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
https://www.melani.admin.ch/

SÛRETÉ DE L'INFORMATION

SITUATION EN SUISSE ET SUR LE PLAN INTERNATIONAL

Rapport semestriel 2019/1 (janvier à juin)

29 OCTOBRE 2019

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

1 Aperçu / sommaire

2 Éditorial

Rançongiciels – les administrations ne sont pas épargnées

Martin Müller est responsable de la cybersécurité de la Ville de Berne. Il fait partie de divers groupes de travail nationaux pour la sûreté de l'information et du réseau Swiss Certified ICT Leaders.

Rançongiciels, cryptogiciels, chevaux de Troie verrouillant les données ou logiciels de chantage, peu importe le nom qu'on leur donne, de tels maliciels et la demande de rançon qu'ils formulent une fois introduits dans un système piraté nous sont familiers depuis que WannaCry a fait les gros titres. Les revendications vont de quelques centaines de dollars à plusieurs centaines de milliers de dollars, payables en bitcoins pour récupérer ses fichiers chiffrés. Et encore, nul ne peut être sûr de retrouver ses données.

De telles attaques se sont produites dans l'administration municipale bernoise, en 2017 et en 2019. Les agresseurs n'avaient pas délibérément attaqué l'administration locale mais lancé des attaques de grande envergure, afin de générer le plus gros butin possible. De nombreux préposés à la sécurité sont d'autant plus inquiets que de telles attaques sont devenues possibles aujourd'hui avec très peu de connaissances et de ressources. Certains acteurs de l'Internet clandestin proposent déjà pour une somme modique le modèle *ransomware as a service* (RaaS). Loin d'être réservée aux cyberescrocs par métier, une telle technique d'attaque est désormais accessible à tout le monde, aux jeunes pirates amateurs visant la célébrité comme aux hacktivistes mus par des mobiles politiques.

Outre toutes les mesures techniques de sécurité envisageables – pare-feu, systèmes de détection d'intrusion et de prévention des attaques, antivirus, solutions de sécurisation de la messagerie, actualisation permanente des logiciels et du matériel –, une importante mesure technique consiste à effectuer régulièrement des copies de sécurité (back up). De telles sauvegardes seront isolées, de manière physique ou logique, du reste du réseau d'entreprise afin qu'en cas d'incident, le cours normal de l'exploitation puisse rapidement reprendre et la perte de données rester limitée au minimum. À ce jour, la gestion des sauvegardes de la municipalité a fait ses preuves à chaque attaque subie par les serveurs de l'administration.

Or les mesures techniques que le monde numérique actuel met à notre disposition ne suffisent pas et à côté, l'humain joue nécessairement un rôle central. Par conséquent, la formation ou la sensibilisation des collaborateurs constitue à nos yeux la principale mesure à prendre, ainsi qu'un pilier essentiel de la sécurité informatique. En particulier, la transformation numérique de l'environnement administratif devra jeter les bases nécessaires pour que les collaborateurs puissent utiliser leurs nouveaux instruments de travail de manière sûre et responsable, en toute confiance. Par ailleurs, une saine méfiance et le bon sens contribuent également à la sécurité. Dans sa stratégie numérique 2021 comme dans sa campagne de 2019-2020 sur la sécurité informatique, l'administration municipale de Berne a volontairement insisté sur le renforcement des capacités individuelles, et nous vous recommandons de faire de même.

Martin Müller

3 Thème prioritaire: rançongiciels

Les rançongiciels (chevaux de Troie chiffrant les données) sont un outil bien établi dans le monde de la cybercriminalité. De tels chevaux de Troie rendent les données inaccessibles à des fins de chantage ou, plus rarement, pour causer un préjudice à une entreprise. Au fil des ans, les développements techniques et tactiques ont fait des chevaux de Troie chiffrant les données une des menaces les plus dangereuses pour les entreprises. Le premier semestre 2019 a été marqué par une forte augmentation mondiale des attaques ciblées contre des organisations, avec une recrudescence des demandes de rançon.

3.1 Évolution historique

Il y a huit ans déjà, MELANI avait décrit l'apparition de logiciels malveillants qui bloquent les ordinateurs dans un but d'extorsion.[1] Il s'agissait d'une des toutes premières versions, qui affichait à l'écran un message prétendument envoyé par la Police fédérale. Il y était dit qu'il fallait payer une amende parce que du matériel illégal avait été repéré sur l'appareil en question. Ce type de *maliciel* était relativement inoffensif et dans la plupart des cas, il suffisait d'analyser l'ordinateur avec un antivirus en version live CD pour l'éliminer.

Deux ans plus tard Cryptolocker, était le premier *maliciel* doté d'une fonction de chiffrement à faire les gros titres.[2] Il verrouillait les données stockées tant sur le disque dur que sur les supports de données lui étant raccordés. Une clé spécifique était générée sur un serveur *C2* pour chaque victime. La restauration des données était plus délicate qu'avec les chevaux de Troie utilisant une clé dont la valeur est programmée par défaut et d'autant plus facile à extraire. Cryptolocker se répandait par l'intermédiaire de l'annexe infectée de spams malveillants (*malspam*), lors d'infections par *drive-by download* (sur des pages manipulées), ou encore au moyen d'injecteurs (*dropper*, fichier exécutable contenant d'autres virus afin de les installer). Les injecteurs constituent entre-temps un mode de diffusion très répandu.

En 2014, le maliciel Synolocker s'est propagé en utilisant une faille de sécurité des appareils *NAS* de la société Synology.[3] Il s'agissait d'une vulnérabilité connue, pour laquelle une mise à jour de sécurité avait été publiée des mois auparavant. Ce cas a montré la nécessité de mettre régulièrement à jour non seulement les programmes et les systèmes d'exploitation des ordinateurs, mais aussi les routeurs, les appareils *NAS* et autres composants similaires du système. En 2014, les programmeurs de rançongiciels ont commencé à prendre des mesures pour déjouer l'identification et l'analyse des serveurs *C2*. Ainsi le cryptologiciel CTB-Locker, diffusé sur des pages piratées de médias en ligne, communiquait sous forme chiffrée avec ses serveurs *C2* et utilisait le service d'anonymisation Tor pour brouiller les pistes et empêcher les acteurs de la sécurité de le localiser et d'analyser son mode opératoire.

Les escrocs ont toujours été à l'affût de nouvelles cibles. Ils ont par exemple traqué les bases de données de sites Internet insuffisamment protégés, qu'ils ont chiffrées pour exiger ensuite

---

1 MELANI, rapport semestriel 2011/2, chap. 3.5.
2 MELANI, rapport semestriel 2013/2, chap. 3.1.
3 MELANI, rapport semestriel 2014/2, chap. 3.6.

une rançon de leurs administrateurs.[4] En 2015, Teslacrypt et Cryptowall étaient les familles de rançongiciels les plus actives.[5]

Le phénomène des rançongiciels a connu un véritable boom en 2016.[6] Pour la première fois, il a frappé des infrastructures d'importance vitale, notamment des hôpitaux en Allemagne et aux États-Unis. Or le secteur de la santé ne doit pas seulement faire face au défi de l'actualisation de systèmes informatiques et appareils médicaux certifiés, et procéder à toutes les mises à jour de sécurité; il lui faut encore réagir plus vite que bien d'autres victimes, sachant qu'une infrastructure informatique défaillante menace des vies humaines. Ainsi mis sous pression, un hôpital sera tenté de payer la rançon exigée, pour redevenir rapidement opérationnel. Or ce n'est pas nécessairement la panacée, comme le montrent les déboires du Kansas Heart Hospital.[7] Les escrocs n'ont libéré qu'une partie des fichiers et ont exigé qu'une seconde rançon leur soit versée en échange du déblocage du reste.

Un rançongiciel techniquement plus sophistiqué, baptisé Locky, a sévi à partir de février 2016 en Suisse.[8] Il chiffrait les fichiers stockés sur des unités de réseau (lecteurs virtuels, partages réseau, etc.). L'augmentation exponentielle du phénomène a amené les autorités de sécurité à renforcer leurs mesures préventives. MELANI a organisé en collaboration avec divers offices fédéraux, des associations ou organismes suisses ainsi que des fabricants de logiciels, une journée de sensibilisation aux rançongiciels.[9] De son côté, l'Office fédéral allemand de la sécurité des technologies de l'information (BSI) a publié un rapport complet sur le thème des rançongiciels.[10]

Au premier semestre 2017, deux attaques internationales dues à des rançongiciels ont clairement montré le risque potentiel lié à de telles attaques: WannaCry a infecté au moins 200 000 ordinateurs situés dans 150 pays. Parmi ses victimes illustres figuraient l'opérateur espagnol Telefonica, des hôpitaux britanniques ou encore la Deutsche Bahn. En Suisse, plusieurs centaines de victimes ont été identifiées, mais aucune infrastructure d'importance vitale. Peu après, le *maliciel* NotPetya causait de graves dégâts, tout d'abord en Ukraine. Il a notamment frappé l'aéroport de Kiev, la banque centrale ukrainienne et la station de mesure de la radioactivité de Tchernobyl. Le maliciel s'est par la suite propagé plus globalement par l'entremise de filiales ukrainiennes d'entreprises multinationales. Le groupe danois Maersk – première compagnie maritime et plus grand armateur de porte-conteneurs du monde – et le groupe pharmaceutique américain Merck ont notamment été touchés. En Suisse, la régie publicitaire Admeira a notamment été touchée par NotPetya.[11] Dans le cas de WannaCry comme de NotPetya, le *maliciel* se propageait à la manière d'un ver – donc de façon autonome –, en

---

4 MELANI, rapport semestriel 2014/2, chap. 5.3.

5 MELANI, rapport semestriel 2015/1, chap. 4.6.1.5 et 2015/2, chap. 4.5.1.

6 MELANI, rapport semestriel 2016/1, chap. 5.4.3.

7 https://www.csoonline.com/article/3073495/kansas-heart-hospital-hit-with-ransomware-paid-but-attackers-demanded-2nd-ransom.html

8 MELANI, rapport semestriel 2016/1, chap. 4.6.3.

9 https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/ransomwareday.html; https://www.switch.ch/news/ransomware-day/; https://www.ebas.ch/fr/securitynews/509-journee-suisse-de-sensibilisation-aux-rancongiciels

10 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Lagedossier_Ransomware.pdf

11 MELANI, rapport semestriel 2017/1, chap. 3.

exploitant une faille du *protocole SMB*. Or si WannaCry semble se déplacer au hasard, tout indique que NotPetya cherchait surtout à infecter des entreprises ukrainiennes. Dans les deux cas, les experts n'ont pas cru à des mobiles purement criminels. Même s'ils n'ont pu déterminer ni l'identité du commanditaire ni ses mobiles, il semblerait que les agresseurs visaient surtout à commettre des actes de sabotage et à semer la panique.

Au deuxième semestre 2017, le rançongiciel BadRabbit a procédé à des attaques géolocalisées, en Russie surtout, mais également en Ukraine, en Allemagne et en Turquie. BadRabbit s'est propagé par l'intermédiaire de fausses mises à jour d'Adobe Flash: il associait l'exploit EternalRomance et l'outil de récupération des mots de passe Mimikatz pour se déplacer dans le système des entreprises et se propager à tous les ordinateurs.[12]

De graves pertes de production sont à craindre jusqu'à la restauration des systèmes paralysés par un rançongiciel, comme l'a appris à ses dépens en 2018 le fabricant de puces taïwanais TSMC (Taiwan Semiconductor Manufacturing Company). Une variante de WannaCry l'a contraint à interrompre temporairement la production de plusieurs fabriques.[13]

Jusqu'en 2018, les attaques menées à l'aide de rançongiciels n'étaient généralement pas ciblées. Seul le groupe SamSam était connu pour opérer de manière chirurgicale, s'attaquant surtout à des organisations américaines. Le rançongiciel Ryuk, apparu en 2018, semble avoir été délibérément placé auprès d'organisations susceptibles de verser des rançons élevées. Déjà abordé dans le précédent rapport semestriel,[14] Ryuk s'est montré très actif en 2019 aussi (voir chapitre 3.4.1). D'autres rançongiciels sont employés à la fois de manière ciblée et pour des attaques opportunistes, comme GandCrab et Dharma.[15]

3.2 Incidents récents

Le nombre d'attaques ciblées basées sur des rançongiciels a connu une recrudescence au premier semestre 2019. À Ryuk, GandCrab et Dharma se sont ajoutés LockerGoga, MegaCortex et RobbinHood. Ce dernier a paralysé à fin mai l'administration municipale de Baltimore.[16] Les attaques basées sur des rançongiciels comptent parmi les cybermenaces les plus dangereuses pour les entreprises, les organisations et les administrations. En plus d'exiger du temps, du personnel et de l'argent pour le nettoyage des systèmes et la restauration des données perdues, une attaque fructueuse peut nuire à la réputation d'une entreprise ou entraîner une perte de productivité pendant de longs jours.[17] Ainsi le producteur d'aluminium Norsk Hydro a dû basculer en mode manuel ses activités de production automatisées, à la suite d'une attaque avec demande de rançon[18], ou les policiers du comté de Jackson en Géorgie (USA) se sont remis à écrire leurs rapports à la main, Ryuk ayant bloqué les systèmes de l'administration municipale[19]. En Suisse la société Offix Holding AG, elle aussi victime de Ryuk (voir chapitre

12 MELANI, rapport semestriel 2017/2, chap. 5.4.2.
13 MELANI, rapport semestriel 2018/2, chap. 5.3.5.
14 MELANI, rapport semestriel 2018/2, chap. 4.5.4.
15 https://www.symantec.com/blogs/threat-intelligence/targeted-ransomware-threat
16 https://www.tripwire.com/state-of-security/featured/ransomware-baltimore-network/
17 https://www.symantec.com/blogs/threat-intelligence/targeted-ransomware-threat
18 https://www.bleepingcomputer.com/news/security/lockergoga-ransomware-sends-norsk-hydro-into-manual-mode/
19 https://statescoop.com/georgia-county-paid-400k-to-ransomware-hackers/

3.4.1), a évité le pire en activant dans les heures qui ont suivi le mode d'urgence, ce qui lui a permis d'informer les clients et de poursuivre son travail pendant la résolution de ses problèmes informatiques. Elle n'est pas entrée en matière sur la demande de rançon de 45 bitcoins (env. 330 000 francs).[20]

Certains incidents signalés au cours de la période sous revue relèvent à la fois de l'extorsion et de l'hameçonnage (phishing). Le cheval de Troie à l'œuvre ne se borne pas à verrouiller les fichiers, mais cherche également à dérober aux victimes des données sensibles. Les victimes peuvent au choix payer la rançon en bitcoins ou par PayPal. Si elles optent pour PayPal, elles seront attirées sur un site de phishing. Les escrocs les prieront d'indiquer tant les informations relatives à leur carte de crédit que leurs données d'accès à PayPal et d'autres données personnelles encore.[21]

Quand les agresseurs ont réalisé que les copies de sauvegarde (back up) pouvaient faire échouer leurs plans, ils ont changé d'approche. Ils se procurent depuis lors les accès et mots de passe nécessaires pour pouvoir détruire ou verrouiller aussi les copies de secours, avant de verrouiller les systèmes opérationnels.

Il n'est guère étonnant que les entreprises n'ayant pas de sauvegarde, ou dont la sauvegarde a été rendue inutilisable et dont la survie est ainsi en péril, décident de payer la rançon exigée. En 2014 déjà, MELANI avait expliqué que les rançongiciels auront le vent en poupe tant que les victimes acceptent de payer pour récupérer leurs données.[22] C'est ce qu'ont fait au premier semestre 2019 deux villes de Floride, Riviera City et Lake City. Elles ont consenti à verser des rançons exorbitantes, de 65 bitcoins (600 000 dollars) ou 42 bitcoins (500 000 dollars). Dans le cas de Lake City, les pirates avaient pris contact directement avec l'assureur municipal à propos du paiement de la rançon.[23] Une telle tendance risque de s'établir en Suisse aussi.[24] Or à long terme, le paiement de rançons n'est pas un «investissement profitable». Car plus les entreprises sont disposées à payer une rançon, et plus les cybercriminels seront tentés d'adopter ce modèle d'affaires.[25]

3.3 Ransomware as a service

Le marché au noir évolue lui aussi, avec la division croissante du travail et sa spécialisation. Des cyberattaques préconfigurées sont proposées de longue date dans l'Internet clandestin.[26] On peut parler ici de «cybercrime *as a service*» (*CaaS*), ou de *RaaS* dans le cas des rançon-

---

20 https://www.inside-it.ch/articles/54898

21 https://www.bleepingcomputer.com/news/security/new-ransomware-bundles-paypal-phishing-into-its-ransom-note/

22 MELANI, rapport semestriel 2014/2, chap. 5.3.

23 https://www.zdnet.com/article/second-florida-city-pays-giant-ransom-to-ransomware-gang-in-a-week/

24 https://www.nzz.ch/wirtschaft/ransomware-warum-zahlreiche-firmen-loesegeld-zahlen-duerften-ld.1489507

25 https://www.symantec.com/blogs/threat-intelligence/targeted-ransomware-threat

26 Voir MELANI, rapport semestriel 2009/2, chap. 4.7: «Le modèle commercial Crimeware-as-a-Service (CaaS) a été mis au point l'année dernière. Grâce à lui, les pirates peuvent «louer» le service désiré, sans avoir à s'embarrasser de considérations techniques.»

giciels. Il n'est plus nécessaire de s'y connaître en informatique pour lancer une cyberattaque[27]. De tels services clés en main incluent, pour un prix donné, tous les éléments nécessaires à une attaque: instructions pour la mise au point du *maliciel*, panneau de bord livrant toutes les informations utiles sur les infections fructueuses, clé de déchiffrement, et même parfois un tutoriel. À partir de ce paquet de base, le «client» peut lui-même ajuster le rançongiciel et son attaque à ses besoins[28].

3.4 Principaux rançongiciels actifs aujourd'hui

3.4.1 Ryuk

Le rançongiciel Ryuk, qui sévit depuis le deuxième semestre 2018, a déjà été évoqué dans le précédent rapport semestriel.[29] En décembre dernier, il s'en est pris au groupe Tribune Publishing à Los Angeles. Concrètement, les escrocs ont verrouillé le serveur de la plateforme de production servant à l'impression et à la distribution de plusieurs journaux américains. La panne a retardé, voire partiellement empêché, la publication des éditions du samedi du Los Angeles Times et de la San Diego Union Tribune, ainsi que sur la côte Est celle du Wall Street Journal et du New York Times.[30]

Ryuk permet de lancer des attaques ciblées contre les ordinateurs et les serveurs de réseau des entreprises. Le chiffrement des données constitue fréquemment la phase finale d'une attaque en trois étapes, qui débute par une infection au moyen d'Emotet. Ce cheval de Troie est souvent diffusé par courriel, avec un lien ou une annexe infectés (*malspam*). Il suffit qu'une personne dans l'entreprise clique dessus par inadvertance pour qu'Emotet s'installe sur son ordinateur et envoie depuis là des courriels à tous les contacts existants afin de se propager. Emotet fait office d'injecteur (*dropper*) d'autres logiciels malveillants. Par exemple, Trickbot est parfois téléchargé (voir chapitre 4.6) et procède à une analyse du réseau pour déterminer si l'ordinateur appartient à un particulier ou à une entreprise. Dans le second cas, il cherchera à se propager dans le réseau au moyen d'une faille du protocole *SMB*. Des informations sur la victime potentielle sont ainsi collectées, et le téléchargement de Ryuk n'intervient généralement que si elle est jugée suffisamment attrayante.[31]

Cette année aussi, Ryuk a mené des attaques ciblées et exigé des rançons exorbitantes. Parmi les victimes figurent les administrations de plusieurs villes américaines, qui ont payé entre 130 000 et 600 000 dollars de rançon chacune.[32]

En Suisse, des cas sont apparus dans le secteur de la construction, dans les transports publics et dans l'industrie. Ainsi Offix Holding AG, entreprise spécialisée dans la vente d'articles de bureau et de papeterie, a subi à la mi-mai une «cyberattaque ciblée, planifiée, massive et

---

27 Pour plus de détails, voir MELANI, rapport semestriel 2016/2, chap. 6.1.

28 https://securityaffairs.co/wordpress/84273/breaking-news/inpivx-ransomware-service.html

29 MELANI, rapport semestriel 2018/2, chap. 4.5.4.

30 https://www.heise.de/newsticker/meldung/Cyber-Attacke-verzoegert-Druck-grosser-Tageszeitungen-in-den-USA-4260103.html

31 MELANI, rapport semestriel 2018/2, chap. 4.5.4.

32 https://www.bleepingcomputer.com/news/security/la-porte-county-pays-130-000-ransom-to-ryuk-ransomware/

soigneusement orchestrée».[33 et 34] Tout a commencé avec l'envoi, par courriel, d'un document Word qui a installé à l'aide d'une macro le *maliciel* Emotet. Ce dernier a téléchargé par la suite Trickbot et Ryuk. Deux jours plus tard, la majeure partie des systèmes d'exploitation étaient à l'arrêt (enregistrement du temps de travail, administration des salaires, banques d'images, serveur de téléphonie, serveur Citrix, serveur Exchange, etc.)[35]. Seules ont été épargnées les boutiques en ligne, hébergées sur des serveurs Linux, ainsi que le système de gestion des marchandises.

