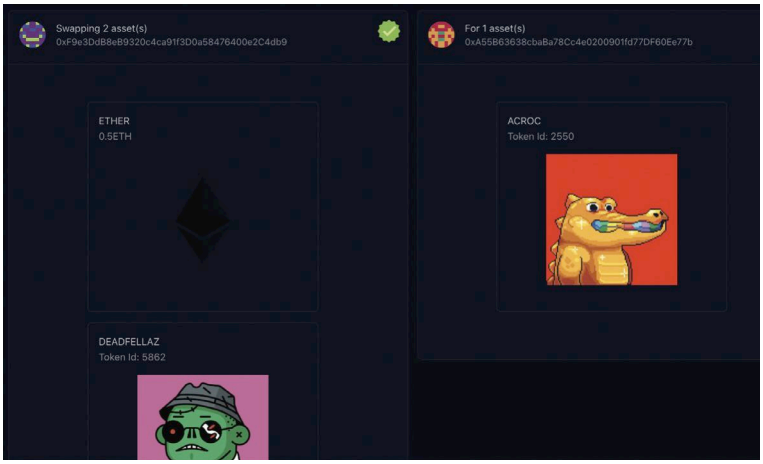
les investissements étrangers, faisant croître l'économie et facilitant le commerce. Le tout en éliminant les trafics illicites, la criminalité armée et les souffrances de la population locale. Sur le papier, ce projet, au-delà d'un discours discutable sur la vie privée, avait tout pour être considéré bon.

Mais malheureusement, au début de la chaîne, il y avait un plus gros problème : la confiance de ceux qui contrôlaient l'exploitation de l'or. Qui aurait pu certifier que tel mineur avait effectivement extrait cette quantité ? Qui aurait eu l'autorité d'enregistrer dans la blockchain que l'extraction avait eu lieu ? Ce serait les mêmes agents qui avaient jusqu'à présent évité de mettre l'or extrait dans le circuit légal en le faisant passer par des voies illégales et risquées. Ainsi, à la base de toute cette technologie innovante, de la traçabilité, de la visibilité et de l'immuabilité des transactions, de la naissance d'une nouvelle monnaie future stabilisatrice pour le pays, il n'y a rien d'autre que le vieux concept de confiance. Sans confiance, même la technologie la plus moderne ne peut fonctionner.

De la plateforme de recyclage à la nouvelle frontière de la cybercriminalité

Depuis quelques années, on parle surtout du Web3, du DeFi et des crypto-monnaies comme d'une plateforme de blanchiment d'argent pour des schémas criminels établis tels que les ransomwares. Mais le blanchiment d'argent via des monnaies ou des NFT se transforme depuis un an en crime contre les acteurs de ces plateformes où contre les plateformes elles-mêmes. Et là aussi, la confiance joue le rôle principal. Par exemple dans les NFTs. La technique d'escroquerie commence par un contact via Discord, entre l'escroc et la personne qui tente de vendre son jeton.

Ensuite, l'arnaqueur montre «son» portefeuille sur OpenSea, pour donner plus de confiance au vendeur, qui se sentira rassuré d'échanger avec une personne qui collecte également des NFTs. La victime sera alors «détournée» vers une plateforme d'échange, créée ad-hoc pour exécuter l'arnaque.



La plateforme d'échange Swaptic.io (@hoffcolors)

Dans ce cas, le criminel convainc la victime qu'elle va payer 0,5 ETH plus un NFT Deadfellaz pour recevoir son NFT Acroc. Le criminel envoie ensuite un lien pour signer l'échange. Mais lors de la confirmation, le propriétaire se rend compte qu'il a donné accès à l'ensemble de son portefeuille au criminel, qui l'a utilisé et vidé.

Mais la criminalité dans ce domaine ne se limite pas à la petite fraude. Les gens font confiance à des innovations technologiques qui, bien qu'elles soient encore dans une version bêta de développement, sont déjà utilisées dans la productivité. Pensez aux «ponts» pour les différentes blockchains et sidechains. Les codes béants qui permettent aux criminels de s'infiltrer et de voler des dizaines de millions de dollars. Ou encore les nombreuses manipulations d'oracles. Les propres plateformes de DeFi deviennent des victimes. Une fois encore, comme dans le cas de l'or congolais, l'innovation technologique qui a voulu la transparence des transactions et de la gouvernance ne peut rien contre la confiance mal placée de ses utilisateurs.

