Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Unité de pilotage informatique de la Confédération UPIC
Service de renseignement de la Confédération SRC

Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI

SÛRETÉ DE L'INFORMATION

SITUATION EN SUISSE ET SUR LE PLAN INTERNATIONAL

Rapport semestriel 2018/II (juillet à décembre)

30 AVRIL 2019

CENTRALE D'ENREGISTREMENT ET D'ANALYSE POUR LA SÛRETÉ DE L'INFORMATION (MELANI)
https://www.melani.admin.ch/

1 Aperçu / sommaire

2 Éditorial

Rôle de l'État aujourd'hui et demain dans le cyberespace

Myriam Dunn Cavelty est directrice adjointe du Centre d'études sur la politique de sécurité (Center for Security Studies, CSS) de l'EPF de Zurich. La politique de cybersécurité est au cœur de son activité de chercheuse et d'enseignante.

Il y a dix ans encore, la cybersécurité passait pour être une simple niche de marché, et faisait l'objet de discussions techniques dans les cercles d'experts. Dans l'intervalle, avec l'aggravation de la menace, elle est devenue un enjeu brûlant de la politique de sécurité, abordé dans les plus hautes sphères gouvernementales.

Le rôle de l'État et de son administration est soumis à un processus de négociation politique loin d'être terminé, dans bien des pays de la planète. La cybersécurité est un thème transversal, qui se recoupe avec de multiples domaines d'action politique. L'un des défis majeurs, à l'heure où les ressources se raréfient, consiste à trouver un juste équilibre entre de nouvelles structures et un usage rationnel des compétences existantes, ainsi qu'à faire intervenir là où c'est judicieux les acteurs pertinents du monde économique et de la société civile. D'autres exercices s'avèrent encore plus périlleux, à savoir l'intégration (verticale) des stratégies nationales de cybersécurité dans le cadre de la sécurité nationale et dans une stratégie globale, couvrant tous les domaines politiques, de même que la coordination et le contrôle (horizontaux) des divers services impliqués dans la cybersécurité.

Il est généralement reconnu que pour parvenir à un niveau satisfaisant de cybersécurité, l'État, les milieux économiques et la société civile doivent travailler main dans la main. Or les objectifs et les intérêts diffèrent d'un secteur à l'autre. Il en résulte au moins trois champs de tension, qu'il convient de prendre en compte dans toute politique de cybersécurité.

Dans le premier champ de tension, entre l'État et les milieux économiques, il faut formuler une politique de protection des infrastructures d'importance vitale, qui remédie aux conséquences négatives de la libéralisation, de la privatisation et de la mondialisation sur la politique de sécurité, sans en étouffer les effets positifs. Dans le deuxième champ de tension, qui se situe entre l'État et les citoyens, il s'agit de trouver l'équilibre politiquement souhaitable entre davantage de sécurité et la préservation des droits civils dans l'espace numérique. Quant au troisième champ de tension, situé entre les citoyens et les milieux économiques, il importe de formuler des conditions propices à la création d'un bon écosystème de sécurité, de façon à instaurer un équilibre optimal entre sécurité et fonctionnalité, mais aussi pour inciter les prestataires de services à dûment assumer leurs obligations liées à la sécurité.

Ce qui va de soi pour les acteurs de l'économie et de la société civile vaut également pour l'État, qui doit assumer plusieurs rôles à la fois. La prise de conscience des diverses facettes de l'action étatique constitue un bon point de départ pour gérer et aborder systématiquement les conflits de rôles au niveau politique, et par là pour mettre en place une politique proactive et tournée vers l'avenir.

Myriam Dunn Cavelty

3 Thème prioritaire: relations avec les fabricants de solutions informatiques ou logicielles d'importance vitale

Les fabricants de solutions informatiques ou logicielles de certains États ont fait parler d'eux déjà avant les révélations d'Edward Snowden. Peu après l'arrivée sur les marchés mondiaux du fabricant chinois Huawei, des doutes avaient été émis sur l'intégrité de ses produits et sur son indépendance envers les autorités chinoises. En 2013, les documents divulgués par le lanceur d'alerte américain ont étayé au moins en partie les soupçons selon lesquels des fabricants américains comme Cisco, Microsoft, Google et d'autres encore accorderaient aux autorités un droit d'accès à leurs produits, afin d'en surveiller les utilisateurs. À la suite des reproches d'espionnage russe sur leur territoire, les autorités américaines ont interdit en 2017 l'utilisation des produits Kaspersky pour le gouvernement et les agences fédérales. Ce thème est discuté en Suisse aussi, dans les milieux économiques comme dans les administrations.

Il est sans doute indiqué, dans le cadre des mesures visant à assurer la sécurité, de bien réfléchir avant d'utiliser les produits de certains fabricants. D'un autre côté, une partie importante de cette discussion est motivée par des intérêts purement politiques et économiques. Une discussion différenciée, indépendante de tout fournisseur, est par conséquent nécessaire ici.

3.1.1 Matériel et logiciel au service d'intérêts d'État

Avec la numérisation croissante des processus d'affaires, les solutions matérielles ou logicielles deviennent une composante centrale et d'importance vitale. À première vue, les prestataires semblent particulièrement nombreux sur le marché, et l'offre de solutions très variée. Mais si l'on considère les pays d'origine, il ne reste plus grand-chose de cette apparente diversité. Le marché est clairement dominé par les entreprises américaines, talonnées par la Chine et par quelques autres acteurs mondiaux du secteur, comme la Corée (Samsung), la Russie (Kaspersky) et l'Allemagne (SAP).

Si l'on prend la peine d'analyser dans les pays d'origine les bases juridiques régissant l'industrie des technologies de l'information et de la communication (TIC) locale, on constate qu'il ne s'agit pas que d'un moteur économique bienvenu. Son rôle clé pour le traitement, l'acheminement et le stockage d'informations est dûment reconnu, et la législation autorise les services étatiques à assouvir leurs convoitises en la matière.

En conclusion, la numérisation en profondeur des processus que nous connaissons n'aurait pas lieu sans les solutions matérielles et logicielles d'entreprises américaines, chinoises ou autres. Or cette numérisation va aussi en théorie simplifier l'accès aux systèmes informatiques des fabricants locaux, soit aux informations sauvegardées, traitées ou acheminées.

3.1.2 Exclusion de fabricants, cybersouveraineté et normes internationales

Les discussions vont bon train sur la meilleure manière de gérer le risque que les États d'origine fassent valoir leur droit d'accès aux fabricants informatiques, et qu'ils prennent ainsi le contrôle de leur matériel et de leurs logiciels au niveau mondial.

Plusieurs des approches pratiquées visent essentiellement les fabricants et les fournisseurs de matériel et de logiciels.

Les fabricants peuvent en règle générale être exclus des marchés publics, s'ils sont soupçonnés de servir les intérêts d'un pays. C'est arrivé par exemple dans l'administration américaine qui, en décembre 2017, a interdit l'emploi des produits du groupe Kaspersky domicilié en Russie. Dans le cas des produits Huawei aussi, des appels à écarter les offres de ce fabricant ont été lancés, depuis quelques mois, dans des pays très divers.

De telles solutions peuvent certes être, à court ou moyen terme, un gage de sécurité face au risque de contrôle des processus numériques locaux par un État tiers. Un débat général est par ailleurs mené dans plusieurs pays, dont la Suisse, sur la manière de s'affranchir de toute dépendance des deux géants technologiques que sont les États-Unis et la Chine.

Au niveau de la politique de sécurité internationale aussi, l'ingérence étatique dans l'activité des fabricants de solutions TIC est discutée de longue date. Par exemple, le rapport de 2015 du groupe d'experts gouvernementaux des Nations Unies a formulé de premières normes visant à endiguer certains aspects spécifiques de telles pratiques. Or le rapport de suivi de 2017, qui aurait dû concrétiser ces normes, n'a pas obtenu le consensus nécessaire, le climat international s'étant dégradé dans l'intervalle.

3.1.3 Les fabricants de matériel et d'outils informatiques, jouet d'intérêts étatiques

Dans le fameux roman d'anticipation «1984» de George Orwell, critique véhémente des dérives autoritaires, la phrase «Qui contrôle le passé contrôle l'avenir. Qui contrôle le présent contrôle le passé» revient à plusieurs reprises, tel un credo. Une telle affirmation repose sur l'idée d'un accès absolu et sans entraves aux informations et aux données. Or aucun des pays d'origine des principaux fabricants de solutions TIC ne peut être soupçonné de telles visées hégémoniques ou totalitaires. Le fait de pouvoir ponctuellement accéder, dans le cadre légal en vigueur, aux informations et aux données des fabricants indigènes de matériel et de logiciels, constitue toutefois un avantage comparatif majeur qu'aucun de ces États ne cédera de son plein gré en s'imposant de lui-même des limites.

Il faut replacer dans ce contexte les déclarations publiques des États-Unis, réfractaires à l'idée que la Chine leur ravisse le leadership technologique. Autrement dit, les sanctions et les interdictions infligées aux fabricants doivent être vues comme des décisions de politique économique et de politique de sécurité, qui ne reposent que ponctuellement sur de véritables préoccupations sécuritaires, liées à un souci d'autoprotection. En effet, un recul des composants vendus par les fabricants américains priverait les États-Unis de la possibilité de procéder à des contrôles ciblés à travers ces solutions matérielles ou logicielles, dans l'entreprise des clients finaux.

Les fabricants de solutions informatiques sont l'outil des intérêts de leur pays d'origine et à l'avenir aussi, il leur faudra collaborer avec les services étatiques compétents, dans les limites du droit en vigueur. Il est peu probable que même dans un cas extrême, une entreprise privée s'oppose au droit en vigueur dans son État d'origine. De même, la Chine et les États-Unis continueront vraisemblablement à s'affronter pour dominer le marché mondial des produits TIC.

3.1.4 Absence d'alternatives

Il est permis de douter que dans un proche avenir, la place industrielle suisse conçoive des alternatives aux solutions matérielles et logicielles dominantes des fournisseurs étrangers. Même une politique industrielle coordonnée – solution atypique pour la Suisse – ne déploierait

qu'à long terme des effets dans ce domaine, pour autant qu'elle en ait. Or la numérisation des processus d'affaires, la cybersanté, la mise en place du réseau 5G et d'autres chantiers similaires ont déjà lieu, et les composants ou solutions TIC nécessaires ne sont pratiquement pas fabriqués en Suisse, ou alors seulement en petite partie et à grands frais.

Dotée d'une petite économie ouverte sur le monde, la Suisse est certes dépendante de fabricants informatiques étrangers. D'un autre côté, elle peut en profiter pour mettre en balance les intérêts respectifs des États qui ont une industrie informatique de pointe. Sur le terrain de la numérisation aussi, l'économie suisse continuera d'avoir besoin de composants fabriqués à l'étranger. C'est pourquoi il est essentiel de mettre en place une gestion rigoureuse des risques qui englobe tous les fabricants, les fournisseurs et les sous-traitants de solutions matérielles et logicielles, également en ce qui concerne les risques d'ingérence étatique.

Appréciation

Les constatations qui précèdent amènent aux appréciations suivantes, concernant la menace due aux fabricants informatiques dont la maison mère est étrangère:

- L'arsenal juridique des pays d'origine des principaux fabricants mondiaux de solutions matérielles et logicielles autorise presque toute collecte d'information sur des cibles étrangères, pour autant qu'elle serve les intérêts nationaux.
- Une simple obligation contractuelle faite aux entreprises du secteur de respecter le droit suisse ne saurait constituer une garantie suffisante. Elle devrait être assortie de conditions contraignantes, et accompagnée d'audits périodiques sur place. Ce constat vaut également pour les installations situées à l'étranger, si elles permettent d'exercer, sur le plan technique ou organisationnel, une influence sur l'entreprise suisse leur étant liée sur le plan organisationnel ou par des prises de participation au capital.
- En fonction du matériel et des logiciels, et aussi des prestataires choisis, il faudrait adopter des mesures adéquates pour prévenir autant que possible les accès non autorisés aux systèmes et données, ou du moins pour les identifier et y mettre fin.
- Tout projet d'acquisition devra inclure des mesures adaptées aux risques, dont les coûts seront pris en compte. Il se peut en effet que l'offre en apparence la plus avantageuse d'un prestataire entraîne des surcoûts internes au titre de mesures d'accompagnement, ou qu'il faille acquérir une autre prestation à des fins de contrôle et de protection.

4 Situation nationale

4.1 Espionnage

4.1.1 Cyberattaque contre l'OIAC – le laboratoire de Spiez aussi pris pour cible

Dans son dernier rapport semestriel, MELANI avait évoqué dans cette rubrique l'emploi abusif d'une invitation publique à une conférence internationale du laboratoire de Spiez. Lors d'une attaque ciblée, pour amener leurs victimes à cliquer sur l'annexe envoyée, les attaquants avaient plagié ladite invitation et l'avaient envoyée à diverses adresses, au nom de l'Office fédéral de la protection de la population (OFPP) et du laboratoire de Spiez.

Le laboratoire de Spiez est lui aussi dans la ligne de mire des pirates, comme l'a montré l'annonce, en septembre dernier, de l'arrestation de quatre personnes survenue le 13 avril 2018 aux Pays-Bas[1]. Il leur était reproché d'avoir voulu s'introduire dans le réseau sans fil de l'Organisation pour l'interdiction des armes chimiques (OIAC). Les quatre collaborateurs présumés du Service de renseignement militaire russe (GRU) seraient arrivés aux Pays-Bas via l'aéroport de Schiphol, avec des passeports diplomatiques, puis auraient loué un véhicule qu'ils ont stationné sur le parking de l'hôtel Marriott de La Haye. Cet établissement se situe juste à côté des bureaux de l'OIAC. Le coffre de l'auto renfermait tout un équipement conçu pour pénétrer dans les réseaux sans fil et pour lancer des cyberattaques. L'antenne de l'appareil prêt à l'emploi était dissimulée sous un manteau, sur la tablette arrière du véhicule. Les quatre espions arrêtés ont été expulsés le jour même des Pays-Bas, où ils ont dû laisser leur équipement.

Il s'est avéré que ce groupe s'intéressait aussi au laboratoire de Spiez. On a notamment retrouvé dans ses bagages un billet de train Utrecht – Bâle. Et les enquêteurs ont découvert sur un ordinateur portable des requêtes portant sur la section consulaire de l'ambassade de Russie à Berne, ainsi que sur le laboratoire de Spiez[2]. Tant l'OIAC que le laboratoire de Spiez ont participé aux investigations sur l'empoisonnement de l'ancien agent double russe Sergei Skripal et de sa fille, survenu en mars 2018 à Salisbury en Angleterre. Le Service de renseignement de la Confédération (SRC) a confirmé plus tard avoir mené cette opération avec ses partenaires néerlandais et britanniques, contribuant ainsi à éviter qu'une infrastructure suisse d'importance vitale ne soit victime d'actions illégales.

Le laboratoire de Spiez satisfaisait déjà auparavant aux prescriptions relatives aux objets particulièrement exposés. La protection a toutefois été accrue, et des mesures additionnelles ont été prises pour renforcer encore les normes de sécurité.

4.1.2 Opération Sharpshooter contre des infrastructures d'importance vitale

L'entreprise de cybersécurité McAfee a publié en décembre 2018 un rapport sur une campagne APT (*Advanced Persistent Threat*) visant des entreprises actives dans la défense, l'énergie, le secteur nucléaire ainsi que la finance[3]. La campagne intitulée Sharpshooter avait débuté le 25 octobre 2018 par l'envoi de documents infectés à des employés de 87 organisations du monde entier, mais principalement basées aux États-Unis. Selon ce rapport, la campagne était aussi dirigée contre des entreprises suisses du secteur financier. Le Service de renseignement de la Confédération n'a à ce jour pas trouvé de trace d'infection dans une entreprise suisse.

L'ingénierie sociale vise à amener les destinataires à ouvrir des documents infectés. En l'occurrence, une prétendue lettre de candidature renfermait un lien vers un document dans Dropbox, où était censé se trouver le dossier complet. La méthode a ceci d'insidieux que les services du personnel reçoivent souvent des candidatures spontanées, et donc ouvrent couramment de tels documents. Les entreprises ayant correctement mis en place des

---

1 https://www.government.nl/government/members-of-cabinet/ank-bijleveld/news/2018/10/04/netherlands-defence-intelligence-and-security-service-disrupts-russian-cyber-operation-targeting-opcw (état: le 31 janvier 2019)

2 https://www.justice.gov/opa/page/file/1098571/download (état: le 31 janvier 2019)

3 https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-sharpshooter.pdf (état: le 31 janvier 2019)

mesures de sécurité n'avaient toutefois pas grand-chose à craindre. L'infection se propageait par une macro contenue dans un document Word. De telles macros sont désormais bloquées dans beaucoup d'entreprises, ou alors elles ne s'activent que si la personne confirme avoir pris connaissance d'une mise en garde spécifique. Si la macro est exécutée malgré tous les avertissements, le maliciel fait entrer Sharpshooter dans la mémoire vive de Word. Puis il installe une porte dérobée modulaire, portant le nom de Rising Sun. Ce composant est à même de compiler et d'envoyer des informations concernant les documents, les noms d'utilisateurs, la configuration du réseau et les réglages du système. Le maliciel peut en outre télécharger d'autres fonctions. De même, il est capable d'effacer ses traces pour être indétectable. Il peut ainsi vider la mémoire, ou effacer ses activités. Le maliciel communique à cet effet avec un serveur de commande et de contrôle appartenant aux attaquants.

En analysant cette campagne, McAfee a découvert des similitudes avec d'autres attaques menées par le groupe Lazarus. En effet, Rising Sun renferme du code et des données de configuration qui proviennent de la famille de chevaux de Troie Duuzer. Or Duuzer avait participé à la cyberattaque contre Sony, attribuée au groupe Lazarus. Diverses entreprises de cybersécurité soupçonnent la Corée du Nord d'être à l'origine de ces attaques. Cependant, dans le cas actuel, une autre routine de décryptage est à l'œuvre. Il semblerait ainsi que Rising Sun ait été conçu à partir de Duuzer. Il n'est donc pas possible de dire avec certitude si cette campagne doit être réellement attribuée au groupe Lazarus. Ses méthodes, leurs traces et les maliciels sont entre-temps connus dans le monde entier, et se prêtent à des opérations sous fausse bannière (*false flag*), cherchant à faire soupçonner des tiers non impliqués.

4.2 Systèmes de contrôle industriels

4.2.1 Systèmes de contrôle industriels et Internet des objets

Il n'y a heureusement pas eu d'opération de sabotage majeure au deuxième semestre 2018. Pourtant, si aucune attaque ciblée contre des systèmes de contrôle industriels n'a été rendue publique, les infections commises à l'aide de maliciels usuels, comme les rançongiciels dans les réseaux des systèmes de contrôle, ont fait parler d'elles à l'étranger[4] (voir chapitre 5.3.5). Des installations interconnectées modernes sont régulièrement mises en service et des systèmes plus anciens, isolés jusque-là, sont reliés à Internet, leur intégration dans d'autres processus d'affaires visant à accroître l'efficience opérationnelle. Or la mise en réseau et le raccordement à Internet de toutes sortes d'objets (Internet des objets, IdO) accroissent d'autant le risque, pour les systèmes vulnérables, d'être victimes des multiples dangers d'Internet.

4.2.2 Les hackers font chou blanc à Ebikon – la commune repousse les attaques présumées contre son système d'approvisionnement en eau

La Suisse est réputée pour la qualité de son eau potable. Afin de garantir leur bon approvisionnement, les communes ne ménagent pas leurs efforts et rénovent régulièrement leurs installations. À cette occasion, elles optent pour les systèmes de contrôle dernier cri.

[4] https://dragos.com/year-in-review/ (état: le 31 janvier 2019)

Même des délégations d'autres pays d'Europe s'informent volontiers auprès de la Suisse sur les expériences réalisées avec l'exploitation des nouveaux systèmes[5].

Les cyberpirates du monde entier s'intéressent hélas aussi à de telles installations. La commune d'Ebikon a ainsi enregistré l'automne dernier plusieurs milliers de tentatives d'intrusion dans le réseau de son système d'approvisionnement en eau fonctionnant en pilotage autonome[6].

Des pirates aux mobiles variés sont constamment à la recherche de services atteignables de l'extérieur. Ils en testent par exemple les failles et cherchent à s'introduire dans les systèmes repérés, à l'aide de données d'accès standard connues ou d'identités obtenues lors de fuites de données. Dans le cas d'Ebikon, ces tentatives sont heureusement restées vaines et, après leur découverte, les mesures de sécurité ont même été renforcées. À supposer même que la prévention et la détection n'aient pas correctement fonctionné et que l'attaque ait abouti, la commune aurait été en mesure d'arrêter les systèmes automatisés et de poursuivre l'exploitation des installations en mode manuel.