3.4.2 LockerGoga et MegaCortex

LockerGoga est apparu pour la première fois en janvier 2019, lors d'une attaque visant Altran, groupe français d'ingénierie et de conseil en technologies leader au niveau mondial.[36] LockerGoga fait typiquement partie de la seconde phase d'une infection: son exécution est prise en charge par un utilitaire PsExec installé sur une machine préalablement infectée. Les escrocs utilisent des outils de piratage disponibles sur le réseau, afin d'accéder au système et de se procurer des droits d'administrateur qui leur serviront à désactiver le logiciel de sécurité et les sauvegardes pour installer leur rançongiciel. Cette technique, combinée à l'utilisation de certificats légitimes, permet au *maliciel* de déjouer les mesures de protection.[37] Une fois installé, LockerGoga modifie les données d'accès au système et tente d'interrompre la session des utilisateurs en ligne. Son approche consiste à verrouiller un maximum d'appareils à la fois. À cet effet, le rançongiciel utilise un processus différent par fichier à chiffrer, pratique d'autant plus rare qu'elle ralentit considérablement le verrouillage.[38]

En mars, au moins trois entreprises réputées auraient fait les frais de LockerGoga, soit Hexion et Momentive, deux sociétés américaines qui appartiennent au fonds d'investissement Apollo Global Management et qui fabriquent entre autres des résines et du silicone,[39] et le producteur d'aluminium norvégien Norsk Hydro. Dans le dernier cas, l'infection a apparemment commencé dans une succursale américaine, d'où le *maliciel* s'est déplacé «latéralement» dans le réseau pour infecter la quasi-totalité des postes de travail. À certains endroits, il a fallu en revenir au mode de production manuel, car le système de production n'était plus disponible. Les escrocs ont apparemment modifié les mots de passe des comptes dans le service d'annuaire. Il se peut qu'ils aient obtenu avec Mimikatz ou un outil similaire les tickets Kerberos avec lesquels ils auront pu indiquer au système l'identité usurpée de ses utilisateurs.[40]

MegaCortex utilise une approche similaire à LockerGoga. Ce rançongiciel lance des attaques ciblées contre des entreprises ou organisations. Selon différentes sources, MegaCortex aurait infecté en 48 heures une cinquantaine d'entreprises ou organisations situées aux États-Unis,

---

33 Information transmise par Offix Holding AG à sa clientèle, voir: https://www.inside-it.ch/articles/54898

34 https://www.nzz.ch/wirtschaft/cyber-angriff-auf-schweizer-firma-offix-ein-kampf-ums-ueberleben-ld.1492862

35 https://www.inside-it.ch/articles/54898

36 https://ml.globenewswire.com/Resource/Download/0663f8d4-0acf-4463-b0fd-bb05042d1373, https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware

37 https://www.symantec.com/blogs/threat-intelligence/targeted-ransomware-threat

38 https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware

39 https://www.chemistryworld.com/news/hexion-momentive-and-norsk-hydro-all-hit-by-ransomware-cyber-attacks/3010328.article

40 https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware

en Europe et au Canada.[41] Comme l'ont indiqué les chercheurs de Sophos, il n'y a pas de similitudes de code entre MegaCortex et LockerGoga, mais dans un cas comme dans l'autre les exploitants se servent d'un *contrôleur de domaine* compromis pour envoyer des *maliciels* aux machines d'un réseau pris pour cible. Des commandes PowerShell sont exécutées pour contacter les serveurs *C2* contrôlés par les escrocs et pour procéder au verrouillage. Or au moins un des serveurs *C2* a été utilisé tant pour MegaCortex que pour LockerGoga, soulignent encore les chercheurs.[42] À l'instar de Ryuk, MegaCortex a souvent été décelé dans des entreprises préalablement infectées par Emotet et Qbot.[43] Tous ces cryptologiciels ont également sévi en Suisse.

3.4.3 GandCrab

Au deuxième semestre 2018, GandCrab représentait 50 % du marché mondial des rançongiciels. Il faut dire que ses concepteurs ont travaillé selon un modèle de rançongiciel en tant que service (RaaS), proposant leur *maliciel* dans l'Internet clandestin. Le prix était fixé à 40 % des bénéfices générés par les attaques lancées avec cet outil.[44] Cela explique le grand nombre de vecteurs utilisés pour diffuser le *maliciel*, avec diverses variantes de pourriels (*malspam*), de prétendus dossiers de candidature, ainsi que des sites Web spécialement conçus ou d'autres légitimes ayant subi une infection par *drive-by download.*[45]

Depuis l'apparition de GandCrab en janvier 2018, différentes versions ou refontes de son code ont rendu les attaques toujours plus efficaces et difficiles à combattre. Les auteurs de ce *maliciel* recourent d'ailleurs à des moyens redondants: cette année, il est apparu que diverses attaques combinaient GandCrab avec BetaBot ou AzorUlt. Or BetaBot est doté de fonctions spéciales pour passer inaperçu, en désactivant l'antivirus et le pare-feu. Puis BetaBot analyse l'appareil de la victime et collecte diverses informations, comme les données d'accès et les informations d'ouverture de session d'e-banking. Pendant ce temps, le deuxième *maliciel* (p. ex. GandCrab) agit de manière redondante, afin que le système soit infecté même s'il se bloque.[46]

Meta10, prestataire de services d'informatique en nuage basé à Zoug, a subi le 22 février 2019 une attaque due au rançongiciel GandCrab v5.2.[47] Outre plusieurs serveurs de bases de données et d'applications, des serveurs de sauvegarde ont également été infectés. Le nettoyage du système et la restauration des documents ont entraîné pour 10 % de sa clientèle une baisse sensible des performances. L'entreprise a aussitôt opté pour une communication proactive, en informant sa clientèle de l'incident survenu. Les clients pouvaient se renseigner en tout temps sur l'évolution de la situation, en consultant la page portant sur l'«état du service». L'administration municipale bernoise a également été victime de GandCrab en 2019, mais grâce

41 https://www.darkreading.com/perimeter/lockergoga-megacortex-ransomware-share-unlikely-traits/d/d-id/1334696
42 https://news.sophos.com/en-us/2019/05/10/megacortex-deconstructed-mysteries-mount-as-analysis-continues/
43 https://www.darkreading.com/perimeter/lockergoga-megacortex-ransomware-share-unlikely-traits/d/d-id/1334696
44 https://www.europol.europa.eu/newsroom/news/just-released-fourth-decryption-tool-neutralises-latest-version-of-gandcrab-ransomware
45 MELANI, rapport semestriel 2018/2, chap. 4.5.4.
46 https://www.scmagazineuk.com/gandcrab-returns-trojans-redundency/article/1523389
47 https://www.computerworld.ch/security/hacking/cyberangriff-legt-zuger-cloud-provider-meta10-lahm-1684975.html

à sa gestion exemplaire des sauvegardes, le temps de récupération après l'incident a été très bref.[48]

À la fin de mai 2019, les exploitants de GandCrab ont annoncé que leur rançongiciel avait généré 2 milliards de dollars de rançon et qu'ils voulaient se retirer des affaires. Ils invitaient donc leurs partenaires à ne plus diffuser GandCrab dans un délai de 20 jours, et encourageaient leurs victimes à payer au plus vite leur rançon, pour éviter de perdre à tout jamais leurs données.[49]

Depuis la mi-juin 2019, un outil publié à l'adresse nomoreransom.org déchiffre les versions actuellement en circulation (1, 4 et 5 jusqu'à 5.2) de GandCrab. Ce programme, conçu en collaboration avec les ministères publics de différents pays et le soutien de la société Bitdefender, permet aux victimes de restaurer leurs fichiers chiffrés[50]. Une semaine avant sa publication, un père syrien avait signalé dans un tweet que faute d'argent pour payer la rançon exigée, il ne pouvait pas récupérer les photos de son fils tué lors d'une attaque. Pris de pitié, les administrateurs de GandCrab avaient décidé de fournir une clé de déchiffrement pour les victimes syriennes du rançongiciel.[51]

Il se pourrait qu'en annonçant leur départ à la retraite, les pirates aient voulu détourner l'attention d'eux afin de se réorganiser à l'abri des regards. Selon certains experts en cybersécurité, les exploitants de GandCrab sont déjà de retour aux affaires et utilisent désormais les cryptogiciels REvil et Sodinokibi.[52] Le *maliciel* Sodinokibi a déjà fait ses premières victimes en Suisse.

3.5 Perspectives

D'autres développements techniques et méthodologiques sont à prévoir pour les rançongiciels durant les années à venir. Il faut ainsi s'attendre à des attaques toujours mieux ciblées et à des vecteurs d'attaque encore plus perfectionnés du point de vue technique. Il sera d'autant plus important de remédier aux vulnérabilités et d'assurer la protection de base du réseau. Les cybercriminels sont opportunistes par excellence: si l'effort est trop grand et le succès se fait attendre, ils cherchent une autre cible.

Comme on le voit depuis plusieurs années, la croissance exponentielle des appareils reliés à Internet (Internet des objets) offre aux escrocs un terrain d'action toujours plus grand.[53] Cette évolution fait que la plupart des appareils électroniques que nous utilisons au quotidien sont

---

48 Voir au chapitre 2 ci-dessus l'éditorial du responsable de la cybersécurité de la Ville de Berne.

49 https://securityaffairs.co/wordpress/86438/malware/gandcrab-shutdown-operations.html

50 https://www.europol.europa.eu/newsroom/news/just-released-fourth-decryption-tool-neutralises-latest-version-of-gandcrab-ransomware

51 https://krebsonsecurity.com/2019/07/is-revil-the-new-gandcrab-ransomware/

52 https://krebsonsecurity.com/2019/07/is-revil-the-new-gandcrab-ransomware/ et https://www.tesorion.nl/aconnection-between-the-sodinokibi-and-gandcrab-ransomware-families/

53 MELANI, rapport semestriel 2014/2, chap. 5.3.

reliés à notre réseau domestique, voire directement à Internet, et donc potentiellement vulnérables. Or il existe toutes sortes de scénarios où des criminels rendent un appareil temporairement inutilisable, afin d'extorquer de l'argent à son propriétaire.

De leur côté, les autorités de poursuite pénale se modernisent et collaborent à divers niveaux avec les services de sécurité et avec des acteurs privés, afin de couper l'herbe sous les pieds des escrocs. Elles se coordonnent à l'échelon tant national qu'international, et comptent déjà de premiers succès à leur actif.[54]

3.6 Tribune: tous ensemble contre les cybercriminels

par Daniel Nussbaumer, chef de la section Cybercriminalité au sein de la police cantonale zurichoise et responsable du réseau NEDIK

A des criminels agiles dans le monde digitale, doivent répondre des autorités de poursuite pénale tout autant agiles. Dans la lutte face aux cybercriminels, il est crucial que la Confédération et les cantons aient des échanges permanents et soient en mesure de réagir rapidement. Les corps de police suisses ont donc formé le réseau de contacts policiers NEDIK, afin de mener ensemble leur travail de répression et de prévention, en étroite collaboration avec MELANI.

Des cyberattaques ciblées et de qualité professionnelle peuvent mettre en péril l'existence d'entreprises. Il en va souvent de leur survie. Par conséquent, leurs besoins ont changé à l'égard des autorités. Lorsqu'une entreprise subit une attaque, il est important pour elle de savoir comment les pirates se sont introduits et quels systèmes ont été compromis, comment elle doit réagir aux éventuelles demandes de rançon et si elle est la seule victime.

Outre MELANI, les corps de police suisses sont d'un grand secours en pareil cas. Tous ont adhéré au réseau intercantonal de soutien aux enquêtes dans la lutte contre la criminalité informatique (NEDIK), pour pouvoir réagir rapidement et de façon concertée aux cyberattaques. Grâce aux échanges opérationnels réguliers menés dans ce réseau et au signalement immédiat des nouveaux cas ou des développements récents, nous découvrons très vite les interactions et parvenons à y apporter la réponse adéquate – nos étroits contacts avec MELANI nous facilitant la tâche lors d'incidents –, ainsi qu'à formuler les recommandations utiles. Et comme l'Office fédéral de la police (fedpol) fait partie de NEDIK tout en collaborant avec Europol, notre champ d'action en cas de nouvel événement dépasse les frontières nationales.

NEDIK apporte une valeur ajoutée, et pas seulement dans la gestion des incidents. Nous produisons avec MELANI, dans le cadre de NEDIK, des bulletins sur la situation dans le cyberespace et formulons ensemble des conseils de prévention et des stratégies visant à prévenir et combattre la cybercriminalité. Ces bons exemples sont ensuite distribués à tous les corps de police, de façon à offrir à tous les cantons un soutien optimal en matière de protection contre les cyberrisques, sur le terrain de la prévention comme de la répression.

---

54 https://www.justice.gov/opa/pr/two-iranian-men-indicted-deploying-ransomware-extort-hospitals-municipalities-and-public, https://www.maketecheasier.com/man-arrested-for-spreading-shame-driven-ransomware/

Recommandations:

MELANI recommande de prendre au plus vite les mesures suivantes pour se protéger des rançongiciels:

- **Veillez à effectuer régulièrement des sauvegardes de vos données, par exemple sur un disque dur externe. Procédez selon un plan de rotation (sauvegardes quotidiennes, hebdomadaires, mensuelles [méthode grand-père - père - fils], minimum de deux générations). Après la sauvegarde, veillez à déconnecter physiquement 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.**
- Si vous utilisez une solution de sauvegarde en nuage, assurez-vous qu'elle propose au moins deux générations, de manière analogue à une sauvegarde classique. Et pour empêcher les rançongiciels de sévir, prévoyez par exemple un deuxième facteur d'authentification pour les opérations à risque.
- Il convient de toujours garder à jour son système d'exploitation et toutes les applications (p. ex. Adobe Reader, Adobe Flash, Java, etc.) installées sur sa machine, de manière automatique lorsque c'est possible.
- Protégez avec un deuxième facteur d'authentification toutes les ressources accessibles depuis Internet (p. ex. serveur de terminal, RAS, accès VPN, etc.). Placez le serveur de terminaux derrière un portail VPN.
- Bloquez la réception des courriels contenant des fichiers dangereux sur votre passerelle de messagerie, y c. les fichiers Office contenant des macros.
- Vérifiez si le fichier journal de votre antivirus signale des irrégularités.

4 Situation nationale

4.1 Espionnage

4.1.1 Lazarus s'en prend aux banques suisses

En mars 2019, le fabricant de logiciels de sécurité McAfee a publié un suivi de son rapport de décembre 2018 sur la campagne Sharpshooter. Cette campagne menée l'année dernière avait infecté 87 entreprises du monde entier, mais surtout des sociétés basées aux États-Unis. Les entreprises visées étaient actives dans la défense, l'énergie, le secteur nucléaire ainsi que la finance.[55] Dans ce second rapport, McAfee a confirmé son soupçon initial: les attaques sont bel et bien dues au groupe Lazarus.

[55] MELANI, rapport semestriel 2018/2, chap. 4.1.2.

Lazarus est connu pour avoir attaqué les systèmes de différentes banques,[56] et beaucoup d'experts l'associent avec le régime nord-coréen.

Dans son premier rapport déjà, McAfee avait fait état de tentatives de cyberattaques contre des établissements financiers suisses. MELANI est en contact avec différentes banques, comme le souligne son dernier rapport semestriel.[57] Or à ce jour, aucune trace d'infection n'a été trouvée dans les entreprises potentiellement touchées en Suisse.

4.1.2 APT40

La stratégie actuelle poursuivie par la Chine pour améliorer les relations commerciales entre l'Asie et l'Europe consiste à développer les infrastructures de logistique et de transport. L'entreprise de sécurité FireEye a découvert une opération d'espionnage[58] menée depuis au moins 2013 et dirigée contre les pays stratégiques pour la nouvelle route de la soie (Belt and Road Initiative, BRI), dont la Suisse fait partie.[59] Elle émane du groupe APT40 (aussi appelé Leviathan ou TEMP.Periscope), qui bénéficierait de l'appui du gouvernement chinois selon FireEye. L'opération visait à obtenir des informations utiles à la modernisation du secteur maritime en général, et au renforcement des compétences de construction navale en particulier.

Le groupe envoie des courriels de phishing avec des annexes renfermant des maliciels, ou procède à des infections par *drive-by download* pour attaquer les secteurs de la défense, des transports et des technologies navales. En 2017 déjà, il avait usurpé l'identité d'un fabricant de sous-marins autonomes pour infiltrer des instituts universitaires menant des recherches dans le domaine de la construction navale. Ce secteur revêt une importance fondamentale pour le gouvernement chinois, d'un point de vue tant commercial que militaire.[60] Aussi réapparaît-il dans d'autres campagnes d'espionnage également attribuées à Pékin (voir aussi chapitre 4.1.4).

Outre ses campagnes axées sur la recherche et l'industrie, le groupe APT40 a mené des campagnes d'espionnage contre des organisations d'Asie du Sud-Est, ou alors est impliqué dans les conflits territoriaux en mer de Chine. En 2018, les systèmes de diverses autorités cambodgiennes impliquées dans l'organisation d'élections locales ont été piratés.[61] Or le Cambodge fait partie des pays stratégiquement importants pour la nouvelle route de la soie.

À ce jour, aucune trace d'infection n'a été découverte dans les entreprises potentiellement touchées en Suisse.

---

56 https://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks

57 MELANI, rapport semestriel 2018/2, chap. 4.1.2; https://www.tagesanzeiger.ch/sonntagszeitung/nordkorea-greift-schweizer-banken-an/story/15090344

58 https://www.fireeye.com/blog/threat-research/2019/03/apt40-examining-a-china-nexus-espionage-actor.html

59 Au sujet de la nouvelle route de la soie: http://english.www.gov.cn/beltAndRoad/ et http://english.www.gov.cn/archive/publications/2015/03/30/content_281475080249035.htm

60 Cf. la stratégie «Made in China 2025» : http://english.www.gov.cn/2016special/madeinchina2025/; http://en.people.cn/n/2015/0522/c98649-8895998.html

61 https://www.fireeye.com/blog/threat-research/2018/07/chinese-espionage-group-targets-cambodia-ahead-of-elections.html

4.1.3 VPN Filter

En mai 2018 Talos, la branche de Cisco spécialisée dans la cybersécurité, a révélé l'existence de VPN Filter. Ce réseau de zombies comprendrait plus d'un demi-million de routeurs et appareils *NAS* situés dans 54 pays, à commencer par l'Ukraine.[62]

Le *maliciel* VPN Filter possède une structure modulaire avec différentes fonctionnalités. Il peut par exemple rendre un appareil inutilisable, tout comme il est en mesure de se répandre dans le réseau et d'infecter d'autres systèmes (mouvement latéral). Le maliciel est à même de dérober des informations (données d'accès notamment) et de dévier le trafic Internet vers un autre destinataire. En outre, un module recherche et surveille le cas échéant le trafic en ligne de données Modbus.[63] Modbus est un protocole de communication souvent utilisé par les systèmes de contrôle industriels.

Le réseau de zombies VPN Filter aurait également pu servir à des actes de sabotage. Le FBI a cependant pris le contrôle d'une partie de son infrastructure *Command & Control* pratiquement au moment où son existence était révélée. En conséquence, il a été possible non seulement d'identifier les appareils infectés, mais aussi d'empêcher les exploitants du réseau de leur donner des instructions.

Bien que les mises à jour publiées permettent aux logiciels de sécurité d'identifier et de bloquer les *maliciels*, MELANI a connaissance de plusieurs centaines d'infections encore actives en Suisse. Afin de supprimer le maliciel et de combler cette faille de sécurité, il faut en revenir aux paramètres d'usine des appareils, puis les actualiser.

Recommandations:

Les cyberattaques contre l'infrastructure du réseau ont redoublé. Les routeurs et les commutateurs constituent des cibles idéales, étant bien souvent directement reliés à Internet sans forcément bénéficier d'un niveau de protection suffisant. Ils représentent ainsi une porte d'entrée bien commode dans les réseaux domestiques ou d'entreprise.

Tout appareil directement relié à Internet a besoin d'une protection spécifique contre les accès non autorisés. À cet effet, il ne suffit pas d'utiliser un mot de passe sûr, il faut encore installer au plus vite les mises à jour.

4.1.4 APT10

La liste des victimes d'APT10 s'est allongée au premier semestre 2019. Ce groupe de pirates sévissant depuis 2006 s'est fait connaître par l'opération Cloud Hopper, lancée en 2015 au niveau mondial contre les fournisseurs de services d'infogérance (*managed service provider, MSP*).[64] Le Département de la justice des États-Unis (Department of Justice, DoJ) et les quatre

62 MELANI, rapport semestriel 2018/1, chap. 5.1.2.

63 https://blog.talosintelligence.com/2019/05/one-year-later-vpnfilter-catastrophe.html

64 MELANI, rapport semestriel 2018/2, chap. 5.1.1 et 2017/1, chap. 5.1.1.

autre pays du groupe des Five Eyes ont officiellement blâmé le gouvernement chinois pour sa participation à cette campagne d'espionnage.[65]

Le 20 décembre 2018, le DoJ a accusé d'escroquerie et de vol d'identité deux ressortissants chinois soupçonnés d'avoir participé à Cloud Hopper. Les noms de deux grands fournisseurs de services informatiques ont été avancés: Hewlett Packard Enterprise (HPE) et IBM ont fait les frais de cette campagne d'espionnage. Tout indique, du moins dans le cas de HPE, que le pirate sévissait dans son réseau depuis des années.

En juin 2019, l'agence de presse Reuters a publié les noms de six autres victimes d'APT10.[66] Il s'agit de Fujitsu, Tata Consultancy Services, Dimension Data, NTT, Computer Sciences Corporation et DXC Technology. Cette nouvelle découverte a fait exploser le nombre des victimes potentielles. Car les MSP ne sont pas un but en soi: ils servent de moyen d'accès aux grandes entreprises dont ils exploitent ou soutiennent l'infrastructure. L'infection subie par HPE a par exemple été découverte par l'équipe d'Ericsson responsable de la sécurité informatique. Le géant des télécoms suédois était à la recherche de la porte d'entrée de diverses infections par des *maliciels* survenues entre 2014 et 2017. Il est impossible de dire combien d'entreprises ont été infiltrées par ce vecteur. Les fournisseurs de services d'infogérance constituent une cible très attrayante, dans la mesure où ils disposent d'un droit d'accès direct aux systèmes de leurs clients, dont ils traitent parfois aussi les données.

Les attaques relèvent du vol de la protection intellectuelle. Les victimes sont actives par exemple dans la construction navale militaire ou la conception de sous-marins nucléaires. Or il est crucial pour la Chine de moderniser sa technologie marine.[67] Les attaques visent également à surveiller des rivaux. Ericsson fait par exemple concurrence aux fabricants chinois de téléphones mobiles. Ce n'est pas tout: le vol d'informations confidentielles sur le chiffre d'affaires permet de savoir si une société serait intéressante à acquérir.

La campagne d'espionnage ne poursuivait apparemment pas des objectifs uniquement commerciaux. On le voit par exemple à la présence, parmi les victimes confirmées, de la société Sabre Corp. Elle gère les systèmes de réservation de milliers d'hôtels à travers le monde, ainsi que les billets d'avions de centaines de compagnies aériennes. Bien qu'il n'y ait pas eu de vol d'informations de voyage, les pirates auraient pu se procurer par ce canal des informations sur les déplacements de très nombreuses personnes.

Le document publié par le DoJ mentionne la Suisse parmi les États où des organisations ont été piratées. Même en l'absence de toute preuve concrète d'infection subie par une organisation ayant son siège en Suisse, les sociétés en quête d'un repreneur constituent des cibles potentielles d'espionnage informatique.

---

65 https://www.securityweek.com/five-eyes-nations-blame-china-apt10-attacks;
États-Unis: https://www.justice.gov/opa/press-release/file/1121706/download;
Grande-Bretagne: https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign;
Canada: https://cse-cst.gc.ca/fr/media/media-2018-12-20;
Australie: https://foreignminister.gov.au/releases/Pages/2018/mp_mr_181221.aspx;
Nouvelle-Zélande: https://www.ncsc.govt.nz/newsroom/cyber-campaign-attributed-to-china/

66 https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/

67 Cf. la stratégie «Made in China 2025» : http://english.www.gov.cn/2016special/madeinchina2025/;
http://en.people.cn/n/2015/0522/c98649-8895998.html

4.2 Systèmes de contrôle industriels

Bien souvent, le confort moderne dont nous jouissons nous vient de systèmes de contrôle industriels. Si le courant produit par les turbines des barrages alimente en tout temps notre prise électrique privée, nous le devons notamment aux systèmes de contrôle des distributeurs d'électricité locaux. Une étude présentée au chapitre 4.2.1 montre ce que les petites et moyennes entreprises d'approvisionnement en électricité (EAE) font sur le plan de la sûreté de l'information. Par ailleurs, lors de tous nos déplacements, des systèmes de contrôle nous aident à arriver rapidement et confortablement à bon port. Le chapitre 4.2.2 expose les défis à relever dans le cadre de l'atterrissage aux instruments.