PoH, Worldcoin, POAP : résoudre les problèmes par la technologie

Entre-temps, plusieurs initiatives ont vu le jour pour surmonter le problème de la confiance, essentiellement pour identifier que les personnes avec lesquelles on interagit sur le Web3 sont réelles et peuvent être reconnues comme telles. Proof of Humanity (PoH), où pour s'inscrire au registre, il faut faire une courte vidéo de soi, mettre en jeu un dépôt remboursable de 1,5 ETH (plus ou moins 400 dollars, ce qui est peut-être la chose la plus difficile à mettre en œuvre dans le Sud) et trouver une personne déjà certifiée pour se porter garante de vous[2]. Ou WorldCoin, qui scanne des centaines de milliers d'iris, mais qui s'inquiète d'acquérir des tonnes de données biométriques[3]. Ou encore le protocole de preuve de présence (Proof of Attendance Protocol, POAP), dans lequel les utilisateurs collectent des jetons de présence pour prouver qu'ils étaient physiquement présents à un événement spécifique. Toutes ces initiatives sont expérimentales et certaines partent d'une bonne intention. Mais les problèmes liés à une technologie immature sont résolus par une technologie encore plus immature. Ce que l'on appelle le «solutionnisme technologique»[4] ne changera probablement rien au fait que la confiance est au cœur de toute technologie.

Dans son blog, MoxieMarlinspike écrit[5] : *«Nous devrions accepter le principe que les gens ne géreront pas leurs propres serveurs en concevant des systèmes qui peuvent distribuer la confiance sans avoir à distribuer l'infrastructure. Cela signifie une architecture qui anticipe et accepte le résultat inévitable de relations client/serveur relativement centralisées, mais qui utilise la cryptographie (plutôt que l'infrastructure) pour distribuer la confiance. L'une des choses qui me surprend dans le web3, bien qu'il soit construit sur la «cryptographie», est le peu de cryptographie qui semble être impliquée !»*

Plus de centralisation et plus de distribution de la confiance par le cryptage. Si sur le premier point, l'expérience démocratique des dernières décennies semble confirmer la nécessité de la centralisation pour un bon fonctionnement social, sur le second, nous devrons réfléchir à la manière dont nous voulons accroître la confiance dans le monde virtuel. ■

1 http://cegemi.com/wp-content/uploads/2015/08/Nkuba-Zahinda-Chakirwa-Murhi-de-Haan-Bashwira-2018.-Lor-artisanal-congolais_Rapport-d%C3%A9valuation-du-mercure-en-ASGM-avec-ACE-UNITAR.pdf
2 https://time.com/6142810/proof-of-humanity
3 https://podcasts.apple.com/us/podcast/worldcoin-where-techno-optimism-meets-techno-colonialism/id1552627235?i=1000558511758
4 https://www.publicbooks.org/the-folly-of-technological-solutionism-an-interview-with-evgeny-morozov/
5 https://moxie.org/2022/01/07/web3-first-impressions.html

La sensibilisation à la cyber-sécurité pour tous : un impératif que les entreprises ne peuvent plus ignorer.

Auteur : Veronica Patron

Un programme avancé de sensibilisation à la cyber-sécurité se doit d'analyser le facteur humain dans le contexte de la cyber-sécurité, en s'appuyant sur des contributions multidisciplinaires provenant, par exemple, des sciences sociales, de la psychologie et de la sociologie.

Il est important d'inclure certaines caractéristiques psychologiques dans un cours de formation, car elles sont à la base du comportement humain et sont utilisées par les cybercriminels.

En exploitant nos émotions, les pirates informatiques nous poussent à agir instinctivement, sans faire appel à la partie plus rationnelle et logique de notre cerveau. En se basant sur des principes de psychologie et de sociologie, ils créent des mécanismes pour déjouer la façon dont notre cerveau prend des décisions.

