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 2018/I (janvier à juin)

8 NOVEMBRE 2018

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

1 Aperçu / Sommaire

2 Éditorial

Dr. Bruce Nikkel
Responsable Cybercrime Intelligence & Forensic Investigation, UBS
Président de l'European FI-ISAC
Professeur d'informatique légale, Haute école spécialisée bernoise

Chère lectrice, cher lecteur,

D'un point de vue historique, la Suisse s'est construite sur des relations de confiance entre les différents cantons, qui ont uni leurs forces pour faire face aux menaces. Cet exemple de confiance entre divers groupes d'intérêt résulte d'une évolution durable vers une société sûre. Dans le monde numérique d'aujourd'hui, la confiance continue de jouer un rôle central. En effet, une collaboration basée sur la confiance au sein de groupes visant les mêmes buts est devenue essentielle dans tous les secteurs de l'industrie. Les buts de ces groupes sont d'endiguer et de lutter contre les cybermenaces et la cybercriminalité.

Il existe des groupes ad hoc, dont les membres se rencontrent de manière informelle pour discuter des menaces techniques et des solutions envisageables. En outre, les services gouvernementaux et les entreprises constituent des groupes de confiance plus formels: notamment les ISAC (*Information Sharing and Analysis Centers*) et les CERT (*Computer Emergency Response Teams*). En Suisse, la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) a organisé la coordination de groupes d'exploitants d'infrastructures d'importance vitale dans différents secteurs tels que ceux de l'énergie, des télécommunications ou encore de la finance. Au sein de ces groupes, des entreprises concurrentes joignent leurs forces pour atteindre un objectif commun supérieur, contribuant ainsi à la sécurité de la société.

Les cybermenaces ne s'arrêtent pas aux frontières. Aussi est-il primordial de collaborer également avec des personnes et des communautés hors de la Suisse. C'est là le point de départ de nombreuses initiatives internationales qui sont fondées sur la confiance et dont le but est d'analyser, ensemble, les menaces d'un point de vue mondial. MELANI et plusieurs autres organisations suisses participent à ces initiatives internationales. Ces groupes se composent généralement de représentants de l'industrie, de CERT étatiques (comme MELANI), des autorités de poursuite pénale et de spécialistes de la sécurité.

La sécurité de notre société numérique repose sur la collaboration formelle et informelle, tant au niveau national qu'international. Il faut donc continuer de favoriser et de développer cette collaboration car, seule, une organisation ne peut pas juguler les cybermenaces et la cybercriminalité. La coopération entre des entreprises et des organisations concurrentes, de même qu'entre le secteur public et le secteur privé, est d'une importance capitale, et la confiance entre les individus est la clé du succès. Or, cette confiance nécessite de soigner et de développer sans cesse les relations entre les entreprises et les organisations de part et d'autre des frontières. La participation de MELANI au développement et à la coordination de groupes dignes de confiance est très précieuse et améliore la sécurité de notre monde numérique.

Dr. Bruce Nikkel

3 Thème prioritaire: vulnérabilités du matériel informatique

3.1 Spectre et Meltdown

Dans le domaine informatique, la gestion des vulnérabilités fait désormais partie intégrante du quotidien. Des failles de sécurité sont publiées chaque semaine. Or toutes n'ont pas le même degré de gravité, beaucoup n'ayant que des effets mineurs ou alors très spécifiques. On a surtout parlé des vulnérabilités pouvant être exploitées à distance, et donc par n'importe quel utilisateur de l'Internet («remote code execution»). Les dommages potentiels sont très graves en pareil cas. La vulnérabilité Heartbleed ou le maliciel Wannacry, qui exploite une lacune du protocole SMB, en sont de bons exemples. Par chance, les mises à jour logicielles ne tardent généralement pas à être fournies après la publication des failles, les éditeurs s'étant organisés en conséquence, et ayant optimisés leurs processus visant à combler les failles de sécurité. Or que se passe-t-il si une faille est due non pas à des logiciels mais au matériel? Il y avait bien eu des précédents, comme le Bug de la division du Pentium[1] en 1994 ou encore Rowhammer en 2014[2]. Cette lacune permettait d'altérer le contenu de certaines puces mémoire RAM, en accédant de façon répétée à certaines zones de stockage. Les interactions électriques ainsi produites modifiaient les bits des données dans les zones voisines. Les failles matérielles Spectre et Meltdown, rendues publiques pendant la première semaine de janvier 2018, portaient toutefois bien plus à conséquence.[3] Une erreur de conception donne à un pirate la possibilité de lire les données stockées sur un processeur. Une simple mise à jour logicielle ne permet pas de remédier à de telles erreurs.

3.2 D'où venait cette erreur de conception?

Soucieux d'accélérer les applications, les fabricants de processeurs ont eu l'idée suivante: les processeurs font des spéculations sur la nature de la prochaine instruction puis l'exécutent et enregistrent le résultat («speculative execution» et «out of order execution»). Si cette spéculation s'avère inexacte, les résultats seront rejetés. Dans le cas contraire, le résultat est plus rapidement disponible. Les ordinateurs sauvegardent les instructions et données régulièrement utilisées dans une mémoire cache. Cette dernière est directement implémentée sur le microprocesseur, afin de garantir un accès rapide. Pour un attaquant, l'accès aux données convoitées peut être facilité. Une donnée se trouvant déjà dans le cache sera plus rapidement lue que si elle devait être nouvellement calculée.

En vue d'accéder à des informations protégées, l'attaquant profite du fait que des informations sur lesquelles il n'a aucun droit vont également se trouver dans la mémoire. Ce n'est que lorsque le besoin d'un résultat correspondant, se fait sentir que des vérifications interviennent. Faute des droits nécessaires, l'opération sera interrompue par un message d'erreur mais les informations correspondantes restent stockées pendant une brève période dans la mémoire cache, du moins si ces dernières n'ont pas encore été écrasées.

---

1 https://fr.wikipedia.org/wiki/Bug_de_la_division_du_Pentium (état: le 31 juillet 2018).

2 https://fr.wikipedia.org/wiki/Martèlement_de_mémoire (état: le 31 juillet 2018).

3 https://meltdownattack.com (état: le 31 juillet 2018).

La procédure s'emploie depuis 20 ans. Elle aboutit à une plus grande performance de calcul, et donc à des économies de temps. Il y a 20 ans, les ordinateurs étaient principalement des systèmes fermés. A l'époque de l'informatique en nuage et des systèmes virtuels, cette vulnérabilité est d'autant plus grave qu'elle est découverte alors que désormais de nombreux utilisateurs accèdent à un même processeur. En particulier, les prestataires de services informatiques en nuage se sont d'autant plus empressés de corriger cette faille que plusieurs systèmes virtuels s'y partagent le même matériel.

Mais la plupart des ordinateurs, serveurs, smartphones ou tablettes sont concernés. Quasiment tous les utilisateurs de tels appareils risquent ainsi, d'une manière ou d'une autre, de faire les frais de cette vulnérabilité. Les systèmes infectés sont à la merci des agresseurs qui, à partir des processeurs, ont largement accès aux informations qu'ils renferment. Les systèmes utilisés par différentes personnes sont les plus exposés.

3.3 Approche

Lorsqu'un appareil est potentiellement dangereux, il est d'usage que le fabricant le rappelle. Dans l'industrie automobile, les rappels de véhicules en vue du changement d'une pièce défectueuse sont monnaie courante. Ce n'est toutefois pas transposable à l'informatique, où l'échange de la composante matérielle problématique est un défi. Un échange a cependant eu lieu lors du Bug de la division du Pentium en 1994, sous la pression des utilisateurs. Aujourd'hui le nombre d'appareils concernés, avec l'effort logistique nécessaire, serait bien plus grand. En outre, des erreurs d'installation seraient à craindre. Car loin d'être normés comme dans l'industrie automobile, les systèmes font l'objet de configurations très différentes. Les fabricants de processeurs ont donc privilégié les mises à jour des logiciels et des microcodes (qui gèrent les processus du processeur). Une telle approche semble à première vue paradoxale pour corriger une défaillance matérielle. Concrètement, les mises à jour réduisent par exemple la précision de la résolution temporelle ou désactivent partiellement les zones où les processeurs procèdent aux calculs préalables et à l'accélération qui s'ensuit. On corrige ainsi l'erreur à distance, au prix d'une baisse de performance du processeur. Cette péjoration devra être compensée par une puissance de calcul accrue. L'approche choisie ne convient donc pas pour une solution à long terme.

Il faudra donc à l'avenir revoir la conception des microprocesseurs, et plus généralement l'architecture des processeurs. Cela prendra sans doute des années. Le processeur est au cœur des systèmes actuels, dont il constitue l'élément le plus optimisé. La mémoire et la communication sont actuellement au service du processeur[4]. Dans une nouvelle architecture, il faudrait mieux intégrer au système la mémoire et donc la sûreté de l'information, selon une approche axée sur la sécurité dès le stade de la conception («security by design»). La question qui se pose est celle de la méthode choisie pour atteindre un meilleur niveau de sécurité dans le développement des éléments matériels (hardware).

[4] https://www.netzwoche.ch/storys/2018-03-07/wie-meltdown-und-spectre-zukuenftige-computerarchitekturen-beeinflussen (état: le 31 juillet 2018).