4.2.1 Devoirs des petites et moyennes EAE

Dans le domaine de l'approvisionnement électrique, les incidents affectant les centrales électriques, les barrages ou les lignes à haute tension font parfois les gros titres. Pour le client final toutefois, la fiabilité de l'approvisionnement dépend en général davantage du distributeur local. Aussi l'association faîtière Electrosuisse a-t-elle consacré une étude[68] à la cybersécurité dans les petites et moyennes entreprises du secteur (EAE).

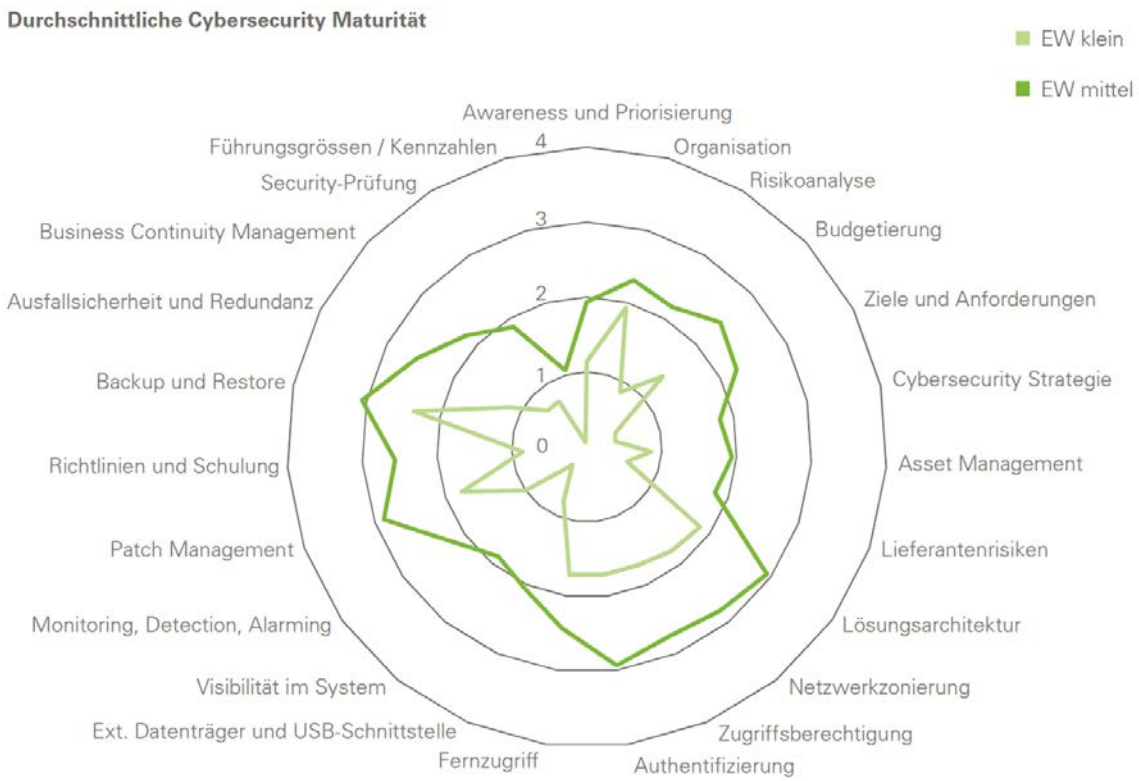

Figure 1: Aperçu des résultats de l'étude sur les divers aspects de la cybersécurité.

Il ressort de cette analyse que toutes les entreprises se préoccupent de cybersécurité, mais qu'il reste beaucoup à faire dans la mise en œuvre systématique des mesures destinées à

68 https://www.electrosuisse.ch/wp-content/uploads/2019/03/Electrosuisse_Cybersecurity-Erhebung-EVU_.pdf

garantir la sûreté de l'information, dans les petites sociétés notamment. L'étude a ainsi relevé une focalisation sur les mesures de prévention, au détriment des autres éléments du cadre de référence NIST de cybersécurité.[69]

Les inventaires dressés (*asset management*) sont souvent incomplets, et la visibilité au sein du système laisse à désirer. En plus d'être peu réactives et de ne pas réaliser d'exercices d'urgence, les EAE ont du mal à détecter les incidents et à les gérer. Sur les questions générales d'organisation, il est apparu qu'elles ne tenaient pas suffisamment compte des risques, en fixant leurs priorités et en établissant leurs budgets. Elles pèchent par négligence des risques liés aux fournisseurs, et par oubli du facteur humain en tant que risque. De telles faiblesses souvent dues au manque de compétences professionnelles et de ressources, notamment chez les participants de petite taille à l'étude, font que la cybersécurité n'est pas envisagée comme processus à part entière.

Pour combler ces lacunes, il serait indiqué que les petites et moyennes EAE coopèrent dans les domaines de leur activité qui sont identiques pour tous. Un projet mérite d'être salué à cet égard, soit l'initiative d'une organisation de cybersécurité interentreprises pour les services industriels.[70] Grâce à cette plateforme, tous les partenaires pourront tirer parti de leurs expériences respectives et améliorer progressivement ensemble le niveau de sûreté de l'information.

4.2.2 Mauvais guidage vertical – vulnérabilité du système d'atterrissage aux instruments

La plupart des aéroports civils du monde ont installé un système d'atterrissage aux instruments (*instrument landing system*, ILS), qui aide les pilotes pendant la phase d'approche. De tels systèmes ont été conçus à une époque où la radionavigation n'était accessible qu'à un petit cercle d'utilisateurs. Les mesures cryptographiques de sécurisation et d'authentification n'ont donc pas été jugées prioritaires. Or à la dernière conférence Usenix[71], des chercheurs de l'université Northeastern de Boston ont présenté une méthode peu coûteuse permettant de falsifier les signaux pour la radionavigation censés garantir une approche selon un angle de descente correct.[72] L'appareil utilisé dans le document de recherche[73] utilise des composants disponibles dans le commerce pour simuler les signaux ILS. Pour garantir une attaque fructueuse, il doit être placé soit dans l'avion, soit dans un rayon de cinq kilomètres de la piste d'atterrissage. Les signaux émis par l'agresseur doivent encore avoir une intensité supérieure à la communication légitime de l'aéroport, afin que l'avion règle son récepteur sur eux.

Des problèmes similaires se posent avec d'autres aides de radionavigation, comme les systèmes GPS (voir chapitre 5.2.2). Sachant que les pilotes sont formés pour gérer les pannes ou dysfonctionnements du système ILS, ils réagiront bien dans une hypothèse favorable. Mais si à l'avenir cette approche devait être encore affinée et utilisée dans la pratique, ce genre d'attaque pourrait perturber les vols et l'activité des aéroports. On pourrait alors imaginer des

---

69 https://www.nist.gov/cyberframework

70 https://swisspower.ch/fr/medias/communiques-de-presse/swisspower-lanciert-kooperation-f%C3%BCr-cybersecurity-in-stadt-werken

71 https://www.usenix.org/

72 https://arstechnica.com/information-technology/2019/05/the-radio-navigation-planes-use-to-land-safely-is-insecure-and-can-be-hacked/

73 https://aanjhan.com/assets/ils_usenix2019.pdf

attaques ayant des conséquences similaires à celles des évènements de décembre 2018, lorsque des drones utilisés sans autorisation avaient paralysé l'aéroport londonien de Gatwick.[74]

Recommandation:

Si vous découvrez sur Internet des systèmes de contrôle ouverts au premier venu ou mal protégés, 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

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 Attaques par déni de service distribué – DDoS

Durant la période sous revue, plusieurs nouvelles attaques *DDoS* ont été signalées à MELANI. Cela montre que divers acteurs continuent d'employer cette méthode pour rendre inaccessibles les systèmes de leurs victimes. Il peut s'agir de purs maîtres-chanteurs, ou d'activistes cherchant à nuire à des entreprises ou à des organisations. Mais on trouve aussi des cas où les motifs restent mystérieux. On peut supposer que les pirates testent parfois leur infrastructure sur des victimes choisies au hasard.

Recommandation:

MELANI recommande toute une série de précautions utiles et de mesures à prendre en cas d'attaque *DDoS*.

Liste de mesures à prendre contre les attaques DDoS

https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/massnahmen-gegen-ddos-attacken.html

[74] MELANI, rapport semestriel 2018/2, chapitre 5.2.3.

4.3.2 Piratage de sites Web

Des sites Web continuent d'être compromis et utilisés à des fins criminelles. Les escrocs tirent en général parti de versions désuètes des systèmes de gestion de contenu (CMS), ou alors de données d'accès FTP dérobées, pour y placer des maliciels ou une page de phishing. Le cas échéant, MELANI informe les exploitants du site afin qu'ils puissent résoudre le problème à l'aide de ses instructions techniques.[75]

Recommandation:

Mieux vaut prévenir que guérir: si vous utilisez un CMS comme Typo3, Wordpress ou encore Joomla, MELANI vous recommande de jeter un coup d'œil à sa liste de contrôle «Mesures de prévention pour les systèmes de gestion de contenu (CMS)», afin de dûment protéger votre site Web.

DOKU

Liste de contrôle avec mesures de prévention pour les systèmes de gestion de contenu (CMS)

https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/mesures-de-prevention-pour-les-systemes-de-gestion-de-contenu--c.html

4.3.3 Cybersquattage – quand une société de tir se met à vendre des chaussures ou une campagne politique à promouvoir des contrefaçons

La récupération de noms de domaine devenus caducs ne constitue pas vraiment une attaque, mais une forme de parasitisme. Les cybersquatteurs (*domain grabber*) observent les noms de domaine dont le cycle de vie a expiré, puis les enregistrent à leur nom à l'expiration du délai de carence. On y trouve souvent de fausses boutiques en ligne,[76] mais les modèles d'affaires peuvent varier. De tels domaines profitent, du moins à court terme, de la bonne réputation acquise au fil des ans par leur ancien propriétaire légitime. Et comme la plupart du temps, des pages de tiers continuent de renvoyer à ces domaines, ils figurent parfois en bonne position dans la liste des résultats affichée par les moteurs de recherche Internet.

Recommandation:

Les enregistrements de noms de domaine doivent être régulièrement renouvelés. Si vous avez un site Web, vous devriez garder à l'esprit les délais en vigueur, pour ne pas perdre soudainement votre nom de domaine. Il faudrait également planifier la désactivation d'un tel site. Ce n'est pas cher, et il peut être judicieux d'arrêter de manière contrôlée l'activité d'un domaine. Concrètement, il importe d'en poursuivre l'exploitation pendant un certain temps, afin que tous les visiteurs potentiels sachent que vous avez renoncé à cette

[75] https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/instructions-relatives-a-la-suppression-des-maliciels-sur-les-si.html

[76] En Suisse, le phénomène a commencé à se répandre en 2016. SWITCH, registraire des domaines en «.ch», traque depuis lors les abus de façon systématique. D'autres pays n'en font pas autant: https://www.nzz.ch/digital/kampf-gegen-fake-shops-im-netz-ld.1484852

présence sur le Web. Par ailleurs, une analyse des pages référentes (*referrer*) vous aidera à informer les exploitants d'autres sites comportant un hyperlien à votre domaine. Enfin, il s'agit de protéger la réputation de l'entité associée au site Web et de ne pas exposer à des risques sa clientèle et ses sympathisants, qu'il s'agisse d'une entreprise, d'une association, d'un particulier ou d'une quelconque communauté d'intérêts.

4.4 Ingénierie sociale et phishing

Une cyberattaque réussie suppose d'inventer une histoire plausible, pour amener la victime potentielle à effectuer une action irréfléchie. Plus les escrocs parviennent à recueillir d'informations, et plus leurs attaques d'*ingénierie sociale* ont de chances d'aboutir. Ils puisent aussi bien dans les sources en libre accès que dans le butin des vols de données. Les données dérobées sont passées au crible, reliées à d'autres données volées ou publiques, traitées puis revendues à d'autres pirates. Ce genre de données permet de lancer des attaques sur mesure contre des cibles précises, ou d'envoyer de manière automatisée des spams malveillants (*malspam*) personnalisés.

4.4.1 Phishing

Le nombre de tentatives de phishing signalées à MELANI a augmenté au premier semestre 2019. Quelque 2521 adresses URL différentes utilisées pour du phishing ont été annoncées et transmises aux organisations luttant contre ce fléau (exploitants de navigateurs, organisations combattant les attaques d'hameçonnage, fournisseurs d'hébergement). Les cibles n'ont fondamentalement pas changé: les escrocs ont tenté aussi bien de dérober les données de cartes de crédit, que d'obtenir les noms d'utilisateur/mots de passe de services Internet comme Paypal, Spotify ou Apple. Les comptes de messagerie, qui peuvent servir à lancer d'autres attaques, sont par ailleurs toujours plus souvent pris pour cibles. À cela s'ajoute une méthode d'attaque relativement nouvelle, le phishing en temps réel (voir chapitre 4.4.2).

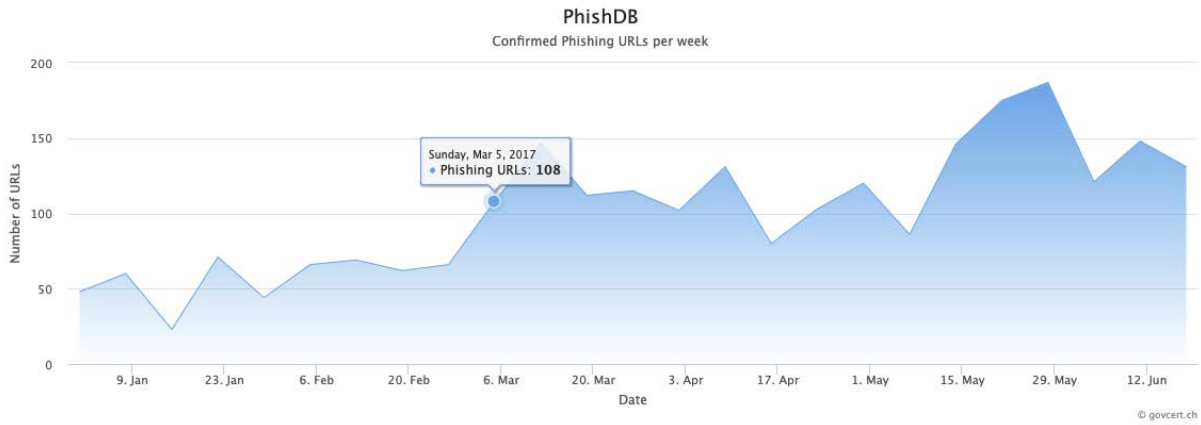

Figure 2: Sites de phishing annoncés et confirmés par semaine sur le site antiphishing.ch au premier semestre 2019

Une partie de cette recrudescence s'explique par les vagues de phishing visant à dérober des informations sur les cartes de crédit.

4.4.2 Phishing en temps réel contre PostFinance et UBS

La méthode de phishing la plus répandue consiste à collecter des données d'accès à grande échelle et à s'en servir quelques heures ou jours plus tard pour s'annoncer sur le compte de la victime. Il arrive souvent aussi que les données d'accès dérobées soient revendues. Cette approche ne fonctionnera toutefois pas si l'utilisateur se connecte avec un second facteur d'authentification (p. ex. mot de passe unique, *one time password*, OTP). En réponse à l'usage toujours plus fréquent d'OTP, le phishing en temps réel a vu le jour. Autrement dit, l'agresseur passe à l'action au moment précis où la victime est réacheminée sur son serveur Web, après avoir cliqué sur l'hyperlien du message de phishing lui ayant été adressé.

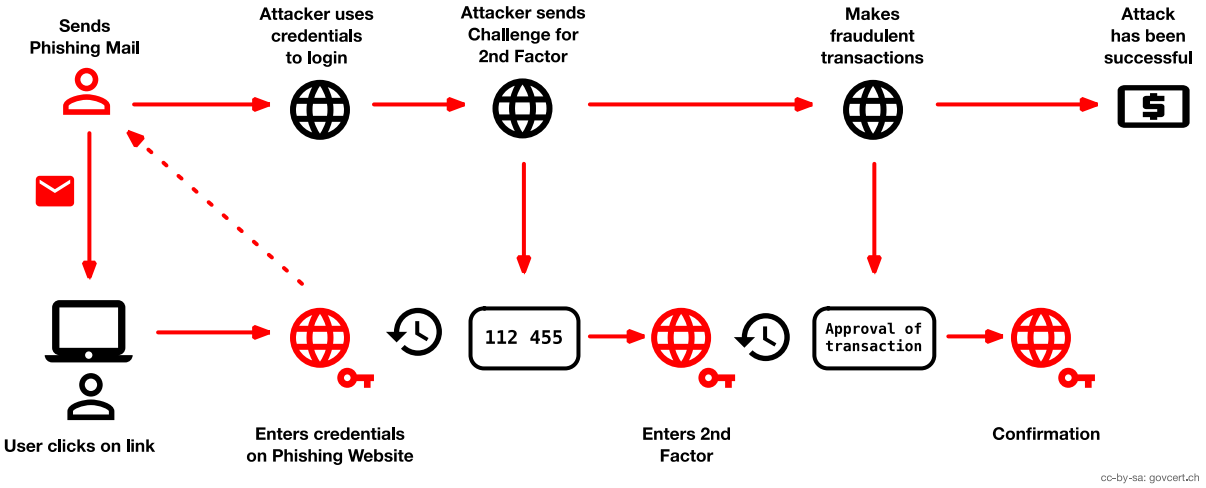

Figure 3: Schéma du déroulement d'une attaque de phishing en temps réel

Le pirate présente une page d'ouverture de session parfaitement imitée, sur laquelle la victime va chercher à s'authentifier. L'agresseur relève ses données et s'en sert pour s'annoncer lui-même sur la vraie plateforme d'e-banking. Quand il est invité à s'identifier avec un deuxième facteur, il en fait à son tour la demande à l'utilisateur sur le serveur Web falsifié. Dès que l'utilisateur a inscrit le deuxième facteur, le pirate peut accéder au portail d'e-banking, tout en transmettant un message d'erreur à l'utilisateur afin de le faire patienter.

Deux campagnes de ce genre dirigées contre des établissements financiers suisses ont été observées durant la période sous revue.

4.4.3 Attrait des comptes sur les réseaux sociaux

Le phishing ne s'intéresse pas qu'aux comptes de messagerie et aux informations des cartes de crédit. Tous les comptes en ligne sont en danger. Alors qu'un compte Twitter usurpé permet de mener une campagne de désinformation pour donner une piètre image de son utilisateur légitime, des profils Instagram[77] ou des comptes Youtube piratés risquent encore d'occasionner un préjudice financier à leur propriétaire. Car les abonnés ou suiveurs acquis constituent le capital des influenceurs. À supposer que leur présence en ligne échappe à leur contrôle, il leur faudra reconstruire leur communauté à partir de zéro. Dans l'intervalle, ils n'auront pu publier aucun contenu en ligne, et auront ainsi vu de précieuses recettes leur échapper. Les

[77] https://blog.trendmicro.com/trendlabs-security-intelligence/how-a-hacking-group-is-stealing-popular-instagram-profiles/

personnalités en vue ne sont pas seules à souffrir d'une telle situation. La vie d'un nombre croissant de personnes se déroule, du moins en partie, sur les plateformes des médias sociaux. Or quiconque n'a plus accès par exemple à son compte Facebook aura peut-être à court terme de la peine à cultiver ses contacts.

Recommandation:

Il est important de protéger autant que possible ses comptes en ligne, en privilégiant p. ex. l'*authentification à deux facteurs*. Familiarisez-vous par avance avec les mesures de sécurité des prestataires, et avec les éventuels processus qui permettent de reprendre le contrôle d'un compte piraté. Il convient également d'utiliser un mot de passe complexe, et différent pour tous vos comptes en ligne.

4.4.4 Les mini-écrans accroissent le risque de tromperie

Les smartphones sont des ordinateurs miniatures. Ils sont devenus l'outil de communication préféré de beaucoup de gens. Il est ainsi courant de gérer ses rendez-vous au moyen de l'application calendrier de son smartphone. Il incombe dès lors aux programmeurs d'applications d'afficher autant que possible de manière conviviale toutes les informations pertinentes sur un écran de dimensions réduites. Avec pour effet que bien souvent on ne découvre qu'au prix de manipulations fastidieuses, des informations de base comme l'adresse complète d'un hyperlien indiqué ou l'adresse électronique sous-jacente au nom s'affichant à l'écran (que l'expéditeur peut d'ailleurs librement choisir). Cette réduction à l'essentiel est sans doute judicieuse et utile en cas d'usage normal du smartphone. Mais elle offre aux criminels de nombreuses possibilités de tromper les destinataires de leurs envois. Outre l'expédition de courriels, SMS et autres messages courts à caractère frauduleux, il est possible selon les réglages du smartphone et des applications d'y introduire automatiquement des demandes de rendez-vous,[78] ou de faire apparaître à l'écran des notifications et autres communications.

Recommandation:

Ne vous laissez pas duper par les messages inattendus s'affichant sur votre smartphone, même s'ils ont été envoyés par un canal usuel et dans un format familier. Demandez-vous toujours si un message ne pourrait pas venir de quelqu'un cherchant à vous faire cliquer par inadvertance sur un lien malveillant. Contrôlez les réglages de votre smartphone et de ses applications, afin p. ex. que seules les demandes de rendez-vous acceptées figurent dans votre calendrier et que votre sphère privée soit dûment protégée.

4.4.5 Persistance de l'arnaque au président

Un rapport MELANI avait décrit pour la première fois en 2013 l'arnaque au président (*CEO fraud*).[79] Si le phénomène n'est pas nouveau, il n'en continue pas moins de faire recette. Différents types d'organisations sont systématiquement prises pour cibles. À côté des entreprises privées, il s'agit surtout aujourd'hui d'associations sportives ou autres, ou encore de com-

[78] Cf. MELANI, rapport semestriel 2018/1, chap. 4.4.4.

[79] MELANI, rapport semestriel 2013/1, chap. 3.4.

munes. En effet, leurs sites Internet sont fréquemment une mine d'informations pour les escrocs. Un organigramme y indique les noms et adresses électroniques des personnes-clés (président de la société, maire, caissier, responsable des finances, etc.). Le mode opératoire classique de l'*arnaque au président* consiste à envoyer un courriel au responsable des finances, en usurpant l'identité du président, afin de le prier d'effectuer sous divers prétextes un important versement.

De: [adresse falsifiée du président de l'association]
Date: Mardi 19 mars 2019 à 14:00
À: [caissier de l'association]
Objet: DEMANDE

Salut Corinna,
J'aimerais que tu fasses un versement. Dis-moi si tu peux t'en charger tout de suite pour que je puisse t'envoyer les coordonnées bancaires.
J'attends ta réponse.