En outre, les pirates utilisent les moments d'inattention, comme le lundi matin lorsqu'un utilisateur vérifie les e-mails qu'il a reçus durant le week-

end, ou cinq minutes avant la pause déjeuner. Ils peuvent aussi mettre à profit la fin de la journée de travail, lorsque l'utilisateur se prépare à terminer ses activités professionnelles.

Examinons ensemble les principales caractéristiques qu'un programme innovant de sensibilisation à la cyber-sécurité doit avoir pour être efficace et réussi :

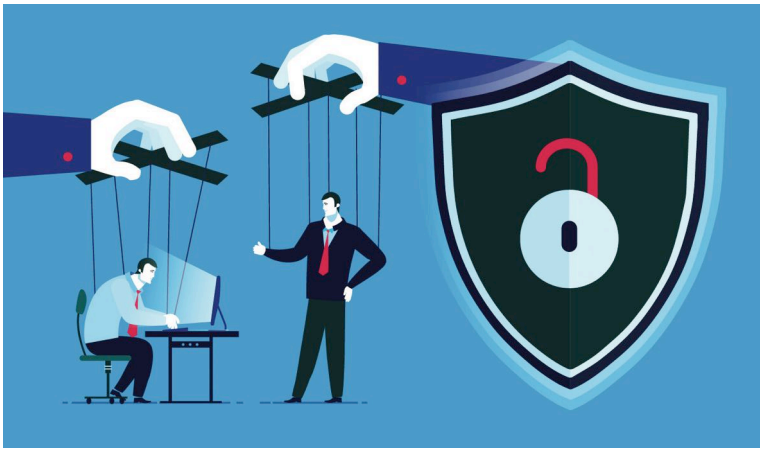
Se concentrer sur le facteur cognitif et sur la manière dont le contenu est transmis.

Le but de l'ingénierie sociale est de nous inciter à prendre une décision sans réfléchir, mais pourquoi, lorsque nous sommes dans un contexte numérique, notre perception du risque diminue t'elle?

La raison principale est liée au fait que dans le monde réel, nous avons développé des capteurs qui nous aident à percevoir le danger. Si nous voyons un tigre dans la rue, nous n'avons pas besoin de réfléchir beaucoup, nous percevons immédiatement qu'il y a un danger.

Ce sont nos cinq sens qui nous aident à vivre dans le monde physique et qui nous protègent.

Lorsque nous entrons dans un contexte numérique, le scénario change, nous manquons de capteurs pour nous mouvoir en toute sécurité.



Utilisation d'un langage simple, compréhensible même par des personnes inexpérimentées en matière de cyber-sécurité.

La cyber-sécurité concerne tous les employés d'une organisation: ainsi, il est crucial de communiquer de façon simple et de surmonter l'idée fausse selon laquelle les concepts de sécurité n'intéressent et ne concernent que les techniciens du domaine informatique; au contraire, la meilleure stratégie consiste à adopter un langage adapté à l'ensemble des équipes de l'entreprise.

À l'avenir, nous devrions donc aller au-delà des compétences techniques et considérer l'importance de les combiner avec des compétences de communication et aux habilités sociales. Beaucoup se concentrent sur les compétences techniques, oubliant qu'une organisation est composée de personnes dont les niveaux de connaissances et de besoins sont très différents. C'est ainsi qu'un programme de sensibilisation à la cyber-sécurité exige des compétences de communication adéquates.

Cette particularité permet à une culture de sécurité d'intégrer la façon de penser et de se comporter de chaque employé, puis de l'étendre non seulement à la sphère professionnelle mais aussi à la sphère personnelle, évitant ainsi de limiter l'utilisation des bonnes pratiques au seul comportement professionnel en l'étendant aussi à l'environnement familial.