3.4 Développements possibles

Spectre et Meltdown ont suscité un vaste débat sur les failles matérielles. Au niveau mondial, toujours plus de chercheurs étudient la question, afin de découvrir d'autres vulnérabilités. Huit nouvelles failles exploitables selon la même méthode que Spectre et Meltdown ont ainsi été rendues publiques en mai, sous le nom de Spectre-NG (NG signifiant «next generation»).[5] Parmi celles-ci se trouve notamment Foreshadow alias L1 Terminal Fault, par laquelle un attaquant peut, depuis une machine virtuelle, accéder à une zone de mémoire protégée d'une autre machine virtuelle se trouvant sur la même machine. En juillet 2018, trois autres vulnérabilités ont été divulguées: ret2spec, SpectreRSB et NetSpectre.

Tout indique que d'autres vulnérabilités matérielles seront découvertes. En effet, la plupart des systèmes informatiques actuels reposent sur des développements datant d'il y a plus de 20 ans. Pour des raisons de compatibilité, les systèmes et architectures n'ont jamais été remaniés de fond en comble. On a préféré perfectionner ce qui existait, alors même que le système et l'architecture n'avaient pas toujours été pensés pour les nouvelles fonctions. Dans un domaine aussi dynamique que l'informatique, les conséquences d'un tel choix se feront toujours plus sentir quand de nouvelles failles surgiront. À la différence des logiciels, des échanges de matériel au niveau mondial sont irréalistes. Le véritable défi consistera donc à réduire les risques dus à de telles vulnérabilités et à s'accommoder des baisses de performance ainsi occasionnées.

Recommandation:

INFO

Recommandations concernant les vulnérabilités du matériel informatique sur le site web MELANI:

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

[5] https://www.heise.de/ct/artikel/Super-GAU-fuer-Intel-Weitere-Spectre-Luecken-im-Anflug-4039134.html (état: le 31 juillet 2018).

4 Situation nationale

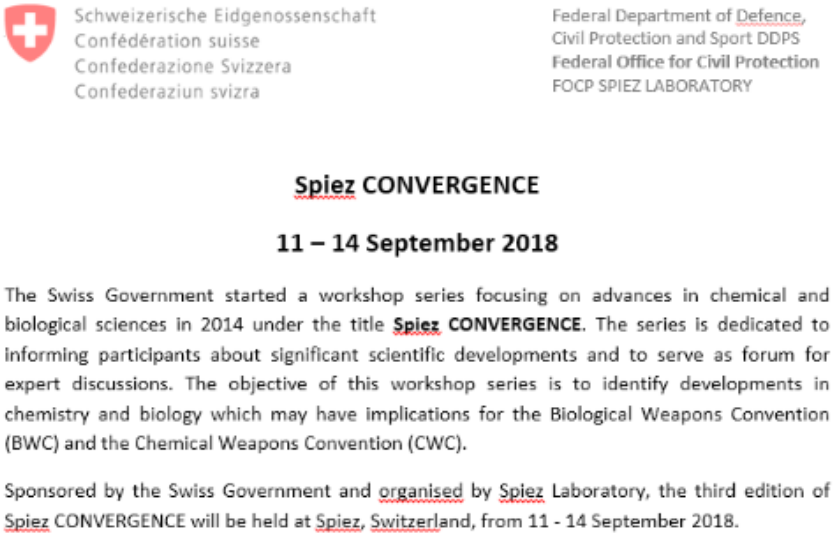
4.1 Espionnage

4.1.1 Envoi d'Olympic Destroyer au nom du laboratoire de Spiez

Le 19 juin 2018, l'entreprise de cybersécurité Kaspersky a publié un rapport sur Olympic Destroyer, maliciel ayant sévi durant les jeux olympiques d'hiver de Pyeongchang, en Corée du Sud. Ce ver doté de fonctions de sabotage avait lancé pendant la cérémonie d'ouverture une attaque contre l'infrastructure de l'organisateur. Divers experts en sécurité ont pensé à une opération sous fausse bannière (false flag operation) et soupçonné l'agresseur de vouloir faire porter le chapeau à un tiers (ici la Corée du Nord). L'implication de la Corée du Nord, plausible à première vue, était fausse, ce qui a montré une fois de plus les difficultés d'attribution d'une cyberattaque. Entre-temps, Kaspersky a démontré les liens d'Olympic Destroyer avec le groupe de pirates Sofacy (voir chapitre 5.1.1).

Des courriels d'hameçonnage ciblé (spear phishing) ont été découverts en mai et juin 2018. Les documents annexés reprenaient certains éléments d'Olympic Destroyer, qui avait sévi trois mois plus tôt. Selon Kaspersky, les attaques visaient des organisations financières basées en Russie, ainsi que des laboratoires de prévention des menaces biochimiques. Lorsqu'un destinataire ouvre le courriel, le maliciel cherche à infecter son ordinateur et à l'ajouter à un réseau de bots. L'infection est complexe et combine différentes technologies comme VBA, Powershell et MS HTA, avec un code JavaScript. Kaspersky a publié les détails techniques dans un billet de blog[6]. Aucune action de sabotage n'a été observée à cette occasion. Dans un cas d'attaque ciblée, pour amener leurs victimes à cliquer sur l'annexe, les agresseurs ont plagié une invitation à une conférence internationale lancée par le laboratoire de Spiez. Ils ont ensuite envoyé leur courriel à diverses adresses, au nom de l'Office fédéral de la protection de la population (OFPP). Les serveurs de l'administration fédérale n'ont été impliqués à aucun moment dans cette cyberattaque. Les pirates ne s'en sont pas pris au laboratoire de Spiez, contrairement à ce qu'ont insinué certains médias. Son nom a seulement été utilisé de manière abusive pour dissiper la méfiance des destinataires de l'envoi.

6 https://securelist.com/olympic-destroyer-is-still-alive/86169/ (état: le 31 juillet 2018).



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence,
Civil Protection and Sport DDPS
Federal Office for Civil Protection
FOCP SPIEZ LABORATORY

Spiez CONVERGENCE

11 – 14 September 2018

The Swiss Government started a workshop series focusing on advances in chemical and biological sciences in 2014 under the title **Spiez CONVERGENCE**. The series is dedicated to informing participants about significant scientific developments and to serve as forum for expert discussions. The objective of this workshop series is to identify developments in chemistry and biology which may have implications for the Biological Weapons Convention (BWC) and the Chemical Weapons Convention (CWC).

Sponsored by the Swiss Government and organised by Spiez Laboratory, the third edition of Spiez CONVERGENCE will be held at Spiez, Switzerland, from 11 - 14 September 2018.

Figure 1: Courriel frauduleux expédié au nom de l'Office fédéral de la protection de la population (OFPP) (source: Kaspersky)

Les 12 et 14 mars 2018, des courriels d'hameçonnage ciblé refermant une prétendue invitation à une conférence internationale ont été envoyés selon le même mode opératoire à des organisations gouvernementales européennes. Le courriel contenait un document Word intitulé «Defence & Security 2018 Conference Agenda.docx». Là encore, les pirates avaient directement recopié le programme du site Internet, avant de l'envoyer à des participants potentiels à la conférence. En l'occurrence, le document renfermait un objet Flash avec un script d'action qui cherchait à télécharger le maliciel (charge virale, «payload»). Cette attaque avait pour particularité que la composante ne s'activait que lorsque la victime parvenait à la troisième page du document[7]. Une telle méthode avait vraisemblablement été choisie pour rendre l'attaque indétectable. Les experts en cybersécurité de l'entreprise PaloAltoNetworks pensent que le groupe Sofacy en serait l'auteur[8].

Appréciation:

Les attaques ciblées reposent souvent sur une invitation à une conférence. Premièrement, les informations correspondantes sont publiques, et donc accessibles aux attaquants. Ils peuvent ainsi lancer de véritables attaques chirurgicales, puisque seules les personnes travaillant dans le secteur s'intéresseront à l'invitation. Deuxièmement, les pirates s'épargnent de fastidieuses recherches. L'histoire est authentique, et l'envoi ne contient généralement pas d'erreur linguistique ou de contenu.

7 https://www.zdnet.com/article/hackers-are-using-a-flash-flaw-in-fake-document-in-this-new-spying-campaign/ (état: le 31 juillet 2018).

8 https://researchcenter.paloaltonetworks.com/2018/03/unit42-sofacy-uses-dealerschoice-target-european-government-agency/ (état: le 31 juillet 2018).

4.2 Systèmes de contrôle industriels

4.2.1 Systèmes ouverts en ligne – menace ou «courant normal»?

L'interconnexion croissante ainsi que la pénétration de l'informatique dans pratiquement tous les domaines de l'existence ouvrent d'énormes potentiels économiques et sociaux, auxquels un pays hautement développé et industrialisé comme la Suisse ne peut renoncer. Or la numérisation croissante comporte aussi de nouveaux risques.

Les systèmes de contrôle industriels qui, jusque-là, étaient exploités de manière isolée sont toujours plus souvent reliés à Internet. Cette mise en réseau offre de nombreux avantages. Pourtant, tous ces appareils n'ont pas été conçus dans cette optique, et une bonne partie possèdent encore des systèmes d'exploitation désuets et n'étant plus pris en charge. Diverses mesures de sécurité s'imposent par conséquent, afin d'en garantir le bon fonctionnement.