Cordialement,
[nom du président]

Envoyé de mon iPhone

Courriel n° 1: L'escroc se fait passer pour le président et prie la caissière d'effectuer un paiement urgent.

Salut Corinna,

[coordonnées bancaires d'un compte à l'étranger]

Informe-moi quand le versement sera fait.

Cordialement,
[nom du président]

Envoyé de mon iPhone

Courriel n° 2: En cas de réponse, le «président» fournit les coordonnées d'un compte à l'étranger.

Comme toutes les informations sont aisées à trouver sur Internet, les escrocs ont tendance à automatiser leurs envois de courriels, sans trop s'embarrasser de contrôles de qualité, ce qui conduit parfois à des résultats étonnants. Dans certaines petites communes ou associations, le président, respectivement maire, peut en effet également être responsable des finances et figurer avec le même e-mail sous les deux fonctions. Ainsi, dans un cas reporté à MELANI, la caissière d'une commune a reçu un e-mail lui étant soi-disant adressé par la maire. Seul problème, les fonctions étaient dans ce cas occupées par la même personne: la caissière a donc reçu un e-mail envoyé en son propre en nom.

Recommandation:

MELANI recommande de contrôler régulièrement les informations publiées en ligne à propos de personnes, d'associations, d'entreprises, etc., en se demandant si c'était bien nécessaire de les divulguer. Les autres mesures de prévention consistent à sensibiliser le personnel et à formuler des consignes précises, en matière de paiements notamment.

INFO

Informations et recommandations sur l'arnaque au président (*CEO fraud*):

https://www.melani.admin.ch/melani/fr/home/themen/CEO-Fraud.html

4.4.6 Malspam: intimidation ou appel à la curiosité pour diffuser des maliciels

Les cybercriminels inventent toujours de nouveaux scénarios pour amener les imprudents à cliquer sur un lien ou à ouvrir un fichier annexé à leurs messages. Toutes les fantaisies sont permises. Au premier semestre 2019, les escrocs ont tenté d'amener les utilisateurs à installer un maliciel, avec des histoires parfois abracadabrantes:

Abonnement payant: un courriel lapidaire remerciait le destinataire d'avoir conclu un abonnement payant à tel ou tel journal ou magazine, en le priant de consulter dans le document annexé les modalités de paiement et les conditions d'utilisation. La ligne Objet du courriel indiquait même les prénom et nom du destinataire, afin de mieux le duper.

Plaintes contre d'anciens clients: une petite entreprise s'était fait pirater sa base de données de clients; tous ont reçu par la suite un courriel personnalisé, les informant qu'ils avaient violé ses conditions contractuelles et qu'une action en dommages-intérêts avait été intentée contre eux. Pour plus de détails, il leur fallait consulter le document annexé. L'adresse de l'expéditeur n'avait pas été usurpée et n'apparaissait que comme nom d'affichage, afin de leurrer les destinataires peu attentifs.

Réclamations contre des établissements de restauration: un courriel expliquait qu'un client, ayant subi une intoxication alimentaire lors d'un repas servi par le destinataire, avait porté plainte contre lui. Ce message ne servait qu'à une première prise de contact. Seuls les gens qui répondaient recevaient un courriel avec un lien aboutissant au *maliciel*. En l'occurrence, les criminels réservent leurs programmes malveillants aux personnes ayant réagi à leur prise de contact initiale. Ils font d'une pierre deux coups: d'une part, le *maliciel* n'est pas diffusé à grande échelle, et donc les fabricants d'antivirus découvriront moins vite son existence. D'autre part, la probabilité que les destinataires cliquent sur le lien infecté augmente, dans la mesure où ils ont déjà été en contact avec l'expéditeur et savent qu'il doit leur récrire[80].

[80] La presse spécialisée a mis en garde les restaurants contre cette fraude: https://www.hotellerie-gastronomie.ch/de/artikel/achtung-ein-gastro-schreck-geistert-herum/ du 19.03.2019; https://www.baizer.ch/aktuell?artID=6788&lvl=2 du 09.04.2019; https://www.onlinewarnungen.de/warnungsticker/e-mail-lebensmittelvergiftung-trojaner-im-anhang-enthalten/ du 21.05.2019.

Aide à une jeune fille enfermée: une enfant enchaînée dans une cave par un tortionnaire demandait au destinataire de prévenir ses parents afin qu'ils la libèrent. Ses coordonnées figuraient dans le document annexé.

Aide au suicide commandée et payée: dans cette escroquerie de mauvais goût, le destinataire était informé que des démarches de mort volontaire avaient été effectuées et payées d'avance en son nom. Des infirmiers passeraient le prendre à domicile trois jours plus tard. Des compléments d'information figuraient dans le courriel annexé. Là encore, les destinataires étaient appelés par leur nom, et leur adresse postale correcte était indiquée.

Conclusion / Recommandation:

Le stratagème est toujours le même: des explications plus ou moins crédibles visent à amener le destinataire à cliquer machinalement sur un lien ou à ouvrir un fichier pour obtenir «davantage d'informations». Presque tous les courriels étaient personnalisés, autrement dit le destinataire était appelé par son nom, et son adresse ou son numéro de téléphone étaient parfois aussi indiqués. Ces données provenaient typiquement de boutiques en ligne victimes d'un vol de données, ou alors de répertoires d'adresses piratés.

Ce n'est pas parce qu'un message vous est adressé personnellement, en mentionnant votre lieu de domicile ou votre numéro de téléphone, qu'il émane d'un expéditeur légitime. Méfiez-vous des courriels qui exigent une action de votre part et vous menacent sinon de représailles (perte financière, plainte pénale ou procédure judiciaire, blocage d'un compte ou d'une carte, occasion manquée, malheur), a fortiori si on vous presse d'agir. Ne cliquez jamais sur les annexes de courriels suspects, et ne suivez aucun lien – même par curiosité. Vous risquez sinon d'infecter votre appareil avec un maliciel, ou d'aboutir à des sites louches. En cas de doute sur l'authenticité du message, adressez-vous à l'entreprise concernée, par un des canaux indiqués sur son site ou par l'intermédiaire des contacts connus de vous, pour savoir de quoi il s'agit et si le message vient véritablement d'elle.

4.4.7 Nouvelles tentatives de chantage au nom du DFJP

Les cyber-racketteurs ont commencé à sévir à grande échelle en 2011 et en 2012. La plupart du temps, ils verrouillaient le navigateur ou l'ordinateur complet et prétendaient, au nom d'autorités de poursuite pénale ou de sociétés de gestion des droits d'auteur, que l'utilisateur avait diffusé du matériel pornographique illégal ou partagé sans autorisation de la musique et des films.[81] Ce type de fraude a depuis été généralement remplacé par les chevaux de Troie chiffrant les données,[82] mais n'a pas complètement disparu, comme le montre l'exemple suivant. Les criminels ont beau s'être basés sur le graphisme actuel de l'administration fédérale, leur langage rappelle les anciens courriels de phishing et autres tentatives d'escroquerie qui, par leurs fautes de grammaire et leurs incohérences entre versions linguistiques, révélaient que le site indiqué ne pouvait émaner d'une autorité suisse. Aucun *maliciel* n'infecte d'ailleurs l'ordinateur. Les escrocs se contentent d'intimider leurs victimes, afin de les amener à payer. Or la police ne verrouillerait jamais un ordinateur dans le but de recouvrer des amendes ou peines pécuniaires.

81 Voir rapport semestriel 2011/2, chap. 3.5 et 2015/2, chap. 4.5.2.

82 Voir ci-dessus le thème prioritaire sur les rançongiciels, au chap. 3.

Figure 4: Message au logo de la Confédération signalant le blocage de l'ordinateur

4.4.8 Faux messages de sextorsion: beaucoup de gens tombent encore dans le piège

Dans de faux messages de sextorsion expédiés au premier semestre 2019, des escrocs prétendent avoir pris le contrôle de l'ordinateur de la victime et l'avoir filmée en train de se masturber. MELANI a publié une lettre d'information en février 2019,[83] puis lancé avec les polices cantonales et d'autres partenaires un site Web[84] pour sensibiliser la population à cette imposture. Beaucoup de gens continuent hélas à payer la rançon, faute de savoir que les allégations de tels courriels sont infondées. Le site stop-sextortion.ch indique toutefois comment procéder, au cas où les maîtres-chanteurs posséderaient réellement du matériel compromettant (p. ex. en cas de conversation préalable en mode vidéo, ou si la victime a spontanément envoyé des photos d'elle nue).

Diverses vagues de faux messages de sextorsion ont été observées en anglais, en allemand, en français et même parfois en italien. Si la plupart des textes étaient rédigés dans un langage plutôt correct, quelques-uns semblaient être des traductions approximatives, aux arguments peu convaincants.

Au total, 4565 adresses bitcoin différentes ont été signalées à MELANI en six mois. Les versements constatés se limitaient à quelques adresses, et aucune transaction n'avait été effectuée sur la plupart d'entre elles. Au total, 283 bitcoins ont ainsi été encaissés (soit l'équivalent de 2,8 millions de francs à fin juin 2019). Les versements ne provenaient pas tous de Suisse, encore qu'il soit très difficile de démontrer qui a effectué des paiements à partir d'où. Mais ces

83 https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/fake-sextortion.html

84 https://www.stop-sextortion.ch/fr/

chiffres montrent que de l'argent continue d'être versé, alors même que ce phénomène de la sextorsion est connu de longue date.

Dans le contexte international, l'Internet Storm Center conçu par SANS a publié ses analyses des adresses bitcoin apparaissant dans de faux messages de sextorsion.[85] Sur 434 adresses analysées, seules 56 avaient été employées pour des paiements. L'argent y dormait quelque temps. Les escrocs le plaçaient ensuite sur des comptes consolidés, avant de revendre leurs bitcoins. SANS a identifié deux adresses bitcoin consolidées, l'une avec 6190 bitcoins (soit 62 millions de francs à fin juin), l'autre avec 5312 bitcoins (53 millions de francs à fin juin). L'auteur de l'article de SANS soupçonne qu'il ne s'agit toutefois que du début des sorties de liquidités (*cash out*), et que le montant effectif est un multiple de ces sommes. Pour encaisser leurs gains, les pirates fractionnent les bitcoins en plus petits montants et font appel à un mixeur de bitcoins, afin de brouiller les pistes.

Recommandation:

Si vous ne connaissez pas personnellement l'expéditeur d'un courriel de chantage et en l'absence de tout dialogue en ligne préalable, nous vous recommandons de l'ignorer et de l'effacer. Ne versez en aucun cas la rançon demandée.

Au cas où vous auriez reçu un tel courriel, vous pouvez contribuer à la prévention en discutant de cette thématique avec votre entourage professionnel et personnel. En sensibilisant vos collègues, vos proches et vos connaissances à ce stratagème, vous éviterez qu'ils n'en soient victimes.

En cas de contact préalable avec le maître-chanteur et si celui-ci possède réellement du matériel compromettant, adressez-vous au plus proche poste de police de votre canton (www.polizei.ch).

4.5 Fuites de données

4.5.1 Détournement du trafic de Swisscom via China Telecom

Le 6 juin 2019, une part importante du trafic Internet mobile européen a transité pendant plus de deux heures par l'infrastructure de China Telecom. L'incident s'est produit à la suite d'une erreur du protocole de passerelle frontière (*border gateway protocol, BGP*)[86] survenue au centre de calcul suisse Safe Host, qui a attribué par mégarde au fournisseur d'accès à Internet chinois plus de 70 000 routes de sa table de routage interne.

Les fuites de routage font que le trafic de données emprunte un itinéraire imprévu, ce qui peut provoquer une surcharge ou un «trou noir»[87]. Il peut ainsi arriver que des données ne soient pas transmises mais abandonnées en route – et donc effacées sans que leur destinataire en ait pris

85 https://isc.sans.edu/forums/diary/Sextortion+Follow+the+Money+Part+3+The+cashout+begins/24592/; https://isc.sans.edu/forums/diary/Sextortion+Follow+the+Money+The+Final+Chapter/25204/

86 https://www.thousandeyes.com/learning/glossary/bgp-route-leak

87 https://fr.wikipedia.org/wiki/Black_hole_(informatique)

connaissance. Des analyses du trafic ou sa mise sous écoute sont également possibles. Les fuites de routage découlent en général d'erreurs de configuration commises par inadvertance.

Or au lieu d'ignorer cette erreur de BGP, China Telecom a immédiatement repris les routes et dévié le trafic d'un grand nombre de réseaux de téléphonie mobile d'Europe sur son propre réseau. Contrairement à l'usage en la matière, voulant que les fournisseurs d'accès à Internet mettent en place des filtres pour régler l'acheminement du trafic de données et pour empêcher la propagation des fuites.

Parmi les réseaux européens les plus touchés figurent les opérateurs de téléphonie mobile de Suisse (Swisscom), de France (Bouygues Telecom, Numericable-SFR) et des Pays-Bas (KPN). Les experts ont qualifié d'exceptionnellement longue cette déviation, qui a duré plus de deux heures. Les communications mondiales en ont pâti. Les connexions au réseau se sont faites au ralenti, tandis que certains serveurs restaient inatteignables. On ignore à ce jour si le trafic des données a été intentionnellement dévié, ou s'il s'agissait d'une défaillance technique ou humaine.

De façon générale, il est recommandé aux fournisseurs d'accès à Internet de s'en tenir aux normes de sécurité BGP, pour éviter tout acheminement fautif du trafic Internet.

4.5.2 Vol de données et chantage contre le prestataire de services CityComp

En avril 2019, des cybercriminels se sont introduits dans le réseau de Citycomp, prestataire allemand de services d'infrastructure informatique.[88] Ils ont copié des données internes et menacé l'entreprise de publier les fichiers dérobés. Comme elle ne cédait pas au chantage, les agresseurs ont publié sur des sites Web spécialement conçus les 516 Go de données collectées. Parmi les clients touchés, on trouve les filiales allemandes de clients aussi prestigieux qu'Oracle, Volkswagen ou Airbus. La fuite comprenait également des fichiers concernant des entreprises suisses.

Les cybercriminels n'ont mis sous pression que ce prestataire de services et pas ses clients, qui n'étaient pas responsables du «terrible système de sécurité» de la société. Dans sa prise de position[89], Citycomp a souligné ne pas être entré en matière sur les demandes des maîtres-chanteurs et collaborer étroitement avec des spécialistes externes pour venir à bout de cet incident. Les clients et les autorités chargées de la protection des données ont été informés en toute transparence, et la police judiciaire du Land de Bade-Wurtemberg a ouvert une enquête.

Recommandation:

Les données figurant dans vos propres systèmes ne sont pas seules menacées. Vos fournisseurs, prestataires ou clients stockent parfois aussi des données sensibles sur votre propre entreprise. Il vaut donc la peine de s'assurer par contrat que vos partenaires adoptent des mesures de sécurité et des méthodes de gestion des incidents équivalentes à ce que vous avez prévu à l'interne. Même si cela devait impliquer un effort de contrôle supplémentaire, vous vous éviterez ainsi des surprises désagréables.

88 https://www.vice.com/en_us/article/d3np4y/hackers-steal-ransom-citycomp-airbus-volkswagen-oracle-valuable-companies

89 https://www.citycomp.de/unternehmen/stellungnahme.html

4.6 Logiciels criminels (*crimeware*)

Le mot-valise *crimeware* désigne un groupe de logiciels malveillants utilisés dans un dessein criminel. Plutôt que de chercher à donner un aperçu exhaustif des *maliciels* sévissant en Suisse, les graphiques ci-après reflètent la tendance actuelle en matière de logiciels criminels. Ils se fondent sur les vagues de *spams malveillants* observées par MELANI avec les spécialistes en sécurité des infrastructures d'importance vitale, mais aussi sur les données extraites de gouffres DNS (*DNS sinkhole*)[90].

Au premier semestre, le principal sujet d'inquiétude est venu des rançongiciels, dont les attaques ciblées ont infligé de sérieux dommages à des entreprises (voir thème prioritaire au chapitre 3). Les données d'accès dérobées à l'aide d'Emotet ont été revendues, et les pirates en ont fait usage pour accéder au réseau des victimes et s'y mouvoir latéralement.

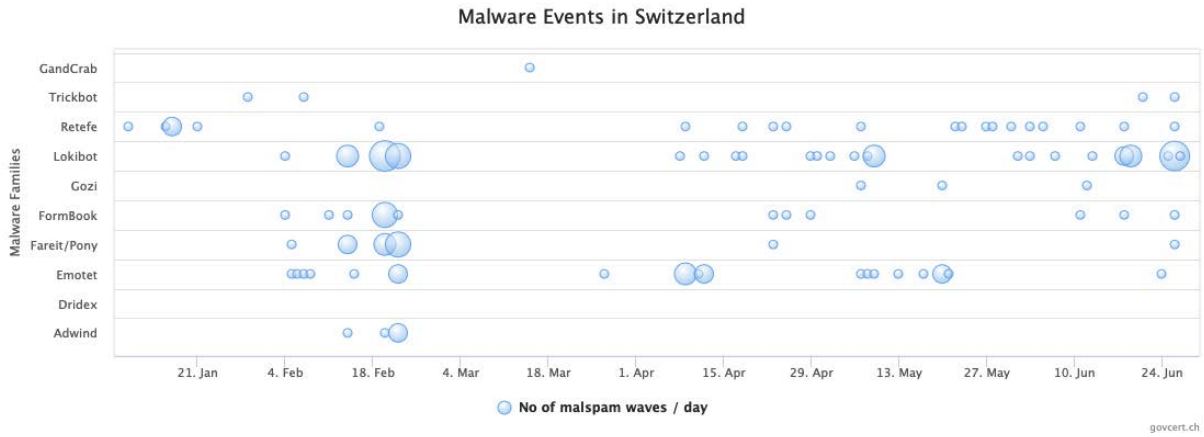

Figure 5: Vagues de spams malveillants observées

Le graphique fait ressortir les attaques incessantes lancées à l'aide de LokiBot, ainsi que l'activité persistante de Retefe. Emotet est un peu sous-représenté, car MELANI procède à un suivi non pas individuel mais global des vagues de spams malveillants.

Durant la période sous revue, Emotet est devenu une menace d'autant plus redoutable qu'en 2018 déjà, les escrocs avaient commencé à revendre les ordinateurs zombies d'entreprises où ils s'étaient introduits avec ce cheval de Troie. Autrement dit, Emotet sert de porte d'entrée à des attaques ciblées, basées sur des rançongiciels (voir aussi chapitre 3.4.1). À l'instar de Trickbot, qui ne renferme aucune banque suisse dans ses fichiers de configuration mais peut s'y introduire à la suite d'Emotet. L'agresseur tire ici parti de la sophistication de Trickbot, qui dispose de divers modules, p. ex. pour dérober des données d'accès ou pour se diffuser grâce à l'exploit EternalBlue (utilisation d'une faille de sécurité du *protocole SMB*).

Outre les cyberattaques ciblées basées sur des rançongiciels, il y a eu durant la période sous revue de nombreux cas d'attaques non ciblées, souvent menées à l'aide de GandCrab. En l'occurrence, la victime avait cliqué par imprudence sur l'annexe d'un courriel infecté, et en s'exécutant le maliciel avait aussitôt chiffré tous les fichiers archivés sur son appareil.

---

90 Le principe des gouffres DNS (*DNS sinkhole*) consiste à rediriger le trafic entrant de noms de domaine malveillants vers l'infrastructure d'organisations de sécurité, après avoir réenregistré les domaines concernés.

Retefe n'a pas chômé non plus: les pirates l'ont diffusé par vagues de *spams malveillants* aux thèmes variés. Certaines de ces vagues étaient plutôt dirigées contre les entreprises, alors que d'autres visaient en priorité les utilisateurs finaux.[91] Sur le plan technique, Retefe a généralement été distribué par courriel, dans une annexe Word. Les messages se référaient souvent à une marque connue, pour paraître crédibles. Le code actif incorporé aux documents Word installait sur l'appareil de la victime différentes composantes, soit un certificat racine afin qu'aucune alerte de sécurité ne s'affiche en cas d'attaque de l'intermédiaire (*man-in-the-middle attack, MITM*), le protocole *SOCKS* en vue de l'utilisation de services mandataires, ainsi qu'un logiciel client Tor pour détourner le trafic à destination des plateformes d'e-banking. Retefe modifiait au passage les paramètres du navigateur (*proxy settings*), afin que le trafic puisse être réacheminé. La première fois que l'utilisateur se connectait à sa plateforme d'e-banking, Retefe essayait de l'amener à installer sur son téléphone mobile une application supplémentaire conçue pour intercepter le deuxième facteur d'authentification.

MELANI collecte et diffuse des informations concernant les appareils infectés en Suisse auprès des fournisseurs d'accès à Internet et des infrastructures d'importance vitale. Le graphique ci-après indique, par famille de *maliciels*, le nombre actuel d'appareils infectés mais rendus inoffensifs grâce à un dispositif de gouffre DNS (*DNS sinkholing*):

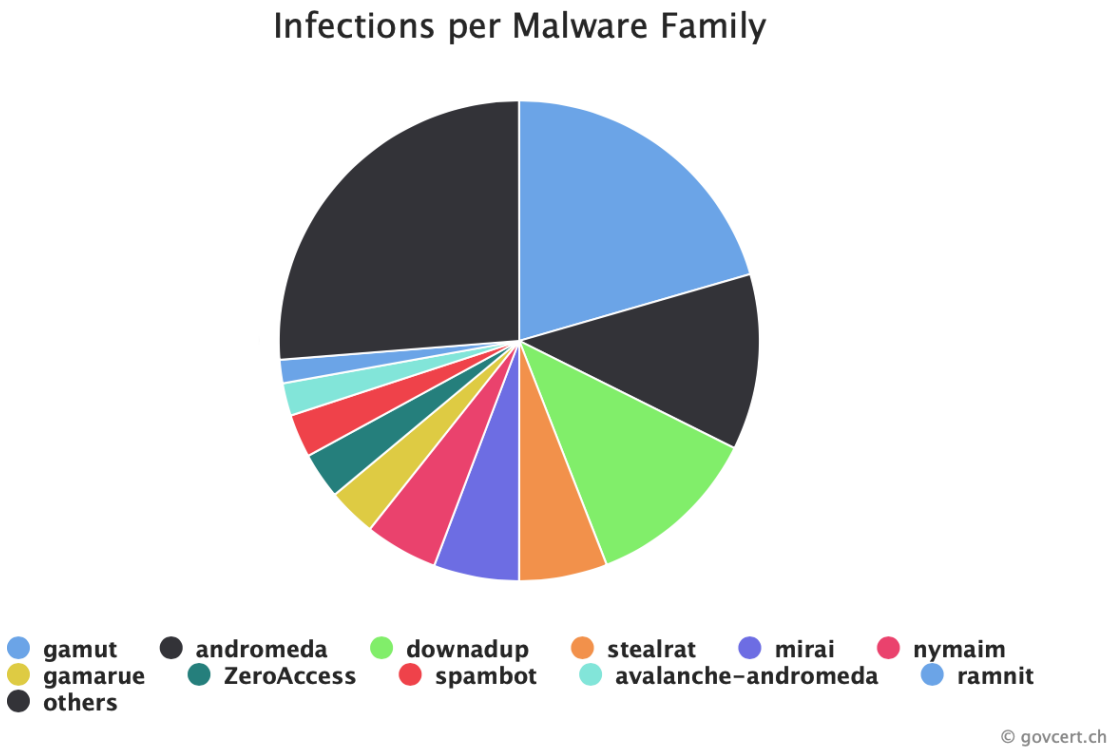

Figure 6: Répartition des maliciels en Suisse, selon les informations en possession de MELANI. La date de référence est le 30 juin 2019. Des donnée actuelles sont publiées sous: http://www.govcert.admin.ch/statistics/malware/

Il est révélateur que 20 % des infections proviennent du robot d'envoi de spams Gamut. Andromeda, programme de téléchargement installant d'autres maliciels (*malware dropper*), se classe deuxième. Downadup (aussi appelé Conficker), *ver* sévissant depuis 2008 et qui continue à causer de nombreuses infections, occupe la troisième marche du podium.