Le cas d'Ebikon montre de façon exemplaire comment les mesures prévues aux différentes phases du cadre de référence NIST de cybersécurité[7] contribuent à déjouer au quotidien les cyberattaques visant les infrastructures d'importance vitale, et le cas échéant à bien réagir. Il vaut la peine non seulement d'investir dans la protection préventive, mais aussi de se préparer à des incidents concrets. La norme minimale de l'Office fédéral pour l'approvisionnement économique du pays (OFAE) offre ici une solution de mise en œuvre, basée sur le cadre de référence NIST.

Recommandation

Dans le cadre de la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), adoptée par le Conseil fédéral en 2012, l'Office fédéral pour l'approvisionnement économique du pays (OFAE) a analysé la vulnérabilité aux cyberrisques dans différentes branches d'importance vitale. Il a notamment examiné l'approvisionnement en électricité, en eau potable et en aliments, ainsi que les transports par la route et le rail. Fort de ces résultats, l'OFAE a mis au point une norme minimale pour améliorer la résilience informatique. Même si cette norme est plus spécialement destinée aux exploitants d'infrastructures d'importance vitale en Suisse, toute entreprise peut l'appliquer.

La norme minimale pour augmenter la résilience informatique comprend diverses fonctions: identifier, protéger, détecter, réagir et récupérer. Elle donne aux utilisateurs 106 indications concrètes pour améliorer leur propre résilience face aux cyberrisques:

Norme minimale visant à renforcer la résilience informatique

https://www.bwl.admin.ch/bwl/fr/home/themen/ikt/ikt_minimalstandard.html

5 https://www.ebikon.ch/verwaltung/aktuelles/news/daenemark-auf-besuch-in-ebikon (état: le 31 janvier 2019)

6 https://www.inside-it.ch/articles/53204 (état: le 31 janvier 2019)

7 https://www.nist.gov/cyberframework (état: le 31 janvier 2019)

4.2.3 MadIoT – danger d'un réseau d'appareils électroménagers zombies

Beaucoup de gens se souviennent de la panne électrique géante survenue en Italie le 28 septembre 2003. Une réaction en chaîne avait abouti à une surcharge des réseaux de transport, et à un black-out dans tout le pays[8]. Au départ, en effleurant les câbles d'une ligne à haute tension, un arbre mal élagué avait provoqué un arc électrique et un court-circuit en Suisse. Par un malheureux concours de circonstances, le réseau était devenu instable et s'était effondré. Or qu'arriverait-il si quelqu'un provoquait volontairement l'instabilité du réseau, en manipulant la consommation d'un grand nombre d'appareils électroménagers?

Des chercheurs de l'université de Princeton ont examiné la question, dans une étude[9] présentée en août 2018 au USENIX Security Symposium, conférence dédiée à la sécurité informatique. Leur analyse est fondée sur l'hypothèse voulant qu'un acteur malveillant parvienne à créer un réseau de zombies à partir d'appareils de l'Internet des objets (*Internet of things*, *IoT*) gourmands en énergie, à l'instar des équipements de climatisation et de chauffage, ou des lave-linge. Pour peu qu'il coordonne géographiquement leur consommation de puissance et qu'il la modifie brusquement à grande échelle, les scénarios des chercheurs indiquent une instabilité du réseau similaire à celle ayant entraîné le black-out italien évoqué plus haut[10].

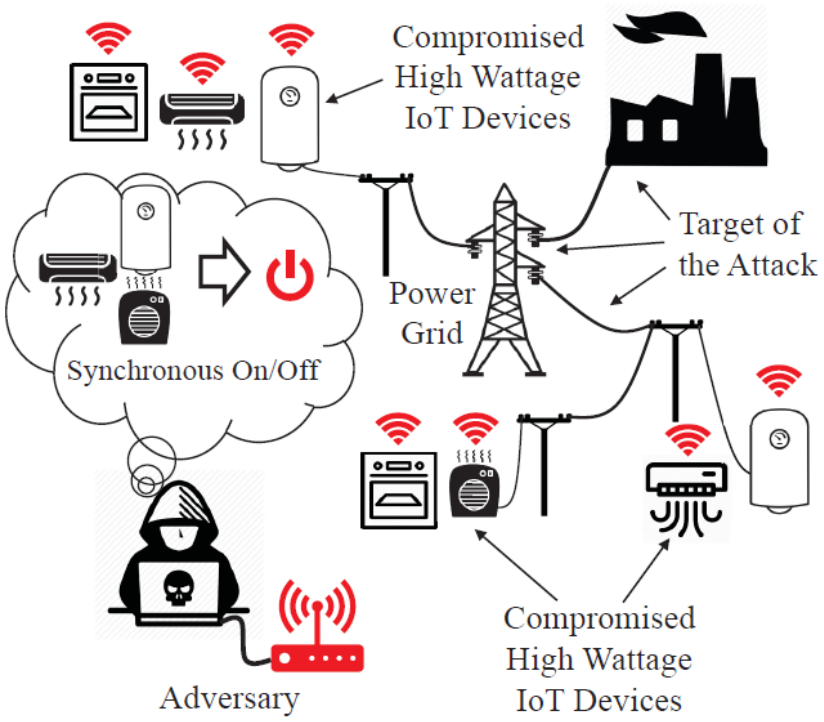

Figure 1: Schéma d'une attaque de type *Manipulation of demand via IoT* (Quelle: usenix.org, https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-soltan.pdf)

8 http://www.rae.gr/old/cases/C13/italy/UCTE_rept.pdf (état: le 31 janvier 2019)

9 https://www.usenix.org/system/files/conference/usenixsecurity18/sec18-soltan.pdf (état: le 31 janvier 2019)

10 https://securityintelligence.com/how-an-iot-botnet-could-breach-the-power-grid-and-cause-widespread-blackouts/ (état: le 31 janvier 2019)

De tels scénarios d'attaque sont inédits en ce sens que pour provoquer la panne, les agresseurs ne perturbent pas la production d'énergie ou son transport, mais agissent sur les consommateurs. Or bien souvent, les terminaux des consommateurs ne sont que faiblement protégés, en comparaison notamment des centrales électriques ou des réseaux de transport qui, depuis des années, consacrent beaucoup de ressources à leur sécurité.

La stabilité du réseau électrique tient à la fiabilité des prévisions de consommation, qui reposent essentiellement sur les valeurs empiriques du passé. Inversement, une manipulation contraire aux prévisions et soigneusement coordonnée, entre de nombreux appareils vulnérables à forte consommation, aurait tôt fait d'épuiser les réserves de tolérance usuelles. Par exemple, un pirate informatique pourrait régler simultanément, en plein été, tous les radiateurs électriques sur la pleine puissance. L'expression consacrée ici est manipulation of demand via IoT (MadIoT).

Les hypothèses sous-jacentes à ces simulations peuvent paraître tirées par les cheveux. Toutefois, les retombées du réseau de zombies Mirai en 2016 ont clairement montré le potentiel de nuisance d'un réseau d'appareils électroménagers zombies. En 2017 déjà, le concepteur anglais de solutions de sécurité Sophos avait démontré dans un essai que dans les maisons intelligentes, les appareils connectés sont exposés à des attaques simultanées de divers côtés[11]. Ce prestataire de services de sécurité avait constaté au passage une forte concentration en Suisse d'appareils de l'IdO susceptibles d'être pris pour cibles.

En plus des exploitants d'infrastructures énergétiques, les fabricants d'appareils connectés doivent contribuer à éviter que de telles attaques ne se concrétisent. Bien des efforts visent à instaurer des règles de bonnes pratiques, qui ne sont toutefois obligatoires que dans très peu de régions et de domaines. Une analyse[12] du Département britannique du numérique, de la culture, des médias et du sport (Department for Digital, Culture, Media & Sport, DCMS) offre un bon aperçu de la situation, et compare les prescriptions et directives en vigueur.

11 https://www.computerworld.ch/security/hacking/smart-home-in-minuten-hacker-da-1435426.html (état: le 31 janvier 2019)

12 https://iotsecuritymapping.uk/ (état: le 31 janvier 2019)

Recommandation

Si vous découvrez dans Internet des systèmes de contrôle mal sécurisés, voire ouverts au premier venu, communiquez-nous leurs coordonnées, afin que nous puissions prévenir l'exploitant:

Formulaire d'annonce MELANI

https://www.melani.admin.ch/melani/fr/home/meldeformular/formulaire.html

Mesures de protection des systèmes de contrôle industriels (SCI)

https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/mesures-de-protection-des-systemes-de-controle-industriels--sci-.html

4.3 Attaques (DDoS, *defacement*, *drive-by download*)

En Suisse, les particuliers, les organisations et les entreprises continuent à faire l'objet de cyberattaques en tous genres.

4.3.1 Détournement de modems de Quickline en vue d'attaques par amplification SNMP

Le 11 octobre 2018, l'opérateur bernois Quickline a fait savoir dans un communiqué de presse qu'il avait subi pendant deux semaines des perturbations d'exploitation irrégulières. Les dérangements concernaient tant la télévision qu'Internet et la téléphonie, mais le problème n'a pas affecté tous les clients au même moment ni avec la même ampleur. La cause a été identifiée: c'était une vulnérabilité d'un type particulier de modem. Des analyses ont montré que les pirates informatiques n'en voulaient pas directement aux clients, qui ont été simplement instrumentalisés en vue du lancement d'une cyberattaque contre des tiers. Il s'agissait d'une attaque par amplification utilisant le protocole *simple network management* (SNMP). Dans ce mode opératoire, une requête via SNMP est tout d'abord envoyée aux appareils. La réponse, d'une taille très supérieure, va être redirigée vers une cible dans le but de la surcharger. Les agresseurs n'ont pas besoin d'infecter au préalable les modems, ils tirent parti du fait que le résolveur SNMP est ouvert. Si les perturbations sont apparues chez les clients, c'est que les requêtes ont saturé de manière involontaire les modems et entraîné ainsi des instabilités. Comme les clients de Quickline n'utilisent pas tous le même type de modem, seuls 9000 clients (5 %) ont été touchés. On ignore combien de temps les modems ont été sujets aux attaques par amplification SNMP. Quickline a pris plusieurs mesures pour corriger cette vulnérabilité. En particulier, des filtres ont été mis en place dans le réseau, et les modems en question ont été davantage sécurisés. Quickline a également déposé une plainte pénale contre inconnu.

4.3.2 Données fiscales sur Internet – application mal configurée

Beaucoup de gens détestent remplir leur déclaration d'impôts et éprouvent des difficultés à le faire. Aussi une entreprise zurichoise du nom de Zurich Financial Solutions (www.zufiso.ch) a-

t-elle conçu l'application pour smartphone steuern59.ch, pour faciliter la vie des contribuables. L'application peut être achetée et téléchargée depuis Google Play, ou dans l'Apple Store. Elle promet de compléter à votre place votre déclaration d'impôts pour 59 francs seulement. Il suffit à cet effet de photographier avec son smartphone les documents nécessaires, puis de les charger dans l'application. Il s'est toutefois avéré que tous ces documents sensibles étaient stockés dans le nuage (*cloud*), sur un serveur non sécurisé d'Amazon Web Services (AWS), accessible à tous les utilisateurs d'AWS. Dans les paramètres par défaut, les données sont configurées comme «privées», et donc personne ne peut les voir. Si on sélectionne dans les paramètres «public», une mise en garde s'affiche[13]. Les programmeurs ayant développé l'application, qui apparemment avaient été recrutés en Inde, ont commis ici une erreur: ils ont réglé ce paramètre sur «public» et ont visiblement oublié de rétablir le réglage «privé» d'origine. Un chercheur en cybersécurité a découvert cette erreur de configuration et en a informé la société exploitante. Mais ce n'est que lorsqu'il a signalé l'incident au magazine allemand Heise que l'entreprise zurichoise a pris contact avec le chercheur[14]. Un tel incident soulève la question de la divulgation responsable des vulnérabilités (responsible disclosure). Comment les chercheurs devraient-ils annoncer les vulnérabilités découvertes, et que devraient ensuite entreprendre les entreprises ainsi prévenues? La société gérant l'application steuern59.ch a admis en avoir délocalisé la production en Inde. Elle ne s'était pas rendu compte du travail bâclé des développeurs. L'incident concernait 80 utilisateurs. Tous ont été informés de l'incident, une fois la faille de sécurité comblée conjointement avec l'expert en sécurité. Désormais, les données sont stockées en Suisse, dans un nuage baptisé «n'cloud»[15].

4.4 Ingénierie sociale et phishing

4.4.1 Recrudescence des appels frauduleux aux entreprises

Au début de juillet 2018, des escrocs se faisant passer pour des employés de banque ont à nouveau sévi. Concrètement, les auteurs des appels invitent à effectuer des paiements, ou prétendent qu'il leur faut procéder à une mise à jour du site e-banking et la tester ensuite.

Typiquement, les agresseurs tentent de persuader les collaborateurs d'une société d'installer un logiciel d'accès à distance (par ex. NTR-Cloud, Teamviewer), puis se connectent à l'ordinateur de leur victime et feignent d'exécuter une mise à jour de son e-banking. Ils expliquent alors qu'un test des fonctionnalités du système de paiement s'impose et demandent à la victime de se connecter au e-banking de l'entreprise et d'effectuer un virement test. Et si le paiement est protégé par signature collective, ils essaieront d'amener leur interlocuteur à récolter toutes les signatures nécessaires pour autoriser une telle opération.

Dans un autre scénario, les collaborateurs sont priés de renoncer pour quelques jours à l'e-banking, sous prétexte de mises à jour urgentes. Si des transactions ne peuvent attendre, la victime est invitée à appeler le numéro indiqué par les escrocs. À supposer qu'elle le fasse, tant son nom d'utilisateur que son mot de passe et celui à usage unique lui sont demandés.

---

13 https://docs.aws.amazon.com/AmazonS3/latest/dev/s3-access-control.html (état: le 31 janvier 2019)

14 https://www.inside-it.ch/articles/52273 (état: le 31 janvier 2019)

15 https://www.heise.de/newsticker/meldung/Steuern59-ch-Geschaeftsfuehrung-entschuldigt-sich-fuer-Datenleck-4169772.html (état: le 31 janvier 2019)

L'escroc a ainsi accès à l'e-banking de l'entreprise. La procédure peut d'ailleurs se répéter aussi longtemps que la victime ne se méfie pas.

Recommandation

Ces exemples montrent que les méthodes d'ingénierie sociale restent d'une actualité brûlante. Les entreprises feraient donc bien de vérifier les informations accessibles en ligne à leur sujet. N'indiquez jamais sur le site Internet de votre entreprise les adresses nominatives des membres de la direction ou de vos collaborateurs – utilisez plutôt des adresses génériques (par ex. «comptabilite@xyz.ch»).

Méfiez-vous si on vous soumet une demande insolite, et considérez d'un œil critique votre interlocuteur. Le cas échéant, il est vivement indiqué de vérifier en interne la légitimité de la demande formulée. Sensibilisez à ce genre d'incidents les collaborateurs, à commencer par les personnes occupant des postes clés.

Ne révélez jamais vos données d'accès personnelles à des tiers par téléphone, par courriel ou sur Internet. Un établissement financier ne vous demandera jamais lors d'un appel téléphonique, par Internet ou par SMS de lui indiquer des données confidentielles.

N'installez jamais de logiciel et ne suivez aucun lien non plus, si on vous en fait la demande au téléphone ou par écrit. Ne permettez jamais à un tiers d'accéder à votre ordinateur. Aucune banque ne vous demandera de participer à de quelconques tests de mises à jour de sécurité.

Tous les processus liés au trafic des paiements devraient faire l'objet de règles internes, et les collaborateurs s'y tenir dans tous les cas.

4.4.2 Tentatives de chantage – un coup de bluff qui rapporte gros

Une escroquerie apparue il y a quelque temps est étroitement liée à l'utilisation des médias sociaux. Tout commence d'ordinaire par une demande d'amitié, que transmet une personne dotée d'un physique attrayant. Elle flirte avec sa victime potentielle et l'amène à se dénuder devant sa webcam. La victime ignore qu'elle est filmée. Le matériel vidéo ainsi obtenu servira ensuite à lui extorquer de l'argent. Cette méthode de chantage a été baptisée «sextorsion»: si la personne ne paie pas la rançon, le matériel sera envoyé à tous ses contacts. L'escroquerie implique un certain effort et comme un contact direct est établi avec la victime, le maître chanteur encourt un risque accru d'arrestation.

Depuis mars 2018 (juillet 2018 en Suisse), les escrocs tirent parti d'une méthode qui exige bien moins d'efforts et qui n'est guère risquée. Ils prétendent dans un courriel avoir pris le contrôle de l'ordinateur et de la webcam du destinataire, et menacent de publier des images et des vidéos de lui à caractère sexuel. Il s'agit toutefois ici de pur bluff et les criminels n'ont pas réellement accès à l'ordinateur de leur victime. Cette escroquerie a reçu le nom de «fake sextorsion». Au deuxième semestre 2018, elle a permis aux criminels d'empocher beaucoup d'argent, en multipliant les demandes de rançon. L'analyse des adresses bitcoin indiquées dans les courriels transmis à MELANI montre que près de 100 bitcoins ont été versés durant cette période, soit l'équivalent de 360 000 francs. Ce gain est d'autant plus élevé que l'envoi en masse de courriels ne coûte pratiquement rien. On ignore cependant si les adresses bitcoin signalées ne sont utilisées que pour la «fake sextorsion» et si elles n'ont reçu des paiements que de victimes suisses.

Bien souvent, un mot de passe provenant d'une fuite de données est ajouté dans le courriel, pour faire office de soi-disant preuve du piratage de l'ordinateur. Dans la plupart des cas, il s'agit toutefois d'un mot de passe ancien. Des numéros de téléphone portable ont aussi été utilisés, pour faire croire au destinataire que son téléphone avait été piraté. Il s'agit cependant de données non sensibles qui, à la suite de différentes fuites d'informations, ont davantage circulé ces derniers temps. Dans un autre scénario, le courriel semble provenir de l'adresse personnelle de la victime, afin de lui prouver que sa messagerie a été infiltrée. En réalité, l'adresse de l'expéditeur est falsifiée, ce qui est très facile à faire, même sans connaissances particulières d'informatique. L'agresseur n'a pas besoin ici d'avoir accès au compte de messagerie de la victime.

Ces courriels frauduleux sont rédigés dans plusieurs langues, dont l'allemand, le français, l'italien et l'anglais. Bien que le mode opératoire reste en gros le même, les criminels veillent toujours à peaufiner leur tactique, afin de renforcer la pression sur leurs victimes et de les amener ainsi à verser la rançon demandée. Le graphique ci-dessous présente les principales innovations apportées par les criminels au cours de l'année 2018.