BIO

Veronica Patron est Co-Fondatrice de Security Mind, et experte en cyber-sécurité auprès de Brinthesis. Diplômée en psychologie du travail et des organisations de l'université de Padoue, Veronica est experte en efficacité de la communication, en programmation neurolinguistique, ainsi qu'en formation et sensibilisation. Toujours fascinée par la dynamique psychologique et comportementale qui caractérise les êtres humains, Veronica est membre de *«Woman for Security»* et rédactrice à *«Red Hot Cyber»*. Veronica est co-fondatrice du projet Security Mind, un programme avancé de sensibilisation à la cyber-sécurité qui décrit non seulement les différentes techniques d'attaque – en utilisant une méthode de divulgation permettant une bonne compréhension du phénomène à tous, spécialement à toutes les personnes qui n'ont aucune expérience en matière de cyber-sécurité – mais analyse également le facteur humain dans le contexte de la cyber-sécurité.

Il s'agit d'un outil utile pour se familiariser puis approfondir ses connaissances dans le langage «technique», car s'il est vrai qu'il est essentiel d'utiliser un langage compréhensible même par des personnes sans aucune expérience en matière de cyber-sécurité, il est également vrai que dans certains cas, il est nécessaire d'utiliser des concepts et des termes plus techniques, qui sont alors expliqués dans une section spéciale du glossaire.

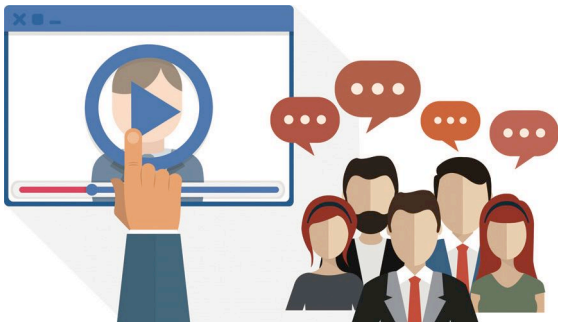
Cours de formation continue à l'aide de pilules de formation

La meilleure solution pour un parcours de sensibilisation efficace consiste à créer de courtes leçons et des modules cohérents organisés dans un parcours continu, par exemple de courtes vidéos à regarder à des moments opportuns de la journée.

Le choix de la formation continue répond également à une caractéristique de l'être humain : une action qui

devient une habitude bien ancrée demande du temps et une répétition constante.

En outre, il faut garder à l'esprit que la cyber-sécurité évolue constamment et qu'il est donc nécessaire de disposer d'un programme de sensibilisation avec des mises à jour constantes.



Mais quel est le temps acceptable à consacrer à ce type de formation ? Notre expérience nous a montré que les sessions d'entraînement autonome devraient être inférieures à 6 minutes, car elles sont compatibles avec tous les types d'exigences professionnelles, éliminant ainsi tout blocage potentiel dû à une surcharge de travail.

Faire participer l'utilisateur à des activités de jeu

Le jeu est souvent identifié comme quelque chose d'enfantin, destiné aux mineurs : à cet égard. George Bernard Shaw a écrit : «*l'homme arrête de jouer parce qu'il vieillit, mais il vieillit parce qu'il arrête de jouer*».

La *gamification* va au-delà de son aspect purement ludique ; grâce à elle, le potentiel du jeu est exploité pour atteindre un résultat commercial et d'apprentissage spécifique.

Grâce à ces expédients, il est en effet possible de modifier le comportement des gens, en favorisant l'émergence et la consolidation d'un intérêt actif de la part des individus concernés.

L'objectif est d'impliquer les gens en générant un changement dans leur comportement. En fait, dans ce scénario, la motivation augmente car elle est perçue comme une activité moins ennuyeuse, moins contraignante et en même temps les gens apprennent et s'impliquent plus, créant des niveaux élevés d'engagement. Le résultat obtenu est que les participants restent imprégnés des leçons apprises, même à long terme.

Comme l'affirment Barradas et Lancastre, la compétition qui est déclenchée par le jeu est positive car elle fait partie du «jeu pour le jeu». Une compétition entre groupes prend une connotation positive lorsqu'elle est appliquée à l'apprentissage, lorsque la dynamique de groupe est activée, comme tout jeu d'équipe, elle déclenche la théorie psychologique de l'identité sociale.