[91] Diffusion de maliciels par des méthodes d'ingénierie sociale, voir ci-dessus chap. 4.4.6.

5 Situation internationale

5.1 Espionnage

5.1.1 Développements significatifs

De nombreuses attaques de cyberespionnage ont été rendues publiques au semestre sous revue, généralement à l'occasion de rapports ou d'analyses d'entreprises de sécurité. Il n'est pas toujours aisé de s'y retrouver face à cette avalanche d'informations, à la multiplication des cibles, à l'ingéniosité des agresseurs et aux nouvelles techniques déployées.

Aussi les experts cherchent-ils souvent à attribuer les cyberattaques à un groupe d'attaquants ou à une région précise. Ce processus[92] est cependant semé d'embûches, en raison des fréquents recoupements entre groupes ou campagnes. Par exemple, de récentes analyses de Kaspersky ont révélé que les groupes Sofacy et Sandworm, connus pour des attaques bien distinctes, présentaient de nombreuses similitudes et opéraient en partie depuis la même infrastructure.[93] Pour compliquer encore les choses, les attaquants mènent souvent leurs actions sous une fausse bannière (*false flag*), afin de brouiller les pistes et de détourner les soupçons. Par exemple, des chercheurs ont identifié dans les activités de Muddy Water des parties de code rédigées en chinois. Or l'agresseur serait plutôt d'origine iranienne. Il s'est beaucoup manifesté au cours de la période sous revue, s'intéressant en plus de ses habituelles cibles au Moyen-Orient à des organisations implantées en Asie et en Europe.[94]

Le véritable défi posé par l'attribution des activités de cyberespionnage est de découvrir les spécificités propres à un attaquant donné: quels sont les éléments suffisamment révélateurs pour que les faits puissent lui être attribués? Les moyens techniques utilisés satisfont toujours moins à ce critère. En effet, beaucoup de groupes se servent aujourd'hui de toutes sortes d'outils de piratage publiquement accessibles – que ce soit pour accéder à un réseau ou pour s'y déplacer. On pense par exemple à des produits «open source», comme l'outil de pénétration Metasploit ou le collecteur d'identifiants Mimikatz, ou à des outils ayant fuité, comme l'exploit Eternal Blue. Un même groupe va déployer au cours d'une cyberattaque quantité d'instruments différents, afin de rester agile et d'avoir en tout temps sous la main l'outil répondant le mieux à ses besoins. L'arsenal déployé par Emissary Panda,[95] qui a attaqué en 2019 divers gouvernements du Moyen-Orient, en offre une bonne illustration. Le cas échéant, des outils propriétaires n'interviennent qu'à un moment précis des opérations. Il est par conséquent difficile d'identifier un groupe sur la base des outils utilisés, aujourd'hui où tout le monde emploie les mêmes techniques.[96] D'autant plus que leur diffusion a sensiblement élargi le cercle des agresseurs potentiels.

---

92 Soit l'attribution publique d'attaques informatiques, consistant à désigner officiellement l'agresseur.

93 https://securelist.com/zebrocys-multilanguage-malware-salad/90680/

94 https://documents.trendmicro.com/assets/white_papers/wp_new_muddywater_findings_uncovered.pdf

95 https://unit42.paloaltonetworks.com/emissary-panda-attacks-middle-east-government-sharepoint-servers/

96 D'autres éléments techniques, comme l'infrastructure utilisée (adresses IP, domaines), jouent également un rôle dans le travail d'attribution.

On peut dès lors s'étonner de voir à tout moment certains gouvernements pointer du doigt d'autres pays[97], alors qu'il est toujours plus hasardeux d'attribuer une cyberattaque sur la seule base d'éléments techniques. Il existe toutefois d'autres éléments utiles à l'élucidation de tels incidents, comme la bonne vieille question de savoir à qui profite le crime. Les agendas politiques et économiques des grandes puissances sont généralement connus (voire font l'objet de stratégies officielles), et il est souvent possible de distinguer les intérêts sous-jacents aux attaques informatiques.

Aussi fascinantes et complexes soient-elles, les analyses visant à attribuer la paternité d'une cyberattaque interviennent trop tard pour la victime. L'entreprise ou l'utilisateur pourront certes revoir leur évaluation des risques, en fonction des centres d'intérêts connus ou supposés des États impliqués. Mais au fond, peu leur importe qui les a agressés. Il s'agit plutôt de connaître ses propres vulnérabilités et de savoir comment un tiers est susceptible d'en tirer parti. De ce point de vue, la prolifération des outils d'attaque n'a rien de réjouissant. Chaque pirate dispose d'un vaste arsenal de cyberarmes pour passer à l'acte.

Il est d'autant plus difficile de protéger et défendre les cibles potentielles que les agresseurs tentent désormais d'y accéder en compromettant des éléments extérieurs à leur périmètre. Il est ainsi beaucoup question, depuis quelque temps déjà, des attaques de la chaîne d'approvisionnement (*supply chain*)[98]. Un exemple révélateur vient des activités d'APT10, groupe de cyberespionnage présumé d'origine chinoise qui s'en est pris à d'importants fournisseurs de services d'infogérance (*managed service provider*, MSP)[99]. Les articles parus durant la période sous revue se sont toutefois bornés à répéter des faits déjà connus[100]. Par ailleurs, les logiciels utilisés par les entreprises sont une proie prisée des pirates, comme l'a appris à ses dépens l'Allemand TeamViewer. En mai 2019, le leader du marché de la téléassistance a admis avoir subi en 2016 une cyberattaque, dont l'impact reste difficile à chiffrer[101]. L'attaque lancée contre les utilisateurs d'appareils ASUS et révélée en 2019 était encore plus pernicieuse[102]. Les attaquants auraient distribué leur code malveillant par le biais des mises à jour automatiques. Un nombre encore inconnu de machines ASUS, identifiées au moyen de leur adresse MAC, ont ainsi été piratées. Les utilisateurs sont démunis en pareil cas, ayant tendance à installer au plus vite les mises à jour du fabricant, pour des raisons de sécurité. Une autre infrastructure externe encore a été compromise au semestre écoulé, soit le *DNS*. Le sous-chapitre ci-après revient en détail sur ces incidents.

5.1.2 Détournement de DNS – vol de données d'accès

Le système de noms de domaine (*Domain Name System, DNS)* veille à ce que les internautes ayant saisi le nom d'un domaine Internet, comme www.melani.admin.ch, aboutissent à l'adresse IP du serveur hébergeant le site demandé (p. ex. 162.23.128.232). Or en janvier

---

97 Au cours des dernières années, les États-Unis ou certains de leurs alliés ont par exemple officiellement attribué NotyPetya à la Russie, Wannacry à la Corée du Nord ou APT10 à la Chine. Voir aussi chap. 4.1.4.

98 La question a déjà été traitée en détail dans le rapport semestriel MELANI 2018/2, chap. 3 et le présent rapport y revient au chap. 5.3.1.

99 Rapport semestriel MELANI 2017/1, chap. 5.1.1 et 2018/2, chap. 5.1.1.

100 https://uk.reuters.com/article/uk-china-cyber-cloudhopper-special-repor/special-report-inside-the-wests-failed-fight-against-chinas-cloud-hopper-hackers-idUKKCN1TR1DC

101 https://www.zdnet.fr/actualites/teamviewer-a-ete-vise-par-le-cyberespionnage-chinois-en-2016-39884875.htm

102 https://www.vice.com/en_us/article/pan9wn/hackers-hijacked-asus-software-updates-to-install-backdoors-on-thousands-of-computers

2019, le CERT américain[103] a signalé des tentatives d'intrusion dans l'infrastructure *DNS* et de modification des entrées *DNS* pour détourner le trafic des visiteurs de domaines sur des systèmes contrôlés par les attaquants.

Talos, la branche de CISCO spécialisée dans la cybersécurité, a fait état d'une première variante baptisée DNSpionage.[104] En plus de s'en prendre aux utilisateurs de systèmes Windows, le *maliciel* redirigeait le trafic du réseau vers des cibles situées au Liban et aux Émirats arabes unis. En effet, comme ils contrôlaient les entrées *DNS*, les pirates pouvaient aussi émettre des certificats SSL valables pour leurs propres serveurs, et donc détourner même les communications chiffrées.

La société de sécurité informatique Fireeye[105] a publié en janvier 2019 un aperçu détaillé des activités de détournement de DNS (*DNS* hijacking). Les analystes des menaces informatiques y mentionnent trois variantes utilisées pour manipuler les requêtes *DNS* émanant de cibles localisées au Moyen-Orient, en Afrique du Nord, en Europe et en Amérique du Nord. Les attaquants cherchaient surtout à faire main basse, dans le flux de données piratées, sur les données d'accès à des comptes de messagerie ou à des serveurs de fichiers, afin de se faire passer pour leurs propriétaires légitimes.

À la fin de janvier 2019, l'entreprise de cybersécurité Crowdstrike[106] a confirmé l'analyse faite des méthodes d'attaque, en soulignant que les campagnes remontaient à l'année 2017 et qu'elles prenaient pour cibles les secteurs de l'administration publique et de l'aviation civile, ainsi que les fournisseurs d'accès à Internet ou d'infrastructures de réseau.

En avril 2019, les spécialistes de Talos ont parlé d'un autre acteur se livrant à des activités similaires contre l'infrastructure *DNS*, baptisé par eux Sea Turtle[107]. Ses victimes comprenaient des organisations nationales de sécurité, des ministères des affaires étrangères et des organisations bien connues du secteur de l'énergie, sans oublier les prestataires de services actifs dans l'environnement *DNS*, comme les registraires ou les opérateurs télécom, qui servaient de tremplin aux attaques contre leur clientèle. Dans un rapport de suivi, Talos[108] cite entre autres victimes le registre grec, qui administre les domaines de premier niveau «.gr». Les attaques se sont étendues aux entreprises du secteur énergétique, aux groupes de réflexion, aux organisations non gouvernementales et à au moins un aéroport. Les fournisseurs de prestations et les organisations basés en Suisse doivent aussi s'attendre à faire l'objet d'attaques de Sea Turtle – que les pirates les prennent directement pour cibles ou qu'ils se servent d'eux pour parvenir à leurs fins.

À la suite de ces attaques, la Société pour l'attribution des noms de domaine et des numéros sur Internet (ICANN) a appelé au déploiement complet des extensions de sécurité du système de noms de domaine (DNSSEC).[109] Il s'agit d'une série de normes visant à sécuriser les données envoyées par le *DNS* en les protégeant de bout en bout, pour en garantir l'authenticité

---

103 https://www.us-cert.gov/ncas/current-activity/2019/01/10/DNS-Infrastructure-Hijacking-Campaign

104 https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html

105 https://www.fireeye.com/blog/threat-research/2019/01/global-dns-hijacking-campaign-dns-record-manipulation-at-scale.html

106 https://www.crowdstrike.com/blog/widespread-dns-hijacking-activity-targets-multiple-sectors/

107 https://blog.talosintelligence.com/2019/04/seaturtle.html

108 https://blog.talosintelligence.com/2019/07/sea-turtle-keeps-on-swimming.html

109 https://www.icann.org/news/announcement-2019-02-22-en

et l'intégrité. De telles normes sonneraient le glas des cyberattaques menées contre l'infrastructure DNS.

L'administration fédérale approuve cette démarche et a introduit le protocole DNSSEC pour tous ses sites Internet.

5.2 Systèmes de contrôle industriels (SCI)

5.2.1 Approvisionnement énergétique: SCI toujours dans le viseur en cas de conflit armé

Le 14 juin 2019 Dragos, société de cybersécurité spécialisée dans les SCI, a publié un article de blog sur les activités d'un groupe surnommé Xenotime qui serait à l'origine de Triton/Trisis, maliciel ciblant les systèmes de sûreté dans la production industrielle.[110] Selon un rapport de FireEye datant du 23 octobre 2018, des développeurs de ce *maliciel* seraient basés en Russie.[111]

Il ressort du rapport de Dragos que Xenotime est davantage actif depuis le deuxième semestre 2018, dans les pays européens et aux États-Unis surtout. Même sans avoir réussi à compromettre d'implantation industrielle, le groupe a inlassablement développé ses activités de reconnaissance. En particulier, Xenotime a élargi son champ d'action.[112] D'abord déployé contre une raffinerie de gaz et de pétrole, son maliciel Triton/Trisis s'intéresse aussi entre-temps aux réseaux de production et de distribution d'électricité.

Le 15 juin 2019, le New York Times a consacré un article aux *maliciels* que l'US Cyber Command (USCYBERCOM) aurait glissés dans le réseau électrique russe.[113] En plus de conférer aux États-Unis un avantage décisif en cas de conflit, de telles opérations conçues ces dernières années serviraient surtout à dissuader la Russie de mener contre eux des opérations dans le cyberespace.

Ces articles montrent que l'intérêt des États pour les infrastructures d'importance vitale ne s'est pas démenti, dans le secteur énergétique surtout,[114] et que les opérateurs doivent mieux protéger leurs réseaux et améliorer leurs capacités de réaction en cas d'attaques informatiques[115]. L'Office fédéral pour l'approvisionnement économique du pays (OFAE) met à disposition une norme minimale pour garantir la sécurité informatique pour l'approvisionnement en électricité[116].

---

110 https://dragos.com/blog/industry-news/threat-proliferation-in-ics-cybersecurity-xenotime-now-targeting-electric-sector-in-addition-to-oil-and-gas/, voir aussi MELANI, rapport semestriel 2017/2, chap. 5.3.2.

111 https://www.fireeye.com/blog/threat-research/2018/10/triton-attribution-russian-government-owned-lab-most-likely-built-tools.html

112 https://www.wired.com/story/triton-hackers-scan-us-power-grid

113 https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html

114 Voir aussi MELANI, rapport semestriel 2015/2, chap. 5.3.1 et 2016/2, chap. 5.3.1.

115 Voir l'étude d'Electrosuisse mentionnée au chap. 4.2.1.

116 https://www.bwl.admin.ch/bwl/fr/home/themen/ikt/ikt_minimalstandard/ikt_branchenstandards/minimalstandard_strom.html (document disponible en allemand seulement)

5.2.2 Pilotes gênés dans l'espace aérien israélien par une attaque GPS

Depuis que l'immense majorité des smartphones comportent un capteur GPS, la plupart des gens s'en remettent à la localisation par satellite pour leurs déplacements à pied ou en voiture. Comme indiqué au chapitre 4.2.2, la navigation aérienne repose largement elle aussi sur les coordonnées GPS. Or durant le mois de juin 2019, plusieurs pilotes se sont plaints d'avoir perdu, dans les environs de l'aéroport Ben Gourion de Tel Aviv, les signaux GPS destinés à l'atterrissage.[117] L'association israélienne des pilotes a imputé le problème des coordonnées incorrectes à une attaque d'usurpation GPS (*GPS spoofing*).

Les autorités de sécurité israéliennes ont identifié la source du brouillage GPS, soit un signal provenant de la base aérienne russe de Khmeimim en Syrie, et ont attribué l'incident aux systèmes russes de guerre électronique. La base située 350 kilomètres au nord de Ben Gourion est activement utilisée par les forces aériennes russes pour soutenir le régime syrien. Si les accusations s'avèrent fondées, les systèmes russes de guerre électronique ont dû déployer des émetteurs particulièrement puissants afin d'obtenir à une telle distance l'effet de brouillage décrit ci-dessus.

L'ambassadeur de Russie en Israël a aussitôt démenti les reproches, affirmant qu'il s'agissait de fausses nouvelles peu crédibles.[118]

5.2.3 Quand la télécommande obéit à un tiers

Sur les chantiers, les immenses grues transportant de lourdes charges ne sont pas toujours pilotées depuis la cabine mais également, spectacle insolite, avec un simple manche à balai depuis le sol. De telles radiocommandes s'utilisent fréquemment dans la construction, dans la logistique ou les usines de production.

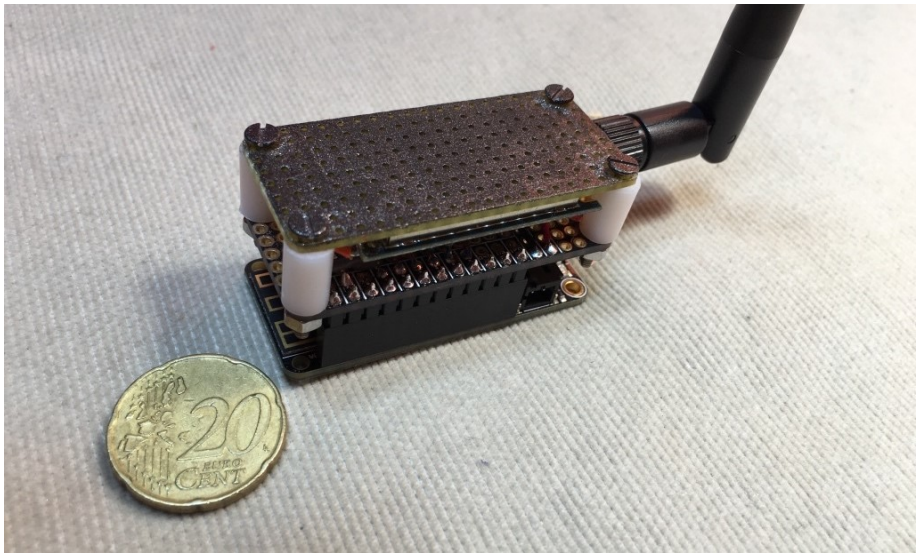

Figure 7: Comparaison de taille avec le module RFQuack

[117] https://www.gpsworld.com/israel-accuses-russia-of-spoofing-in-its-airspace/

[118] https://www.bbc.com/news/technology-48786085

L'entreprise de sécurité japonaise TrendMicro est parvenue à démontrer dans une analyse[119] que cette interface radio est vulnérable aux intrusions, et qu'il est par exemple possible de manipuler les commandes transmises par ce canal. Une attaque fructueuse suppose certes que l'agresseur soit physiquement à proximité de sa victime, afin que ses signaux parviennent à l'engin piraté. Mais il suffit de placer à proximité du système commandé à distance un petit transmetteur acceptant les connexions distantes en Wi-Fi ou en 3G/4G. Pour montrer à quel point une telle menace est plausible, les chercheurs ont conçu un tel appareil fonctionnant sur batterie et baptisé RFQuack (voir figure ci-dessus), qui trouve place dans une poche de pantalon.

Recommandation:

Afin de réduire la probabilité que de tels scénarios d'attaque se réalisent, les analystes recommandent d'étudier de près la documentation de la télécommande qu'il est prévu d'acheter. Il convient de s'assurer que les appareils disposent d'un mécanisme de liaison (jumelage) configurable. Les autres mesures utiles consistent à exploiter à l'écart du réseau l'ordinateur à l'aide duquel la télécommande est programmée, et à utiliser autant que possible des protocoles standard bien étudiés comme «Bluetooth Low Energy».

Conclusion / recommandation:

L'informatisation progressive et la mise en réseau de multiples objets d'usage courant (Internet des objets) nous font bénéficier de nombreuses fonctions inédites et utiles, tout en accroissant notre bien-être. On peut citer à cet égard l'électronique de loisirs et l'accès à Internet dans la voiture ou en avion. Il faut toutefois se garder d'ignorer les risques qui s'ensuivent. En effet, les nouvelles possibilités induisent toujours de nouveaux risques, à prendre en compte dès le stade de la conception (*security by design*).

DOKU

Liste de contrôle des mesures de protection des systèmes de contrôle industriels

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

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

5.3.1 WIPRO, prestataire de services informatiques, victime d'une attaque

En avril 2019, le journaliste d'investigation Brian Krebs annonçait que la multinationale de services informatiques WIPRO avait été victime d'une cyberattaque.[120] Les experts ont craint le pire, en pensant aux activités de groupes comme APT10, qui s'en prennent en général aux

[119] https://blog.trendmicro.com/trendlabs-security-intelligence/demonstrating-command-injection-and-e-stop-abuse-against-industrial-radio-remote-controllers/

[120] https://krebsonsecurity.com/2019/04/experts-breach-at-it-outsourcing-giant-wipro/

fournisseurs de services d'infogérance (*managed service provider*, MSP) afin d'espionner en ligne leurs clients. Une analyse plus récente, menée par l'entreprise Flashpoint[121], privilégie également la piste de l'attaque contre la clientèle de cette société, mais pour d'autres raisons. L'agresseur était apparemment mû par l'appât du gain et ne se livrait pas à des activités d'espionnage. Pour financer ses activités, ce groupe dont l'activité remonterait à 2015 ou 2016 cherchait notamment à s'emparer des bons cadeaux (*gift cards*) émis par les entreprises.

Les criminels ont essentiellement mené des attaques de phishing pour infiltrer les réseaux de leurs victimes. Selon une entreprise de sécurité, ils utilisaient des modèles (*templates*) proposés par une société suisse active dans la sensibilisation. Ce qui ne veut pas forcément dire que cette dernière ait été compromise. Les criminels ont également utilisé des outils de piratage librement accessibles, ou détourné de leur fonction première pour en faire des cyberarmes des outils présents dans le réseau de leurs victimes.

Cette attaque montre une fois de plus les risques que fait courir la chaîne d'approvisionnement (supply chain). Entre-temps, de telles opérations ne relèvent plus seulement de l'espionnage: pour atteindre leur proie, d'autres groupes criminels s'en prennent à ses fournisseurs.

5.3.2 Attaques en force brute d'un réseau de zombies contre les serveurs RDP

Les pirates écument Internet depuis des années, en quête de réseaux aux ports ouverts ou mal sécurisés. Ces ports sont généralement attribués à un service ou protocole Internet et en partie définis par défaut. Entre-temps, des moteurs de recherche permettent de repérer même sans connaissances techniques particulières de telles «portes ouvertes». Certaines sont plus populaires que d'autres. Au semestre sous revue, MELANI a constaté une recrudescence des activités d'analyse des ports *RDP.*[122] Le numéro de port par défaut du service *RDP* est 3389.