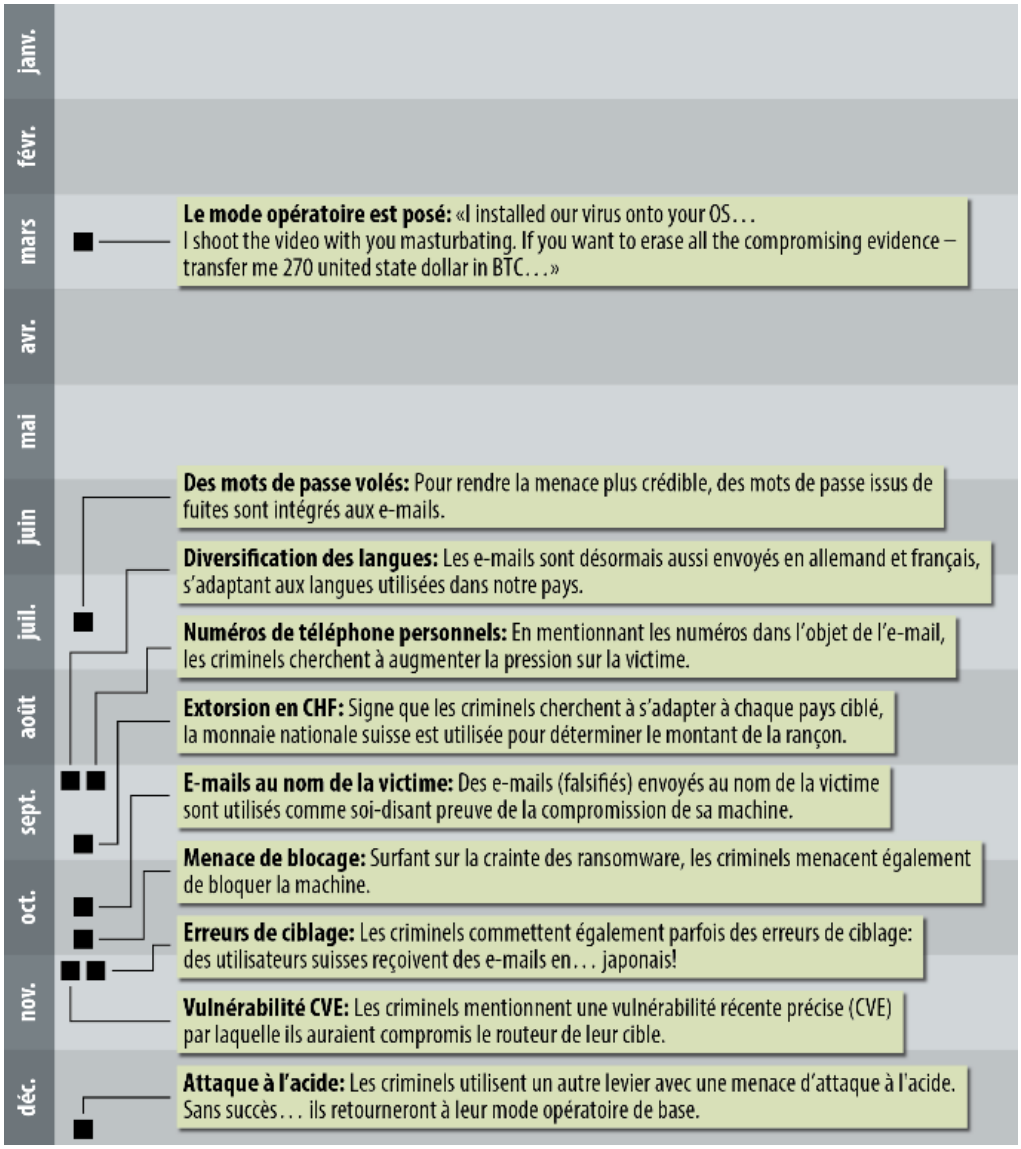

Figure 2: Évolution des scénarios de fake sextorsion durant l'année 2018

Des menaces d'attaque à l'acide ou à la bombe ont même été lancées en décembre. Dans un cas comme dans l'autre, il fallait verser des bitcoins pour prévenir l'agression. On a cependant constaté que les destinataires de telles menaces et intimidations prennent peur, et qu'ils auront davantage tendance à prendre contact avec les autorités qu'à payer une rançon. Cela peut s'expliquer par le plus grand potentiel d'intimidation d'une telle menace sur l'intégrité physique et par le fait que les criminels ne prétendent pas posséder de matériel compromettant. Il ressort du moins des adresses bitcoin signalées à MELANI qu'aucune transaction n'a été effectuée dans ce contexte.

Recommandation

Tant que les victimes céderont aux maîtres chanteurs, ceux-ci continueront de sévir. Tout indique qu'il y aura de nouvelles vagues de courriels frauduleux, qu'elles feront des émules et que le nombre d'escroqueries de ce type va encore augmenter. Vous ne devez en aucun cas payer une rançon. Par ailleurs, vous pouvez participer à la prévention de la population en discutant de cette thématique avec votre entourage professionnel et personnel. En sensibilisant vos collègues, vos connaissances et vos proches à ce stratagème, vous éviterez qu'ils n'en soient victimes.

INFO

Le site «https://www.stop-sextortion.ch», lancé par les autorités, propose des informations sur ce thème et offre la possibilité de signaler des courriels frauduleux.

4.4.3 Fraude au faux fournisseur basée sur les données d'accès à Office 365

Les données d'accès à Office 365, la version en ligne des produits Office, intéressent beaucoup les cybercriminels, comme l'ont déjà signalé de précédents rapports semestriels. [16] Avec plus de 100 millions d'utilisateurs mensuels, les comptes Office 365 sont devenus une proie attrayante. L'attaque commence par un banal courriel signalant par exemple que l'espace de stockage est saturé, et qu'une connexion au lien indiqué permettra de régler le problème. L'internaute imprudent aboutit à un site frauduleux.

Durant la période sous revue, les données d'accès à Office 365 collectées de cette façon ont servi à mener un nombre croissant de fraudes au faux fournisseur (*wire fraud*). Concrètement, les escrocs recherchent dans les comptes compromis des factures électroniques, ils les copient en modifiant leur numéro IBAN, puis les réexpédient. Ils s'intéressent tout particulièrement aux entreprises facturant de gros montants à des destinataires se trouvant à l'étranger. D'une part, le profit est considérable en pareil cas, d'autre part il est plus difficile de détecter un faux compte fournisseur situé à l'étranger.

Un exemple rapporté par le prestataire de services de sécurité Proofpoint montre à quel point de telles attaques peuvent être sophistiquées. Après avoir accédé au compte Office 365 du

[16] MELANI, rapport semestriel 2/2017 https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2-2017.html (état: le 31 janvier 2019)

directeur général d'une entreprise, les escrocs ont passé au crible ses courriels et son calendrier, afin d'inventer une histoire plausible. Pendant une rencontre planifiée entre ce directeur et un fournisseur important, un des pirates informatiques a écrit à son responsable des finances de verser un million de dollars afin que la transaction aboutisse. Il a ajouté, toujours au nom du directeur général, être en pleine séance et ne pas avoir la possibilité de lui parler au téléphone. Le responsable des finances a suivi les instructions et procédé au paiement. [17]

Selon le Bureau fédéral d'enquête américain (FBI), les escroqueries de type BEC (Business Email Compromise) menacent entre-temps sérieusement les finances des entreprises. Aux États-Unis seulement, les pertes liées à la fraude BEC signalées à l'Internet Crime Complaint Center (IC3) atteignent 1,2 milliards de dollars en 2018. Le secteur immobilier y serait particulièrement exposé. [18]

Recommandation

Si la société a opté pour une solution en nuage basée sur Office 365, les escrocs ayant dérobé des données d'accès pourront s'emparer de tous ses documents. Il est donc très imprudent, à l'heure actuelle, de se contenter du nom d'utilisateur et de son mot de passe pour protéger ce genre de données. L'authentification à deux facteurs sera privilégiée partout où c'est possible. Encore faut-il que sa mise en place soit irréprochable. Car même en cas d'accès avec connexion unique (single sign-on) ou d'authentification à plusieurs facteurs, une intrusion demeure possible si l'authentification n'est pas mise en place pour l'ensemble des systèmes. Les agresseurs sauront exploiter les failles.

Il convient encore de sensibiliser les collaborateurs à la nécessité que chacun respecte en tout temps les processus et les mesures de sécurité définis par l'entreprise. Il est notamment recommandé de prévoir, pour tout virement, le principe des quatre yeux avec la signature collective.

4.4.4 Jeux-concours truqués

Du chocolat à volonté pendant un an, un bon d'achat d'IKEA ou un nouvel iPhone – les prétendus jeux-concours sont très répandus dans Internet. Nous en avons déjà parlé dans notre dernier rapport semestriel[19]. Les questions sont choisies de façon à ce que n'importe qui trouve la réponse. Les auteurs veulent en effet un maximum de «gagnants», afin d'identifier le plus grand nombre de victimes possible. Une nouvelle variante est apparue durant la période sous revue. Les gagnants potentiels sont attirés sur Facebook vers une prétendue page de Denner leur signalant qu'ils ont gagné 750 francs. Après avoir inscrit leur numéro de téléphone et leur nom, les participants sont priés d'appeler un numéro surtaxé (0901). Pour obtenir le prétendu gain, il leur faut répondre à un très grand nombre de

17 https://www.proofpoint.com/us/corporate-blog/post/microsoft-office-365-attacks-circumvent-multi-factor-authentication-lead-account (état: le 31 janvier 2019)

18 https://www.ic3.gov/media/annualreport/2018_IC3Report.pdf (état: le 25 avril 2019)
https://www.ic3.gov/media/2018/180712.aspx#fn2 (état: le 31 janvier 2019)

19 MELANI, rapport semestriel 1/2018
https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2018-1.html (état: le 31 janvier 2019)

questions. En réalité, les questions posées ne servent qu'à prolonger le plus longtemps possible la communication avec le numéro surtaxé. Il va sans dire que le gain est fictif.

Recommandation

La prudence est de mise face aux promesses de gain alléchantes, qu'il ne faut surtout pas transmettre plus loin. La meilleure attitude consiste à les ignorer.

INFO

La Fondation pour la protection des consommateurs (SKS) a compilé divers conseils utiles en la matière:

https://www.konsumentenschutz.ch/was-tun-bei-einer-abofalle/

4.4.5 Phishing

De nombreux courriels de phishing ont également circulé au deuxième semestre 2018. Leur teneur ne varie guère: les uns invitent la victime à indiquer les données de sa carte de crédit, pour qu'elles puissent être «vérifiées», alors que d'autres la prient de saisir sur la page indiquée en hyperlien son nom d'utilisateur et son mot de passe. Pour paraître plus respectables, de tels courriels usurpent souvent les logos d'entreprises connues ou du service concerné.

Figure 3: Sites de phishing annoncés et confirmés par semaine sur le site antiphishing.ch au deuxième semestre 2018

Au total, 5756 sites de phishing ont été dénoncés en 2018 sur le portail antiphishing.ch exploité par MELANI. La figure 3 indique le nombre d'annonces hebdomadaires de pages de phishing. Leur nombre a explosé au cours des trois derniers mois de 2018, en raison surtout de courriels de phishing envoyés au nom d'UBS par des escrocs cherchant à faire main basse sur les données de cartes de crédit.

Figure 4: Phishing contre les cartes de crédit UBS au dernier trimestre 2018

Il y a plusieurs années déjà, MELANI avait prédit l'essor des pages de phishing hébergées sur des sites dont l'adresse inclut le cadenas et débute par «https://». Certes, l'évolution a été plus lente que prévu mais, depuis le troisième trimestre 2016, l'entreprise PhishLab a constaté une augmentation continue et a relevé à la fin de 2018 que pour la première fois, plus de 50 % des sites de phishing utilisent le protocole sécurisé https. Ce constat tient cependant en grande partie au fait que, globalement, toujours plus de sites Internet sont en https. Et comme beaucoup des pages de phishing sont hébergées sur des sites ayant été piratés, les malfaiteurs bénéficient le cas échéant, à leur insu parfois, de la confiance accrue accordée par les internautes à ce genre de sites.

4.4.6 Demandes de blocage selon l'art. 15 de l'ordonnance sur les domaines Internet (ODI)

Par souci de combattre toute utilisation abusive des adresses Internet suisses et d'épargner de graves risques aux internautes, la révision de l'ordonnance sur les ressources d'adressage dans le domaine des télécommunications (ORAT, RS 784.104; en vigueur depuis le 1er janvier 2010) a introduit un article en vertu duquel le registre «.ch» (SWITCH) doit bloquer un nom de domaine et supprimer l'assignation y relative à un serveur de noms si des raisons fondées permettent de supposer que le nom de domaine en question est utilisé soit pour accéder par des méthodes illicites à des données sensibles (phishing), soit pour diffuser des logiciels malveillants (maliciels), et si un service de lutte contre la cybercriminalité reconnu par l'Office fédéral de la communication (OFCOM) a présenté une demande de blocage.

Depuis le 15 juin 2010, MELANI a été agréée à ce titre par l'OFCOM, et a ainsi la compétence de proposer à SWITCH de bloquer et supprimer les noms de domaine en «.ch», en cas de soupçon fondé de phishing ou de diffusion de maliciels.

Les blocages demandés par MELANI portent le plus souvent sur des sites de phishing. Alors qu'en 2016 et en 2017 plus de 30 sites avaient été bloqués, seize seulement l'ont été en 2018. Ce petit nombre tient à ce qu'une telle mesure n'intervient que pour les sites entièrement dévolus au phishing ou à la propagation de maliciels. Or les pages de phishing se trouvent la plupart du temps sur des systèmes compromis qui renferment d'autres contenus encore. Le cas échéant, au lieu de bloquer le domaine, MELANI cherchera à retirer du réseau le site frauduleux, avec le fournisseur d'accès compétent.

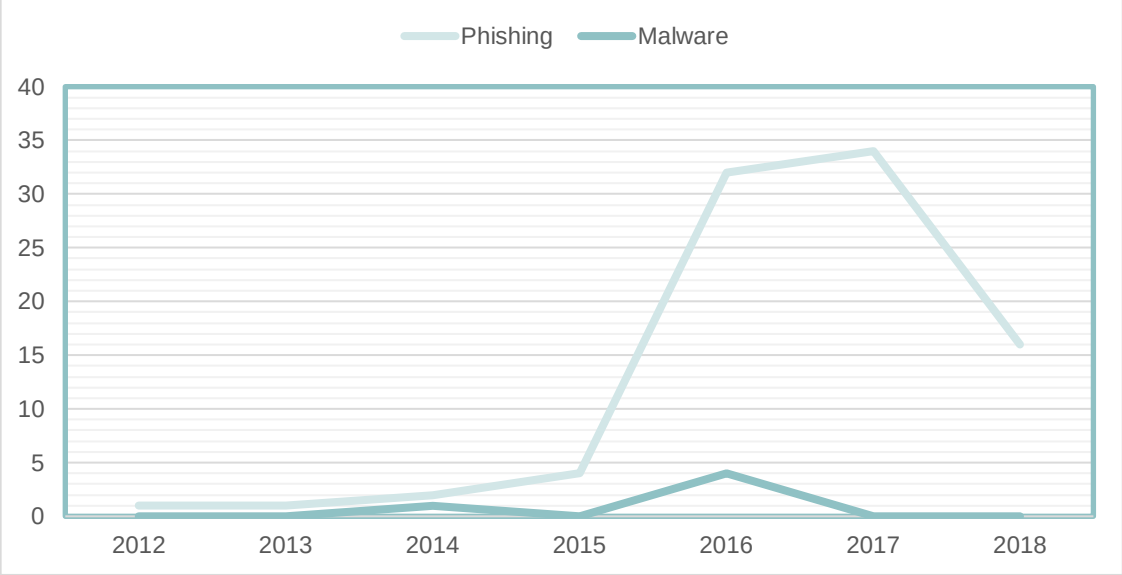

Figure 5: Demandes de blocage faites par MELANI en vertu de l'art. 15 ODI. La courbe bleu clair concerne les pages de phishing, et la courbe bleu foncé les sites renfermant des maliciels.

4.5 Logiciels criminels (crimeware)

De nombreuses infections dues à des logiciels criminels ont été constatées au deuxième semestre 2018. La statistique de la figure 6 montre la répartition des principaux maliciels en Suisse. Il y a également des maliciels très problématiques, mais qui n'apparaissent pas dans la statistique, à l'instar du cheval de Troie bancaire Retefe.

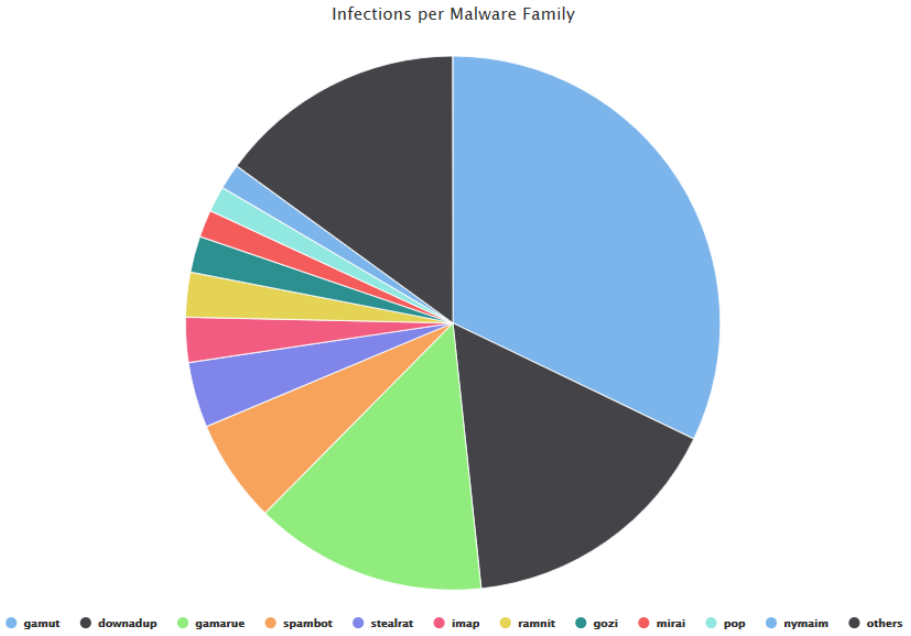

Figure 6: Répartition des maliciels en Suisse, selon les informations en possession de MELANI. La date de référence est le 31 décembre 2018. Des données actuelles sont publiées sous: https://www.govcert.admin.ch/statistics/malware/.

Pour la première fois depuis que cette statistique existe, le maliciel Downadup (aussi appelé Conficker) n'apparaît plus en première place. Il a été détrôné au deuxième semestre 2018 par Gamut, responsable de l'envoi d'une bonne partie des courriers indésirables au niveau mondial. Gamut expédie surtout des offres d'emploi d'agents financiers (passeurs d'argent, *money mules*)[20]. Il est suivi en troisième position par Gamarue[21], nouveau venu également connu sous le nom d'Andromeda, un programme de téléchargement (*downloader*) qui peut ensuite introduire n'importe quel autre virus sur l'ordinateur infecté. Puis viennent en quatrième et cinquième positions les maliciels Spambot et Stealrat, tous deux spécialisés dans l'envoi de pourriels. Stealrat opère à partir de domaines infectés, notamment sur des sites WordPress, Joomla! ou Drupal. Les pourriels expédiés depuis des serveurs de messagerie légitimes sont d'autant plus difficiles à filtrer. Le premier cheval de Troie bancaire, Gozi, ne vient qu'en huitième position. Quant à Mirai, maliciel formant des armées de zombies célèbres pour avoir paralysé le prestataire de services Internet Dyn, il est de retour dans la liste des dix logiciels criminels les plus actifs, dont disparaît le virus de cryptominage Monero Miner.

4.5.1 Retefe, principal cheval de Troie bancaire de Suisse

Retefe fait toujours partie des principaux chevaux de Troie bancaires de Suisse. Ce maliciel diffusé par courriel au nom d'entreprises ou d'institutions bien connues, s'en prend tant à Windows qu'aux systèmes macOS. L'annexe renferme généralement un document Word malveillant, comme une prétendue facture de boutique en ligne, une confirmation de distribution d'une société de livraison de colis, ou des informations de l'administration fédérale à propos d'une contamination d'eau potable. La figure 7 indique le nombre de vagues de pourriels expédiées ces trois dernières années.

[21] https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/BotNetze/Avalanche/Schadsoftware/Andromeda_Gamarue.html (état: le 31 janvier 2018).

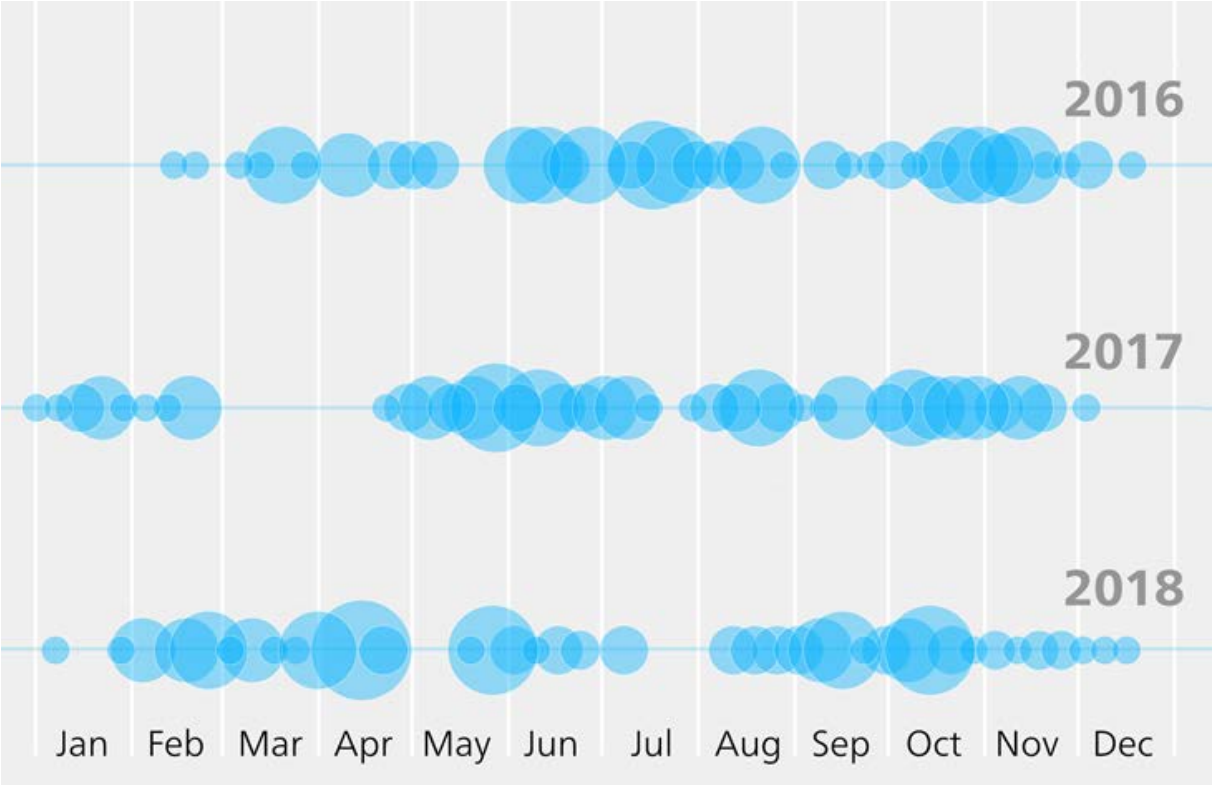

Figure 7: Vagues du maliciel Retefe lancées ces trois dernières années. La taille des disques bleus correspond au nombre de vagues de pourriels.