Quelques systèmes reposent sur des fonctions centrales et importantes, mais qui sont vulnérables pour des raisons historiques ou bien qui n'avaient pas été conçues pour des systèmes d'importance vitale. Il est d'autant plus important d'identifier et de corriger leurs failles éventuelles. Les approches collaboratives aident à découvrir les dysfonctionnements au moyen d'analyses heuristiques. L'Office fédéral de l'armement (armasuisse) a présenté une telle solution en février 2018. Toujours plus de services utilisent les signaux GPS. Les drones, les hélicoptères et même les avions s'en servent pour la navigation. Des pirates pourraient par exemple faire dévier des drones de leur cap, en émettant des signaux destinés à perturber ou à leurrer leurs systèmes. Pour prévenir de telles tentatives, un système pionnier, appelé Crowd-GPS-Sec[9], surveille en permanence l'espace aérien à l'aide de signaux numériques relatifs à la navigation aérienne émis par des avions et des drones. Les chercheurs parviennent à détecter les faux signaux GPS en quelques secondes, à l'aide d'algorithmes d'un type nouveau. Il leur suffit ensuite de quelques minutes pour localiser l'attaquant à quelques mètres près.

Des objets quotidiens aussi sont toujours plus souvent raccordés au réseau interne ou à Internet. À l'instar des webcams, des commutateurs d'éclairage intelligents, des réfrigérateurs ou des téléviseurs connectés, qui possèdent toujours plus souvent une interface réseau. Cela engendre une hausse non seulement des utilisateurs du réseau, mais également du nombre d'appareils susceptibles d'être piratés. Le problème tient notamment aux appareils ouverts au premier venu et non protégés, dont il est possible d'exploiter les failles de sécurité à partir d'Internet. Le moteur de recherche Shodan repère de tels systèmes et permet de dresser pour chaque pays une carte d'exposition aux risques. Selon Shodan, 478 systèmes de contrôle industriels seraient visibles de l'extérieur en Suisse, et Heartbleed demeure la principale faille de sécurité exploitable à distance[10]. On y apprend encore que 405 appareils équipés de la fonction Smart Install Client de Cisco (outil servant à installer de nouveaux commutateurs Cisco) seraient publiquement accessibles (voir aussi chapitre 5.1.5).

---

9 https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-69896.html (état: le 31 juillet 2018).

10 La date de référence était le 31 août 2018.

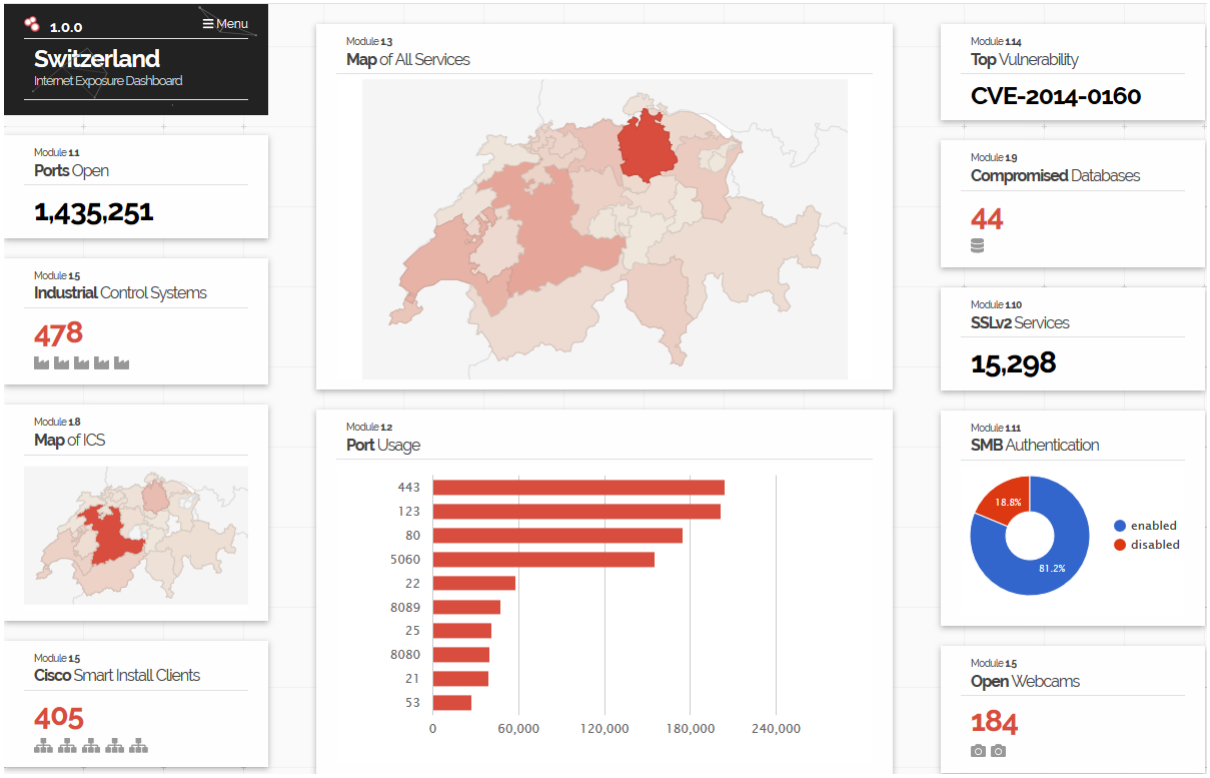


Figure 2: Aperçu des systèmes vulnérables et accessibles depuis Internet en Suisse (source: https://www.shodan.io/. La date de référence était le 31 août 2018)

Les pirates disposent d'instruments toujours plus sophistiqués pour exploiter de telles failles de sécurité sans grandes connaissances professionnelles. Un nouvel outil appelé Autosploit a fait les gros titres en début d'année. Il fait appel à la fois au moteur de recherche Shodan et à Metasploit, module de développement et d'exécution d'exploits contre une machine cible. La combinaison de ces deux services permet de s'engouffrer automatiquement et sans connaissances particulières dans les systèmes vulnérables. Le programme commence par rechercher dans Shodan un service spécifique, comme un serveur Apache ou IIS (Internet Information Services) de Microsoft. Une autre commande déclenche ensuite les attaques. Le script sélectionne automatiquement les exploits adéquats dans la bibliothèque Metasploit.

Jusqu'alors, l'énergie criminelle ne suffisait pas: il fallait de solides connaissances informatiques. Tel n'est plus le cas avec ce genre d'outils, qui élargissent considérablement le cercle des malfaiteurs potentiels.

Il est difficile parfois d'évaluer jusqu'à quel point les systèmes ouverts revêtent une importance vitale, et le cas échéant dans quelle mesure des systèmes sensibles risquent d'être manipulés[11]. Il y a deux ans, des hackers avaient publié à leur Chaos Communication Congress (CCC) de nombreuses copies d'écran de systèmes dans lesquels ils prétendaient s'être introduits – dont l'approvisionnement en eau d'une petite commune suisse. Or une analyse minutieuse du cas et une demande à la commune ont révélé que si cet accès n'était pas publié, les citoyens intéressés étaient autorisés à voir lesdites données. Les graphiques indiquaient quelle quantité d'eau provenant de chaque source alimente le réservoir. On n'y

11 https://www.suedostschweiz.ch/zeitung/wasserwerk-wurde-gehackt (état: le 31 juillet 2018).

voyait cependant pas de données d'importance vitale, et aucune manipulation n'était possible à distance.

Appréciation / Recommandation:

Les objets et appareils reliés à Internet pouvant être détectés par n'importe qui (notamment grâce à un outil d'exploration des ports (portscan) ou à un moteur de recherche comme Shodan), il s'agit d'une cible facile pour les cyberattaques. Tous les appareils reliés à Internet doivent être dûment protégés (mot de passe individuel, accès restreint) et faire l'objet d'actualisations régulières. Il est important de reprendre rapidement les mises à jour disponibles. Or à la différence des ordinateurs de bureau et des smartphones, presque personne ne songe à effectuer, le cas échéant, les mises à jour requises par son interrupteur intelligent ou par son réfrigérateur.

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

La norme minimale pour améliorer la résilience informatique comprend diverses fonctions: identifier, protéger, détecter, réagir et récupérer. Elle donne aux utilisateurs 106 indications concrètes pour améliorer la résilience de leurs technologies de l'information et de la communication face aux cyber-risques:

La norme minimale pour améliorer la résilience informatique

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

Recommandation

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

Formulaire d'annonce MELANI

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

Mesures de protection des systèmes de contrôle industriels (SCI)

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

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

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

4.3.1 Activités d'Apophis Squad en Suisse

Apophis Squad est un groupe qui s'est fait connaître en revendiquant de fausses alertes à la bombe contre des écoles américaines et anglaises en mars et avril 2018.

En juin 2018, le groupe a de nouveau fait parler de lui. Sur Twitter, le groupe s'attribue de nombreuses attaques DDoS qui permettent de rendre des sites indisponibles. Il promeut ainsi son service de «booter» (ou «stresser»). Alors que, bien souvent, ces attaques restent de relativement courte durée, celle qui a touché Protonmail (un service d'e-mail sécurisé basé en suisse) a duré plusieurs jours et a engendré des périodes d'inaccessibilité au système. Cet acharnement est peut-être dû à la réaction d'un des responsables de l'entreprise, qui avait provoqué les attaquants en les traitant de «clowns» sur son compte Twitter. Ces différentes activités ne sont pas restées sans suites légales, puisqu'elles ont donné lieu à une arrestation à la fin de mois d'août 2018.