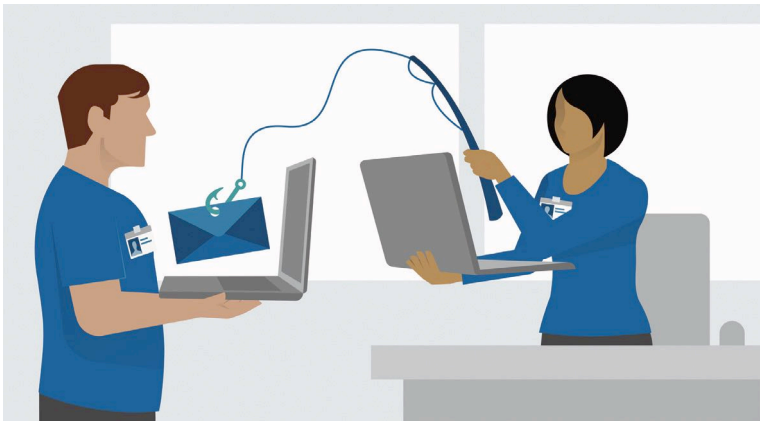
Qu'il s'agisse d'une *gamification* individuelle ou de groupe, l'utilisation de cette technique est l'un des ingrédients-clé d'un processus de formation à la cyber-sécurité, car elle parvient à attirer les participants à susciter leur engagement et, par conséquent, à accroître l'efficacité de la formation elle-même.

Terrain d'entraînement pour augmenter la résilience, une combinaison de pilules d'entraînement et de campagnes de hameçonnage.

La possibilité de simuler des attaques malveillantes devenant progressivement de plus en plus complexe en fonction des équipes de

l'entreprise signifie que l'entreprise peut tester sur le terrain le facteur humain, puis analyser le tout afin d'améliorer sa résilience globale.

Le terrain d'entraînement simulé consiste en une représentation d'un contexte réel : grâce à la création d'un scénario de danger réel tant au niveau du contenu que de sa dynamique relationnelle, l'expérience éducative est proposée dans un environnement sûr.



Suivi et rapports

L'élément fondamental est le suivi et l'établissement de rapports, ce qui permet de passer d'une analyse de l'apprentissage dans son ensemble à la mesure du changement du comportement de chaque utilisateur individuel.

Le suivi des *Indicateurs de Performance Clé* (KPI) de comportement est fondamental car il permet de mesurer les progrès de chaque utilisateur, de mettre en place des actions de remédiation mais surtout de permettre à la direction de mesurer le retour sur investissement.