Retefe indique des informations personnelles des destinataires, comme le numéro de téléphone ou l'adresse postale, afin que l'envoi gagne en crédibilité. Ces informations proviennent de fuites de données. Retefe se concentre pour l'instant sur la clientèle privée en Suisse, au Liechtenstein et en Norvège. La clientèle commerciale est moins touchée. Outre que les systèmes de paiement hors ligne ne font pas partie de ses cibles directes, Retefe doit modifier les paramètres proxy et installer un certificat racine ainsi que le logiciel Tor. Sur les ordinateurs des entreprises, les droits requis à cet effet sont généralement restreints, ce qui rend de telles manipulations impossibles.

Recommandation

La prudence est de mise avant d'ouvrir les documents Word. D'ordinaire, les transactions des entreprises ou organisations (par ex. factures, offres, etc.) s'effectuent au moyen de fichiers PDF et non de documents Word.

4.5.2 Réapparition de Gozi

Alors que les attaques basées sur Gozi avaient quasiment disparu de Suisse, une vague de pourriels renfermant une fausse facture de Swisscom a été lancée le 28 novembre 2018. Les escrocs se servent habilement de méthodes d'ingénierie sociale.

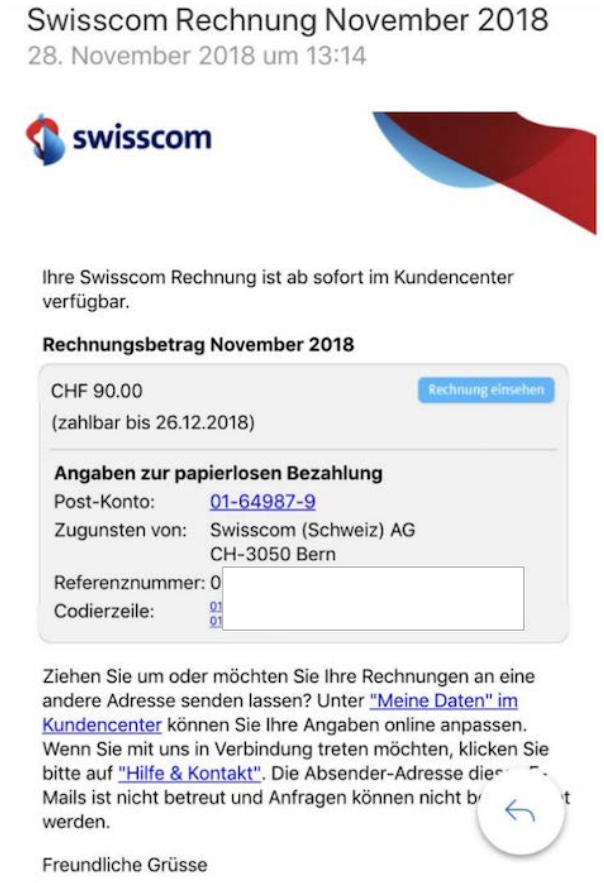

Figure 8: Fausse facture de Swisscom munie d'un lien vers un fichier malveillant

Le courriel renferme un lien à un fichier ZIP contenant un script Visual Basic caché, qui démarre dans l'utilitaire bitsadmin via une commande en langage Powershell[22]. Le maliciel proprement dit est ainsi téléchargé et sauvegardé dans le profil temporaire des utilisateurs. Il peut alors commencer à sévir.

Outre les indications relatives aux serveurs de commande et de contrôle (C&C) fixes, la configuration de Gozi renferme les données nécessaires à l'utilisation d'un algorithme de génération de noms de domaine. Ces noms reposent sur des mots de la Constitution américaine choisis au hasard et recombinés[23]. Cette fonctionnalité permet de définir des points de contact dynamiques avec les serveurs C&C, en cas de défaillance de ceux figurant dans la programmation fixe. Dans le cas d'espèce, Gozi ne s'en est pas servi.

Gozi précise dans sa configuration non seulement les banques à attaquer, mais aussi les produits logiciels à détecter. Ce maliciel prend aussi pour cibles les logiciels de paiement hors ligne, et donc directement aussi les entreprises.

22 https://docs.microsoft.com/en-us/windows/desktop/bits/bitsadmin-tool (état: le 31 janvier 2018).

23 Gozi Blog: https://www.govcert.admin.ch/blog/18/gozi-isfb-when-a-bug-really-is-a-feature (état: le 31 janvier 2018).

Recommandation

Il est recommandé aux PME en particulier d'effectuer leurs paiements sur un ordinateur spécifique avec accès limité à Internet, qui ne sera utilisé ni pour naviguer, ni pour recevoir ou envoyer des courriels, d'actualiser régulièrement leur logiciel de paiement et de conserver les mots de passe en lieu sûr, dans un système prévu à cet effet (*Password Safe*). En outre, les paiements seront validés selon le principe du double contrôle et libérés depuis un autre terminal, lui aussi sécurisé. Les paiements suspects seront aussitôt signalés à la banque.

4.5.3 Fausses applications bancaires

À l'ère des smartphones, les applications jouent un rôle important. Le hic pour les cybercriminels, c'est qu'à la différence d'un navigateur standard, elles possèdent en général une configuration propriétaire. En cas d'usage abusif, le fournisseur ou développeur pourra directement adapter le code et réagir aux attaques en mettant en place des mécanismes de sécurité, chose impensable pour un navigateur standard. Il est par conséquent plus difficile pour un cybercriminel de s'attaquer à une application afin de la manipuler.

Les cybercriminels cherchent dès lors surtout à mettre en circulation des applications falsifiées, plutôt qu'à manipuler les applications légitimes. Dans le secteur financier, de fausses applications apparaissent souvent dans les magasins (*app stores*) officiels ou non. De conception sommaire, elles affichent peu après leur lancement des champs de formulaire où il faut saisir les données de sa carte de crédit, son nom d'utilisateur et ses mots de passe. Comme leurs noms et leurs logos imitent à s'y méprendre ceux des banques, les victimes risquent de tomber dans le piège et de télécharger de telles applications. D'autres méthodes d'ingénierie sociale font partie du répertoire des cyberescrocs: ils ont par exemple prétendu qu'une application (falsifiée par eux) permettait d'augmenter la limite de crédit auprès des banques concernées.

Google a certes mis au point un filtre (Google Play Protect) qui, l'année dernière, a endigué pour la première fois la diffusion des maliciels sous Android. De fausses applications font malgré tout leur apparition de temps à autre.

Même PostFinance en a fait les frais à la fin de septembre. La fausse PostFinance App ne demandait toutefois pas les données d'accès à l'e-banking ou d'autres mots de passe. Les escrocs lorgnaient les données des cartes de crédit. Une fois ces informations saisies, une page de remerciement s'affichait et l'application se refermait. La méfiance s'imposait alors au plus tard, et les victimes avaient tout intérêt à prendre aussitôt contact avec leur fournisseur Internet ou leur société de carte de crédit[24].

4.5.4 Rançongiciels

En ce moment, le chantage commis à l'aide de maliciels chiffrant les données, ou rançongiciels, compte indiscutablement parmi les cyberattaques les plus lourdes de conséquences pour les PME ainsi que pour les infrastructures de l'information d'importance

[24] https://www.blick.ch/news/wirtschaft/ueber-1000-opfer-falsche-postfinance-app-in-play-store-gebracht-id8881643.html (état: le 31 janvier 2019)

vitale, comme le montrent les exemples présentés au chapitre 5.3.5. Les rançongiciels les plus répandus à l'heure actuelle sont Ryuk, GandCrab, Dharma et Locky. Le site «botfrei.de» donne un aperçu de tous les types de rançongiciels existants[25].

Le rançongiciel Ryuk a pour particularité de collecter en amont des données, puis de chiffrer de façon ciblée les systèmes de cibles particulièrement lucratives. Le 12 décembre 2018, MELANI a publié une mise en garde contre différentes vagues de spams malveillants (malspam) renfermant en annexe un document Word malveillant[26]. Ryuk était distribué par Emotet. Ce cheval de Troie connu de longue date recourt à l'ingénierie sociale pour amener ses destinataires, au moyen de courriels falsifiés envoyés au nom de collègues, de partenaires commerciaux ou de connaissances, à ouvrir le document Word annexé et à exécuter ses macros Office. Initialement connu comme cheval de Troie bancaire, Emotet sert surtout aujourd'hui à l'envoi de pourriels et au téléchargement d'autres maliciels. En l'occurrence, c'était tout d'abord le maliciel Trickbot qui était installé et cherchait à se procurer des droits sur les ordinateurs infectés. Une fois installé, ce maliciel procédait à une analyse complète du réseau pour déterminer si l'ordinateur faisait partie d'une grande entreprise ou organisation, et cherchait à se propager dans ce réseau au moyen d'une faille du protocole SMB. Le maliciel communiquait régulièrement avec son serveur C&C. Pour autant que la cible ait été jugée de taille suffisante, le rançongiciel Ryuk était alors téléchargé, et chiffrait les données figurant sur les ordinateurs et serveurs du réseau d'entreprise. Grâce à cette approche très ciblée, les escrocs ont généré depuis août 2018 l'équivalent de 3,7 millions de dollars en bitcoins[27]. On ignore toutefois quelle part de ce pactole a pu être convertie en liquidités, et d'où opéraient les escrocs.

25 https://www.botfrei.de/de/ransomware/galerie.html (état: le 31 janvier 2019)

26 https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/Trojaner_Emotet_greift_Unternehmensnetzwerke_an.html (état: le 31 janvier 2019)

27 https://derstandard.at/2000096143241/Ryuk-Neue-Ransomware-brachte-Cyberkriminellen-vier-Millionen-Dollar (état: le 31 janvier 2019)

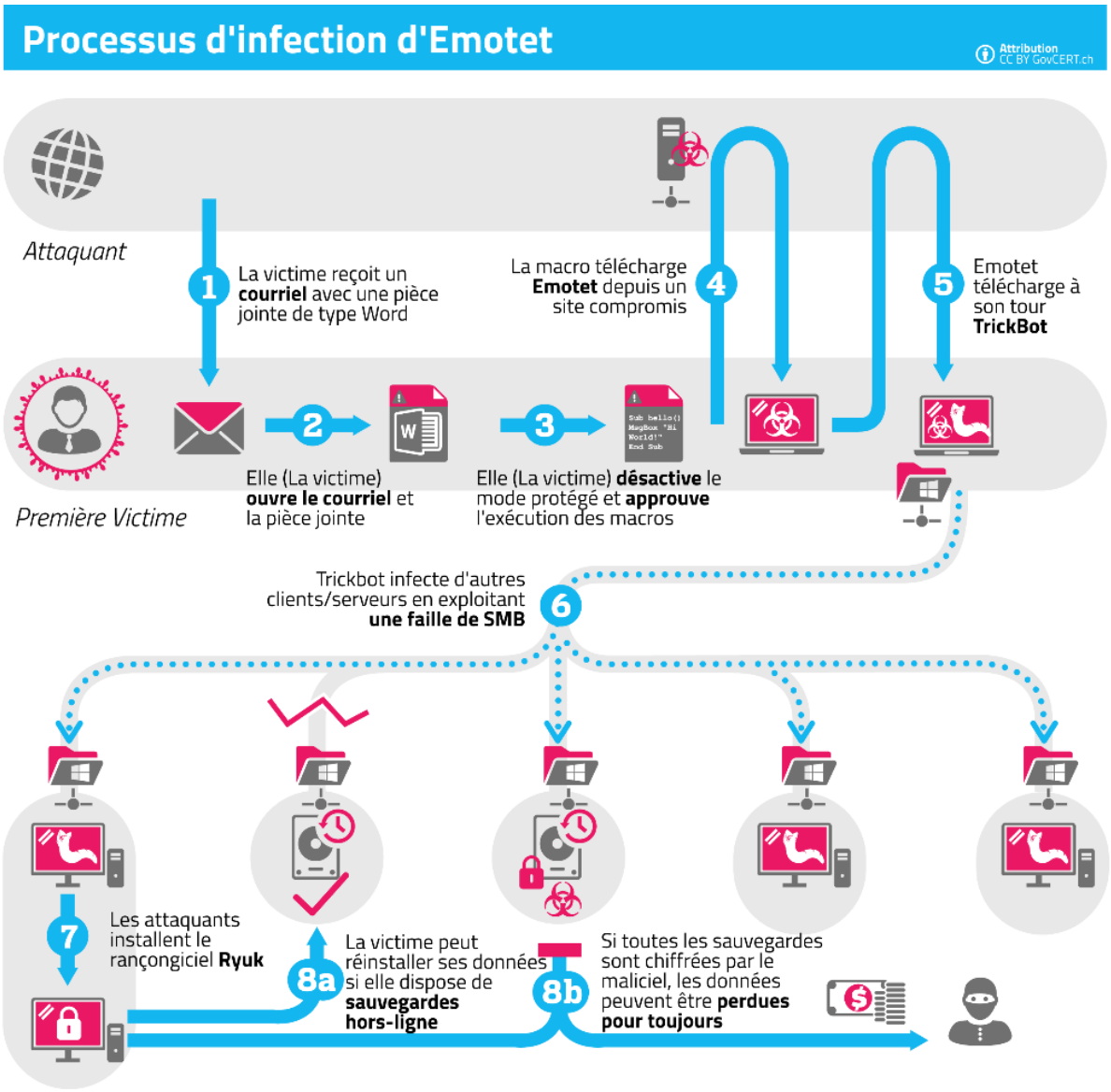

Figure 9: Schéma du processus d'infection du maliciel Emotet

Des cas impliquant le rançongiciel GandCrab ont également été signalés à plusieurs reprises à MELANI au deuxième semestre 2018. Ce rançongiciel apparu pour la première fois en janvier 2018[28] se distingue avant tout par ses multiples vecteurs d'infection. Au départ, GandCrab était diffusé par des pourriels. En été 2018, les escrocs ont changé de tactique avec la version 4 et opté pour des sites Web proposant des versions piratées de logiciels payants. Bien souvent, il s'agit de sites frauduleux que les criminels ont eux-mêmes mis en ligne et que les victimes repèrent à l'aide du moteur de recherche Google. Des dossiers de candidature manipulés font également partie des méthodes de diffusion de Gandcrab[29]. Par ailleurs,

[28] https://blog.comodo.com/comodo-news/gandcrab-the-new-version-of-ransomware/ (état: le 31 janvier 2019)

[29] https://www.heise.de/security/meldung/Erpressungstrojaner-Gandcrab-verbreitet-sich-ueber-gefaelschte-Bewerbungsmails-4154167.html (état: le 31 janvier 2019)

l'entreprise de sécurité FireEye a fait savoir en août 2018 que le rançongiciel utilise un kit d'exploits sur des sites Web compromis. Cet outil installé sur les pages infectées tire parti de deux failles de sécurité de Windows[30].

Bien qu'il sévisse depuis 2016 déjà, Dharma fait partie des rançongiciels les plus dangereux. Ses auteurs publient régulièrement de nouvelles variantes qui résistent à tous les outils de décryptage. Au deuxième semestre 2018, il a surtout été question de Dharma à cause de deux victimes en vue, dont les mésaventures ont fait grand bruit, la brasserie écossaise Arran Brewery, d'une part, et un grand port maritime, d'autre part (voir chapitre 5.3.5).

Il y a toutefois aussi eu de bonnes nouvelles à annoncer durant la période sous revue: le 26 novembre 2018, le FBI a annoncé avoir identifié deux des commanditaires du rançongiciel SamSam. Il s'agissait de ressortissants iraniens âgés de 28 et 35 ans. Le ministère de la justice américain a rendu son ordonnance de mise en accusation. Les escrocs auraient reçu plus de 6 millions de dollars extorqués, dans différents secteurs, à des victimes comprenant des exploitants d'infrastructures d'importance vitale dans les domaines de la santé, des transports et de l'administration.

Recommandation

Veillez à effectuer des sauvegardes régulières de vos données importantes (*backup*) sur un support externe (par ex. un disque dur externe). Après la sauvegarde, déconnectez de l'ordinateur le support contenant les données sauvegardées, sans quoi ces données pourront également être verrouillées et rendues inutilisables en cas d'infection de l'ordinateur par un rançongiciel.

Segmentez votre réseau. Les services particulièrement exposés, comme les ressources humaines ou la communication, qui sont obligés d'ouvrir des annexes d'expéditeurs inconnus, devraient être séparés du reste du réseau.

INFO

Informations sur les rançongiciels publiées sur le site Web de MELANI

https://www.melani.admin.ch/melani/fr/home/themen/Ransomware.html

[30] https://www.fireeye.com/blog/threat-research/2018/09/fallout-exploit-kit-used-in-malvertising-campaign-to-deliver-gandcrab-ransomware.html (état: le 31 janvier 2019)

5 Situation internationale

5.1 Espionnage

5.1.1 APT 10

Le 20 décembre 2018, le Département de la justice américain (DoJ) a accusé deux ressortissants chinois de s'être introduits dans des ordinateurs et d'avoir procédé à des versements frauduleux et à des vols d'identité. Ces individus seraient mêlés à APT 10. Cette campagne, également connue sous les noms de menuPass, CVNX, StonePanda et POTASSIUM, s'en est prise depuis 2016 au moins à d'importants fournisseurs de services d'infogérance (*managed service provider*, MSP)[31]. La publication officielle du DoJ signale des cibles situées dans douze pays, dont la Suisse.

Les MSP constituent une cible attrayante, car ils s'occupent de l'infrastructure informatique de grandes organisations et ont ainsi directement accès aux systèmes et données de leurs clients. Les MSP n'étaient vraisemblablement pas un but en soi: ils auront servi de moyen d'accès aux réseaux de nombreuses grandes entreprises. Le groupe de cyberpirates n'a d'ailleurs opté pour cette approche qu'en 2016. Jusque-là, il s'en prenait directement à ses cibles. Le groupe a commencé à sévir en 2006 et depuis lors, il s'est introduit illégalement dans les réseaux informatiques de plus de 45 groupes technologiques, sans oublier ceux du ministère de l'énergie américain et de la NASA. Les pirates auraient également dérobé des informations personnelles de militaires, dont le numéro de sécurité sociale, l'adresse électronique et les données salariales de 100 000 membres de la marine américaine.

Le Département de la justice américain a insisté sur l'étroitesse des liens unissant les deux accusés au Ministère de la sécurité de l'État chinois (Chinese Ministry of State Security, MSS). Au même moment, les quatre autres membres du groupe des Five Eyes[32] ont publiquement soutenu les propos américains sur une participation du gouvernement chinois à la campagne d'espionnage. Ils ont expliqué que les résultats du travail d'attribution des cyberincidents gagnaient à être publiés, a fortiori si ceux-ci mettaient en péril la croissance économique mondiale, la sécurité nationale et la stabilité internationale. La Chine et tous les autres pays impliqués ont été priés à cette occasion de respecter les engagements résultant des traités internationaux.

5.1.2 Développements d'APT 28

Le groupe d'espionnage APT 28, aussi connu sous les noms de Sofacy et Fancy Bear, a déjà été évoqué à diverses reprises dans ces pages. Il s'agit sans doute de la campagne la plus active et la plus connue au monde. Au deuxième semestre 2018, ce groupe a renforcé ses compétences techniques et accru l'étendue de ses fonctions. L'avancée la plus frappante est ici l'usage du maliciel furtif (rootkit) UEFI LoJax. Comme l'a expliqué à la fin de septembre 2018 le prestataire de services de sécurité ESET, ce rootkit a servi lors d'opérations orchestrées

---

31 MELANI, rapport semestriel 2017/1, chapitre 5.1.1 https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2017-1.html (état: le 31 janvier 2019)

32 États-Unis, Royaume-Uni, Australie, Nouvelle-Zélande, Canada.

contre des organisations situées aux Balkans, ainsi qu'en Europe centrale et orientale[33]. Les rootkits UEFI sont des outils sophistiqués servant à préparer des cyberattaques. Très difficiles à détecter, ils sont capables de résister à des contre-mesures aussi radicales que la réinstallation du système d'exploitation, voire le remplacement complet du disque dur. C'était la toute première fois qu'un rootkit UEFI était découvert dans des conditions réelles.