Mais ces attaques et leur écho médiatique ont semble-t-il motivé des opportunistes à utiliser le nom Apophis Squad à des fins de chantage à l'attaque DDoS. En août, de nombreuses entreprises du secteur de la finance ont ainsi subi une tentative d'extorsion au nom d'Apophis Squad. Dans le courriel qu'elles ont reçu, il était clairement fait allusion aux «exploits» passés du groupe. Si le destinataire de ce courriel ne payait pas la somme très spécifique de 2,01 bitcoin dans les délais, il essuierait une violente attaque DDoS. Le premier courriel était suivi de différents rappels. Rapidement, plusieurs éléments ont poussé MELANI à retenir l'hypothèse d'un opportuniste qui souhaiterait profiter de la réputation d'Apophis Squad, sans avoir l'intention ou même la capacité de mener une attaque. En effet, les mêmes adresses bitcoin étaient fréquemment utilisées, rendant impossible de remonter à l'origine d'un éventuel paiement. Par ailleurs, Apophis Squad avait écrit sur Twitter que des imitateurs («copycats») étaient à l'œuvre et que leur mode opératoire ne correspondait pas au sien.

À la date prévue de l'attaque, rien ne s'est passé. MELANI avait donc raison. Pour une entreprise, un bon niveau de préparation reste cependant nécessaire, car de nombreux autres groupes peuvent mener des attaques DDoS.

Recommandation

DOCU

Une liste de mesures permettant de faire face aux attaques DDoS est disponible sur le site Web de MELANI.

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

4.4 Social Engineering et phishing

Les attaques les plus fructueuses sont celles qui reposent sur une histoire crédible pour inciter la victime à faire ce qu'on lui demande. Elles fonctionnent d'autant mieux que l'escroc détient de nombreuses informations sur sa victime potentielle. Les malfaiteurs puisent dans les sources publiques et utilisent des informations qu'ils ont dérobées. Les données volées sont triées, reliées à d'autres données dérobées ou publiques, traitées puis revendues.

4.4.1 Hameçonnage

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

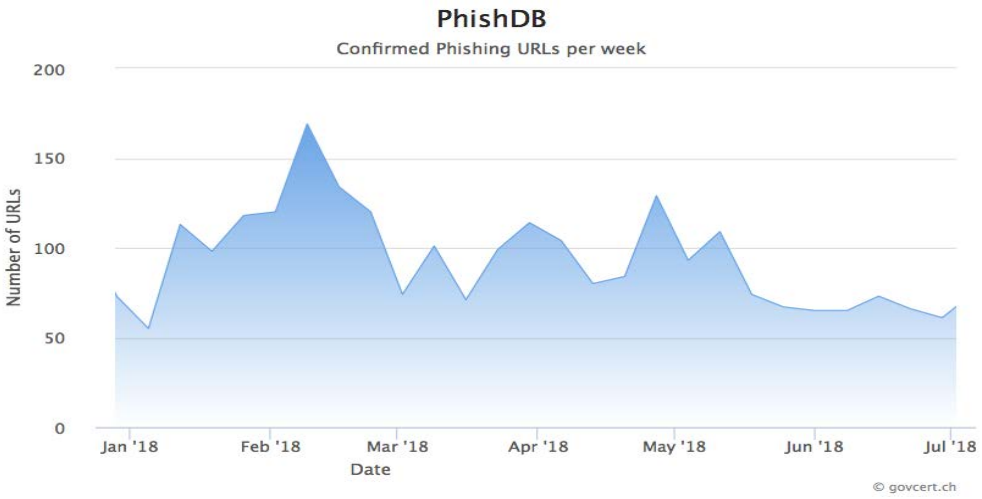


Figure 3: Sites de phishing annoncés et confirmés par semaine sur le site antiphishing.ch au premier semestre 2018

Au total, 2501 sites de phishing avérés ont été dénoncés au premier semestre sur le portail antiphishing.ch exploité par MELANI. La fig. 3 indique le nombre d'annonces hebdomadaires

de pages de phishing, qui fluctue beaucoup en cours d'année. Les raisons en sont diverses: d'une part, les pages signalées sont moins nombreuses en période de vacances, d'autre part les agresseurs passent régulièrement d'un pays à l'autre.

4.4.2 Appels au nom de banques

Une forte recrudescence d'appels frauduleux a de nouveau été constatée contre les entreprises. Concrètement, des escrocs se faisant passer pour des employés de banque invitent à effectuer des paiements, ou prétendent qu'il leur faut procéder à une mise à jour du service d'e-banking et la tester ensuite.

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

Dans une autre variante, les collaborateurs sont priés de renoncer pour quelques jours à l'e-banking, sous prétexte de mises à jour urgentes. Si des transactions ne peuvent attendre, la victime est invitée à contacter le numéro d'appel indiqué par les escrocs. À supposer qu'elle le fasse, tant son nom d'utilisateur que son mot de passe et celui à usage unique lui sont demandés. L'escroc a ainsi accès à l'e-banking de l'entreprise. La procédure peut d'ailleurs se répéter aussi longtemps que la victime ne se méfie pas.

Appréciation

Exemples à l'appui, les méthodes d'ingénierie sociale restent d'actualité. Le meilleur moyen de prévenir efficacement de telles tentatives d'escroquerie consiste à sensibiliser le personnel des entreprises, à faire dûment respecter les processus informatiques, ainsi qu'à contrôler les informations accessibles en ligne à propos des collaborateurs, de la direction et du conseil d'administration.

4.4.3 Phishing basé sur le RGPD

Le règlement général de l'UE sur la protection des données (RGPD) est entré en vigueur le 25 mai 2018, à l'expiration d'un délai transitoire de deux ans (voir chapitre 7.3).
Comme il fallait s'y attendre, les activités abusives déployées à des fins de phishing ont redoublé vers la fin de son délai d'introduction. Car peu avant le 25 mai 2018, les entreprises ont envoyé à leurs clients quantité de courriels d'information sur les mesures qui seraient adoptées dans le cadre de la mise en œuvre du RGPD. Des escrocs ingénieux en ont profité, misant sur le fait que les destinataires étaient informés de l'introduction du RGPD et se sentaient tenus d'adapter leurs profils en conséquence (voir exemple de la fig. 4).

Gesendet: Donnerstag, 5.April 2018
Betreff: Please update your profile for GDPR compliance

Hi
Having recently acquired the business of iProfile, the CV data management company, we are working hard to meet with the requirements of the new GDPR data protection legislation coming in May this year.
Our records show you previously submitted your CV to iProfile, either through a recruitment agency, job board or via a job application and we therefore kindly ask you to check your details to make sure they're up to date.
To update your details, please click on the link below:
http:/

Whether you're actively looking for a new job or simply open to new opportunities, you can take advantage of our smart matching technology that will notify you of any suitable job vacancies, as they arise.
We look forward to staying in touch.

Best regards

Your Support Team

Figure 4: Exemple de courriel frauduleux invoquant le RGPD pour soutirer des données à une victime.

La mise en œuvre conforme du règlement et les lourdes amendes pécuniaires à craindre en cas d'infraction aux règles de la protection des données continueront non seulement à préoccuper les entreprises, mais inspireront aussi aux escrocs de nouvelles manœuvres de chantage. Comme pour l'ingénierie sociale, les informations publiées sont systématiquement utilisées par les cybercriminels à l'affût de la moindre occasion.

4.4.4 Tentatives d'escroquerie par l'intermédiaire du calendrier

Au départ de tout mode opératoire frauduleux, un escroc cherche à entrer en contact avec une victime potentielle en invoquant diverses raisons. Si l'envoi de courriels est souvent la méthode privilégiée, les criminels n'hésitent pas à diversifier leurs modes opératoires. L'envoi de SMS ou de messages sur whatsapp ou sur les réseaux sociaux connaît un succès croissant. Une autre tactique, observée lors de la période sous revue, consiste à envoyer des invitations destinées au calendrier de la victime. Selon les paramètres de celui-ci, l'invitation s'affiche avant même que l'événement n'ait été accepté, et des rappels sont envoyés automatiquement au compte de messagerie électronique. Cette méthode a été observée lors de la période sous revue. En l'occurrence, la victime voyait s'afficher l'invitation dans son calendrier Google. Il s'agissait d'une offre de prêt d'argent et, pour en bénéficier, la victime était priée d'écrire un courriel ou un message whatsapp au numéro indiqué dans l'invitation. Le but final de l'attaque n'a pas été établi, mais l'on peut penser qu'il s'agissait d'une tentative de phishing ou d'escroquerie. Quoiqu'il en soit, cet exemple démontre que la prudence est de mise sur toutes les plateformes. Même les événements figurant dans son calendrier peuvent en effet avoir un contenu malveillant. On ne peut pas exclure que certains internautes se laissent berner, et qu'une invitation ou une notification provenant de leur calendrier personnel leur paraissent fiables et les incitent donc à une action imprudente. Il est recommandé de paramétrer son compte pour que seuls les événements acceptés ne s'affichent dans le calendrier.