Le réseau de zombies GoldBrute, qui comprend un seul serveur de *commande et de contrôle (C2)*, s'était attaqué au moment de l'article de SANS[123] à 1,5 million de *serveurs RDP* disposant d'une connexion exposée sur Internet. La taille de ce réseau ne cesse de gonfler. Le système infecté télécharge le code du programme malveillant, puis analyse d'autres adresses IP choisies au hasard sur les ports *RDP.* Quand il a découvert 80 autres adresses dont un port *RDP* est accessible, il en envoie la liste au serveur C&C. Ce dernier transmet alors à chaque hôte infecté une liste d'adresses IP à attaquer par *force brute*. Curieusement, chaque système tente de s'authentifier avec un seul nom d'utilisateur et UN mot de passe, précaution visant à ne pas attirer l'attention des programmes de sécurité usuels. Les systèmes compromis par le port *RDP* deviendront à leur tour des zombies. En théorie, les agresseurs pourraient aussi installer un autre maliciel (rançongiciel, logiciel de collecte de données, etc.), ce qui serait très embarrassant pour le propriétaire du système piraté.

5.3.3 Des nouvelles d'Anonymous

Ces derniers temps, les actions revendiquées par Anonymous se sont faites rares. Il faut dire qu'elles avaient abouti dans le passé à des arrestations médiatisées. Plusieurs événements

---

121 https://www.flashpoint-intel.com/blog/wipro-threat-actors-active-since-2015/

122 Remote Desktop Protocol (RDP) est un protocole développé par Microsoft, qui permet à un utilisateur de se connecter à un ordinateur distant.

123 https://isc.sans.edu/forums/diary/GoldBrute+Botnet+Brute+Forcing+15+Million+RDP+Servers/25002/

ont néanmoins encore mobilisé les activistes, notamment quand la liberté d'information était en jeu. Ainsi, l'arrestation de Julian Assange à Londres a donné lieu à des cyberattaques contre les intérêts anglais et équatoriens. Le fondateur de Wikileaks vivait réfugié depuis 2012 à l'ambassade équatorienne de Londres. En signe de protestation contre son arrestation en avril 2019, après la levée de son statut d'asile, un groupe se réclamant d'Anonymous a publié peu après des données dérobées à différents services de police anglais. Aucune donnée personnelle n'en faisait apparemment partie. Un autre groupe a lancé au nom d'Anonymous des attaques *DDoS* contre les sites d'autorités britanniques. Les autorités équatoriennes ont également signalé des attaques *DDoS*, subies notamment par les sites de la Banque centrale ainsi que du Premier ministre.

5.3.4 Attaques DDoS contre les détenteurs de bitcoins

Le succès des monnaies virtuelles attise la convoitise, et les braquages numériques tendent à se multiplier. MELANI a déjà évoqué à plusieurs reprises des attaques lancées contre les plateformes d'échange de cryptomonnaies ou leurs utilisateurs.[124] Plus une monnaie ou un service deviennent populaires, et plus le risque de cyberattaques augmente. Electrum, l'un des principaux fournisseurs de portefeuilles bitcoin, en a fait l'amère expérience cette année. Les utilisateurs de ce service étaient amenés à télécharger une version manipulée de l'application. À cet effet, les escrocs avaient déployé une série de «nœuds» malveillants dans le réseau pair à pair utilisé pour valider les transactions. Lorsque l'utilisateur atteignait un de ces nœuds (faisant office de serveur dans le réseau pair à pair), un message d'erreur l'invitait à suivre un lien pour télécharger une prétendue mise à jour de l'application. En réalité, il s'agissait d'un programme malveillant, conçu pour vider son portefeuille.

Ce n'est pas tout. En réponse aux mesures adoptées par les développeurs d'Electrum, les pirates ont lancé des attaques *DDoS* contre ses serveurs. Comme les nœuds légitimes étaient submergés, les utilisateurs étaient redirigés vers des nœuds frauduleux leur délivrant une mise à jour malveillante. En avril, la société de cybersécurité Malwarebytes chiffrait à 771 bitcoins (soit l'équivalent de 4 millions de dollars à cette date) le butin ainsi dérobé par les criminels.[125]

5.4 Fuites de données

5.4.1 Piratage de Citrix

Le 6 mars 2019, l'éditeur de logiciels Citrix a appris du FBI que des cybercriminels internationaux avaient accédé à son réseau interne.[126] Citrix a informé à son tour ses clients de cette intrusion commise depuis l'étranger dans le but de dérober des données. L'enquête se poursuit pour déterminer à quelles données les intrus ont eu accès. Mais selon Citrix, rien n'indique que les pirates aient manipulé ses logiciels officiels ou d'autres produits.

---

124 Voir notamment MELANI, rapport semestriel 2017/2, chap. 5.4.3.

125 https://blog.malwarebytes.com/cybercrime/2019/04/electrum-bitcoin-wallets-under-siege/

126 https://www.citrix.com/blogs/2019/03/08/citrix-investigating-unauthorized-access-to-internal-network/

L'incident s'inscrirait dans une vaste campagne se concentrant sur les gouvernements, le secteur militaro-industriel, les entreprises énergétiques, les établissements financiers ainsi que les exploitants d'infrastructures d'importance vitale.[127]

5.4.2 Magento: sécurité des boutiques en ligne

Les éventuelles extensions (modules tiers) des boutiques en lignes Magento sont aujourd'hui leur talon d'Achille. Une faille du moteur MySQL de leur base de données, qui a été documentée depuis des années, permet aux escrocs d'introduire du code malveillant dans les sites d'e-commerce. Cet exemple montre la difficulté des boutiques en ligne de préserver leurs sites de tout code malveillant, dès lors que les modules tiers utilisés devraient eux aussi être constamment à jour. Il en résulte un conflit d'intérêts entre le souci de stabilité des boutiques en ligne et une politique de mises à jour régulières, notamment parce que Magento n'offre pas de possibilité standardisée de s'informer des mises à jour importantes de fournisseurs tiers.

5.4.3 Fuite de données à Panama

Des chercheurs en cybersécurité ont découvert un serveur Elasticsearch non protégé, sur lequel étaient stockées les données personnelles de quasiment 90 % des habitants de Panama. Les données ainsi exposées comprenaient le nom complet, la date de naissance, le numéro de passeport, le numéro de sécurité sociale et d'autres informations personnelles encore. La base de données renfermait par ailleurs 3,4 millions de jeux de données sur des habitants du pays désignés comme «patients». Le CERT local a sécurisé la base de données aussitôt après avoir été informé de la fuite. Il est toutefois trop tard pour savoir si quelqu'un a accédé aux données, au cours de la période où elles étaient en libre accès.

5.4.4 Découverte de millions de données Facebook sur un serveur en nuage d'Amazon

Des chercheurs en sécurité ont à nouveau découvert d'innombrables données d'utilisateurs Facebook exposées à la vue de tous, sur les serveurs hébergés par Amazon dans le nuage.[128] Cette récente découverte montre qu'un an après le scandale de Cambridge Analytica, les données d'utilisateurs de Facebook ne sont toujours pas stockées de manière sécurisée et continuent d'être visibles en ligne. Il faut dire que pendant des années, Facebook a généreusement fourni ses données à quiconque voulait bien en contrepartie intégrer ce réseau social dans son service, pratique qui a perduré jusqu'à une date récente. Or les nouvelles découvertes confirment que les entreprises obtenant accès, par contrat, aux données de Facebook sont trop peu actives en matière de protection des données. Après tous les scandales survenus, il est permis d'émettre des doutes sur la sécurité des données des utilisateurs sur Facebook, de même que sur la transparence dans la gestion des données pour les utilisateurs individuels. Cela n'est d'ailleurs pas un problème spécifique à Facebook. À l'ère des méga-données et de l'automatisation, où les données ainsi recueillies sont le pétrole du 21e siècle, ce thème est plus que jamais d'actualité. Les utilisateurs feraient bien de réfléchir à leur présence numérique et aux données personnelles qu'ils divulguent. Et comme le montre ce récent

127 https://www.forbes.com/sites/kateoflahertyuk/2019/03/15/who-is-resecurity-the-mysterious-firm-that-blamed-iran-for-the-citrix-hack/; https://www.theregister.co.uk/2019/03/08/citrix_hacked_data_stolen/

128 https://www.upguard.com/breaches/facebook-user-data-leak

exemple, les problèmes touchant à la sécurité et au contrôle des données auront plutôt tendance à s'aggraver, avec la tendance croissante à renoncer aux centres de calcul internes, traditionnellement chargés de l'exploitation et du stockage des données, au profit des services informatiques en nuage des géants de la technologie.

5.5 Vulnérabilités

5.5.1 BlueKeep – faille du protocole RDP se prêtant à la propagation d'un ver

En mai 2019, une vulnérabilité (CVE-2019-0708, BlueKeep) a été découverte dans le protocole de bureau à distance (*remote desktop protocol*, *RDP*) de Microsoft. Peu après l'annonce de cette faille et la publication d'un correctif de sécurité, les pirates se sont empressés d'identifier les ports *RDP* ouverts à l'aide d'outils de balayage automatique.[129] Ils ont ensuite cherché à accéder aux systèmes pour exploiter cette vulnérabilité, lors d'*attaques par force brute* (test de mots de passe simples, faibles ou déjà connus).

Cette faille permet d'exécuter du code à distance sur une machine compromise. Elle a été jugée très critique, car elle concerne toutes les versions de Windows – de Windows 2000 jusqu'à Windows 7, y compris Windows Server 2008 R2. Les nouvelles versions (Windows 8 et 10) ne sont pas affectées. Microsoft a publié le 14 mai 2019 un correctif utile à toutes les versions, y compris celles dont Microsoft n'assure plus la maintenance parce qu'elles ont atteint leur fin de vie.

Il s'agit d'une vulnérabilité de type ver. Autrement dit, un maliciel pourrait se propager «automatiquement», sans interaction humaine, aux systèmes non retouchés. Une telle attaque aurait des effets désastreux, car bien des systèmes sont vulnérables et ne seront pas munis de correctifs dans un proche avenir.

À l'heure actuelle, des indices montrent qu'il serait possible d'utiliser cette vulnérabilité, mais les chercheurs n'ont pas publié de «guide pratique» et à ce jour, les criminels n'ont pas exploité activement cette faille. Une recrudescence des activités de balayage des ports *RDP* a toutefois été observée depuis un certain temps. Une telle approche permet de dresser une liste des systèmes vulnérables, afin de connaître déjà les cibles potentielles quand l'exploit correspondant sera sur le marché. Ce n'est donc qu'une question de temps avant que quelqu'un mette au point un exploit, qui ne tardera pas à se propager.[130]

Recommandation:

Vous devriez absolument mettre en place le correctif de sécurité nécessaire pour vous protéger de BlueKeep. En outre, MELANI conseille de désactiver les services de bureau à distance (port d'écoute RDP), si vous n'en avez pas impérativement besoin.

---

129 https://www.zdnet.com/article/intense-scanning-activity-detected-for-bluekeep-rdp-flaw/

130 Entre la rédaction et la publication de ce rapport, cette prévision s'était d'ailleurs déjà réalisée, puisque Bluekeep est désormais intégré à l'outil de pénétration «open source» Metasploit.

La forte recrudescence des activités de détection de ports *RDP* est préoccupante, sachant qu'il existe de très nombreux ports ouverts, accessibles à partir d'Internet. Des études ont d'ailleurs montré qu'au premier trimestre 2019, les rançongiciels se sont principalement déployés à partir de ports *RDP* ouverts ou mal configurés.[131] Car bien souvent, ni les utilisateurs ni les administrateurs ne savent que le service est activé dans leur réseau. Autrement dit, les utilisateurs sont attaqués par un vecteur face auquel ils n'ont prévu aucune mesure de protection, puisqu'ils en ignorent l'existence. Il est par conséquent indispensable que les utilisateurs et les administrateurs connaissent leurs réseaux et sachent quels services et appareils en font partie, afin de les sécuriser efficacement.

Comme indiqué plus haut au chapitre 3, les rançongiciels ont une capacité de nuisance énorme et peuvent paralyser une entreprise pendant plusieurs jours. De même, les agresseurs ayant utilisé le port *RDP* comme point d'entrée peuvent se mouvoir latéralement dans le réseau de l'entreprise en quête de cibles plus intéressantes. Ils pourront au choix dérober, effacer ou chiffrer des données pour les rendre inutilisables. En l'absence d'une bonne solution de sauvegarde dûment testée, de telles données sont en général perdues – jusqu'à ce que quelqu'un ait mis au point un outil de déchiffrement afin de pouvoir en restaurer au moins une partie.

Pour prévenir une telle attaque, McAfee donne les conseils suivants:[132]

Recommandations:

- N'autorisez jamais les connexions *RDP* en toute liberté depuis Internet; le port *RDP* ne devrait JAMAIS être ouvert dans Internet, où des activités de balayage de port sont déployées en permanence et où votre système serait vulnérable aux attaques DDoS ou à une usurpation de votre compte d'utilisateur.
- Employez des mots de passe complexes, car les ports *RDP* font l'objet de nombreuses *attaques par force brute*.
- Utilisez l'authentification multifactorielle (p. ex. jetons de sécurité, envoi de code par SMS, vérification biométrique).
- Configurez une passerelle *RDP* afin de renforcer vos contrôles (p. ex. pour permettre un historique des événements).
- Bloquez les noms d'utilisateur ou les adresses IP après plusieurs vaines tentatives de connexion.
- Utilisez un pare-feu pour limiter les accès.
- Recourez au chiffrement.
- Activez le mécanisme *Network Level Authentication* (NLA). Cette mesure vous protégera dans une large mesure de la faille BlueKeep, puisqu'un agresseur devra se connecter avec un compte valable pour exploiter cette vulnérabilité.
- Limitez les droits d'accès des utilisateurs se connectant par le port *RDP* (en général, les administrateurs n'ont pas besoin d'un tel accès).

131 https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/rdp-security-explained/

132 https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/rdp-security-explained/

5.5.2 Vulnérabilité d'EXIM affectant des millions de serveurs de messagerie

Le logiciel Exim est un agent de transfert de messages (*mail transfer agent*, MTA), utilisé dans de nombreux serveurs de messagerie pour l'envoi et la réception du courrier. La plupart des systèmes Unix font appel à des composants d'Exim, qui sont même installés par défaut dans les systèmes Debian.[133 et 134]

La faille découverte peut être exploitée à deux niveaux. Ainsi, un attaquant local (initié) pourra d'emblée lancer des commandes système comme utilisateur racine. Or pour certaines configurations non standardisées, même un attaquant à distance avec de faibles privilèges obtiendra le même résultat.

Un mois après la publication de cette faille, des pirates en tiraient déjà profit. Les avis divergent à propos du nombre total de systèmes vulnérables quand la faille de sécurité a été rendue publique: selon skyboxSecurity, il s'agirait de plus de 3,5 millions de serveurs. SecureZoo estime que plus de 4 millions d'appareils (env. 90 % des installations sur le plan mondial[135]) utiliseraient la version vulnérable d'Exim[136]. La faille est absente de la dernière version en date. Tous les systèmes devraient donc d'urgence être actualisés avec la version 4.92 d'Exim. Le logiciel fonctionne sur 57 % de tous les serveurs de messagerie. Les chercheurs qualifient par conséquent d'énormes les dommages potentiels[137].

Évaluation:

De nombreuses vulnérabilités sont publiées au quotidien. Un correctif de sécurité est parfois déjà disponible quand elles sont divulguées, mais pas toujours. Et comme en règle générale, les entreprises utilisent différents systèmes et logiciels, il peut être ardu de procéder au suivi manuel de toutes les failles du matériel ou des logiciels utilisés. Il faudrait donc autant que possible installer automatiquement les mises à jour. Toutes les failles publiées ne sont sans doute pas activement exploitées par les pirates. Mais on en trouve aussi dont il est relativement simple de se servir, qui sont rapidement intégrées dans les *kits d'exploits* et qui occasionnent ensuite de graves dommages potentiels.

5.5.3 Quand votre smartphone espionne vos faits et gestes

Deux vulnérabilités publiées au premier semestre 2019 auraient permis d'introduire un logiciel espion dans les smartphones. L'une a été découverte dans l'application Facetime, l'autre dans WhatsApp.

La vulnérabilité de WhatsApp était une faille de saturation de mémoire tampon (*buffer overflow*), repérée dans le module de téléphonie (VoIP) de ce logiciel de messagerie. Il devenait

133 https://meterpreter.org/cve-2019-10149-exim-remote-code-execution/
134 https://blog.skyboxsecurity.com/exim-vulnerability/
135 https://www.securezoo.com/2019/06/critical-exim-vulnerability-discovered-and-patched/
136 https://www.cisecurity.org/advisory/a-vulnerability-in-exim-could-allow-for-remote-command-execution_2019-061/
137 https://www.securezoo.com/2019/06/critical-exim-vulnerability-discovered-and-patched/

ainsi possible d'envoyer au smartphone pris pour cible des paquets SRTCP[138] spécialement développés. Il suffisait d'un appel WhatsApp manipulé. La personne appelée n'avait même pas besoin de répondre, et les appels en absence ne laissaient aucune trace non plus. La victime ignorait par conséquent que son smartphone avait été compromis. Une attaque dirigée contre le téléphone d'un avocat basé au Royaume-Uni aurait abouti à la découverte de cette faille.[139]

Quant à la vulnérabilité de FaceTime, un adolescent l'a découverte par hasard. Il s'agit d'une erreur logicielle de l'application FaceTime pour iPhone.[140] Une manipulation toute simple permettait à l'utilisateur de voir et d'écouter ce qui se passe chez son correspondant, sans même qu'il décroche. Il suffisait de lancer un appel vidéo en FaceTime et de s'ajouter à la conversation (appel de groupe). Apple a rapidement publié un correctif.[141]

5.5.4 Faille *zero day* d'Internet Explorer: divulgation irresponsable

Il arrive que des chercheurs en sécurité publient des exploits tirant partie de failles de sécurité, afin d'obliger les éditeurs de logiciels à diffuser sans tarder des correctifs pour des vulnérabilités leur ayant été vainement signalées jusque-là.

C'est ainsi qu'une faille *zero day* a été révélée à propos du navigateur Internet Explorer.[142] Un chercheur en sécurité en avait informé Microsoft, qui lui avait fait comprendre qu'aucun correctif ne serait diffusé en urgence. Il a donc publié l'exploit avec une démonstration de faisabilité. On y apprenait qu'il était possible de dérober des fichiers locaux et donc d'effectuer une reconnaissance à distance sur les versions utilisées des programmes, à condition que l'utilisateur ouvre un fichier MHT[143] spécialement préparé (de tels fichiers étant automatiquement ouverts par défaut sous Windows dans Internet Explorer).

Les groupes cybercriminels utilisent souvent des fichiers MHT pour la pêche au harpon (*spear phishing*) ou pour diffuser des maliciels. La course contre la montre est par conséquent ouverte entre les criminels désireux d'utiliser cette méthode et Microsoft qui devra publier un correctif adéquat.

On ne saurait affirmer de manière générale, lors de tels cas de «divulgation irresponsable», si les chercheurs ont fait preuve d'impatience ou si le problème tient au fabricant. Les éditeurs de logiciels devraient dans tous les cas examiner en détail toutes les vulnérabilités signalées et donner aux chercheurs en sécurité une réponse correcte, en précisant dans quel horizon la faille sera corrigée.

---

138 Secure real time control transport protocol: https://tools.ietf.org/html/rfc3711

139 https://securityaffairs.co/wordpress/85477/breaking-news/whatsapp-zero-day.html

140 https://www.buzzfeednews.com/article/nicolenguyen/facetime-bug-iphone

141 https://9to5mac.com/2019/01/28/facetime-bug-hear-audio/

142 https://www.zdnet.fr/actualites/une-zero-day-d-internet-explorer-permet-le-vol-de-fichiers-sur-les-pc-windows-39883433.htm

143 Un fichier contenant l'extension MHT est un fichier unique dans lequel toute la page Web est archivée avec ses composants, tels les graphiques et les autres éléments externes.

5.6 Mesures préventives et poursuites pénales

5.6.1 Démantèlement du réseau criminel de GozNym

La distribution du cheval de Troie bancaire GozNym était assurée par un réseau criminel basé sur une claire répartition des tâches, dont les membres résidaient dans plusieurs États (dont la Géorgie, la Bulgarie, l'Ukraine, la Moldavie, le Kazakhstan et la Russie). Une vaste opération de police, à laquelle participaient plusieurs pays ou organisations internationales, a abouti à plusieurs arrestations – développeur du *maliciel*, spammeur le propageant, spécialistes de la prise de contrôle des comptes bancaires, blanchisseurs d'argent, etc. En mai 2019, dix membres du groupe étaient mis en examen à Pittsburgh, et d'autres procès suivront en Géorgie, en Moldavie et en Ukraine. Une enquête est également en cours contre le fournisseur de services d'hébergement «à l'épreuve des balles» (*bulletproof hosting*), dont les services ont été sollicités par plus de 20 campagnes de maliciels en dehors de GozNym.[144]

5.6.2 Nouvelle victoire contre la fraude au support technique de Microsoft

Il a déjà été question, dans le dernier rapport semestriel MELANI, d'une opération policière lancée contre des escrocs prétendant représenter une société de logiciels. À l'époque, la police indienne avait perquisitionné 26 centres d'où émanaient de tels appels en anglais.[145] Entre-temps, la police française a elle aussi connu un succès.[146] Trois Français soupçonnés d'être à la tête du réseau ont été arrêtés. Dans cette affaire, des fenêtres de sécurité intempestives signalaient aux victimes que leur ordinateur était infecté et qu'il leur fallait appeler le «support Microsoft» au numéro indiqué. Les traces menaient d'abord au Maghreb, où étaient installés les faux opérateurs. Or en remontant les flux financiers, les enquêteurs sont parvenus à identifier les commanditaires français de cette escroquerie.

L'arnaque au faux support technique Microsoft aura bientôt dix ans. MELANI en a régulièrement parlé et continue à mettre en garde contre ce phénomène.[147] Des annonces de fraudes continuent pourtant à lui parvenir, et tout indique que les escrocs ne s'arrêteront pas en si bon chemin. On peut toutefois s'attendre à ce qu'au fil des poursuites pénales, toujours plus d'escrocs se fassent attraper.