Sofacy serait également à l'origine d'une fonction destinée à entraver l'analyse automatique des documents à l'intérieur d'une sandbox. La méthode se base sur la fonction AutoClose, où une macro présente dans le document Word ne s'exécute et ne télécharge le code malveillant qu'au moment où l'utilisateur referme le document. Dans l'analyse automatique, les documents demeurent certes généralement ouverts pendant un certain temps, à des fins d'observation de leur comportement, mais ils ne sont pas refermés. Sachant que le maliciel ne fait l'objet d'un téléchargement qu'à la fermeture, qu'il est enregistré sur un serveur externe et non dans le document Word, le serveur doit impérativement être en ligne à ce moment-là pour que l'attaque soit couronnée de succès. Dans le cas contraire, aucun dommage ne sera engendré. La campagne était dirigée contre des services gouvernementaux situés dans le monde entier. Dans un cas d'espèce, elle s'est référée à l'accident d'un avion de la compagnie Lion Air survenu le 29 octobre 2018, en utilisant le nom de fichier «crash list (Lion Air Boeing 737).docx.».

Le précédent rapport semestriel a déjà évoqué les attaques lancées par Sofacy à l'aide de Zebrocy, programme malveillant doté de différentes composantes (téléchargeur, injecteur, portes dérobées). Si les deux premières servent à la collecte de renseignements, les portes dérobées garantissent un accès permanent pour les activités d'espionnage. Durant la période sous revue, de nouvelles composantes ont été utilisées, et Zebrocy a connu un véritable essor. Ces adjonctions ont par exemple utilisé les protocoles de messagerie SMTP et POP3 pour exporter les données dérobées dans le réseau de la victime. En décembre 2018, le fournisseur de solutions de sécurité PaloAlto[34] a signalé une nouvelle variante de Zebrocy possédant quasiment les mêmes fonctions, mais rédigée pour la première fois dans le langage de programmation Go. Les langages des variantes utilisées jusqu'alors par Sofacy étaient AutoIt, Delphi, VB.NET, C# et Visual C++. Même si le contexte n'est pas clair, il semblerait que la diversité des langages de programmation vise à empêcher la détection des maliciels.

5.1.3 Attaque ciblée contre l'industrie navale et l'industrie de l'armement italiennes?

Du 9 au 15 octobre 2018, des courriels munis d'un document Excel spécialement préparé ont été envoyés à des employés de l'industrie navale et de l'industrie de l'armement italiennes[35]. Selon la société de cybersécurité italienne Yoroi, il s'agissait d'une demande de pièces de remplacement pour des moteurs de bateaux. L'agresseur invitait à lui soumettre une offre pour les articles énumérés dans le fichier Excel. Le destinataire était par conséquent poussé à ouvrir cette annexe. Les pirates ont semble-t-il effectué de solides recherches en amont, pour donner à leur démarche une apparence plausible. La requête était rédigée de manière claire et correcte, et adressée au service compétent. Après l'ouverture du fichier, l'outil d'accès à

33 https://www.welivesecurity.com/2018/09/27/lojax-first-uefi-rootkit-found-wild-courtesy-sednit-group/ (état: le 31 janvier 2019)

34 https://unit42.paloaltonetworks.com/sofacy-creates-new-go-variant-of-zebrocy-tool/ (état: le 31 janvier 2019)

35 https://securityaffairs.co/wordpress/77195/malware/martymcfly-malware-cyber-espionage.html (état: le 31 janvier 2019)

distance QuasarRAT se téléchargeait sur le système de la victime. Ce logiciel livrait aux pirates un accès complet au système. Ils étaient ainsi en mesure de dérober des données et d'effectuer des manipulations sur l'ordinateur infecté. Le code source de QuasarRAT est public et peut être consulté sur le service en ligne GitHub. Alors que Yoroi attribue les attaques à un acteur étatique, Kaspersky penche plutôt dans son analyse pour des mobiles criminels. Selon cet éditeur d'antivirus, il s'agit d'une campagne de grande envergure, dans le cadre de laquelle les documents ont été envoyés sous différents noms à des entreprises situées dans de nombreux pays, dont l'Allemagne, l'Espagne, la Bulgarie, l'Inde et la Roumanie[36].

5.2 Systèmes de contrôle industriels

Il n'y a guère eu, durant la période sous revue, d'attaque ciblée lancée contre des systèmes de pilotage des processus. Les groupes qui, dans le passé, s'étaient profilés en lançant de telles opérations ne sont pas pour autant restés inactifs. Les services de sécurité ukrainiens ont ainsi accusé le Service de renseignement militaire russe (GRU) d'avoir attaqué une station d'épuration avec le maliciel VPNFilter[37]. En outre, de nouveaux groupes lorgnent les exploitants de systèmes de contrôle industriels. Les États-Unis, l'Europe, le Moyen-Orient et l'Extrême-Orient ont constaté diverses activités suspectes. Les prestataires de services de sécurité[38] les ont baptisées RASPITE[39] ou Leafminer[40]. Les sous-chapitres suivants abordent plus en détail trois autres exemples d'exploration informatique à grande échelle.

5.2.1 GreyEnergy: peaufinage d'instruments de sabotage du secteur de l'énergie

Le maliciel BlackEnergy avait fait les gros titres en 2015, durant la période de Noël: des agresseurs avaient accédé aux stations de commande des systèmes de contrôle de plusieurs entreprises électriques ukrainiennes et déclenché une panne de courant de plusieurs heures au niveau régional, privant d'électricité plus de 220 000 personnes[41].

Le spécialiste en cybersécurité slovaque ESET a observé par la suite une cyberopération analogue. En se référant au précédent incident, il l'a baptisée GreyEnergy[42]. Ces trois dernières années, cette famille de maliciels aurait sévi selon ESET contre plusieurs cibles situées en Ukraine et en Pologne. Outre que l'apparition de GreyEnergy coïncide avec la fin des méfaits de BlackEnergy, ESET relève notamment que leur architecture modulaire est identique et souligne les analogies dans la mise en œuvre des attaques et dans le choix des cibles. Aucun module spécifique aux systèmes de contrôle industriels n'a encore été découvert

36 https://ics-cert.kaspersky.com/news/2018/10/22/yoroi/ (état: le 31 janvier 2019)

37 https://www.theregister.co.uk/2018/07/13/ukraine_vpnfilter_attack/ (état: le 31 janvier 2019)

38 https://ics-cert.kaspersky.com/news/2018/08/06/raspite/ (état: le 31 janvier 2019)

39 https://dragos.com/resource/raspite/ (état: le 31 janvier 2019)

40 https://www.symantec.com/blogs/threat-intelligence/leafminer-espionage-middle-east (état: le 31 janvier 2019)

41 MELANI, rapport semestriel 2/2015, chapitre 5.3.1, 26.04.2016 https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2015-2.html (état: le 31 janvier 2019)

42 https://www.welivesecurity.com/2018/10/17/greyenergy-updated-arsenal-dangerous-threat-actors/ (état: le 31 janvier 2019)

dans la famille de maliciels GreyEnergy. Mais il est apparu qu'ils recherchaient systématiquement les postes de travail servant à la gestion des systèmes de contrôle. [43]

En plus de présenter une conception plus moderne que son supposé prédécesseur, il est frappant de voir que GreyEnergy utilise des certificats d'Advantech, fabricant taïwanais de solutions destinées à l'industrie et à l'IdO. Ces certificats, très probablement volés, servaient à doter ses propres maliciels d'une signature digne de confiance, et ainsi à augmenter la probabilité d'infection. Stuxnet, premier maliciel identifié à s'attaquer aux processus industriels[44], utilisait déjà le même mode opératoire.

GreyEnergy montre que les cyberpirates poursuivent leur activité d'exploration contre les exploitants d'infrastructures d'importance vitale. Comme indiqué en 2015, ils s'autorisent ainsi à pouvoir passer à des actes de sabotage à un moment propice.

5.2.2 Données et configurations effacées par Shamoon – panne chez Saipem

«Une attaque a temporairement mis hors service 300 à 400 serveurs et 100 postes de travail personnels», a fait savoir Mauro Piasere, responsable du secteur Numérique et innovation de Saipem, en réponse à une demande de Reuters[45]. Le 10 décembre 2018, le groupe de services pétroliers italien annonçait[46] avoir subi une cyberattaque. Deux jours plus tard, Saipem actualisait son communiqué[47] et signalait que des serveurs basés au Moyen-Orient, en Inde, en Écosse et ponctuellement en Italie avaient été victimes du maliciel Shamoon. Une infrastructure de sauvegarde a permis de restaurer par étapes les systèmes infectés.

À la même période, l'entreprise de cybersécurité Chronicle a étudié une nouvelle variante[48] du maliciel Shamoon, téléchargée à partir d'une adresse IP italienne sur le service gratuit d'analyse Virustotal. Shamoon s'était fait connaître en 2012, lors d'une attaque contre Saudi Aramco qui avait effacé les données de 35 000 systèmes. Quatre ans plus tard, une nouvelle vague du maliciel s'est abattue sur la même région. La version actualisée possède une fonctionnalité supplémentaire, consistant à écraser avec des données aléatoires certains fichiers et le *master boot record* (MBR), secteur du disque dur contenant une routine nécessaire au démarrage du système. Le fait que Saudi Aramco compte parmi les principaux clients de Saipem apporte une preuve supplémentaire d'un lien avec les incidents antérieurs ayant impliqué Shamoon. On ignore toutefois si la variante de maliciel analysée par Chronicle et par Palo Alto Networks[49] est bien celle impliquée dans l'attaque contre Saipem.

---

43 https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf, 17.10.2018

44 https://www.welivesecurity.com/2010/07/19/win32stuxnet-signed-binaries/, 19.07.2010

45 https://www.reuters.com/article/us-cyber-shamoon/saipem-says-shamoon-variant-crippled-hundreds-of-computers-idUSKBN1OB2FA (état: le 31 janvier 2019)

46 http://www.saipem.com/sites/SAIPEM_en_IT/con-side-dx/Press%20releases/2018/Cyber%20attack.page (état: le 31 janvier 2019)

47 http://www.saipem.com/sites/SAIPEM_en_IT/con-side-dx/Press%20releases/2018/Cyber%20attack%20update.page (état: le 31 janvier 2019)

48 https://www.bleepingcomputer.com/news/security/shamoon-disk-wiping-malware-re-emerges-with-a-third-variant/ (état: le 31 janvier 2019)

49 https://unit42.paloaltonetworks.com/shamoon-3-targets-oil-gas-organization/ (état: le 31 janvier 2019)

5.2.3 Drones à l'aéroport

Il existe des drones de formes et de tailles diverses. Leurs fonctions aussi varient, allant du simple jouet aux frappes militaires, en passant par les livraisons de marchandises. Il est bien clair qu'à l'avenir, les drones seront toujours plus nombreux et que de nouveaux débouchés vont apparaître. L'incident survenu aux abords de l'aéroport britannique de Gatwick est là pour le rappeler: le 19 décembre 2018, soit au début des vacances de Noël, des inconnus ont paralysé le trafic aérien pendant 36 heures avec des drones. Au total, plus de 200 observations de drones ont été signalées. Ni la police ni les militaires déployés n'ont pu découvrir les responsables et stopper leurs agissements. Les auteurs des faits courent toujours. Des incidents de moindre gravité impliquant des drones sont désormais fréquents un peu partout. Le 12 décembre 2018, un Boeing de la compagnie aérienne Aeromexico a atterri avec son nez endommagé, sans doute après avoir percuté un drone. Même si dans les cas précités rien n'indique que des systèmes aient été compromis, le risque de tels incidents tend à augmenter.

Appréciation

Le gouvernement britannique a tiré les conséquences des incidents et serré la vis aux drones. En Suisse, il faut une autorisation de l'Office fédéral de l'aviation civile (OFAC) pour exploiter des drones ou modèles réduits d'aéronefs d'un poids supérieur à 30 kg. Les règles applicables en deçà de 30 kg figurent dans l'ordonnance du DETEC sur les aéronefs de catégories spéciales. Par exemple, il est interdit d'utiliser sans autorisation un drone à une distance de moins de 5 km d'un aérodrome ou d'un héliport. Ces règles ne protègent toutefois pas des actes malveillants, ou alors du risque qu'un tiers pirate un drone et en prenne le contrôle.

5.3 Attaques (DDoS, *defacement*, *drive-by download*, etc.)

5.3.1 Version numérique du skimming – victimes réputées

En août 2018, des pirates informatiques ont dérobé les données de plus de 380 000 clients de la compagnie aérienne British Airways. Les informations volées incluaient non seulement le nom, l'adresse postale et l'adresse électronique, mais aussi les données des cartes de crédit et des comptes de facturation. Alors qu'on aurait pu penser à première vue à une attaque contre une base de données, il s'est avéré que le site Internet de British Airways et son application avaient été manipulés. Les agresseurs avaient mis en place une version numérique du skimming. Le skimming classique consiste à introduire dans les distributeurs de billets un équipement spécial, qui copie les données contenues sur la piste magnétique de la carte de crédit. Dans sa version numérique, les escrocs cherchent à obtenir le numéro de carte de crédit, sa date d'expiration et son code sécurisé non pas dans un distributeur, mais lors du processus de paiement sur un site en ligne. Par conséquent, British Airways ne s'est fait dérober que les données inscrites dans le formulaire de paiement par ses clients ayant réservé un billet entre le 21 août et le 5 septembre 2018. Les pirates informatiques n'ont pas eu accès aux données liées aux vols, par exemple à la destination.

Un autre cas a été découvert le 23 juin 2018. La billetterie britannique Ticketmaster a identifié un maliciel ayant permis à un tiers inconnu, depuis février 2018, de connaître le nom de ses clients, leur adresse électronique, leur numéro de téléphone, leurs informations de paiement et celles de connexion à son site.

Le même mode opératoire a été utilisé avec la page de paiement de Newegg, géant de la vente en ligne de matériel électronique. Le 14 août 2018, les pirates y ont injecté 15 lignes de code malveillant. L'escroquerie n'a été découverte que cinq semaines plus tard, le 18 septembre. Le maliciel installé envoyait les données de la carte de crédit des clients à un serveur contrôlé par les malfaiteurs.

Les sites d'e-commerce ont été victimes de piratage dès les débuts d'Internet. La raison en est simple: si un pirate informatique souhaite s'emparer de données de cartes de crédit valables, les boutiques en ligne sont l'endroit idéal pour le faire. En 2000 déjà, la découverte d'une faille dans Cart32, logiciel destiné aux serveurs Microsoft très populaire à l'époque, avait permis aux agresseurs de se procurer un accès administrateur à cette application. Ils avaient ainsi pu lire les données des cartes de crédit et donner des ordres au serveur d'hébergement. En 2011, les escrocs ont surtout exploité les vulnérabilités du logiciel OSCommerce. En Suisse aussi, de nombreux sites Web avaient été compromis à l'époque, ce qui avait conduit MELANI à formuler une mise en garde[50].

Depuis mars 2016, le spécialiste de la sécurité informatique RiskIQ observe les campagnes successives lancées à partir d'infrastructures d'attaque toujours nouvelles,[51] auxquelles il a donné le nom générique de Magecart. Elles émanent d'au moins sept groupes, qui introduisent sur des sites de commerce en ligne compromis des copieurs numériques de cartes de crédit. Ces campagnes exploitent notamment les failles d'extensions de Magento, logiciel de boutique en ligne publié en 2008, en tant que plateforme de commerce électronique à code source libre. Willem de Groot, expert en cybersécurité néerlandais, a identifié dans 2 extensions de Magento des failles *zero day* et a demandé de l'aide pour analyser les failles potentielles des 18 extensions restantes. Or les attaquants étudiés s'intéressent également à deux autres logiciels de boutique en ligne, Powerfront CMS et OpenCart[52].

5.3.2 Risques liés aux VPN: l'exemple de Hola VPN

Un réseau virtuel privé (*virtual private network*, VPN) est un canal de communication chiffré qui permet d'établir une connexion entre deux ordinateurs distants à travers Internet. Pour de nombreux utilisateurs, utiliser un VPN permet d'accroître le niveau de confidentialité de ses activités en ligne. Néanmoins, tous les VPN ne sont pas égaux et il appartient à l'utilisateur de s'assurer que son VPN est digne de confiance et respecte certains standards de sécurité. Un prestataire de VPN n'est pas non plus à l'abri d'une attaque venant compromettre la sécurité de ses utilisateurs. C'est ce qui semble s'être passé en juillet dernier, lorsque MyEtherWallet (MEW), une interface très populaire de gestion de portefeuilles Ethereum (qui contiennent de la cryptomonnaie Ether), a informé ses clients qu'ils couraient un risque s'ils utilisaient l'extension Chrome du VPN Hola. En effet, selon MEW, Hola a été compromis pendant cinq heures le 9 juillet, période durant laquelle les utilisateurs ayant ainsi accédé aux services de MEW risquaient de se faire voler leurs monnaies virtuelles. Dans un communiqué de presse, Hola a reconnu l'incident et précisé que le compte de l'entreprise sur le Google Chrome Store avait été compromis afin de proposer une version modifiée de l'extension pour Google Chrome, qui servirait à capter les informations des utilisateurs se connectant à leur compte

50 https://www.computerworld.ch/business/politik/melani-warnt-schweizer-webshop-betreiber-1321089.html (état: le 31 janvier 2019)

51 https://www.riskiq.com/blog/external-threat-management/inside-magecart/ (état: le 31 janvier 2019)

52 https://www.riskiq.com/blog/labs/magecart-keylogger-injection/ (état: le 31 janvier 2019)

MEW. À la suite de cette découverte, l'entreprise a sécurisé son compte sur le Google Chrome Store et retiré l'extension frauduleuse.

Recommandation

INFO

Recommandations de MELANI pour l'utilisation de réseaux VPN

https://www.melani.admin.ch/melani/fr/home/themen/vpn.html

5.3.3 Des criminels attaquent des banques en accédant physiquement à leur réseau

En décembre, le fournisseur de solutions de Sécurité Kaspersky a rendu publics les résultats d'une série de cyberincidents ayant touché différentes banques en Europe de l'Est. Le point d'entrée dans le réseau de l'entreprise est particulièrement intéressant: les criminels ont directement connecté leurs appareils au réseau. En général, les attaques sont menées à distance, par exemple en envoyant des courriels malveillants ou en piratant un serveur vulnérable. Mais, en l'espèce, les criminels avaient besoin d'accéder physiquement aux locaux de l'entreprise. Après être entrés sur le site en se faisant par exemple passer pour des chercheurs d'emploi ou des livreurs, ils branchaient directement leur appareil au réseau. Selon les cas, il s'agissait d'un petit ordinateur portable, d'un nano-ordinateur Raspberry Pi ou de Bash Bunny, un outil de pénétration utilisant le port USB. Une fois ce premier accès établi, les attaquants procédaient à une phase de reconnaissance, visant en particulier à capter des identifiants et à repérer des postes depuis lesquels des paiements étaient effectués. Ensuite, les attaquants cherchaient à s'assurer un accès à distance durable sur ces postes.

Ce type d'attaques rappelle combien il est crucial d'envisager une stratégie de sécurité globale, ne se limitant pas à des mesures techniques, mais intégrant également des mesures physiques ou organisationnelles. Le contrôle des accès aux locaux est ainsi capital: les points d'entrée au réseau (machines, ports Ethernet) devraient être documentés et surveillés, voire désactivés s'ils n'ont pas besoin d'être utilisés.

5.3.4 Lazarus, un acteur toujours très entreprenant

Le groupe Lazarus est connu pour avoir attaqué les systèmes de différentes banques par le passé, dont ceux de la banque centrale du Bangladesh en 2016. Selon de nombreux experts, Lazarus est lié au régime nord-coréen. C'est ce même acteur qui est montré du doigt dans un cas ayant touché la banque chilienne Redbanc à la fin de décembre 2018. L'entreprise Flashpoint affirme en effet que le maliciel utilisé (PowerRatankba) fait partie de l'arsenal de Lazarus. La méthode utilisée pour installer le code malveillant sur les réseaux de l'entreprise est particulièrement intéressante. Les attaquants se sont en effet fait passer pour un recruteur et ont pris contact avec un employé de la banque sur les réseaux sociaux pour lui proposer un entretien d'embauche par Skype. Lors de cet entretien, ils ont demandé à la cible de télécharger une soi-disant application nécessaire au processus d'embauche. Il s'agissait en réalité d'un exécutable malveillant. Selon les informations disponibles, l'incident a cependant été détecté à temps et n'a pas eu d'impact sur l'infrastructure ou les activités de la banque.