4.4.5 Promesse de gain – publipostages au nom d'IKEA, Milka & Cie

Du chocolat à volonté pendant un an, un bon d'achat d'IKEA ou un nouvel iPhone – des messages WhatsApp, des SMS ou des courriels font régulièrement miroiter de tels gains. Or

au bout du compte, il n'y a pas de chocolat mais de la frustration. Ce genre d'envoi émane de collecteurs de données. Les questions de leurs jeux-concours sont choisies de façon à ce que n'importe qui trouve la réponse. Les auteurs veulent en effet un maximum de «gagnants», afin de recueillir le plus grand nombre de données possible. Pour gagner, il faut indiquer sur une page Web falsifiée des données personnelles comme son nom et son âge, son adresse électronique ou son numéro de téléphone mobile, voire son adresse postale. Des noms de domaines internationalisés interviennent parfois dans de telles arnaques (voir chapitre 4.4.7). Dans une variante de jeu-concours, le domaine Milka comportait comme en turc un «i» sans point. Cette particularité ne frappe pas d'emblée les internautes, qui penseront se trouver sur le site officiel de Milka.

Autre astuce de ce genre de jeux-concours, les participants sont invités à transmettre l'information à 20 contacts pour avoir une chance de gagner. De tels publipostages dispensent l'auteur de se soucier de l'envoi – sa victime s'en charge. Avec pour avantage que le destinataire connaît l'expéditeur du message. D'où de meilleures chances qu'une victime ainsi mise en confiance participe au jeu-concours.

Recommandation

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

4.4.6 D'Internet dans le monde réel – quand les agresseurs viennent en personne

L'avantage des infractions commises par Internet est que leurs auteurs peuvent sévir à distance. Ils résident généralement à l'étranger, hors de portée des autorités de poursuite pénale locales. Les escrocs ont d'autant moins de scrupules à agir qu'ils se trouvent dans leur environnement familier. Un hold-up par exemple nécessite une bien plus grande énergie criminelle que l'envoi de courriels de phishing. Durant la période sous revue, il y a toutefois eu quelques incidents qui supposaient une présence physique sur place. En juin 2018, des alertes au sujet d'appels frauduleux au nom de Google ont été publiées.[12] Il semble que dans certains cas, les escrocs ont cherché à organiser une rencontre sur le site de l'entreprise. Dans un cas en particulier, des entreprises ont été informées que Google souhaitait les rencontrer pour vérifier certaines données. Même si ce procédé pourrait faire sens, la visite personnelle de collaborateurs de Google semble quelque peu exagérée. On ignore toutefois quelle idée les escrocs avaient derrière la tête.

Dans un autre cas, des appels téléphoniques ont été faits au nom de l'Office fédéral de l'énergie (OFEN). Leurs auteurs souhaitaient procéder à un contrôle (check-énergie) sur place. On ignore s'ils souhaitaient épier la victime, lui vendre quelque chose ou accéder à son ordinateur.

12 https://www.itmagazine.ch/Artikel/67409/Polizei_warnt_vor_Anrufen_von_falschen_Google-Mitarbeitern.html (Stand: 31. Juli 2018).

Recommandation

Bien des entreprises en contact avec leur clientèle disposent d'ordinateurs dans leur zone clients. Quand des collaborateurs doivent s'en éloigner, ils renoncent souvent par commodité à le verrouiller. Pendant ce temps, les agresseurs potentiels ont la possibilité d'activer des programmes à partir d'une clé USB, ou de se rendre sur des sites malveillants. Il faudrait donc verrouiller les ordinateurs même en cas de brève absence. En outre, la protection des ports USB procure une sécurité accrue, à plus forte raison quand on n'en a pas l'usage. Les systèmes d'exploitation sont entre-temps conçus pour ne plus exécuter automatiquement les fichiers provenant d'une clé USB. L'utilisateur doit confirmer qu'il souhaite bel et bien effectuer l'action proposée. Il reste néanmoins des failles qui permettent de contourner cette mesure de sécurité.

4.4.7 Domaines d'apparence semblable («look alike»)

Dès 2005, MELANI avait signalé une astuce de phishing: des escrocs créaient à partir de noms de domaine internationalisés (internationalized domain name, IDN) des URL ressemblant à s'y méprendre aux originaux pour un internaute. Par exemple, on ne saurait distinguer le domaine www.epic.com écrit en caractères cyrilliques du site www.epic.com du fabricant de logiciels Epic. Et si en plus le certificat de sécurité correspondant a été émis, il devient possible d'établir une connexion protégée en «https://». Les visiteurs d'un tel site le croient «sécurisé» et donc digne de confiance, du fait de la présence du cadenas dans leur navigateur. De très nombreux caractères internationaux paraissent pratiquement identiques à ceux de notre alphabet, ce qui facilite les abus. Cette manière d'agir a reçu le nom d'attaques homographiques, ou phishing homographique. Alors que ce genre d'attaque ne s'était plus guère vu ces dernières années, de nouveaux cas ont été signalés en Suisse au cours de la période sous revue.

Comme les caractères cyrilliques а, с, е, о, р, х et у ont quasiment la même apparence que les caractères latins a, c, e, o, p, x et y, les attaques homographiques[13] privilégient l'alphabet cyrillique. Les lettres ԧ, і, ј et ѕ conviennent également. Dans l'alphabet grec, seules les lettres omicron «ο» et nu «ν» ressemblent à une minuscule latine. Des signes de l'alphabet arménien ou hébreu sont encore utilisés de façon très ponctuelle.

En 2005, certains navigateurs ont réagi en indiquant dans la barre d'adresse les caractères spéciaux au format punycode, ce qui fait qu'un internaute pouvait aisément repérer un tel domaine. Le nom de domaine paypal.com écrit avec un «а» cyrillique devient xn—pypal-4ve.com. Firefox a en outre dressé une liste blanche de domaines dûment vérifiés, dont le punycode ne s'affichait pas. Cette stratégie a été modifiée en 2012. Avec l'essor des noms de domaine internationalisés (IDN), la liste blanche était devenue trop fastidieuse à actualiser. Depuis lors, Firefox affiche les IDN quand tous les caractères appartiennent au même jeu de caractères, ou si les domaines de premier niveau (top-level domain, TLD) limitent l'usage des IDN. Il en va de même pour Internet Explorer et Opera. Safari signale également les jeux de caractères problématiques avec leur punycode.

[13] https://de.wikipedia.org/wiki/Homographischer_Angriff (état: le 31 juillet 2018).

Les domaines génériques de premier niveau, à l'instar de .com, .net ou .biz sont surtout concernés. Les escrocs veillent à ce que toutes les lettres proviennent du même jeu de caractères, afin que le navigateur n'affiche pas le punycode. Cela limite certes leur champ d'action, mais les lettres susmentionnées permettent d'obtenir des combinaisons qui se prêtent à des attaques de phishing homographique.

Les jeux de caractères sont généralement limités pour les domaines de premier niveau géographiques, à l'instar de «.ch»[14], qui n'autorise que 32 signes spéciaux. Mais on y trouve des lettres à l'apparence similaire, dont les escrocs pourront se servir. Par exemple, un i avec accent circonflexe est difficile à distinguer d'un i normal, et le navigateur n'indique pas le punycode si le nom de domaine s'en tient au jeu de caractères restreint en vigueur.

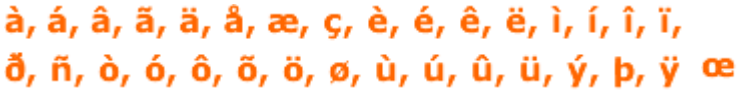


Figure 5: Liste des 32 caractères spéciaux autorisés en Suisse pour des noms de domaine (source: nic.ch)

Appréciation / Recommandation:

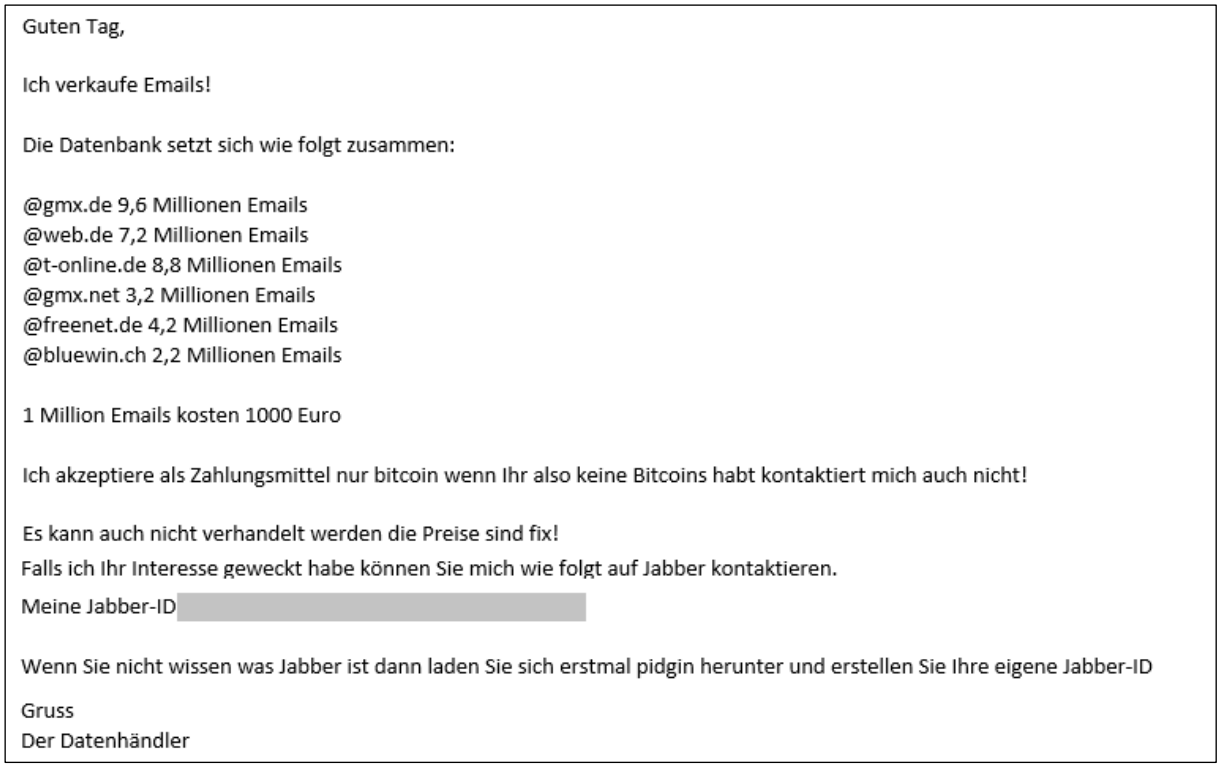
Les mesures prises par les navigateurs règlent en bonne partie le problème. Expérience à l'appui, les agresseurs ne se fatiguent pas à générer des sites de phishing. Ils piratent généralement des sites existants pour y placer des pages frauduleuses. Et personne ne se soucie de savoir si l'adresse URL est correcte. Il en va différemment pour les attaques ciblées. La méthode décrite ici servira par exemple à introduire un cheval de Troie d'espionnage dans le système de la victime.

Firefox permet de désactiver entièrement les noms de domaine internationalisés. Toutes les URL apparaîtront ensuite en punycode dans la barre d'adresse. À cet effet, il faut basculer de «false» à «true», dans la page de configuration (about:config), la variable «network.IDN_show_punycode».

4.4.8 Adresses électroniques à vendre

Une grande quantité d'adresses électroniques ont été mises en vente sur Internet en décembre 2017. L'opération a été répétée en mai 2018, où des destinataires suisses ont à nouveau reçu une offre de vente concernant des adresses électroniques. On ignore toutefois si l'expéditeur était réellement en possession du nombre d'adresses électroniques indiqué.

[14] https://www.nic.ch/fr/faqs/idn/ (état: le 31 juillet 2018).



Guten Tag,

Ich verkaufe Emails!

Die Datenbank setzt sich wie folgt zusammen:

@gmx.de 9,6 Millionen Emails
@web.de 7,2 Millionen Emails
@t-online.de 8,8 Millionen Emails
@gmx.net 3,2 Millionen Emails
@freenet.de 4,2 Millionen Emails
@bluewin.ch 2,2 Millionen Emails

1 Million Emails kosten 1000 Euro

Ich akzeptiere als Zahlungsmittel nur bitcoin wenn Ihr also keine Bitcoins habt kontaktiert mich auch nicht!

Es kann auch nicht verhandelt werden die Preise sind fix!
Falls ich Ihr Interesse geweckt habe können Sie mich wie folgt auf Jabber kontaktieren.
Meine Jabber-ID

Wenn Sie nicht wissen was Jabber ist dann laden Sie sich erstmal pidgin herunter und erstellen Sie Ihre eigene Jabber-ID

Gruss
Der Datenhändler

Figure 6: Des destinataires suisses ont à nouveau reçu une offre de vente concernant des adresses électroniques.

La compilation de listes d'adresses électroniques en vue d'une revente constitue un modèle d'affaires lucratif. Les cybercriminels utilisent des informations provenant aussi bien de vols de données que de sources en libre accès. Les polluposteurs procèdent à l'analyse automatique du Web, à la recherche d'adresses électroniques valables publiées sur des pages Internet (forums, livres d'or, etc.). Les comptes de messagerie compromis sont également une précieuse source d'adresses électroniques. Les escrocs passent au crible tant les carnets d'adresses que les courriels proprement dits pour recueillir des adresses. Une autre méthode consiste à tester des prénoms et noms répandus. Quand des courriels sont expédiés à des adresses créées au hasard, la plupart des serveurs de messagerie signalent si elles n'existent pas – et dans tous les autres cas, l'expéditeur peut partir du principe que l'adresse existe bel et bien. De tels essais sont entièrement automatisés.

De grandes quantités de listes d'adresses électroniques valables circulent au noir. Les données correspondantes sont généralement revendues sur ce marché. Il est donc très atypique que de telles «offres de vente» soient envoyées à grande échelle à des internautes choisis au hasard. On ignore ce qui a pu pousser les escrocs à de tels envois de masse. Peut-être ont-ils voulu amener les destinataires à payer à l'avance pour des adresses qu'ils ne possédaient même pas. Ou alors ils auront voulu mettre à jour une base de données de pourriels, en écartant les adresses refusées par les serveurs de messagerie.

Appréciation / Recommandation:

La vague de pourriels de mai 2018 a abouti à de nombreuses annonces à MELANI. Bien des gens ont cru à tort qu'outre leur adresse électronique, leur mot de passe avait été dérobé et allait être vendu. Il n'est guère agréable de découvrir sa propre adresse dans une telle base de données, mais c'est inévitable: l'adresse électronique est le point d'ancrage de tous les services Internet, et donc s'emploie un peu partout. La sécurité n'en pâtit pas, à condition de respecter les directives usuelles sur l'utilisation de la messagerie.

Règles de comportement propres au courrier électronique sur le site web MELANI:

https://www.melani.admin.ch/melani/fr/home/schuetzen/verhaltensregeln.html

MELANI recommande en pareil cas d'ignorer les courriels, et de ne surtout pas y répondre. Car une réponse confirmerait aux polluposteurs que l'adresse choisie fonctionne et que leur message a été lu. Une recrudescence de pourriels serait donc à craindre.

4.5 Pertes de données

4.5.1 Fuite de données chez un partenaire de distribution de Swisscom

En automne 2017, des cybercriminels ont dérobé les coordonnées de environ 800 000 clients de Swisscom. Le réseau de l'opérateur n'a pas été directement compromis: les pirates, dont le mode opératoire reste inconnu, se sont emparés des données d'accès d'un partenaire de distribution traitant les données de Swisscom. L'incident[15] avait été découvert, lors d'un contrôle de routine.

Les données dérobées sont des informations nécessaires pour identifier le client, comme son nom, son adresse, son numéro de téléphone et sa date de naissance. De telles informations figurent pour la plupart dans les annuaires téléphoniques ou les médias sociaux. Selon Philippe Vuilleumier[16], responsable Group Security de Swisscom, il ne s'agit pas de données considérées comme "particulièrement sensibles" selon la la loi sur la protection des données – mots de passe, données de communication et de paiement. Des mécanismes de protection très stricts sont d'ailleurs en place pour ce type d'informations.

Comme mesures immédiates, Swisscom a bloqué les accès de la société partenaire, avant de renforcer drastiquement ses mesures de sécurité internes. En particulier, les accès par les sociétés partenaires sont surveillés de plus près, une alarme se déclenche en cas d'activités suspectes et une authentification à double facteur a été mise en place.[17]

---

15 https://www.srf.ch/news/wirtschaft/massnahmen-eingeleitet-datendiebstahl-bei-swisscom (état: le 31 juillet 2018).

16 https://www.swisscom.ch/fr/about/medien/actualites/interview-philippe-vuillemier-responsable-group-security.html (état: le 31 juillet 2018).

17 https://www.swisscom.ch/fr/about/medien/press-releases/2018/02/20180207-mm-swisscom-verschaerft-sicherheitsmassnahmen-fuer-kundenangaben.html (état: le 31 juillet 2018).

Swisscom a encore opté, parmi les mesures immédiates, pour une communication transparente. Le Préposé fédéral à la protection des données et à la transparence (PFPDT) a été prévenu, les clients réseau fixe et commerciaux ont été informés par écrit, tandis qu'un service d'information par SMS gratuit était mis en place. Tous les clients mobiles ont ainsi pu savoir si la fuite de données les concernait.

4.5.2 L'utilisation faite des données dérobées

Le 26 avril 2018, la société vaudoise Epsitec, éditrice de logiciels de gestion pour PME, a signalé sur son site Web avoir été victime d'un vol de données. Les auteurs de la cyberattaque se sont emparés de l'adresse électronique, du numéro de téléphone et de l'adresse postale de 35 000 clients. Epsitec a tenu à préciser qu'aucun numéro de carte de crédit ou mot de passe n'avait été dérobé[18]. En l'occurrence, il est frappant de voir l'usage auquel les criminels destinaient les données volées: ces dernières ont été utilisées pour élaborer des courriels personnalisés ayant pour but de transmettre le cheval de Troie bancaire Retefe. Comme les courriels non attendus et impersonnels suscitent une méfiance croissante, les escrocs doivent faire preuve d'imagination. Un envoi personnalisé ou la mention d'un contact professionnel existant de l'entreprise sont susceptibles d'amener la victime à ouvrir un fichier annexé. Dans le cas actuel, les escrocs ne se sont pas contentés d'indiquer les prénom et nom, mais ont encore puisé dans les données dérobées à Epsitec pour donner une plus grande crédibilité à leur courriel. Celui-ci annonçait une prétendue livraison de DHL, ou feignait d'être une requête de l'Administration fédérale des contributions (AFC).