6 Tendances et perspectives

6.1 Coûts dus à la cybercriminalité

Les experts s'accordent à dire que la cybercriminalité est en constante progression, pour des raisons qui elles aussi font l'unanimité. La numérisation croissante de toutes nos activités

144 https://www.europol.europa.eu/newsroom/news/goznym-malware-cybercriminal-network-dismantled-in-international-operation

145 MELANI, rapport semestriel 2018/2, chap. 5.5.1.

146 http://www.leparisien.fr/faits-divers/cybercriminalite-trois-chefs-d-entreprise-soupconnes-d-avoir-pirate-8-000-francais-31-01-2019-8001474.php

147 https://www.melani.admin.ch/melani/fr/home/meldeformular/formular0/meldeformularhaeufigefragen/mich-hat-eine-firma-angerufen-und-gesagt--dass-mein-computer-mit.html; https://www.melani.admin.ch/melani/fr/home/themen/fake_support.html

ouvre un vaste champ d'opportunités criminelles. Par contre, il est plus difficile de traduire en chiffres cette évolution, et a fortiori d'évaluer les dommages subis au niveau d'un pays ou sur le plan mondial. La difficulté d'obtenir des chiffres fiables tient principalement à l'existence, dans le domaine de la cybercriminalité, d'un important chiffre noir. Les délits ne sont pas toujours dénoncés ou signalés, et d'ailleurs il arrive que les victimes ne s'en rendent même pas compte. Il faut donc toujours prendre avec précaution les statistiques des coûts de la cybercriminalité, car il s'agit bien souvent de simples estimations ou d'extrapolations.

Indépendamment de ces difficultés, il est crucial pour les divers acteurs de la lutte contre la cybercriminalité, ainsi que pour leurs autorités politiques de tutelle, de disposer de données quantitatives, notamment pour planifier des mesures adéquates. Le présent chapitre résume plusieurs études sur la cybercriminalité, qui ont paru au semestre sous revue. Les chiffres donnent une idée de l'ampleur des phénomènes observés, voire indiquent certaines tendances de fond, lorsqu'on compare les résultats obtenus à l'aide des mêmes méthodes au cours de périodes différentes.

Les auteurs de l'étude intitulée «Measuring the Changing Cost of Cybercrime»,[148] présentée au 18e atelier sur l'économie de la sécurité de l'information (Workshop on the Economics of Information Security, WEIS) organisé en juin 2019 à Boston, ont procédé à une comparaison entre les chiffres et estimations actuels et ceux de leur première étude sur la question, remontant à 2012. Ils ont ainsi analysé systématiquement les coûts dus à la cybercriminalité, en se concentrant sur l'escroquerie. Au cours des sept années séparant les deux études, un changement de paradigme s'est produit sur le plan de l'accès aux ressources informatiques: les données sont toujours plus souvent sauvegardées dans le nuage, le smartphone a remplacé les ordinateurs, Android a supplanté Windows et la vie des gens se déroule toujours plus (aussi) en ligne et dans les médias sociaux. Avec pour effet qu'entre-temps, la moitié des infractions contre le patrimoine (en nombre comme en valeur) sont commises en ligne. Les auteurs signalent encore la forte recrudescence des attaques de la messagerie professionnelle (*Business E-Mail Compromise*, BEC) ainsi que des infractions liées aux cryptomonnaies. Par ailleurs, ayant constaté que les poursuites pénales n'ont pas la même efficience pour la cybercriminalité que pour les infractions classiques contre le patrimoine, ils recommandent de consacrer encore plus d'argent aux poursuites pénales qu'à la prévention et à l'anticipation. Car la prévention et l'anticipation ont beau être très importantes, le coût total des dégâts demeure excessif d'un point de vue financier.[149]

En ce qui concerne les rançongiciels, l'étude indique que les criminels auraient réalisé 16 millions de dollars de bénéfice en deux ans (2015-2017). On peut néanmoins considérer que le montant effectif des dommages (y c. les données perdues, les arrêts de production, le temps de rétablissement, etc.) constitue un multiple de cette somme.

Selon l'OTA (Online Trust Alliance) de l'Internet Society,[150] les cybercriminels ont adapté leurs activités afin de maximiser leurs gains. Les attaques dues aux seuls rançongiciels auraient causé 8 milliards de dollars de dégâts l'année dernière. L'OTA considère encore que d'ici

148 https://www.repository.cam.ac.uk/handle/1810/294492

149 https://www.inside-it.ch/articles/54646

150 https://www.internetsociety.org/fr/news/communiques-de-presse/2019/les-incidents-cybernetiques-ont-coute-40-milliards-deuros-en-2018-selon-lonline-trust-alliance-de-linternet-society/

2021, les coûts dus aux attaques de rançongiciels grimperont à 20 milliards de dollars et évalue les coûts totaux générés en 2018 par les cyberattaques à plus de 45 milliards de dollars.[151,152]

Les concepteurs du rançongiciel Ryuk auraient amassé, selon une étude de Crowdstrike, plus de 3 millions d'euros en trois mois. Alors même que Ryuk n'est pas un rançongiciel à la distribution massive, mais fait l'objet d'une implantation ciblée.[153]

La compromission de la messagerie professionnelle (*Business E-Mail Compromise*, BEC) est le second phénomène ayant le plus enrichi les escrocs. On y trouve des cyberattaques lancées contre des entreprises, au moyen de courriels renfermant une facture ou des instructions de paiement. En général, les escrocs falsifient l'adresse de l'expéditeur, ou bien ils utilisent des comptes de messagerie électronique compromis du service des finances de fournisseurs ou de partenaires commerciaux. Aux États-Unis, ils ont cherché dans trois quarts des cas à se faire virer de l'argent sur un compte américain alors qu'en Suisse, des comptes étrangers apparaissaient dans la plupart des cas observés. Les fraudes au virement signalées au FBI, soit les tentatives vaines ou fructueuses, ont atteint en moyenne mensuelle 301 millions de dollars en 2018. Il suffit donc qu'une part infirme des destinataires règlent les fausses factures ou exécutent les ordres de virement fictifs pour que les attaquants fassent une bonne affaire. L'étude montre que l'arnaque au président classique (où le service financier reçoit des instructions de paiement urgentes censées émaner du CEO)[154] est en recul et que les ordres de paiement falsifiés sont toujours plus souvent établis au nom de personnes externes (clients, fournisseurs, etc.). Soit les comptes de messagerie des personnes externes ont été piratés, soit l'adresse est simplement usurpée par *spoofing*, et donc le courriel comporte une fausse adresse d'expéditeur. La compromission de la messagerie professionnelle (BEC) est une activité lucrative, car les gains sont relativement élevés pour des risques et des frais plutôt faibles.[155]

Une autre étude provient de l'entreprise de sécurité Positive Technology.[156] Elle tente de chiffrer le prix de revient des attaques *APT*. Leurs auteurs, qui bénéficient d'un soutien étatique, peuvent parfois aussi être au service d'Etats aux moyens financiers plus modestes. À partir de l'analyse des instruments d'attaque utilisés, les chercheurs ont estimé ce qu'il a fallu débourser pour se procurer ou fabriquer de tels outils. Ils en concluent qu'un outil de phishing ciblé destiné à la pêche au harpon (*spear phishing*) revient à environ 2000 dollars. À cela s'ajoute un logiciel de tests de pénétration, pour un prix de 8000 à 40 000 dollars. Les outils nécessaires pour attaquer une banque coûteraient ainsi au moins 55 000 dollars. Par contre, une campagne de cyberespionnage implique une dépense d'au moins 500 000 dollars. De tels chiffres sont à manier avec prudence, sachant que le prix des outils d'attaque varie fortement. S'il a fallu les créer soi-même, l'estimation sera en général plus élevée, puisqu'il faut rétribuer les

151 https://www.hackread.com/cloud-hosting-provider-insynq-hit-by-megacortex-ransomware/

152 https://www.finanzen.ch/nachrichten/aktien/internet-societys-online-trust-alliance-reports-cyber-incidents-cost-$45b-in-2018-1028337623

153 https://www.lemonde.fr/pixels/article/2019/01/14/le-rancongiciel-ryuk-a-rapporte-plus-de-3-millions-d-euros-a-ses-auteurs_5408807_4408996.html

154 Voir ci-dessus, chap. 4.4.5.

155 https://www.fincen.gov/sites/default/files/shared/FinCEN_Financial_Trend_Analysis_FINAL_508.pdf

156 https://www.ptsecurity.com/ww-en/analytics/advanced-persistent-threat-apt-attack-cost-report/

connaissances techniques de pirates et de développeurs de logiciels. Par ailleurs, il existe des outils d'attaque légalement disponibles dans le commerce, dont se servent aussi les testeurs de pénétration recrutés dans ce contexte. Ils sont généralement moins chers et compliquent l'attribution des attaques à des *APT* spécifiques, étant donné que différents groupes ou nations emploient les mêmes outils.

En raison des incidents des dernières années et de la sensibilisation accrue à ces questions, toujours plus d'entreprises augmentent leur budget destiné à la cybersécurité. Il ressort d'une étude d'ESI ThoughtLab[157] que les cyberattaques ont occasionné durant la dernière année fiscale un dommage moyen de 4,7 millions de dollars par victime, avec même des pertes supérieures à 10 millions de dollars pour une entreprise sur dix. Les auteurs de cette étude ont enquêté auprès de différentes sociétés pour savoir si elles avaient été victimes d'une cyberattaque et si elles prévoyaient d'investir à l'avenir davantage dans la cybersécurité. Apparemment, les entreprises de la plupart des secteurs d'activité accroîtront sensiblement leurs investissements consacrés à la cybersécurité.

Appréciation:

La cybercriminalité est en plein essor car bien souvent, elle permet de s'enrichir avec des moyens relativement simples. Les cybercriminels n'ont besoin ni d'un capital de départ considérable, ni de vastes connaissances spécialisées, car il existe toujours plus de méthodes d'attaque commercialisées en tant que service (as a service, *aaS). Ainsi, des groupes de pirates proposent le modèle RaaS (ransomware as a service), que des escrocs peuvent acquérir et utiliser avec assez peu de connaissances pour réaliser de gros bénéfices ou pour infliger des dommages sévères à leurs victimes.

L'un des objectifs de la lutte contre la cybercriminalité est de mettre fin au modèle d'affaires choisi. Concrètement, il s'agit d'en faire grimper les coûts et de rendre les gains plus aléatoires, afin que les bénéfices fondent comme neige au soleil. Les cybercriminels opportunistes tentent de pénétrer dans les réseaux avec les moyens à disposition. Si l'entreprise prise pour cible est un tant soit peu protégée et si les outils standard utilisés n'ont pas eu d'emblée le succès escompté, ils vont rapidement voir ailleurs. Ce constat ne vaut évidemment pas pour les pirates soutenus financièrement par un État, dont la mission est en général de s'introduire dans un réseau bien précis, et donc qui peuvent investir beaucoup de temps et d'argent pour lancer leur cyberattaque.

6.2 Protection individuelle des données ou adoption de mesures par la société – où se situe le juste équilibre?

Dans notre quotidien tant personnel que professionnel, il va désormais de soi d'utiliser des technologies de chiffrement dont nous n'avions pas idée il y a quelques années seulement. Beaucoup de gens se servent par exemple pour communiquer de WhatsApp, dont la version actuelle utilise le protocole Signal pour le chiffrement de bout en bout des conversations. Autrement dit, les messages écrits n'apparaissent sous forme de texte clair que sur l'appareil de l'expéditeur et sur celui du destinataire. Les textes sont transmis par Internet sous une forme

157 https://www.helpnetsecurity.com/2019/07/15/boost-cybersecurity-investments/

chiffrée. À l'instar de la communication interpersonnelle, les connexions aux sites Web sont toujours plus souvent chiffrées. L'analyse des données télémétriques de Chrome[158] et Firefox[159] révèle qu'aujourd'hui, les liaisons établies à l'aide de ces navigateurs sont sécurisées dans 4/5 des cas par des certificats TLS. Il faut dire que les exploitants de sites Web peuvent se faire délivrer gratuitement des certificats, grâce à l'initiative «Let's Encrypt»[160] de l'organisation à but non lucratif Internet Security Research Group (ISRG).

Cette évolution en termes quantitatifs et qualitatifs des connexions chiffrées va encore se renforcer. C'est ainsi que l'année dernière, le groupe international Internet Engineering Task Force (IETF) a autorisé la version 1.3 du protocole de sécurité de la couche de transport (TLS 1.3).[161] De même, les requêtes sont toujours plus souvent chiffrées avant leur transmission au serveur *DNS*. Ainsi, Mozilla prévoit d'activer par défaut, pour son navigateur Mozilla Firefox, le protocole DNS over HTTPS (DoH).[162] Quant à l'actuelle version 9 d'Android, le système sélectionne autant que possible DNS over TLS (DoT),[163] et la nouvelle génération de téléphonie mobile 5G offre une meilleure protection contre les fausses antennes-relais de téléphonie mobile.[164]

Or tout en améliorant la confidentialité des liaisons au profit des utilisateurs de terminaux, ces perfectionnements court-circuitent parfois les mécanismes de protection établis face aux contenus criminels, ou les possibilités de surveillance des autorités de poursuite pénale. En effet, si les requêtes *DNS* chiffrées empêchent toute modification malveillante sur le chemin réseau, elles ne permettent pas non plus, selon le serveur interrogé, aux opérateurs Internet de transmettre des mises en garde face aux pages de phishing ou aux sites tentant de télécharger des *maliciels*. MELANI aussi soutient, par exemple, les administrateurs de listes noires afin que les internautes n'aboutissent pas à des pages de phishing[165] et ne divulguent pas involontairement, le cas échéant, leurs données d'accès à l'e-banking. Un problème similaire se pose avec la terminaison SSL, où des connexions chiffrées sont établies par l'intermédiaire d'un serveur *proxy* afin d'écarter les contenus malveillants, à l'instar des *maliciels*. Le protocole TLS1.3 entrave massivement, voire rend impossibles, les méthodes de protection et de surveillance ayant fait leurs preuves dans de nombreuses entreprises.

Les milieux représentant la poursuite pénale, en particulier, ont d'autant plus critiqué l'évolution vers un chiffrement accru[166] que les mécanismes actuels de protection face aux contenus criminels et de surveillance des criminels reposent sur certaines failles dans la structure des infrastructures. Il est toutefois problématique qu'au lieu de chercher des moyens de ne pas sacrifier, au nom de l'intérêt collectif, la sécurité des utilisateurs individuels des technologies, certains acteurs étatiques aient préféré interdire de nouvelles technologies ou prescrire la mise

158 https://transparencyreport.google.com/https/overview?hl=fr
159 https://letsencrypt.org/fr/stats/
160 https://letsencrypt.org/fr/about/
161 https://www.ietf.org/blog/tls13/
162 https://blog.mozilla.org/futurereleases/2019/04/02/dns-over-https-doh-update-recent-testing-results-and-next-steps/
163 https://android-developers.googleblog.com/2018/04/dns-over-tls-support-in-android-p.html
164 https://www.zdnet.com/article/stingray-spying-5g-will-protect-you-against-surveillance-attacks-say-standards-setters/
165 https://www.antiphishing.ch/fr/informations/
166 https://www.theregister.co.uk/2019/06/25/andrew_sullivan_internet_society_interview/

en place de portes dérobées. Il a longtemps été d'usage de dire que de telles mesures n'affectaient pas la sécurité des utilisateurs. Ce n'est que récemment que le ministre de la justice américain a admis que les mesures proposées pour permettre à l'État de protéger la société impliquaient inévitablement une perte de sécurité pour les utilisateurs finaux.[167]

À partir de là, il devient possible de discuter sur une base transparente, au sein d'une entreprise ou à l'échelon d'un État, des restrictions tolérables au niveau des personnes afin de réduire les risques communs encourus. À titre d'exemple, la terminaison SSL peut très bien être mise en place dans le respect de la protection des données personnelles, comme le montre la liste de contrôle établie par le Préposé zurichois à la protection des données pour le déchiffrement des connexions Internet.[168]

Toutes les organisations devraient mettre à profit, dans leur environnement informatique, les nouvelles technologies visant à renforcer la sécurité de l'infrastructure des personnes concernées, et n'introduire qu'avec circonspection des restrictions en la matière pour se protéger des contenus criminels. En faisant preuve d'intransigeance, elles ne feront qu'inciter les mécontents à contourner leurs mesures de précaution. Il s'agit donc de trouver le juste équilibre, afin que l'Internet de demain offre à tout le monde une sécurité optimale.

6.3 Vers une démondialisation des chaînes d'approvisionnement?

Imaginez le scénario suivant: en raison d'une erreur logicielle commise par un fournisseur, l'unité de commande des véhicules provoque, dans de rares cas, un dysfonctionnement du freinage. L'aveu a beau être embarrassant, un rapide rappel des modèles concernés de tous les fabricants automobiles utilisant la composante défectueuse restaurerait la confiance des clients en un quart d'heure, à l'aide d'une mise à jour logicielle effectuée au garage. Or une telle mise à jour est exclue pour la nouvelle voiture supposé européenne que vous avez achetée, en particulier après une réflexion approfondie sur la sécurité routière. Car l'équipementier a été soumis dans son pays d'origine, au nom de la sécurité nationale, à un régime de contrôle des exportations et ne peut malheureusement plus effectuer de transfert de technologie avec les entreprises dont la maison-mère a son siège en Chine.

Ce scénario peut paraître tiré par les cheveux, et pourtant des faits similaires se sont produits au premier semestre 2019 dans l'industrie de la communication. Le 16 mai 2019, le Bureau de l'industrie et de la sécurité (BIS), agence du Département du commerce américain, édictait un décret (*final rule*) plaçant le géant chinois des télécoms Huawei et ses filiales sur une liste d'organisations avec lesquelles tout transfert de biens et de savoir-faire est soumis à un régime de contrôle des exportations. Il est depuis lors interdit aux entreprises américaines d'entretenir des relations commerciales avec ces organisations, sans autorisation spéciale. Aussi l'entreprise Google annonçait-elle quelques jours plus tard qu'elle ne livrerait plus dans un proche avenir de mises à jour d'Android à Huawei, et qu'à plus ou moins long terme, les téléphones mobiles de cette entreprise ne feraient plus partie de l'écosystème Google. Les fabricants de

167 https://www.schneier.com/blog/archives/2019/07/attorney_genera_1.html

168 https://dsb.zh.ch/internet/datenschutzbeauftragter/de/publikationen/anleitungen/_jcr_content/contentPar/form/formitems/kein_titel_gesetzt__0/download.spooler.download.1562593220478.pdf/Checkliste-Entschluesselung-Webverbindungen.pdf

puces Intel, Qualcomm et Broadcomm devaient faire par la suite l'objet de déclarations analogues.

En réponse aux propos de ces fabricants de puces, Huawei a aussitôt promis à ses clients avoir constitué des stocks de matériel suffisants et disposer d'alternatives aux fournisseurs américains pour honorer les fournitures prévues, par exemple à Sunrise pour la mise en place de l'infrastructure du réseau 5G. Quant à la menace d'exclusion de la famille Android, le fabricant chinois de smartphones a notamment évoqué la possibilité de créer son propre système d'exploitation, et donc un nouvel écosystème.

Par leur ingérence, entretemps quelque peu reportée et atténuée, dans l'industrie informatique locale,[169] les autorités américaines ont donné une dimension planétaire à ce qui n'était au départ qu'un différend commercial bilatéral, faisant ressortir la vulnérabilité des chaînes d'approvisionnement mondialisées, dans l'industrie de la communication notamment. Si jusque-là les sanctions réciproques prises par la Chine et les États-Unis faisaient surtout craindre un renchérissement aux entreprises ainsi qu'à leurs clients établis dans le reste du monde, les utilisateurs suisses de produits et composants Huawei doivent désormais s'interroger sur la garantie des acquis et la durée de vie de leurs produits, sur leur maintenance et leur interopérabilité à l'avenir. Et plus généralement, on peut se demander si le fait qu'un État puisse ainsi se servir de sa puissance commerciale dominante ne constitue pas un précédent qui pourrait déboucher, dans un autre contexte, sur des actions similaires. Car l'hypothèse selon laquelle la politique de sanctions adoptée par les États-Unis face à Huawei est surtout motivée par des considérations économiques est difficile à écarter. Au-delà des incertitudes de planification et des coûts que la situation actuelle entraîne, il convient donc d'examiner, du moins à titre d'hypothèse, si un fabricant qui déplaît sans être forcément chinois ne s'expose pas à des mesures similaires.

Dans le secteur informatique comme dans presque toute la production industrielle, les chaînes d'approvisionnement mondiales sont devenues une manière courante d'organiser le travail. Les fournisseurs ne se limitent pas à une poignée de pays. Ainsi la société U-Blox à Thalwil, spin-off de l'EPF Zurich, est un leader mondial des puces de géolocalisation haute performance nécessaires au développement et à la production des véhicules autonomes. Or le principe de base de ces chaînes d'approvisionnement mondialisées veut que la technologie et le savoir-faire puissent se négocier, se combiner et s'utiliser selon les règles de l'économie de marché afin de fabriquer une large palette de produits finaux, et qu'au bout du compte ce soit le marché qui décide si de tels produits connaîtront le succès ou l'échec.

Les dysfonctionnements de ce système frappent de plein fouet les petites économies ouvertes comme celle de la Suisse qui, faute d'alternatives locales, ont besoin de fournisseurs étrangers et dont la propre industrie est tributaire de sa clientèle internationale pour ses activités en sous-traitance, dans un marché de l'offre et de la demande caractérisé par son ouverture et son interopérabilité au niveau mondial. Ce constat vaut dans une optique de prévisibilité et de sécurité des investissements, ou pour permettre d'opter, dans le cadre de la gestion des risques, pour un bon dosage de composants (d'infrastructure) relevant de la sphère d'influence de divers États.

[169] Voir aussi MELANI, rapport semestriel 2018/2, chap. 3.

La dynamique enclenchée en mai renferme cependant le risque d'une régionalisation de la chaîne d'approvisionnement à moyen ou long terme, et peu dans le pire des cas avoir comme conséquence que la sécurité de base de certains produits ne soit plus assurée. Ou par analogie à l'exemple précédemment évoqué: avant qu'une solution ne soit fournie par le producteur, ce n'est toujours que dans 1 cas sur 100'000 que les freins de la nouvelle voiture ne vont pas fonctionner parce qu'une ingérence dans la chaîne d'approvisionnement ne permet pas une solution rapide.