En octobre déjà, le US-CERT a publié une information sur les activités de Hidden Cobra, qui depuis 2016 a ciblé des banques asiatiques et africaines dans le cadre d'une campagne de

«FastCash», dont le but est de faire libérer simultanément de grandes quantités d'argent liquide par des distributeurs automatiques. Un complice se charge alors de récupérer l'argent expulsé par la machine. Lors d'un incident particulier qui remonte à 2017, des retraits auraient ainsi été effectués en même temps dans plus de 30 pays. Pour certains experts dont l'entreprise de solutions de sécurité Symantec, qui a également publié son analyse de ces cas, Hidden Cobra n'est autre que Lazarus. Symantec décrit en détail le mode opératoire des attaquants: après une compromission initiale, les serveurs utilisés pour administrer les distributeurs automatiques seraient infectés par un cheval de Troie spécifique (Trojan.Fastcash), qui est ensuite chargé de produire des demandes de transactions frauduleuses.

Il est désormais également bien connu que Lazarus s'intéresse de près au marché des cryptomonnaies et y voit un potentiel pour diversifier ses sources de revenus. Selon une analyse de Kaspersky publiée en août, le groupe est responsable d'une attaque visant une plateforme d'échange de cryptomonnaies basée en Asie. En l'occurrence, c'est une application de trading tierce, téléchargée par un employé de l'entreprise, qui a été utilisée comme point d'entrée. Le code malveillant était par la suite délivré sous la forme d'une mise à jour de l'application. Ce qui est particulièrement remarquable dans ce cas, c'est l'existence de versions adaptées au système d'exploitation ciblé. Si Lazarus a par le passé fréquemment ciblé des systèmes Windows, cela semble être la première fois qu'il conçoit un code malveillant spécifique pour les systèmes macOS.

5.3.5 Rançongiciels

Quand il est question de logiciels rançonneurs chiffrant les données de l'ordinateur, ou rançongiciels, on pense essentiellement aux données perdues et aux copies de sauvegarde, dont on espère qu'elles vont fonctionner. Or il faut se garder d'oublier, dans les activités de prévention, les pertes de production qu'un tel maliciel peut occasionner jusqu'à ce que les fichiers aient été restaurés à partir de la copie de sauvegarde et que tous les systèmes fonctionnent à nouveau de manière irréprochable. La situation est particulièrement grave si la cyberattaque touche tout un site de production. De nombreux cas de ce genre ont fait les gros titres durant le semestre sous revue.

En août 2018, le fabricant de puces taïwanais TSMC (Taiwan Semiconductor Manufacturing Company) a été victime d'une cyberattaque. Là encore, il a fallu interrompre la production dans plusieurs fabriques, à cause du rançongiciel utilisé. TSMC est le premier fabricant mondial de semi-conducteurs, et le principal fournisseur d'Apple pour les processeurs de l'iPhone. Une variante du maliciel WannaCry a été identifiée comme étant à l'origine de la panne. WannaCry avait fait grand bruit en mai 2017 et causé des dégâts dans le monde entier. La vulnérabilité du protocole SMB de Windows à l'origine de l'attaque avait été corrigée dès mars 2017. Mais il est parfois délicat, a fortiori pour les systèmes de contrôle, d'appliquer sur-le-champ les correctifs. Ainsi, les machines des robots de manutention possédaient des systèmes Windows 7 non actualisés. Le maliciel s'est introduit dans un nouvel outil logiciel qu'on avait installé sans vérifier l'absence de virus.

Au deuxième semestre 2018, deux grands ports internationaux ont été victimes d'une cyberattaque. Le 20 septembre 2018, le port de Barcelone a signalé que ses infrastructures de sécurité avaient été prises pour cibles par un rançongiciel. Les responsables sont restés muets quant à la nature de l'attaque. Les mouvements de navires n'ont pas été affectés, car une planification préventive est effectuée pour de tels incidents. Une semaine plus tard, le 27 septembre 2018, le port de San Diego subissait le même sort. Là non plus, les activités

portuaires n'ont pas été perturbées et les employés ont continué de travailler. Ils n'ont toutefois pas pu offrir certains services au public, faute d'accès aux données.

Le 21 novembre 2018, l'entreprise allemande KraussMaffei a dû faire face à un rançongiciel. KraussMaffei compte parmi les principaux fabricants mondiaux de machines-outils pour l'industrie de transformation des matières plastiques et du caoutchouc. En raison de cette attaque, certaines machines nécessaires au pilotage des processus de fabrication et de montage n'ont pas pu démarrer. Selon plusieurs rapports, il a fallu par la suite réduire l'activité de production. La sauvegarde a certes permis à KraussMaffei de faire refonctionner d'importants ordinateurs, mais l'entreprise subira sans doute encore longtemps les conséquences de cette attaque. Un porte-parole a confirmé en janvier 2019 que trois quarts seulement des systèmes nécessaires à l'exploitation fonctionnaient à nouveau normalement.[53] Rien n'a filtré sur le type de rançongiciel, ni sur le montant de la rançon exigée et sur son paiement éventuel.

Appréciation / recommandation

Les services du personnel des entreprises sont une cible de choix des maliciels. Les postulations renferment en général toutes sortes de documents à ouvrir. Au deuxième semestre 2018, les rançongiciels ont été plus nombreux à utiliser ce canal. Les conférences organisées par les entreprises et les communiqués de presse se prêtent bien aussi à l'envoi de maliciels.

Entre-temps, les cybercriminels ont découvert que les attaques contre les appareils mobiles pouvaient rapporter gros. Aussi les rançongiciels s'en prennent-ils toujours plus souvent à la téléphonie mobile. La variante Locker est la plus répandue parmi les appareils Android ou autres. Au lieu de crypter les fichiers, le maliciel verrouille l'appareil. L'essor de l'IdO va certainement aussi offrir un nouveau champ d'activité aux escrocs.

Une mesure essentielle permet aux entreprises industrielles de se protéger face aux cyberattaques: elle consiste à séparer les réseaux opérationnels des réseaux informatiques. Car même si les logiciels de bureautique subissent une attaque, les machines continueront de fonctionner. Néanmoins, par commodité, les réseaux sont souvent reliés entre eux, par exemple pour simplifier l'envoi de commandes aux machines.

5.4 Fuites de données

5.4.1 La plateforme Ariane perd le fil de sa sécurité

Le 13 décembre, le Quai d'Orsay (ministère français des affaires étrangères) annonçait que sa plateforme «Ariane» avait été piratée et que des données personnelles y avaient été volées. Depuis 2010, le service Ariane permet aux citoyens français prévoyant un séjour à l'étranger de s'inscrire en ligne afin de recevoir des recommandations de sécurité sur le pays de destination. Si nécessaire, les titulaires de comptes Ariane ont été contactés directement, de même que les personnes de contact qu'ils avaient indiquées. En effet, la fuite de données concerne les noms, prénoms, numéros de téléphone et adresses électroniques de ces personnes de contact. Le Quai d'Orsay précise que les données dérobées ne sont pas

[53] https://www.zeit.de/2019/03/datenschutz-cyberangriffe-unternehmen-digitalisierung-risiken-datendiebstahl-hacker (état: le 31 janvier 2019)

considérées comme sensibles, mais on peut cependant imaginer qu'elles soient utilisées pour l'envoi de courriels ciblés ou pour des tentatives d'escroquerie par exemple. Les victimes, parmi lesquelles se trouvent des citoyens suisses, ont été informées par courriel. Certaines d'entre elles, ignorant que leurs données étaient enregistrées sur la plateforme, ont d'ailleurs suspecté un message de phishing.

5.4.2 Faille de la fonction «Aperçu du profil en tant que…» de Facebook

Le 28 septembre, Facebook révélait les détails de ce qui pourrait être le plus important incident de sécurité de l'histoire de l'application. La faille concernait la fonctionnalité «Aperçu du profil en tant que…», qui sert aux utilisateurs à visualiser ce à quoi ressemble leur propre profil quand il est consulté par d'autres. Par mesure de sécurité, les 50 millions d'utilisateurs touchés ont été déconnectés de leurs comptes. De plus, 40 millions d'utilisateurs de la fonctionnalité vulnérable ont également dû se reconnecter. Le service a depuis été supprimé. En exploitant cette vulnérabilité, les attaquants auraient réussi à prendre possession du jeton qui permet aux utilisateurs de rester connectés à leur compte lors de plusieurs sessions. Ils ont ainsi pu avoir un accès complet non seulement aux comptes de leurs victimes, mais également à tout autre service pour lequel Facebook est utilisé pour l'identification (authentification unique). Cette pratique, désormais très répandue, consiste à utiliser une identification à un service considéré sûr pour se connecter à différents autres services, et ainsi éviter de devoir se connecter à chaque fois. L'incident démontre que cette pratique peut aussi constituer un risque de sécurité.

5.4.3 Fuite de données médicales à Singapour

En juillet, les détails d'une attaque massive dans le secteur de la santé à Singapour ont été révélés. Au total, 1,5 million de personnes ayant visité entre début mai et début juillet 2018 un établissement faisant partie de SingHealth – le plus grand groupe d'établissements de santé du pays – ont vu leurs données personnelles dérobées. Pour 150 000 patients, ce sont en outre des informations sur leurs prescriptions médicales qui ont été subtilisées. Parmi eux se trouve le premier ministre Lee Hsien Loong, qui selon les autorités aurait été spécifiquement pris pour cible.

5.4.4 Faille du portail en ligne de Movistar

L'entreprise espagnole de télécommunication Telefonica a également été touchée par une faille importante lors de la période sous revue. L'incident a été rendu public par l'organisation de défense des consommateurs FACUA en juillet 2018. En l'occurrence, des tiers non autorisés ont pu consulter les données des clients de la marque Movistar de l'opérateur. En effet, une faille dans la programmation du portail en ligne a permis à toute personne disposant d'un compte Movistar d'accéder aux noms, adresses, numéros de téléphone de tous les autres clients. L'entreprise a par la suite corrigé la faille, sans que l'on sache si des personnes malintentionnées ont eu le temps de collecter des données personnelles.

5.4.5 La chaîne d'hôtel Starwood victime d'une fuite de longue durée

Le 30 novembre 2018, Marriott annonçait qu'un accès non autorisé avait permis de dérober les données de 500 millions de clients d'hôtels de son groupe Starwood. En janvier, l'entreprise revoyait ce chiffre à la baisse, avançant alors que la fuite portait sur un maximum de 383 millions d'enregistrements uniques . Outre des données personnelles comme les adresses et les numéros de téléphone, sont concernées dans certains cas des données plus

problématiques: numéros de passeport et données de cartes de crédit. Les données de cartes de crédit et, dans certains cas, les numéros de passeport étaient bien chiffrés, mais Marriott ne peut exclure que les attaquants soient également en possession des clés permettant de lire les données. Ces derniers auraient eu accès aux données depuis 2014, et jusqu'à la découverte de l'incident en septembre 2018.

Starwood, marque acquise par Marriott en 2016, comprend plus de 1200 hôtels dans près de 100 pays. La fuite communiquée en novembre est remarquable non seulement de par le nombre de personnes concernées et la durée de l'accès indu, mais aussi par la nature des données collectées. Si les données personnelles, données de cartes de crédit et numéros de passeport ouvrent de vastes possibilités criminelles en matière de fraude ou d'usurpation d'identité, on peut également imaginer que des acteurs menant des opérations d'espionnage seront tout particulièrement intéressés à savoir dans quels hôtels résident certaines cibles. Par le passé, plusieurs campagnes sophistiquées de cyberespionnage ont en effet visé des hôtels, en détournant par exemple leurs réseaux wifi. En 2014 déjà, MELANI exemplifiait ce type de possibilités en évoquant la campagne Darkhotel, dans le cadre de laquelle un groupe de pirates s'en serait pris aux réseaux sans fil de grands hôtels pour espionner des voyageurs d'affaires.[54] Cependant, avant de monter une telle opération, il faut savoir quelle cible se trouvera dans quel hôtel à quel moment. La fuite survenue chez Starwood risque d'avoir apporté ce type d'informations sur un plateau. Même si le commanditaire de l'attaque et son but précis ne sont pas connus, on ne peut pas exclure que ces informations aient été utilisées en vue de préparer une attaque d'espionnage, par des moyens informatiques ou physiques. Les informations nécessaires à cette préparation peuvent également tout à fait avoir été acquises par un acteur différent de celui ayant mené l'attaque.

5.5 Mesures préventives

5.5.1 Lutte contre la fraude au support technique

Quand le téléphone sonne à l'improviste et qu'un collaborateur de Microsoft s'annonce à l'autre bout du fil, il y a de fortes chances pour que ce soit un escroc. Il en va de même si en cours de navigation, vous voyez s'afficher à l'écran un message qui vous explique que votre ordinateur court des risques, voire a été infecté, et qu'il vous faut appeler le numéro indiqué. Les pirates cherchent par cette manœuvre à accéder à distance aux ordinateurs et, en plus de faire main basse sur les données, à gagner de l'argent en facturant leurs prétendus services de support ou en vendant des licences inventées. Cette fraude affecte aussi les consommateurs en Suisse[55]. Les escrocs falsifient souvent leur numéro d'appel. Le cas

[54] MELANI rapport semestriel 2/2014 https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/halbjahresbericht-2014-2.html (état: le 31 janvier 2019)

[55] MELANI met en garde contre cette fraude depuis 2011: https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/appels-d_escrocs-se-faisant-passer-pour-le-service-support-de-mi.html; comme elle fait encore recette, elle figure parmi les «Thèmes actuels»: https://www.melani.admin.ch/melani/fr/home/themen/fake_support.html (état: le 31 janvier 2019)

échéant, les numéros helvétiques s'affichant dans la fenêtre contextuelle leur ont typiquement été attribués par des fournisseurs de services VoIP étrangers[56].

Étant donné que les escrocs se font généralement passer pour des employés de Microsoft et que Windows reste le système d'exploitation le plus répandu, Microsoft a tout intérêt à mettre fin à leurs agissements et collabore activement à cet effet avec les autorités de poursuite pénale[57]. Les victimes de fraude au support technique peuvent porter plainte auprès de la police locale, ou signaler directement l'incident à Microsoft[58].

Alors que les commanditaires et les exploitants d'infrastructures se trouvent un peu partout dans le monde[59], les traces des appels remontent régulièrement à des centres d'appel situés en Inde. L'automne dernier, la police indienne a perquisitionné 26 centres situés à New Delhi et arrêté plus de 60 personnes[60]. On ignore dans quelle mesure ces arrestations aboutiront à une réduction durable du phénomène. Il est toutefois réjouissant de constater que la coopération internationale en matière de poursuite pénale rencontre un succès croissant, et que les bandes organisées au niveau supranational ne peuvent plus se croire à l'abri de toute sanction.

5.5.2 Volonté d'endiguer les numéros d'appel falsifiés

Le régulateur britannique des télécommunications (OfCom) a mis en vigueur le 1er octobre 2018 de nouvelles conditions générales destinées aux opérateurs téléphoniques[61]. Il leur incombe désormais de mettre à disposition gratuitement les données d'identification de la ligne appelante, et de s'assurer que le numéro s'affichant soit valable. Les appels à partir de numéros falsifiés seront bloqués. Cette mesure vise à mieux protéger les consommateurs face aux appels frauduleux et aux autres appels indésirables.

Les avis divergent sur l'utilité pratique de telles prescriptions. En Suisse, une révision partielle de la loi sur les télécommunications est en chantier. Le message du Conseil fédéral[62] aborde le problème des numéros d'appel falsifiés et explique que malgré tous les efforts internationaux, l'introduction d'une procédure efficace de vérification des numéros d'appel au niveau mondial prendra des années. Il est néanmoins prévu d'étendre aux appels publicitaires non sollicités l'obligation légale faite aux fournisseurs de services de lutter contre le spamming. La Suisse serait ainsi disposée à édicter et mettre en œuvre par voie d'ordonnance des mesures ciblées, dès que l'état de la technique le permettra.

---

56 La révision partielle en cours de la loi sur les télécommunications (LTC) prévoit d'accorder au Secrétariat d'État à l'économie (SECO) la compétence de bloquer rapidement de tels numéros.

57 https://blogs.microsoft.com/on-the-issues/2018/11/29/new-breakthroughs-in-combatting-tech-support-scams/; https://www.zdnet.com/article/after-microsoft-complaints-indian-police-arrest-tech-support-scammers-at-26-call-centers/ (état: le 31 janvier 2019)

58 Le formulaire de plainte de Microsoft est publié ici: https://www.microsoft.com/fr-ch/concern/scam

59 En Allemagne et en Angleterre notamment: https://winfuture.de/news,96690.html; https://www.t-online.de/digital/sicherheit/id_81548210/trickbetrueger-mit-microsoft-masche-verhaftet.html (état: le 31 janvier 2019)

60 https://www.nytimes.com/2018/11/28/technology/scams-india-call-center-raids.html (état: le 31 janvier 2019)

61 https://www.ofcom.org.uk/about-ofcom/latest/features-and-news/new-rules-protect-consumers

62 https://www.admin.ch/opc/fr/federal-gazette/2017/6185.pdf, pages 6207 et 6221 (état: le 31 janvier 2019)

5.5.3 Opération coordonnée contre l'hameçonnage par téléphone

Un groupement actif au niveau international est soupçonné d'avoir obtenu au moyen de pourriels et d'appels téléphoniques des données bancaires, et de les avoir utilisées de manière illicite, lors de tentatives d'hameçonnage par téléphone (*voice phishing*). Des clients d'établissements financiers en Suisse sont également touchés.

Grâce à la collaboration en matière d'entraide judiciaire avec les Pays-Bas, les auteurs présumés ont pu être identifiés; leur base d'opérations a été localisée dans la région de Rotterdam. Une opération coordonnée a eu lieu le 17 juillet 2018 aux Pays-Bas, avec le soutien des autorités de poursuite pénale hollandaises et de l'Office fédéral de la police (fedpol) et grâce à la coordination effectuée par l'unité de coopération judiciaire de l'Union européenne Eurojust. Concrètement, deux personnes ont été arrêtées et des perquisitions ont été effectuées. L'auteur présumé des appels de phishing en Suisse fait l'objet d'une demande d'extradition. L'autre personne est poursuivie dans le cadre d'une procédure pénale hollandaise[63].

Appréciation

Le succès de l'opération coordonnée aux Pays-Bas montre que la cybercriminalité exige une réponse pénale au niveau international.

5.5.4 Exclusion d'une société pour détournement de trafic (*BGP hijacking*)

BGP (*Border Gateway Protocol*) est un protocole de routage d'Internet, utilisé pour la connectivité entre des systèmes autonomes (*autonomous system*, AS). Chacun de ces systèmes dispose d'adresses IP, et à eux tous ils forment le réseau Internet. Le terme *BGP hijacking* (de l'anglais: *to hijack* = détourner / s'emparer de) désigne le détournement illégal d'adresses IP commis par l'opérateur d'un AS ayant préalablement manipulé les tables de routage Internet.

Une société portugaise s'est plusieurs fois signalée par de telles pratiques. Elle aurait essentiellement loué les adresses IP détournées à des polluposteurs, dont les adresses figurent rapidement sur des listes noires et qui ont donc régulièrement besoin de nouvelles adresses pour l'envoi de leurs courriels. Au cours des dernières années, 130 fausses routes auraient ainsi été créées, ce qui aurait permis d'utiliser illégalement 225 000 adresses IP. Diverses listes de diffusion ont abordé ce dysfonctionnement et, au bout du compte, les fournisseurs de transit vers Internet et les points d'échange Internet ont décidé d'un commun d'accord de couper les ponts avec le système autonome de la société indélicate[64].

63 https://www.bundesanwaltschaft.ch/mpc/fr/home/medien/archiv-medienmitteilungen/news-seite.msg-id-71647.html (état: le 31 janvier 2019)

64 https://www.bleepingcomputer.com/news/security/internet-transit-providers-disconnect-infamous-bgp-hijack-factory/ (état: le 31 janvier 2019)

Appréciation

On peut se demander si une telle approche relève de l'autorégulation ou alors de l'autojustice. Au bout du compte, cette première exclusion totale constitue un clair avertissement à tous les exploitants du réseau, afin qu'ils respectent certaines règles d'Internet même en l'absence de base légale formelle et exécutable. En particulier, quiconque manipule l'infrastructure de base d'Internet aura rapidement affaire à une communauté planétaire qui ne goûte guère de telles actions, et qui est susceptible de prendre en commun des contre-mesures.