4.5.3 Mots de passe utilisés pour la «sextorsion»[19]

Dans un autre cas apparu dans la période sous revue, des escrocs se sont servis de données dérobées dans le but de s'enrichir. Il s'agissait certes de données sensibles, à l'instar de mots de passe, mais qui remontaient à plusieurs années parfois. À première vue, de telles données d'accès ne sont pas toujours encore valables. Les escrocs ont néanmoins trouvé un moyen de faire fructifier ce butin. Durant l'été 2018, MELANI a enregistré toute une série de vagues de courriels de chantage. Leurs destinataires étaient menacés de la publication de matériel compromettant, recueilli auparavant à l'aide d'un maliciel sur leur ordinateur. Les escrocs prétendaient avoir pris le contrôle de la webcam de la victime. À titre de preuve, ils mentionnaient un mot de passe ou un numéro de téléphone mobile utilisés par elle. De telles données visent à rendre la demande de rançon plus crédible et à déstabiliser la personne. Elles proviennent en général de fuites de données relativement anciennes. C'était le cas dans tous les incidents signalés à MELANI.

---

18 https://www.watson.ch/digital/schweiz/581594688-hacker-klauen-35-000-kundendaten-bei-schweizer-software-firma-epsitec (état: le 31 juillet 2018).

19 https://www.skppsc.ch/fr/sujets/internet/sextortion/?noredirect=fr_FR (état: le 31 juillet 2018).

Appréciation

Les maîtres chanteurs ont expédié leurs courriels au hasard, dans l'espoir que des personnes ayant récemment consulté des sites pornographiques figurent parmi leurs destinataires. Ceux-ci se laisseraient d'autant plus facilement intimider. MELANI n'a connaissance d'aucun cas où les escrocs auraient été en possession de photos ou de vidéos compromettantes, et a fortiori où ils auraient diffusé ou publié un tel matériel.

4.5.4 Attaques de «credential stuffing» basées sur d'anciens mots de passe

De nombreux utilisateurs changent régulièrement de mot de passe. Mais si un escroc parvient à se procurer un grand nombre d'identifiants, quelques-uns d'entre eux seront forcément encore valides. Car beaucoup d'internautes emploient le même mot de passe pour différents services, et cela sur une période prolongée. Cette négligence arrange bien les escrocs qui testent systématiquement, sur toutes sortes de plateformes, les données d'ouverture de session dérobées lors de fuites de données. De telles attaques robotisées ont été baptisées «credential stuffing». Autrement dit, si des internautes réutilisent à plusieurs endroits le même mot de passe, des escrocs parviendront peut-être, avec un peu de chance et de persévérance, à se connecter sous leur identité à un service pour en faire un usage frauduleux. Dans un cas signalé en 2018 à MELANI, près d'un million de combinaisons nom d'utilisateur/mot de passe qui avaient été volées ont été testées sur un portail en ligne. En l'occurrence, ces données d'accès provenaient de fuites de données parfois très anciennes, dont d'autres prestataires Internet avaient été victimes.

Appréciation / Recommandation:

Les boutiques en ligne et d'autres services Internet sont des cibles de choix pour les pirates, qui convoitent leurs fichiers clients. Au cas où les mots de passe ne seraient pas chiffrés ou si leur protection laisse à désirer, les escrocs entreront en possession de leurs données d'accès. Forts de ces données, les criminels cherchent à se connecter à un grand nombre d'autres plateformes Internet, en espérant que les utilisateurs auront repris les mêmes données d'ouverture de session pour plusieurs services.

Les services constatant de telles tentatives abusives peuvent s'annoncer à MELANI. Le cas échéant, ces données seront intégrées à l'outil MELANI checktool (www.checktool.ch), où chacun pourra ensuite vérifier si ses propres données y figurent.

Les mots de passe en ligne doivent être suffisamment longs pour être difficiles à deviner. Il est recommandé d'utiliser un mot de passe différent par boutique en ligne ou service. En outre, on optera dans la mesure du possible pour une authentification à deux facteurs.

4.6 Logiciels criminels (crimeware)

De nombreuses infections dues à des logiciels criminels ont été constatées au premier semestre 2018. La statistique de la fig. 6 montre la répartition des principaux maliciels en Suisse. Il y a également des maliciels très problématiques mais qui n'apparaissent pas dans la statistique, à l'instar du cheval de Troie bancaire Retefe. Cela s'explique par le fait que Retefe n'est pas un maliciel à proprement parler, car il se contente de modifier les paramètres du navigateur.

Comme les années précédentes, la majeure partie des infections sont imputables à Downadup (aussi appelé Conficker). Ce ver apparu il y a plus de dix ans se répand par une faille de sécurité des systèmes d'exploitation Windows, découverte en 2008. Le correctif correspondant est pourtant disponible depuis 2008 aussi. Il est suivi en deuxième position par Gamut, spécialisé dans l'envoi de pourriels, qui serait à l'origine de 37 % des courriels indésirables envoyés dans le monde au dernier trimestre 2017. Gamut expédie surtout des offres d'emploi d'agents financiers (passeurs d'argent, «money mules»).[20] Gamarue[21], également connu sous le nom d'Andromeda, se classe troisième. Ce programme de téléchargement (downloader) parvient à introduire n'importe quel autre virus sur l'ordinateur infecté. Puis viennent en quatrième et cinquième positions les maliciels Spambot et Stealrat, tous deux spécialisés dans la diffusion de pourriels. Stealrat opère à partir de domaines ou adresses IP infectés, notamment sur des sites WordPress, Joomla! ou Drupal. Les pourriels expédiés depuis des serveurs de messagerie légitimes sont d'autant plus difficiles à filtrer. Le numéro six de la liste, Monero Miner, est aussi le premier virus de cryptominage de la liste, tandis que le premier cheval de Troie bancaire, Gozi, ne vient qu'en neuvième position. Quant à Mirai, maliciel formant des armées de zombies célèbre pour avoir paralysé le prestataire de services Internet Dyn, il a disparu entre-temps de la liste des logiciels criminels les plus actifs.

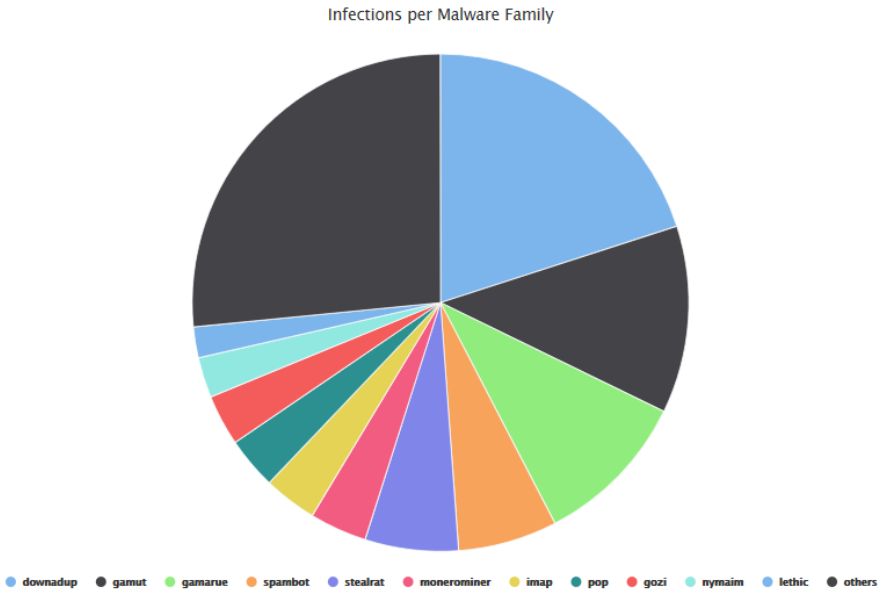


Figure 7: Répartition des maliciels en Suisse, selon les informations en possession de MELANI. Date de référence: le 30 juin 2018. Des données actuelles sont publiées sous: http://www.govcert.admin.ch/statistics/dronemap/

20 https://sensorstechforum.com/de/necurs-gamut-botnets-spam/ (état: le 31 juillet 2018).

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

4.7 Chevaux de Troie bancaires en Suisse

Les systèmes de paiement en ligne constituent d'attrayantes cibles pour les cybercriminels, car ils génèrent de gros profits pour un risque globalement faible. La plupart des cybercampagnes observées combinaient des méthodes d'ingénierie sociale avec l'envoi de maliciels. Les escrocs font encore preuve d'ingéniosité pour contourner les antivirus, pour protéger leur infrastructure face aux tentatives de neutralisation («takedown»), ainsi que pour se soustraire aux mesures des autorités de poursuite pénale. Divers chevaux de Troie bancaire ont à nouveau sévi au cours de la période sous revue.