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	19.3009	Programme d'impulsion visant à diffuser des projets de numérisation innovants dans le domaine de la formation	CSEC-CN	21.02.2019	CN	CSEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193009
Mo	19.3010	Lancement d'un programme visant à donner un élan à la numérisation dans les universités fédérales et cantonales, dans les hautes écoles spécialisées et dans les domaines de la formation professionnelle et de la formation continue	CSEC-CN	21.02.2019	CN	DEFR	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193010
Ip	19.3051	Huawei et les défis de la 5G. Risques et chances pour la Suisse	Regazzi Fabio	06.03.2019	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193051
Mo	19.3121	Traitement des fuites de données au niveau national	Buffat Michaël	14.03.2019	CN	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193121
Po	19.3135	Acquisitions de l'armée. Avons-nous la maîtrise de la cybersécurité?	Dobler Marcel	18.03.2019	CN	DDPS	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193135
Po	19.3136	Infrastructures critiques. Avons-nous la maîtrise des composants matériels et logiciels?	Dobler Marcel	18.03.2019	CN	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193136
Ip	19.3139	Instituer des "attachés de cybersécurité" pour réduire les menaces informatiques	Müller Damian	18.03.2019	CE	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193139
Ip	19.3185	Achats de la Confédération. Pas de portes dérobées numériques	Vogler Karl	20.03.2019	CN	DDPS	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193185
Po	19.3199	Améliorer la sécurité des objets connectés	Reynard Mathias	21.03.2019	CN	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193199

Objet	Numéro	Titre	Déposé par	Date de dépôt	Conseil	Dép.	État des délibérations et lien
Ip	19.3205	Que fait le Conseil fédéral pour relancer la dynamique de la transition numérique?	Burkart Thierry	21.03.2019	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193205
Ip	19.3255	Défendre la démocratie libérale contre la montée de l'antisémitisme et de l'extrémisme de droite	Wermuth Cédric	21.03.2019	CN	DFI	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193255
Ip	19.3267	La pratique du service SCPT est-elle conforme à la loi en ce qui concerne les obligations des fournisseurs de services de communication dérivés?	Flach Beat	21.03.2019	CN	DFJP	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193267
Ip	19.3321	Le lancement en Suisse de la nouvelle technologie de téléphonie mobile qu'est la 5G requiert de la Confédération qu'elle informe dûment la population	Amman Thomas	22.03.2019	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193321
Ip	19.3330	Les données des patients vont-elles être vendues au plus offrant?	Reynard Mathias	22.03.2019	CN	DFI	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193330
Po	19.3342	Système de régulation de l'accès aux données publiques	Badran Jacqueline	22.03.2019	CN	DFI	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193342
Ip	19.3377	Différences cantonales dans les procédures pénales pour pédopornographie. Aucun besoin d'agir?	Guhl Bernhard	22.03.2019	CN	DFJP	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193377
Mo	19.3428	Nécessité d'améliorer la représentativité de l'organe consultatif du DEFR-DETEC "Transformation numérique"	Kälin Irène	07.05.2019	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193428
Ip	19.3431	Quels sont les avantages économiques et les conséquences sanitaires de la 5G?	Fiala Doris	07.05.2019	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193431
Mo	19.3448	Mainlevée provisoire. Prendre en compte l'évolution des pratiques commerciales (numérisation)	Dobler Marcel	08.05.2019	CN	DFJP	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193448
Ip	19.3461	Avancer seul ou à plusieurs dans le domaine de la cybersécurité?	Béglé Claude	08.05.2019	CN	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193461
Ip	19.3505	Attribution de concessions de téléphonie mobile pour la 5G alors que les autorités chargées de délivrer les autorisations ne disposent pas des bases légales nécessaires	Töngi Michael	09.05.2019	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193505

Objet	Numéro	Titre	Déposé par	Date de dépôt	Conseil	Dép.	État des délibérations et lien
Ip	19.3534	5G. Un groupe de travail planche sur l'impact des ondes éléctromagnétiques en Suisse, l'indépendance des membres est au moins aussi importante que leurs compétences	Borloz Frédéric	03.06.2019	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193534
Ip	19.3535	Lancement de la 5G en Suisse. Charge supplémentaire pour les cantons. Quelle compensation de la part de la Confédération?	Gschwind Jean-Paul	03.06.2019	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193535
Po	19.3574	Offensive pour un service public numérique	Marti Min Li	11.06.2019	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193574
Po	19.3593	Numérisation des collections de sciences naturelles au profit des chercheurs suisses	Germann Hannes	12.06.2019	CE	DEFR	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193593
Mo	19.3649	Base légale pour un fonds de numérisation	Savary Géraldine	18.06.2019	CE	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193649
Ip	19.3659	Le lancement par Swisscom de l'aspirateur à données Beem est-il conciliable avec la stratégie de propriétaire de la Confédération?	Marti Samira	19.06.2019	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193659
Mo	19.3663	Un conseil numérique, au nom du peuple!	Pardini Corrado	19.06.2019	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193663
Ip	19.3686	Déclaration de Tallinn relative à la cyberadministration. Où en est la Suisse et que reste-t-il à faire??	Groupe libéral-radical (RL)	19.06.2019	CN	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193686
Ip	19.3693	La numérisation, un grand défi	Fiala Doris	19.06.2019	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193693
Po	19.3759	Loi sur le crédit à la consommation. Exigences de forme compatibles avec la numérisation	Dobler Marcel	20.06.2019	CN	DFJP	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193759
Po	19.3785	L'illettrisme numérique conduit à l'exclusion sociale	Reynard Mathias	20.06.2019	CN	DFI	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193785
Ip	19.3787	Comment le Conseil fédéral lutte-t-il contre les propos haineux sur Internet?	Seiler Graf Priska	20.06.2019	CN	DFJP	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193787
Po	19.3850	Comment assurer une contribution efficace du secteur privé à des projets de développement et promouvoir les nouvelles technologies?	Béglé Claude	21.06.2019	CN	DFAE	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20193850

Objet	Numéro	Titre	Déposé par	Date de dépôt	Conseil	Dép.	État des délibérations et lien
Ip	19.3865	Genève internationale. Comment la Suisse peut-elle soutenir le développement numérique des organisations internationales et ONG tout en protégeant les données de victimes de guerres?	Derder Fathi	21.06.2019	CN	DFAE	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AfairId=20193865
Ip	19.3866	Un cybercommandement pour l'armée suisse?	Candinas Martin	21.06.2019	CN	DDPS	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AfairId=20193866
Po	19.3878	La 5G ne doit pas menacer la neutralité du Net	Béglé Claude	21.06.2019	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AfairId=20193878
Mo	19.3884	Une stratégie pour la souveraineté numérique suisse	Derder Fathi	21.06.2019	CN	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AfairId=20193884
Ip	19.3919	Intelligence artificielle et transformation numérique. Une stratégie holistique s'impose	Ricklin Kathy	21.06.2019	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AfairId=20193919
Pl	19.417	Perception d'une redevance sur les plateformes numériques destinée à aider les médias	Töngi Michael	21.03.2019	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AfairId=20190417
Pl	19.418	Pour un modèle destiné à aider les médias électroniques	Töngi Michael	22.03.2019	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AfairId=20190418
Q	19.5274	5G. Informer et expliquer pour éliminer certains préjugés	Regazzi Fabio	05.06.2019	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AfairId=20195274
Q	19.5286	Antennes 5G. Quelles sont les valeurs limites applicables?	Schneider Schüttel Ursula	05.06.2019	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AfairId=20195286
Q	19.5296	Comment éviter la 5G?	Schneider Schüttel Ursula	05.06.2019	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AfairId=20195296
Q	19.5315	La 5G est-elle déjà exploitée?	Hardegger Thomas	11.06.2019	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AfairId=20195315
Q	19.5349	5G. Et maintenant?	Bigler Hans-Ulrich	12.06.2019	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AfairId=20195349
Q	19.5355	5G. Des retards et des frais à la charge des milieux économiques?	Brunner Hansjörg	12.06.2019	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AfairId=20195355

Objet	Numéro	Titre	Déposé par	Date de dépôt	Conseil	Dép.	État des délibérations et lien
Q	19.5370	Beem	Masshardt Nadine	12.06.2019	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20195370

7.2 Étude comparative du CSS sur les stratégies nationales de cybersécurité – défis attendant la Suisse

Le Center for Security Studies (CSS) de l'EPF Zurich a publié en mars 2019 une étude comparative sur les stratégies nationales de cybersécurité de sept pays (Allemagne, Finlande, France, Israël, Italie, Pays-Bas et Suisse), où il parvient aux constats suivants.[170] De telles stratégies présentent en général des similitudes conceptuelles, à l'instar de leur approche holistique, couvrant tant la sécurité nationale que les questions socio-économiques, de la valeur accordée à la coopération internationale, de l'accent mis sur la collaboration avec le secteur privé, ainsi que du rôle central de la sensibilisation, de la formation et de l'information. Les principales différences concernent tant la place accordée à la cybersécurité dans les structures étatiques, que la répartition des responsabilités. Ainsi le degré de centralisation varie d'un pays à l'autre, tout comme les relations définies entre les forces civiles ou militaires. Ces différences relèvent essentiellement de la culture politique et de l'organisation des systèmes politiques.

Le CSS a encore identifié les défis se posant, au stade de l'élaboration des stratégies nationales ou de leur mise en œuvre. Il faut par exemple veiller à l'intégration verticale de la cybersécurité nationale dans le cadre de la sécurité nationale, ou à la coordination horizontale des divers services impliqués dans la cybersécurité. Les pays devront par ailleurs renforcer au niveau international la coopération ainsi que l'apprentissage de codes de conduite dans le cyberespace. Enfin, il faudra brosser des tableaux adéquats de la situation et prévoir une gestion efficace des crises.

7.3 Mise en œuvre de la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC)

Au cours des deux dernières années, le Conseil fédéral a pris des décisions fondamentales visant à protéger la Suisse contre les cyberrisques. En avril 2018, il a adopté la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) 2018-2022.[171] La SNPC entend contribuer à ce que tout en saisissant les chances offertes par le numérique, la Suisse soit protégée de façon appropriée contre les cyberrisques, et résiliente en cas de cyberincident. À partir de cette vision, la stratégie identifie sept objectifs stratégiques et formule au total, pour les atteindre, 29 mesures à prendre dans dix champs d'action.

À la différence de la première SNPC, qui concernait les années 2012 à 2017, la nouvelle stratégie englobe aussi le domaine de la cyberdéfense, qui précise le rôle de l'armée et du Service de renseignement dans l'attribution et la maîtrise des cyberattaques, tout en garantissant la

170 https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/MELANI%20Studie_final_AW_18März2019.pdf

171 https://www.isb.admin.ch/isb/fr/home/themen/cyber_risiken_ncs/ncs_strategie.html

disponibilité opérationnelle de l'armée. Par ailleurs, le groupe cible a été étendu à toute l'économie ainsi qu'à la société (la première stratégie se concentrait sur la protection des infrastructures d'importance vitale), tandis que la normalisation et la réglementation jouent un rôle accru, avec l'examen d'une obligation de notifier les cyberincidents. Grâce à ces adaptations, la SNPC peut mieux remplir sa fonction de stratégie globale, elle tient compte de l'aggravation des cyberrisques pour l'ensemble des entreprises et offre la base nécessaire à l'élaboration de futures normes et autres mesures de réglementation.

7.3.1 Plan de mise en œuvre et organisation de la Confédération dans le domaine des cyberrisques

Il est bien clair que la bonne mise en œuvre de l'ambitieux portefeuille de la SNPC dépendra de la coordination optimale des divers travaux, ainsi que de la mobilisation de l'ensemble des compétences disponibles. Les services fédéraux concernés, les cantons, les milieux économiques et les hautes écoles ont donc conçu ensemble le plan de mise en œuvre[172] de la SNPC, que le Conseil fédéral a adopté le 15 mai 2019.[173] Ce document précisant, pour chaque mesure, quelle organisation réalisera quels projets et dans quels délais, servira de base pour le contrôle de gestion stratégique de l'avancement de tous les travaux liés à la SNPC.

En plus d'élaborer un tel plan, la Confédération a réexaminé et adapté sa propre organisation[174]. La figure ci-après montre les éléments essentiels de cette organisation axée sur la mise en œuvre de la SNPC.

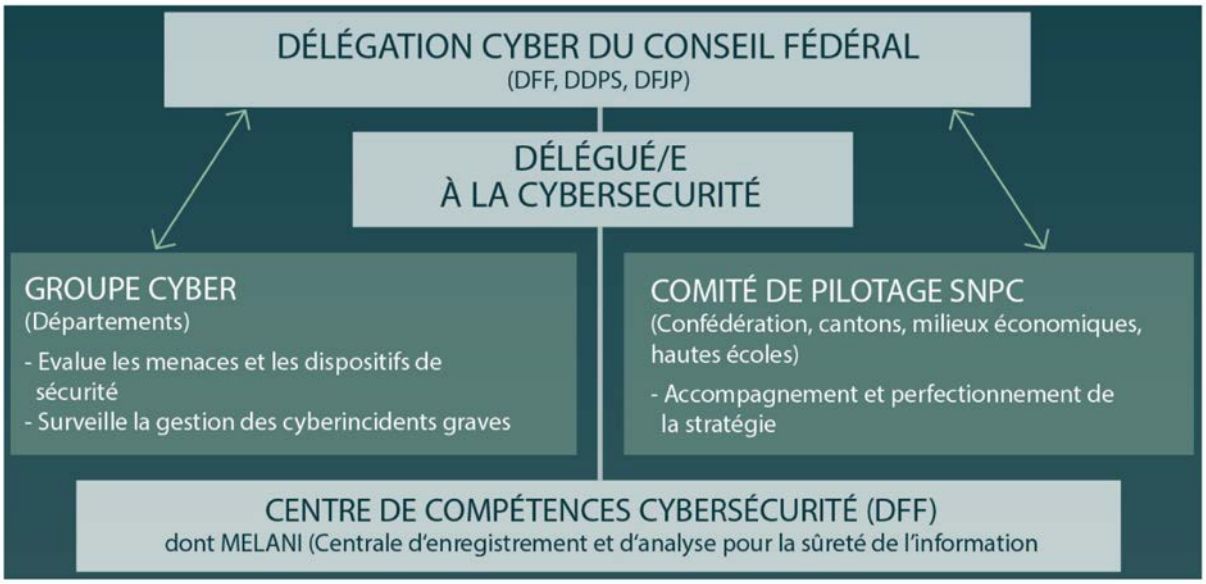

Figure 8: Organisation de la Confédération dans le domaine des cyberrisques

La nouvelle organisation mise tant sur le renforcement de la coordination interdépartementale que sur la collaboration avec les milieux économiques, les cantons et les hautes écoles. Divers comités ont été créés pour mener à bien ces tâches:

172 https://www.isb.admin.ch/isb/fr/home/themen/cyber_risiken_ncs/umsetzungsplan.html
173 https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-75046.html
174 https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-73839.html

- La **Délégation Cyber du Conseil fédéral,** composée des chefs du Département fédéral des finances (DFF), du Département fédéral de justice et police (DFJP) et du Département fédéral de la défense, de la protection de la population et des sports (DDPS), a pour tâche de surveiller la mise en œuvre de la SNPC.
- Le **groupe Cyber** renforce la coordination entre les trois domaines de la sécurité, de la défense et de la poursuite pénale, veille à leur évaluation conjointe de la menace et supervise la gestion par les services fédéraux des incidents graves et impliquant plusieurs départements.
- Le **comité de pilotage de la SNPC** assure la mise en œuvre coordonnée et ciblée des mesures de la SNPC et formule des propositions visant à son développement ultérieur.

7.3.2 Délégué à la cybersécurité et Centre de compétences pour la cybersécurité

Outre les autorités de coordination, deux structures centrales ont été créées, à savoir le poste de délégué à la cybersécurité et le Centre de compétences de la Confédération pour la cybersécurité. Le délégué à la cybersécurité exerce à l'échelon de la Confédération la direction stratégique de la cybersécurité, préside le Centre de compétences et les comités interdépartementaux créés par la Confédération (à l'exception de la Délégation Cyber) et représente la Confédération dans d'autres comités. La candidature de Florian Schütz a été retenue pour ce poste-clé[175]. Directement subordonné au chef du DFF, il a pris ses fonctions au début du mois d'août 2019.

Le Centre de compétences de la Confédération pour la cybersécurité, implanté au DFF, sert de guichet unique national pour les questions relatives à la cybersécurité. Il repose sur l'organisation actuelle de MELANI, qu'il renforce pour être à même d'offrir ses services à l'ensemble de l'économie et de diffuser parmi la population des messages d'alerte et des informations sur les cyberrisques. Il soutient par ailleurs de ses connaissances les offices fédéraux dans leurs activités de prévention, de normalisation et de réglementation. Il est enfin habilité à donner des instructions aux offices fédéraux, en cas de cyberincident.

En adoptant le plan de mise en œuvre de la SNPC, le Conseil fédéral a augmenté les ressources à disposition du Centre de compétences pour la cybersécurité, afin qu'il puisse élargir comme prévu, dès le 1er janvier 2020, les activités opérationnelles déployées jusque-là par MELANI.

Le prochain rapport semestriel MELANI décrira plus en détail le Centre de compétences de la Confédération pour la cybersécurité et ses tâches.

[175] https://www.efd.admin.ch/efd/fr/home/dokumentation/nsb-news_list.msg-id-75421.html

8 Produits publiés par MELANI

8.1 GovCERT.ch Blog

8.1.1 Severe Ransomware Attacks Against Swiss SMEs

09.05.2019 - As we have seen an ever-increasing number of ransomware cases that show a rather sophisticated modus operandi, we are publishing a warning via MELANI Newsletter along with this blog post, documenting technical details about the recent ransomware attacks against Swiss small and medium enterprises (SMEs). The goal of this blog post is to give you a better understanding of the various modus operandi of the most common ransomware families we have encountered hitting Swiss targets in the past months.

➔ https://www.govcert.admin.ch/blog/36/severe-ransomware-attacks-against-swiss-smes

8.2 Lettre d'information MELANI

8.2.1 Les Suisses victimes de sextorsion: les autorités lancent le site «stop-sextortion.ch»

24.04.2019 - Dans un courriel, des escrocs prétendent avoir pris le contrôle de l'ordinateur et de la webcam du destinataire et menacent de publier des images et des vidéos à caractère sexuel de celui-ci s'il ne verse pas une rançon. Dans cette arnaque, qui appartient au phénomène de la sextorsion, un paiement en bitcoins est généralement exigé. Bien que les sommes demandées soient modestes, cette méthode a permis à des criminels de soutirer des bitcoins pour une valeur avoisinant les 360 000 francs ces six derniers mois. En continuant de payer les rançons, les victimes encouragent l'utilisation de ce mode opératoire. Aidez-nous à enrayer ces arnaques en ne payant plus de rançons. Lancé aujourd'hui par les autorités, le site «stop-sextortion.ch» propose des informations sur ce thème et offre la possibilité de signaler des courriels frauduleux.

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

8.2.2 Les rançongiciels menacent de plus en plus les réseaux des entreprises

09.05.2019 - Depuis le début de l'année 2019, de nombreuses PME et grandes entreprises en Suisse et à l'étranger ont signalé que leurs données avaient été chiffrées et rendues inaccessibles par des chevaux de Troie appelés rançongiciels. Dans certains cas, les sauvegardes ont également été verrouillées, empêchant la reprise des activités des entreprises concernées.

➔ https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/verschluesselungstrojaner-greifen-vermehrt-gezielt-unternehmensn.html

9 Glossaire

Dénomination	Description
Advanced Persistent Threat (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.).
BGP Border Gateway Protocol	Protocole de routage externe utilisé pour l'échange d'informations entre différents réseaux.
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 programmes malveillants (*malicious bots*) peuvent diriger à distance les systèmes compromis et leur faire exécuter toutes sortes d'actions.
C2 Command & Control	Infrastructure de commande et de contrôle de réseaux de zombies. La plupart des machines zombies peuvent être surveillées et recevoir des instructions par un canal de communication.

Dénomination	Description
CaaS Cybercrime as a service	Le développement d'outils malveillants vendus «clés en main» permet à des criminels de mener des cyberattaques même sans compétences techniques.
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.
DNS	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).
drive-by download	Infection d'un ordinateur par un maliciel, lors de la simple visite d'un site Web. Différents exploits, tirant parti des lacunes de sécurité non comblées par le visiteur, sont souvent testés à cet effet.
Dropper / Downloader	Injecteur; programme conçu pour charger et activer un ou plusieurs programmes malveillants.
Failles de sécurité	Erreur inhérente au matériel ou aux logiciels, permettant à un pirate d'accéder au 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.
Internet des objets	Ensemble des objets branchés à Internet capables de communiquer pour collecter, transmettre et traiter des données, avec ou sans intervention humaine.

Dénomination	Description
ISP Internet Service Provider	Fournisseur d'accès à Internet, entreprise ou société fournissant aux utilisateurs finaux une connexion Internet et d'autres services réseau (boîte aux lettres, hébergement de contenu, etc.).
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.
Malspam	Courriel indésirable (spam) envoyé à grande échelle pour diffuser des maliciels.
Malware / Malicious code	Maliciel / 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).
Man-in-the-Middle attack (MITM)	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.
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.
MSP Managed Services Provider	Fournisseur de services d'infogérance, prestataire externe s'occupant de la totalité ou d'une partie de l'infrastructure informatique de ses clients.

Dénomination	Description
NAS Network Attached Storage	Serveur de stockage en réseau; serveur de fichiers autonome, relié à un réseau pour permettre à ses utilisateurs de stocker et de mettre en commun leurs données.
Patch	Rustine. Programme qui remplace une partie de programme comportant des erreurs par une partie exempte d'erreurs et remédie ainsi p.ex. à une lacune de sécurité.
Peer to Peer (P2P)	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.
Phishing	Hameçonnage. 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 (*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.
Protocole SMB	Server Message Block (SMB) est un protocole permettant le partage de ressources (fichiers, imprimantes, etc.) sur des réseaux locaux.
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.

Dénomination	Description
RaaS Ransomware as a service	Service vendu clés en main pour qu'un criminel puisse rançonner les utilisateurs informatiques même sans compétences techniques.
Ransomware	Maliciel utilisé comme moyen de chantage contre le propriétaire de l'ordinateur infecté. Typiquement, le pirate chiffre ou efface des données et ne fournit la clé nécessaire pour les sauver qu'après le versement d'une rançon.
Remote Administration Tool (RAT)	Un RAT (*Remote Administration Tool*, outil de télémaintenance) est un programme permettant la prise de contrôle totale, à distance, d'un ordinateur depuis un autre ordinateur.
Remote Desktop Protocol (RDP)	Protocole propriétaire, servant à la prise de contrôle à distance des postes Microsoft Windows.
Réseau de zombies	Plusieurs ordinateurs infectés peuvent former ensemble un réseau, dirigé par une infrastructure de commande et de contrôle (C&C).
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.
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. Une forme commune d'attaque de social engineering est le phishing.

Dénomination	Description
Spear Phishing	Pêche au harpon. La victime aura p. ex. l'illusion de communiquer par courriel avec une personne connue d'elle.
Spoofing	Action malveillante consistant à utiliser délibérément l'adresse d'un autre système au lieu de la sienne.
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 / Adresse IP	*Transmission Control Protocol* / *Internet Protocol*. Adresse identifiant l'ordinateur sur Internet (ou dans un réseau TCP/IP) (exemple : 172.16.54.87).
Top-Level-Domain (TLD)	Chaque nom de domaine est formé d'une suite de signes, séparés par des points. Le domaine de premier niveau (TLD) est toujours situé à l'extrême droite du nom Internet. Par exemple, dans l'adresse http://www.melani.admin.ch, le TLD est «ch». Quand il correspond à un code de pays, représenté par des abréviations à deux caractères, on parle de domaine national (ccTLD).
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	À 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.

Dénomination	Description
Watering Hole Attack	Attaque dite du point d'eau, attaque ciblée par un maliciel, diffusé à travers des 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.