6 Tendances et perspectives

6.1 La manipulation, corollaire de la circulation de l'information

La désinformation ou la manipulation de l'information existe depuis que l'information circule entre les individus et leur permet d'adapter leurs comportements ou leurs opinions. Au IV^{e} siècle avant J.-C., Sun Tzu décrivait déjà ces méthodes dans l'«Art de la Guerre». Aujourd'hui, notre société hyperconnectée offre des potentialités extrêmement vastes en matière de transmission de l'information et de son corollaire, la manipulation de l'information. Dans le contexte d'une attention sociétale, médiatique et politique soutenue, le débat perd parfois en clarté et il devient difficile de faire la part des choses entre fake news, junk news, propagande, méthodes d'influences, etc. En cette année électorale, nul doute que l'intérêt pour ces thèmes ne faiblira pas. Des exemples à l'étranger nous démontrent que le débat précédant une élection est justement une période propice à des opérations de manipulation de l'information, entendue ici comme la diffusion massive et organisée d'informations fausses, biaisées ou n'étant pas destinées à être divulguées publiquement (données personnelles ou classifiées en particulier), lorsque cette diffusion a lieu à des fins politiques hostiles.

6.1.1 Un contexte sociétal et technologique favorable

Si les campagnes de manipulation de l'information s'appuient sur des caractéristiques propres à la nature humaine, telles que certains biais cognitifs, elles trouvent dans certaines tendances actuelles un terreau fertile leur permettant de prospérer.

Ces médias cèdent en particulier du terrain face aux médias en ligne et aux réseaux sociaux, qui deviennent la source d'information principale pour de nombreuses personnes[65]. Chacun peut désormais devenir diffuseur d'information, sans devoir se soucier du respect de tout standard de qualité journalistique. Ces mêmes réseaux sociaux ont d'ailleurs ouvert des perspectives inédites pour le ciblage de la population. Il est possible d'adresser un message précis à un sous-groupe de la population que l'on saura être particulièrement réactif à un type d'information. Mais les réseaux sociaux et Internet ne présentent pas uniquement un avantage lorsqu'il s'agit de cibler des utilisateurs, ils permettent aussi de multiplier la diffusion d'une

[65] Selon le Reuters Digital News Report 2016, les réseaux sociaux sont désormais une source d'information pour 62 % des adultes américains et 48 % des Européens. (état: le 31 janvier 2019)

information par l'utilisation de bots. Ces derniers permettent à un petit nombre d'acteurs de donner une visibilité disproportionnée à certaines informations ou avis.

Ce ne sont cependant pas uniquement des bots qui vont diffuser ces informations. Il a ainsi été démontré que les informations manipulées circulent plus rapidement que les informations véridiques, parmi les utilisateurs des médias en ligne[66]. Leur côté tapageur, simpliste et peut-être également distrayant augmente leurs chances d'être partagées. En plus des utilisateurs lambda, on trouve des acteurs qui relayeront consciemment des informations manipulées, leur donnant même parfois un semblant de légitimité en les reprenant sur des blogs ou même des journaux en ligne.

6.1.2 Des exemples marquants

Les opérations de manipulation révélées ces dernières années ont été menées dans des contextes bien spécifiques. Des campagnes précédant une élection ou une votation populaire dans des contextes très clivants ont en particulier été ciblées. L'exemple le plus marquant et parlant dans cette catégorie concerne certainement les élections présidentielles américaines de 2016. Dans un contexte déjà fortement conflictuel, les contenus de comptes électroniques de personnalités et d'organisations politiques avaient été rendus publics. Le 7 octobre 2016, les autorités américaines avaient alors accusé le gouvernement russe d'avoir cherché à perturber les élections à la présidence. En février 2018, dans un document de mise en accusation[67], l'équipe de procureur spécial R. Müller fournit des détails sur un autre aspect des tentatives de déstabilisation des élections 2016: la fabrication et la propagation systématique de fausses nouvelles, depuis l'«Internet Research Agency», basée à Saint-Pétersbourg. Le but de l'opération était, semble-t-il, avant tout d'éroder la confiance dans les institutions démocratiques, de renforcer les lignes de fractures de la société américaine et de radicaliser les électeurs. Les contenus montés de toutes pièces et portant sur des thèmes clivants (armes à feu, racisme, etc.) devaient donner l'illusion d'être issus des États Unis et étaient bien souvent relayés par des sympathisants ou des groupes locaux. Les réseaux sociaux, en particulier Facebook, ont joué un rôle majeur dans cette diffusion. L'Europe n'a pas été épargnée par ce type d'opérations. La campagne électorale française de 2017 a ainsi également été marquée par la propagation de fausses informations, dont la soi-disant existence d'un compte offshore détenu par l'ex-candidat à la présidence et actuel président Emmanuel Macron. Des documents issus des comptes piratés de proches collaborateurs de Macron ont par ailleurs été publiés peu avant l'élection. Même si certains experts accusent clairement la Russie, les autorités françaises n'ont pas officiellement attribué l'attaque. Mais les opérations de manipulation de l'information peuvent également cibler des votations, par exemple à l'occasion de référendums. Aussi des soupçons d'ingérence russe ont-ils pesé sur les votes portant sur la sortie du Royaume-Uni de l'Union européenne («Brexit») et sur l'indépendance de la Catalogne.

6.1.3 Perspectives en Suisse

Difficile d'imaginer une opération telles que celles ayant ciblé les élections américaines ou françaises se dérouler en Suisse. Tout d'abord, le rôle stratégique de notre pays n'est pas comparable. Mais ensuite, les élections au niveau fédéral sont peu clivantes en comparaison,

---

66 Voir en particulier une étude du M.I.T.: http://news.mit.edu/2018/study-twitter-false-news-travels-faster-true-stories-0308 (état: le 31 janvier 2019)

67 https://www.justice.gov/file/1035477/download (état: le 31 janvier 2019)

pour des raisons de culture politique et d'utilisation du scrutin proportionnel notamment. Les combats politiques les plus acharnés donnant lieu à une plus forte polarisation au sein de la société ont souvent lieu lors de votations sur des référendums ou initiatives populaires traitant de sujets tels que l'immigration ou plus généralement l'indépendance face à l'Union européenne. En ce sens, le système suisse de démocratie directe pourrait tout à fait se prêter à des tentatives de déstabilisation. De plus, certaines opérations ponctuelles de manipulation de l'information ont été menées après des évènements très spécifiques, difficilement prévisibles à l'avance. Par exemple, selon certains experts, la destruction du vol MH17 de Malaysia Airlines aurait donné lieu à une intense désinformation venant de Russie, pays ayant été accusé d'avoir détruit l'appareil. Il en va de même pour l'empoisonnement sur sol anglais de l'ancien agent russe Skripal. Tout pays peut donc se retrouver touché par une telle opération lorsqu'il est lui-même concerné par un évènement parfois indépendant de sa volonté, mais présentant un intérêt pour un État tiers. Au vu de ce qui précède, on ne peut pas partir du principe que notre pays est hors d'atteinte face à ce type de menace. Et le potentiel perturbateur d'une telle campagne ne doit pas être sous-estimé. Le doute sur la légitimité du résultat d'un vote critique pourrait en effet gravement atteindre le bon fonctionnement du débat politique suisse et de la confiance dans les institutions.

6.1.4 Quelle réponse?

Avant de mettre en place des mesures visant à contrer d'éventuelles opérations de manipulation de l'information, différents chantiers s'imposent. En premier lieu, un travail de clarification du débat et des notions utilisées est nécessaire. Le terme de fake news est par exemple trop vague et regroupe de nombreuses réalités. Il s'agit donc de clairement définir la problématique, et sur cette base de décider ce qui est acceptable dans une démocratie et ce qui ne l'est pas. On ne peut en effet pas mettre dans une même catégorie des informations erronées ou la propagation de rumeurs relevant plus d'un mauvais travail journalistique que d'une volonté de nuire, et une campagne de désinformation orchestrée depuis l'étranger dans le but d'influencer l'opinion publique. En deuxième lieu, c'est une capacité de détection qui doit être développée. Quels sont les indicateurs permettant de déceler une campagne menée avec la volonté de nuire? À ce niveau, une intense collaboration avec les acteurs privés (gestionnaires de contenus, fournisseurs de services Internet) et des partenaires internationaux travaillant également sur ces questions sera nécessaire. Dans un tel dispositif, des évènements clés (votations sensibles par exemple) seront scrutés particulièrement attentivement. Les mesures envisagées nécessiteront elles aussi une étroite collaboration avec les acteurs privés ayant la possibilité d'agir, de même que de détecter les contenus problématiques. Le travail préalable de définition prendra ici tout son sens, puisqu'une définition trop large du problème que l'on cherche à aborder risquera d'être interprétée comme un travail de censure. Mais au-delà de mesures techniques pouvant être prises, ou même des mesures légales (poursuite pénale notamment), c'est tout un travail de sensibilisation qui reste encore à faire. Le succès d'une campagne de manipulation de l'information repose en effet sur la manière dont cette information est assimilée puis éventuellement retransmise par des utilisateurs. Une amélioration des compétences médiatiques et technologiques peut ainsi permettre de limiter l'impact d'une campagne. Les composantes de ces compétences seront par exemple la capacité à vérifier la source d'une information ou la légitimité d'une plateforme, mais davantage encore le développement d'un regard critique face à l'information d'une manière générale. Un travail de sensibilisation spécifique à ces problématiques pourrait également intervenir dans le cadre d'une éducation civique visant à améliorer la connaissance du fonctionnement de nos institutions et processus politiques.

6.2 Élaboration des normes

Qui dirige Internet? Pendant longtemps, de nombreux États ont ignoré ou tourné en dérision ce nouveau média et ses utilisateurs. La société civile a tiré parti de toutes les possibilités s'offrant à elles, et les entreprises ont fait de même. Les acteurs d'Internet, soit en particulier les entreprises de télécommunication qui mettent en place les lignes et connexions ainsi que l'industrie des noms de domaine, se sont largement autorégulés. L'accent était mis sur la diffusion et la croissance. Le contrôle des utilisateurs et la surveillance de ce qu'ils font n'étaient pas à l'ordre du jour. Car Internet était un espace de liberté, où chacun pouvait librement exprimer son opinion. Mais elle est bien révolue, l'époque où Internet ne servait qu'aux échanges d'informations. Entre-temps, presque tous les domaines de l'existence sont interconnectés, et il n'est plus concevable de vivre sans Internet. Ce média est devenu nécessaire à d'importants processus économiques ou sociaux. Son fonctionnement doit par conséquent être fiable et sûr. Et comme la sécurité constitue traditionnellement une tâche relevant de la puissance publique, beaucoup d'autorités s'estiment aujourd'hui responsables d'Internet et cherchent à combler le vide réglementaire. Cependant, l'approche traditionnelle des législations nationales, qui s'arrête aux frontières, a ses limites ici et les États doivent prendre en compte la dimension planétaire d'Internet.

Il semble peu réaliste d'attendre des États qu'ils élaborent une réglementation mondiale d'Internet. Les Nations Unies ont bien établi plusieurs groupes d'experts gouvernementaux (United Nations Group of Governmental Experts, UN GGE), chargés de délibérer sur les risques et les mesures à prendre afin de garantir la sécurité internationale et la paix dans ce contexte. Mais il s'agit d'un processus de longue haleine et la dernière réunion d'experts, qui remonte à 2017, n'a pas débouché sur un résultat consensuel. Ce n'est d'ailleurs qu'une illustration parmi d'autres des tensions géopolitiques croissantes, qui se répercutent dans tous les domaines de la coopération internationale. Une solution multilatérale qui recueillerait l'approbation de tous les pays du monde risque donc de se faire attendre encore longtemps.

Or tout le monde ne veut ni ne peut attendre. La numérisation avance à grands pas, et les pressions se sont accrues de tous côtés sur les acteurs d'Internet – elles n'émanent plus seulement de quelques exploitants d'infrastructure, mais de tous les prestataires ou utilisateurs. Quelques États cherchent à réglementer et contrôler Internet au moins sur leur propre territoire; par exemple en imposant aux exploitants de plateformes étrangères des prescriptions sur la protection des données et sur l'effacement de certains contenus, en censurant l'information ou en isolant leur segment d'Internet. D'un autre côté, des multinationales (Google, Facebook, Microsoft, etc.), tiennent à préserver en l'état actuel le réseau mondial (et aussi le marché mondial), et refusent d'être le jouet des conflits géopolitiques. À cela s'ajoutent les représentants de la société civile, qui veulent faire contrepoids tant au pouvoir excessif des États qu'à la course au profit des entreprises.

Il faut par conséquent instaurer certaines règles dans Internet, souvent qualifié de «zone de non-droit». Comme les États ne sont pas en mesure d'instaurer la sécurité juridique sur le plan mondial, des acteurs privés prennent le relais et formulent des propositions de codes de conduite ou font des déclarations sur leurs principes d'action. De telles initiatives émanent souvent de l'industrie informatique au sens large, ou de comités multiparties.

Les trois exemples qui suivent illustrent les efforts visant à accroître la prévisibilité, la fiabilité et la sécurité d'Internet et des ressources informatiques.

6.2.1 Commission mondiale sur la stabilité du cyberespace (Global Commission on the Stability of Cyberspace, GCSC)[68]

La Commission mondiale sur la stabilité du cyberespace réunit des représentants de haut niveau de gouvernements, d'entreprises, du domaine technique et de la société civile de toute la planète. Elle a pour mission d'encourager la paix, la sécurité et la stabilité au niveau international en formulant des normes pour un comportement responsable des acteurs étatiques et non étatiques dans l'espace numérique et en lançant des initiatives à cet effet.

6.2.2 Cyber Security Tech Accord[69]

Près de 80 entreprises du secteur high-tech ont signé à ce jour le Cyber Security Tech Accord[70]. Par leur signature, elles reconnaissent quatre principes clés visant à améliorer la sécurité, la stabilité et la résilience du cyberespace:

- Défense et protection: tous les clients ont partout droit, indépendamment de toute considération d'origine, à une protection efficace contre les cyberattaques.
- Non-agression: aucune aide ne sera apportée aux gouvernements qui voudraient lancer des cyberattaques contre des citoyens ou des entreprises innocents. Il s'agit encore de prévenir toute manipulation des produits ou services.
- Renforcement des capacités: les développeurs et les utilisateurs seront responsabilisés et aidés à mieux se protéger.
- Actions collectives: l'accent sera mis sur la collaboration technique et sur la divulgation coordonnée des vulnérabilités, ainsi que sur la lutte contre la diffusion des maliciels.

68 https://cyberstability.org/ (état: le 31 janvier 2019)

69 https://cybertechaccord.org/ (état: le 31 janvier 2019)

70 https://cybertechaccord.org/about/ (état: le 31 janvier 2019)

6.2.3 Appel de Paris pour la confiance et la sécurité dans le cyberespace[71]

Plus de 500 organisations, entreprises ou États ont signé l'Appel de Paris pour la confiance et la sécurité dans le cyberespace, qui prône l'élaboration de principes communs de sécurisation d'Internet. Les soutiens de l'Appel de Paris s'engagent à travailler ensemble en vue:

- d'accroître la prévention et la résilience face aux activités malicieuses en ligne;
- de protéger l'accessibilité et l'intégrité d'Internet;
- de coopérer afin de prévenir les interférences aux processus électoraux;
- de travailler ensemble contre les violations de la propriété intellectuelle par voie cyber;
- de prévenir la prolifération des programmes et techniques cyber malicieux;
- d'accroître la sécurité des produits et services numériques ainsi que la «cyber-hygiène» de tous;
- de prendre des mesures contre le cyber-mercenariat et les actions offensives des acteurs non-étatiques;
- de travailler ensemble pour renforcer les normes internationales pertinentes.

71 https://www.diplomatie.gouv.fr/fr/politique-etrangere-de-la-france/diplomatie-numerique/la-france-et-la-cybersecurite/article/cybersecurite-appel-de-paris-du-12-novembre-2018-pour-la-confiance-et-la (état: le 31 janvier 2019)

7 Politique, recherche et politiques publiques

7.1 Suisse: interventions parlementaires

Objet	Numéro	Titre	Déposé par	Date de dépôt	Conseil	Dép.	État des délibérations et lien
Mo	18.4387	En 2019, Conseil fédéral et DDPS font de la cybersécurité une priorité absolue	Guggger Niklaus-Samuel	14.12.2018	CN	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184387
Mo	18.4051	Cyberprotection et cyberdéfense. Où en est-on vraiment?	Golay Roger	28.09.2018	CN	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184051
Mo	18.4000	Participation de la Suisse au Centre d'excellence de cyberdéfense coopérative de l'OTAN à Tallinn	Fridez Pierre-Alain	28.09.2018	CN	DDPS	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184000
Mo	18.4375	Vote électronique. Pour un engagement rapide et fort en faveur d'un système en main publique et en "open source"	Sommaruga Carlo	14.12.2018	CN	ChF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184375
Po	18.4346	Plus d'honnêteté pour les portails de comparaison. Publication de toutes les commissions déclarées et cachées perçues par les comparateurs	Reimann Lukas	14.12.2018	CN	DEFR	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184346
Ip	18.4230	Le wi-fi gratuit dans les trains des CFF. Un minimum à l'heure de la Suisse numérique	Tornare Manuel	13.12.2018	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184230
Ip	18.4178	Pour un "smart farming" réalisable	Page Pierre-André	12.12.2018	CN	DEFR	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184178
Ip	18.4121	De plus en plus d'enfants sont victimes de harcèlement sexuel sur Internet. Que fait le Conseil fédéral?	Frei Yvonne	29.11.2018	CN	DFJP	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184121
Po	18.4004	Adapter la loi sur les voyages à forfait aux habitudes de consommation actuelles	Birrer-Heimo Prisca	28.09.2018	CN	DFJP	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184004
Po	18.3858	Limiter la consommation de pornographie des enfants et des jeunes sur Internet	Nordmann Roger	26.09.2018	CN	DFI	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183858
Mo	18.3856	Pour une meilleure prise en compte de la santé dans le secteur de la téléphonie mobile (1)	Estermann Yvette	26.09.2018	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183856
Mo	18.3855	Pour une meilleure prise en compte de la santé dans le secteur de la téléphonie mobile (2)	Estermann Yvette	26.09.2018	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183855
Ip	18.3800	Comment prévenir l'analphabétisme du visuel?	Fehlmann Rielle Laurence	20.09.2018	CN	DEFR	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183800
Qu	18.5450	La radio a-t-elle un avenir?	Wasserfallen Flavia	12.09.2018	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185450

Ip	18.4404	Stratégie Suisse numérique. Simplifier le processus de consultation des entreprises	Derder Fathi	14.12.2018	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184404
Mo	18.4037	Pour un centre de compétences dans le domaine de l'intelligence artificielle au sein de l'administration fédérale	Bendahan Samuel	28.09.2018	CN	DEFR	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184037
Mo	18.3788	Permis de conduire et de circulation. Solution numérique	Grüter Franz	19.09.2018	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183788
Qu	18.5478	Stratégie Suisse numérique. Le pilotage politique permettra-t-il une mise en œuvre rapide du plan d'action?	Derder Fathi	12.09.2018	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185478
Qu	18.5476	Stratégie Suisse numérique. Associer les entreprises fondées sur la science et spécialisées dans le numérique au plan d'action	Derder Fathi	12.09.2018	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185476
Mo	18.3958	Pour une seule et unique collecte de données par les pouvoirs publics	Müller-Altermatt Stefan	27.09.2018	CN	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183958
Ip	18.3853	OFIT. Des externalisations discutables frappent les collaborateurs âgés de 50 ans ou plus employés de longue date	Gysi Barbara	26.09.2018	CN	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183853
Po	18.3783	Accroître l'efficacité de la Confédération au moyen de l'automatisation intelligente des processus au sein de l'administration	Groupe libéral-radical Dobler Marcel	19.09.2018	CN	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183783
Ip	18.4299	Potentiel d'une utilisation de logiciels libres dans le domaine de l'éducation en Suisse	Quadranti Rosmarie	14.12.2018	CN	DEFR	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184299
Ip	18.4197	Sécurité informatique des infrastructures critiques. Quels sont les moyens et mesures mis en œuvre par le Conseil fédéral?	Wasserfallen Christian	12.12.2018	CN	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184197
Mo	18.4276	Faciliter l'échange d'informations en créant des interfaces électroniques au sein de l'administration fédérale	Vonlanthen Beat	13.12.2018	CE	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184276
Ip	18.4235	La Suisse rate le coche en matière de santé numérique. Quelles mesures le Conseil fédéral prévoit-il de prendre?	Graf-Litscher Edith	13.12.2018	CN	DFI	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20184235

7.2 Évolution du cadre légal lié à la technologie blockchain

Le thème de la blockchain est l'objet de toutes les discussions. Tout le monde a les yeux rivés sur le développement des cryptomonnaies et sur la «crypto valley» émergente en Suisse. Une série de questions se sont récemment posées sur la manière dont le système juridique suisse pourrait appréhender la technologie sous-jacente, et offrir ainsi à l'économie la sécurité

juridique nécessaire – condition sine qua non de la promotion et du développement de cette industrie.