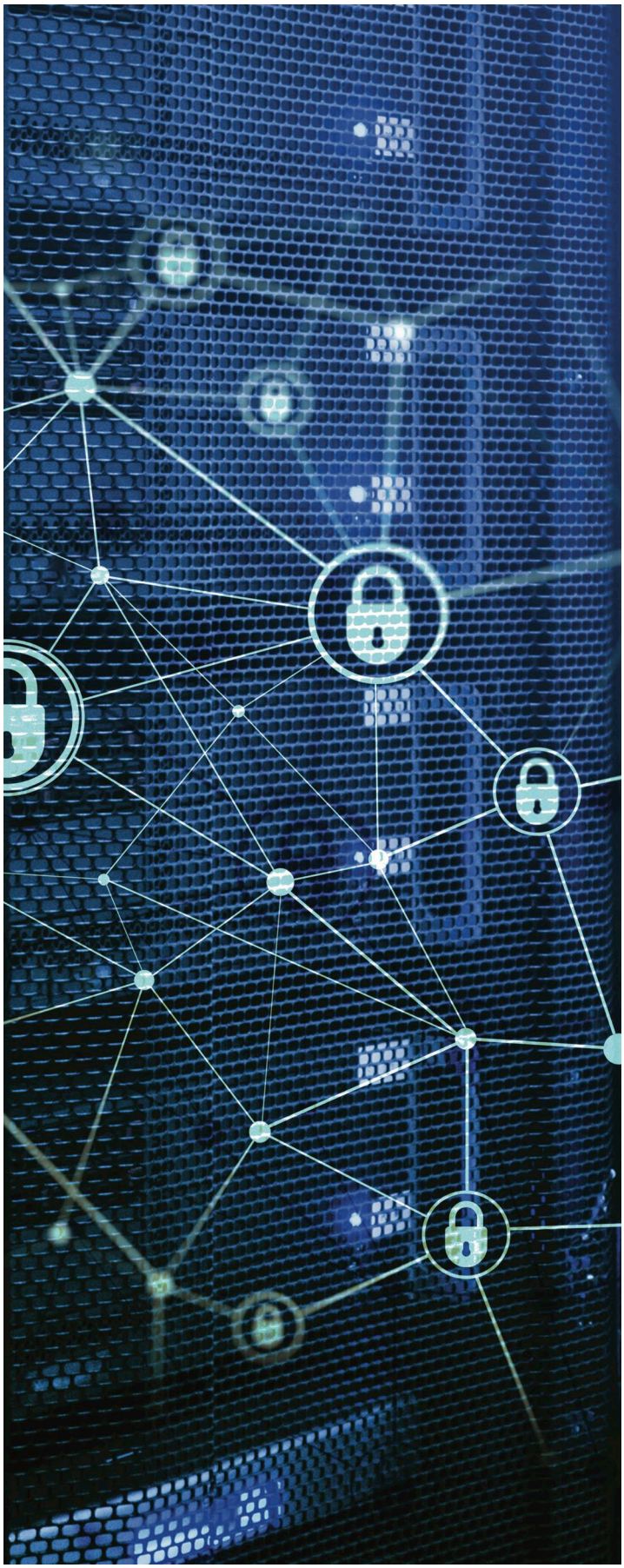
Dans ce sens, il est clairement préférable de procéder à une évaluation préliminaire afin de créer une base de référence initiale permettant de mesurer les performances futures.

Parmi les métriques générées par un cours de formation nous pouvons trouver :

- nombre total de personnes ayant cliqué sur le lien proposé
- nombre total de personnes ayant signalé l'attaque
- nombre de personnes ayant cliqué et signalé l'attaque
- nombre de personnes qui n'ont ni cliqué ni signalé l'attaque
- nombre de personnes qui n'ont pas cliqué et qui ont signalé l'attaque : le meilleur comportement possible.

Lorsque cela est possible, il est intéressant de créer les rapports en se basant sur la «zone géographique» (départements), sur le rôle des participants dans l'entreprise et aussi en fonction des heures et jours de la semaine.

En conclusion, un programme innovant de formation à la sensibilisation à la cyber-sécurité doit s'appuyer sur une méthodologie efficace et axée sur les résultats obtenus, afin de transformer vraiment le comportement de chaque individu. ■



Une publication

web for business
swiss webacademy

Rédaction :

Laurent Chrzanovski et
Romulus Maier (†)

ISSN 2559 - 1789
ISSN-L 2559 - 1789

Adresse :

Şcoala de Înot nr.18,
550005, Sibiu, Roumanie
https://swissacademy.eu/
https://cybersecurity-dialogues.org

Page spéciale pour télécharger ce numéro :

https://swissacademy.eu/
cyberespionage/

web for your business
swiss webacademy

NTT DATA
Trusted Global Innovator

Host and support:

CYBERSECURITY DIALOGUES
- ROMANIA -
8th Edition - September 21-22, 2022

A WAR-TORN POST-PANDEMIC WORLD: ATTACKS AT 360°.

SOLUTIONS FOR SECURING YOUR BUSINESS.

www.cybersecurity-dialogues.org

Under the aegis of:

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Embassy of Switzerland in Romania

Media partner:

BURSA
ZIARUL OAMENILOR DE AFACERI

In partnership with:

1949.2019
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
Gendarmerie nationale
Centre de recherche de l'EOGN
POLICE GENÈVE
ROMANIA CYBERINT
IGPR POLIȚIA ROMÂNĂ
GUVERNUL ROMÂNIEI
DIRECTORATUL NAȚIONAL DE SECURITATE CIBERNETICĂ
CMCS INTERNATIONAL
FIC Forum International de la Cybersécurité
ULBS Universitatea "Lucian Blaga" din Sibiu
SIBIU COUNTY COUNCIL