Afin d'y trouver une réponse, le Secrétariat d'État aux questions financières internationales (SFI) a créé en janvier 2018 un groupe de travail sur la technologie blockchain et les ICO (*Initial Coin Offering*). Comme au-delà du droit des marchés financiers, la technologie blockchain touche à d'autres domaines juridiques comme le code civil et le code des obligations, l'Office fédéral de la justice (OFJ), la FINMA et des représentants de la branche financière font partie du groupe de travail. Les travaux ont pour but d'accroître la sécurité juridique, de préserver l'intégrité de la place financière et de garantir une réglementation neutre en matière de technologie.

En août 2018, le groupe de travail a consulté le secteur financier et la branche de la technologie financière, en leur donnant la possibilité de prendre position sur les travaux en cours et sur l'orientation des recommandations proposées. Outre des aspects généraux comme l'accès aux comptes bancaires pour les entreprises Fintech, la consultation abordait des questions dans les domaines du droit civil, de la lutte contre le blanchiment d'argent et le financement du terrorisme, ou encore du droit des marchés financiers. De l'avis des participants, les points sur lesquels il serait potentiellement nécessaire d'agir englobent notamment la qualification des jetons sous l'angle du droit civil et leur transfert, le traitement des cryptoactifs en cas d'insolvabilité, et la mise en place de nouvelles possibilités quant à l'infrastructure des marchés financiers.

À la mi-décembre 2018, le Conseil fédéral a adopté le rapport «Bases juridiques pour la *distributed ledger technology* et la *blockchain* en Suisse» du groupe de travail Blockchain/ ICO, et décidé de renoncer à créer une loi à ce sujet. Le rapport montre que la législation suisse se prête bien à l'utilisation des nouvelles technologies. Des changements légaux ponctuels sont cependant nécessaires. Le Conseil fédéral a donc chargé le Département fédéral des finances (DFF) et le Département fédéral de justice et police (DFJP) d'élaborer en 2019 un projet, qui sera mis en consultation et qui visera:

- à augmenter, dans le droit civil, la sécurité juridique lors du transfert de droits au moyen de registres numériques,
- à clarifier définitivement, dans le droit de l'insolvabilité, la question de la disjonction des cryptoactifs et à examiner la possibilité de créer un droit à la restitution des données qui n'ont aucune valeur patrimoniale,
- à élaborer, dans le droit des marchés financiers, une catégorie d'autorisation nouvelle et flexible pour les infrastructures des marchés financiers basées sur la blockchain,
- à adapter, dans le droit bancaire, les dispositions du droit sur l'insolvabilité des banques aux modifications apportées au droit général de l'insolvabilité, et
- à inscrire de manière plus explicite, dans la législation sur le blanchiment d'argent, la pratique actuelle concernant l'assujettissement des plateformes de négociation décentralisées à la loi sur le blanchiment d'argent.

En résumé, le Conseil fédéral entend créer un cadre juridique optimal permettant au pays de devenir un leader pour les sociétés Fintech et blockchain, mais aussi lutter systématiquement contre les abus et préserver l'intégrité et la bonne réputation de la place économique et financière suisse.

Le Conseil fédéral a en outre publié un rapport du Groupe interdépartemental de coordination sur la lutte contre le blanchiment d'argent et le financement du terrorisme (GCBF) consacré aux risques de blanchiment d'argent et de financement du terrorisme liés aux cryptoactifs et

au financement participatif. L'analyse montre que les cryptoactifs constituent un danger dans le domaine du blanchiment d'argent et du financement du terrorisme. Cependant, vu le petit nombre de cas, le risque réel encouru par la Suisse ne peut pas être évalué définitivement. La priorité va donc aux mesures coordonnées sur le plan international pour réaliser des améliorations dans ce domaine. Le DFF a toutefois été chargé d'examiner s'il y a lieu de modifier la législation sur le blanchiment d'argent, eu égard à certaines formes de financement participatif.

Il est trop tôt pour dire si ces mesures suffiront à garantir durablement l'attrait de la place helvétique pour les sociétés blockchain, ainsi que l'implantation de la «crypto valley» suisse. La Swiss Blockchain Federation, présidée par le conseiller d'État zougois Heinz Tännler, a l'intention de s'engager pour préserver et renforcer les atouts et la compétitivité de la Suisse dans ce secteur, mais aussi de mettre en réseau les acteurs concernés et de renforcer l'écosystème de la blockchain.

Cette tâche paraît centrale, alors que pour rehausser son attrait le Liechtenstein mettra en vigueur en été 2019 une loi sur la blockchain. Un tel cadre ne va pas manquer d'attirer des entreprises de la «crypto valley» suisse.

La Principauté de Liechtenstein s'est rendu compte que la densité réglementaire élevée des marchés financiers était un casse-tête pour les entreprises novatrices. Adrian Hasler, président du gouvernement liechtensteinois, juge important d'un point de vue institutionnel que de telles sociétés soient au clair sur leurs possibilités et sur les limites en vigueur. En outre, il est évident pour lui que le potentiel de la technologie blockchain ne réside pas seulement dans le secteur des services financiers, mais qu'elle permet de transposer dans le monde numérique une bien plus large palette d'actifs, afin d'offrir tous les services imaginables. Le Liechtenstein a pris le parti de légiférer sur la blockchain, parce que les champs d'application de l'économie des jetons s'étendent à toute l'économie et qu'ils marquent une étape supplémentaire sur le terrain de la numérisation. Avec le «jeton» comme nouvelle notion juridique, le Liechtenstein s'est par conséquent doté d'un instrument permettant de transposer dans le monde numérique n'importe quel droit appartenant au monde analogique. Mais la loi réglera aussi les limites ainsi que les activités dignes de protection, afin de limiter le risque d'abus.

Une telle approche apporte de la sécurité et constitue une base importante pour l'innovation et les investissements.

Information

INFO

Rapport Bases juridiques pour la distributed ledger technology et la blockchain en Suisse

https://www.newsd.admin.ch/newsd/message/attachments/55151.pdf

Rapport du Groupe interdépartemental de coordination sur la lutte contre le blanchiment d'argent et le financement du terrorisme «Le risque de blanchiment d'argent et de financement du terrorisme par les crypto-assets et le crowdfunding»

https://www.newsd.admin.ch/newsd/message/attachments/55112.pdf

FINMA Guide pratique pour les questions d'assujettissement concernant les *initial coin offerings* (ICOs):

https://www.finma.ch/fr/~/media/finma/dokumente/dokumentencenter/myfinma/1bewilligung/fintech/wegleitung-ico.pdf?la=fr

Rapport de consultation du gouvernement du Liechtenstein (Vernehmlassungsbericht der Regierung Liechtenstein betreffend die Schaffung eines Gesetzes über auf vertrauenswürdigen Technologien (VT) beruhende Transaktionssysteme (Blockchain-Gesetz; VT-Gesetz; VTG):

https://www.llv.li/files/srk/vnb-blockchain-gesetz.pdf

8 Produits publiés par MELANI

8.1 GovCERT.ch Blog

8.1.1 Reversing Retefe

Approximately one year ago, we have published our blog post The Retefe Saga. Not much has changed since last year except that we have seen a rise of malspam runs in the last couple of weeks and we want to use the opportunity to show how to reverse engineer the Retefe malware.

➔ https://www.govcert.ch/blog/35/reversing-retefe

8.2 Lettres d'information de MELANI

8.2.1 Les appels frauduleux aux entreprises se multiplient

05.07.2018 – Ces derniers jours, les appels aux entreprises durant lesquels des escrocs se font passer pour des employés d'une banque se multiplient. Concrètement, des escrocs se faisant passer pour des employés de banque invitent à effectuer des paiements, ou prétendent qu'il leur faut procéder à une mise à jour du site e-banking et la tester ensuite.

➔ https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/truffe-via-e-mail-e-telefono-in-aumento.html

8.2.2 Les outils de partage et de collaboration en ligne des entreprises ciblés par des attaques de phishing

02.10.2018 – À l'heure actuelle, de nombreuses entreprises permettent à leurs employés de partager des documents en ligne, et même d'y accéder à des suites bureautiques entières. Un simple mot de passe donnera parfois accès à un compte de messagerie, mais également à de nombreux autres documents. Il n'est dès lors guère étonnant que ces accès soient des cibles privilégiées pour des attaques de phishing. La compromission d'un compte est par ailleurs bien souvent utilisée comme vecteur d'attaque vers d'autres collaborateurs.

➔ https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/phishing_online_datenaustausch_kollaborationsplattformen.html

8.2.3 Réutiliser un mot de passe aide les cybercriminels

08.11.2018 – Le 27e rapport semestriel de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), publié le 8 novembre 2018, a porté sur les principaux cyberincidents survenus en Suisse et à l'étranger durant le premier semestre de cette année. MELANI a choisi les vulnérabilités du matériel informatique («hardware») comme thème prioritaire de cette édition. Il y est aussi question du maliciel que des cybercriminels ont transmis de manière ciblée en usurpant le nom du laboratoire de Spiez, de différentes fuites de données et du problème que pose la réutilisation des mots de passe pour plusieurs services sur Internet.

➔ https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/melani-halbjahresbericht-1-2018.html

8.2.4 Le cheval de Troie Emotet cible les réseaux d'entreprises

12.12.2018 – Ces dernières semaines, la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI a observé différentes vagues d'e-mails malveillants avec des documents Word en pièce jointe. Ces vagues contiennent le maliciel Emotet, connu depuis longtemps et se faisant aussi appeler Heodo. Ce maliciel était originellement un cheval de Troie bancaire. Actuellement, Emotet est utilisé pour envoyer du spam, mais aussi pour télécharger des maliciels supplémentaires. Emotet recourt à de l'ingénierie sociale et cherche, à travers des e-mails falsifiés au nom de collègues, partenaires commerciaux ou connaissances, à inciter le destinataire à ouvrir des documents Word et activer les macros.

➔ https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/Trojaner_Emotet_greift_Unternehmensnetzwerke_an.html

8.3 Listes de contrôle et instructions

MELANI n'a pas publié de listes de contrôle ou d'instructions supplémentaires durant le deuxième semestre de 2018.

9 Glossaire

Dénomination	Description
Advanced Persistent Threats (APT)	Menace pouvant infliger de sérieux dommages à une organisation ou à un pays. L'agresseur est disposé à investir beaucoup de temps, d'argent et de savoir-faire dans ce genre d'attaque ciblée et furtive, et dispose d'importantes ressources.
Agent financier	Un agent financier est un intermédiaire légal effectuant des opérations de courtage en devises. Depuis peu, cette notion s'utilise aussi à propos de transactions financières illégales.
Attaque DDoS	Attaque par déni de service distribué (Distributed Denial-of-Service attack) Attaque DoS où la victime est inondée de messages envoyés simultanément par de nombreux systèmes.
Attaque de la chaîne d'approvisionnement (supply chain)	Méthode consistant à s'en prendre à un maillon de la chaîne logistique de la victime afin de l'infecter.
Authentification à deux facteurs	Au moins deux des trois facteurs d'authentification sont exigés : un élément que l'on connaît (p. ex. mot de passe, code PIN, etc.) un élément que l'on détient (p. ex. certificat, jeton, liste à biffer, etc.) un élément qui nous est propre (p. ex. empreinte digitale, scanner rétinien, reconnaissance vocale, etc.)
Bitcoin	«Bitcoin» désigne à la fois un système de paiement à travers le réseau Internet et l'unité de compte utilisée par ce système de paiement.
Bot	Du terme slave «robota», signifiant travail. Programme conçu pour exécuter, sur commande, certaines actions de manière indépendante. Les bots malveillants peuvent diriger à distance les systèmes compromis et leur faire exécuter toutes sortes d'actions.
CEO Fraud	On parle de l'arnaque au président (CEO Fraud) quand l'identité d'un dirigeant d'entreprise est usurpée et le service compétent (service financier, comptabilité) est prié en son nom de procéder à un versement sur un compte (typiquement) à l'étranger.
CPU / Processeur	Le CPU (Central Processing Unit) désigne un processeur ou un microprocesseur, c'est-à-dire l'organe

	central d'un ordinateur, qui contient les circuits logiques exécutant les instructions des programmes.
Defacement	Défiguration de sites Web.
Domain Name System	Système de noms de domaine (Domain Name System). Le DNS rend les services Internet plus conviviaux, puisqu'au lieu de l'adresse IP les utilisateurs composent un nom (p. ex. www.melani.admin.ch).
Downloader	Programme dont la fonction est de télécharger et installer un ou plusieurs composants malveillants.
Faille de sécurité	Vulnérabilité dans un logiciel ou dans du matériel, grâce à laquelle un attaquant peut chercher à accéder à un système.
Force brute	La recherche par force brute (brute force) ou recherche exhaustive consiste, en informatique, en cryptanalyse ou dans la théorie des jeux, à tester toutes les combinaisons possibles pour résoudre les problèmes.
Global Positioning System (GPS)	Global Positioning System (GPS), dont le nom officiel est NAVSTAR GPS, est un système mondial de navigation par satellite, permettant de déterminer à un moment précis une position géographique.
Infection par «drive-by download»	Infection d'un ordinateur par un maliciel, lors de la simple visite d'un site Web. Les sites concernés contiennent dans bien des cas des offres sérieuses, mais ont été compromis auparavant pour la diffusion de maliciels. Différents exploits, tirant parti des lacunes de sécurité non comblées par le visiteur, sont souvent testés à cet effet.
Internet des objets	Ensemble des objets branchés à Internet capables de communiquer pour collecter, transmettre et traiter des données, avec ou sans intervention humaine.
Javascript	Langage de script basé objet pour le développement d'applications. Les Javascripts sont des éléments de programmes intégrés au code HTML qui permettent d'implémenter certaines fonctions dans le navigateur Internet. Un exemple est le contrôle des indications saisies par l'utilisateur dans un formulaire Web. Il permet de vérifier que tous les caractères introduits dans un champ demandant un numéro de téléphone sont effectivement des chiffres. Comme les composants ActiveX, les Javascripts s'exécutent sur l'ordinateur de l'internaute. Outre les fonctions utiles, il

	est malheureusement possible aussi d'en programmer de nuisibles. Au contraire d'ActiveX, le langage JavaScript est compatible avec tous les navigateurs.
Kit d'exploits	Outil permettant de générer des scripts, programmes ou codes, visant à exploiter des failles de sécurité.
Malware	Programme malveillant. Terme générique employé pour tout logiciel exécutant des fonctions nuisibles sur un ordinateur (comme p.ex. les virus, les vers ou les chevaux de Troie).
Métadonnées	Les métadonnées ou métainformations sont des données renseignant sur la nature de certaines au-tres données.
Minage	Utilisation de la puissance de calcul d'un ordinateur pour valider et sécuriser, par blocs, les transactions d'un réseau de cryptomonnaie. Cette activité est rémunérée à cause de sa forte consommation d'énergie.
MITM	Man-in-the-Middle attack, attaque de l'intermédiaire Attaque où le pirate s'immisce dans le canal de communication de deux partenaires pour lire ou modifier les données échangées.
P2P	Peer to Peer Architecture de réseau où tous les postes de travail ont les mêmes possibilités de communication (à l'inverse des réseaux client/serveur). P2P sert fréquemment aux échanges de données.
Patch	Programme qui remplace une partie de programme comportant des erreurs par une partie exempte d'erreurs et remédie ainsi par exemple à une lacune de sécurité.
Phishing	Via l'hameçonnage, des pirates tentent d'accéder aux données confidentielles d'utilisateurs Internet ne se doutant de rien. Il peut s'agir p. ex. d'informations concernant les comptes pour des soumissionnaires de ventes aux enchères en ligne (p. ex. eBay) ou des données d'accès pour le e-banking. Les pirates font appel à la bonne foi, à la crédulité ou à la serviabilité de leurs victimes en leur envoyant des courriels avec des adresses d'expéditeur falsifiées.
Porte dérobée	Une porte dérobée (en anglais: backdoor) désigne une fonctionnalité inconnue de l'utilisateur légitime, qui permet à un pirate d'accéder secrètement à un

	programme ou à un système d'exploitation, en contournant les mécanismes de sécurité en place.
Pourriel (Spam)	Désigne le courrier électronique non sollicité, constitué surtout de publicité, envoyé automatiquement. L'auteur de tels messages est qualifié de polluposteur (spammer) et ses envois de pollupostage (spamming).
PowerShell (script)	PowerShell est une suite logicielle Microsoft qui intègre une interface en ligne de commande et un langage de script, permettant d'automatiser des tâches ou de configurer et d'administrer des systèmes.
Proxy	Programme servant d'intermédiaire pour accéder à un autre réseau, en collectant les requêtes et en les transmettant vers l'extérieur à partir d'une même adresse.
Remote Administration Tool ou Remote Access Tool (RAT)	Un Remote Administration Tool, outil de télémaintenance, est un programme permettant la prise de contrôle totale, à distance, d'un ordinateur depuis un autre ordinateur.
Router	Dispositif intelligent assurant la connexion physique entre plusieurs réseaux (informatique, télécommunication, Internet). Un router s'utilise par exemple dans un réseau domestique, où il optimise la transmission de l'information entre le réseau interne et Intranet.
Serveur Command & Control	La plupart des réseaux de zombies reçoivent des instructions de leur créateur, qui les surveille par un canal de communication. Le cas échéant, on parle de serveur Command & Control (C&C).
Smartphone	Un smartphone est un téléphone mobile doté des fonctions d'un assistant numérique personnel (agenda, calendrier, navigation Web, consultation du courrier électronique, messagerie instantanée, GPS, etc.).
SMS	Short Message Service Service de messages courts. Service permettant d'envoyer des messages courts (max. 160 caractères) à un (utilisateur de) téléphone mobile
Social Engineering	Les attaques de social engineering (subversion psychologique) utilisent la serviabilité, la bonne foi ou l'insécurité des personnes pour accéder par exemple à des données confidentielles ou conduire la victime à exécuter certaines actions spécifiques.

Spear Phishing	Pêche au harpon. La victime aura p. ex. l'illusion de communiquer par courriel avec une personne connue d'elle.
Spearphishing-Mails	Pêche au harpon. La victime aura par ex. l'illusion de communiquer par courriel avec une personne connue d'elle.
Systèmes de contrôle industriels (SCI)	Les systèmes de contrôle-commande sont formés d'un ou plusieurs appareils qui pilotent, règlent et/ou surveillent le fonctionnement d'autres appareils ou systèmes. Dans le domaine industriel, l'expression «systèmes de contrôle industriels» (Industrial Control Systems, ICS) est entrée dans le langage courant.
Take Down	Retrait de contenu frauduleux, désactivation d'adresse Web par un hébergeur ou un registraire.
TCP/IP (Transmission Control Protocol / Internet Protocol)	Ensemble de protocoles de communication conçu pour la transmission des données sur Internet.
Top-Level-Domains	Tout nom de domaine dans Internet est formé d'une série de signes séparés par des points. Le domaine de premier niveau ou de tête (TLD) désigne le dernier élément de cette série et se situe au niveau hiérarchique le plus élevé du nom. Par exemple, si le nom de domaine d'un ordinateur ou d'un site est de.example.com, le TLD sera «com».
UDP	User Datagram Protocol; protocole sans connexion, utilisé pour expédier de petits messages (datagrammes) d'une application Internet à l'autre.
USB	Universal Serial Bus Bus série permettant (avec les interfaces physiques) de raccorder des périphériques tels qu'un clavier, une souris, un support de données externe, une imprimante, etc. Il n'est pas nécessaire d'arrêter l'ordinateur pour brancher ou débrancher un appareil USB. Les nouveaux appareils sont généralement (selon le système d'exploitation) reconnus et configurés automatiquement.
Ver	A la différence des virus, les vers n'ont pas besoin de programme hôte pour se reproduire. Ils utilisent les lacunes de sécurité ou des erreurs de configuration des systèmes d'exploitation ou des applications, pour se propager d'ordinateur en ordinateur.

Watering Hole Attack	Attaque dite du point d’eau, attaque ciblée par un maliciel, diffusé à traversdes sites supposés être visités par un groupe spécifique d’utilisateurs.
WLAN	Un WLAN (Wireless Local Area Network) est un réseau local sans fil.
Zero-Day	Vulnérabilité, pour laquelle aucun correctif de sécurité n’est pour l’instant disponible.
Zip	zip est un algorithme et un format de compression des données destiné à réduire l’espace mémoire occupé par les fichiers lors de l’archivage ou du transfert.