4.7.1 Retefe et l'ingénierie sociale

Retefe fait actuellement partie des chevaux de Troie les plus répandus en Suisse. Après s'être surtout propagé par de fausses factures de boutiques en ligne, comme Zalando ou Ricardo, ce maliciel figure depuis peu en pièce jointe d'envois effectués au nom de nombreuses autres entreprises connues. MELANI a ainsi enregistré au premier semestre 2018 plusieurs vagues de pourriels censés émaner de DHL, des CFF, de plusieurs polices cantonales, de l'Administration fédérale des contributions (AFC) ou encore de la compagnie aérienne Swiss. En outre les envois ciblés, au contenu personnalisé, ont pris le relais des publipostages à grande échelle. Bien des courriels indiquent le nom exact et le numéro de téléphone des destinataires. Cette personnalisation a beau exiger des préparatifs plus minutieux, l'effort semble en valoir la peine. Les victimes se laissent tromper plus aisément, et donc la probabilité d'infection augmente sensiblement.

Le maliciel cherche à modifier les paramètres du navigateur (Internet Explorer, Firefox, Chrome) pour qu'en se connectant à un site d'e-banking, la victime soit redirigée vers une copie gérée par les escrocs. Quand elle s'annonce sur ce prétendu portail d'e-banking, la victime voit d'abord s'afficher un code QR qui, si elle le lit avec son smartphone, aboutit à un cheval de Troie SMS. Une fois cette application Android installée, tous les SMS envoyés par la banque pour l'authentification à deux facteurs seront transférés aux malfaiteurs. Ces derniers pourront dès lors se connecter en tout temps à la plateforme e-banking de la victime et procéder à des paiements à son insu. Dans un autre cas, les cybercriminels ont cherché à se procurer les données d'activation. En règle générale, la banque envoie par poste à ses clients une lettre qui renferme un code QR à numériser à l'aide d'une app, à la première ouverture de session d'e-banking. Le smartphone utilisé est dès lors agréé par la banque comme moyen de communication pour l'authentification à deux facteurs. Les escrocs ont incité par courriel la victime à numériser ou photographier à leur intention cette lettre de la banque[22]. Même si Retefe s'en prend d'ordinaire aux systèmes Windows, plusieurs vagues de maliciels ont ciblé en 2017 les utilisateurs suisses du système d'exploitation MacOS[23].

Depuis septembre 2017, l'exploit EternalBlue complète les fonctionnalités de Retefe. Si dans une entreprise un collaborateur ouvre par mégarde une pièce jointe infectée, le maliciel se fraie à partir de cette faille de sécurité un chemin jusqu'au poste où l'entreprise effectue ses paiements par e-banking. Un tel mode opératoire suppose naturellement la persistance de

---

22 https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/e-banking--angreifer-haben-es-auf-aktivierungsbriefe-abgesehen.html (état: le 31 juillet 2018).

23 https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/malware---si-raccomanda-prudenza-indipendentemente-dal-sistema-o.html (état: le 31 juillet 2018).

cette vulnérabilité, pour laquelle un correctif a été publié le 14 mai 2017. En optant pour EternalBlue, Retefe a montré que ce sont surtout les PME qui l'intéressent.

4.7.2 Dridex et les logiciels de paiement hors ligne

Le cheval de Troie bancaire Dridex est également répandu sous nos latitudes. Il s'agit d'un ver informatique apparu en 2012 sous le nom de Cridex. Sa diffusion en tant que ver présentait toutefois des inconvénients: il lui fallait des failles de sécurité non corrigées, et son activité en arrière-plan était aisément repérable. Aussi ses plus récentes versions se propagent-elles presque exclusivement lors d'envois en masse de pourriels. Des documents Word infectés et se faisant passer pour une facture, une confirmation de commande en ligne, une injonction de payer, etc. sont utilisés à cet effet. L'expéditeur semble être une vraie entreprise, qui a souvent son siège dans le même pays que la victime. La plupart des courriels sur mesure diffusés en Suisse sont rédigés en allemand. Au premier semestre 2018, une vague de pourriels cherchant à répandre Dridex a déferlé sur la Suisse: des courriels expédiés au nom de Swisscom renfermaient une facture électronique imitant fidèlement celles du géant bleu. Un hyperlien dissimulé derrière le champ actif «Visualiser la facture» conduisait à un JavaScript malveillant, qui cherchait ensuit à installer le cheval de Troie bancaire Dridex.

Une fois installé, Dridex lance une attaque de type MITM («man in the middle», attaque de l'homme du milieu ou de l'intercepteur). Selon cette technique, le pirate s'immisce dans un canal de communication entre deux partenaires – ici la banque et le client e-banking – pour lire et manipuler les données échangées. Dridex possède une organisation décentralisée et une architecture de réseau à plusieurs niveaux, avec des sous-réseaux gérés par différents groupes criminels. Cette structure complique la tâche aux autorités. Il s'ensuit que Dridex continue de représenter un danger considérable, alors même qu'en octobre 2015 le ministère de la justice américain et le FBI[24] ont probablement réussi à arrêter le cerveau du réseau et que par la suite, d'autres membres influents ont été mis sous les verrous.

En juillet 2016, Dridex a élargi son mode opératoire aux systèmes de paiement hors ligne[25]. Beaucoup d'entreprises adoptent de telles solutions pour transmettre de grandes quantités de paiements par Internet à une ou plusieurs banques. Dridex se met en quête, sur un ordinateur préalablement infecté, d'un logiciel de paiement hors ligne. S'il en repère un, il pourra télécharger depuis Internet d'autres maliciels servant à effectuer des paiements frauduleux. Cobalt Strike a par exemple été utilisé dans quelques cas, et dans d'autres Carbanak. En l'absence de tout logiciel de paiement hors ligne, Dridex s'attaquait dans la mesure de ses possibilités aux connexions e-banking.

Depuis 2016, Dridex sévit également contre les portefeuilles de cryptomonnaie. Ses fichiers de configuration mentionnent cette année toujours plus de cibles dans ce domaine.

Dridex n'affiche qu'une activité modérée à l'heure actuelle, en Suisse comme à l'étranger. Tout danger n'est pas pour autant écarté. Le calme actuel s'explique peut-être par une phase de mise à jour et de préparation de nouvelles cyberattaques. En outre, d'autres organisations

---

24 https://www.fbi.gov/contact-us/field-offices/pittsburgh/news/press-releases/bugat-botnet-administrator-arrested-and-malware-disabled (état: le 31 juillet 2018).

25 https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/offline-payment-software.html (état: le 31 juillet 2018).

comme le Cobalt Gang, qui collaborent probablement avec Dridex, continuent d'utiliser les ressources de ce cheval de Troie.

4.7.3 Gozi ISFB et sa diffusion par «drive-by download»

La présence de Gozi a été observée en Suisse pour la première fois en janvier 2009. Il est communément admis que ce cheval de Troie bancaire a été créé par le Russe Nikita Kuzmin, arrêté en août 2011 par le FBI[26]. Mais comme Gozi s'était déjà fait connaître sur le marché au noir, des cybercriminels continuent à s'en servir ici ou là. Sa nouvelle version, baptisée ISFB, s'en est prise pour la première fois à la clientèle des banques suisses en mai 2015. Gozi utilise la méthode MITM («man-in-the-middle») pour ses fraudes à l'e-banking.

La nouvelle variante de Gozi est principalement diffusée par drive-by download. La version en ligne des quotidiens, consultée par de très nombreuses personnes, constitue une cible idéale pour ce type de maliciel. Plus leur popularité est grande, plus les possibilités de propagation augmentent. En mars 2017, le site 20min.ch[27] a été attaqué pour diffuser ce cheval de Troie bancaire. Des vagues de pourriels renfermant des annexes .zip infectées ont également été observées. Au début de mars dernier, par exemple, il s'agissait d'un prétendu paquet envoyé par FedEx. Gozi a recouru en 2018, pour la première fois, au «malvertising» pour diffuser des logiciels malveillants. Il s'agit d'inciter les victimes, au moyen d'annonces publicitaires frauduleuses, à télécharger un logiciel manipulé. Dans les moteurs de recherche, la publicité s'affiche souvent avant les résultats de la recherche proprement dite, ce qui accroît le risque de confusion pour les internautes. Concrètement, les cybercriminels ont fait la promotion, sur google.ch, de logiciels Java et Firefox qui renfermaient à la fois le programme souhaité et leur propre maliciel.

À l'heure actuelle, Gozi ne s'en prend pas seulement aux systèmes d'e-banking, mais s'attaque aussi aux logiciels de paiement hors ligne et aux portefeuilles de cryptomonnaie. L'intérêt pour ces cibles modernes va apparemment se renforcer dans un proche avenir.

---

26 https://www.justice.gov/usao-sdny/pr/nikita-kuzmin-creator-gozi-virus-sentenced-manhattan-federal-court (état: le 31 juillet 2018).

27 https://www.srf.ch/news/schweiz/nach-malware-attacke-auf-20-minuten-was-sie-jetzt-tun-koennen (état: le 31 juillet 2018).

Appréciation / Recommandation:

Les trois campagnes décrites ci-dessus éclairent certaines tendances dans le domaine des attaques contre les systèmes de paiement. Outre les vecteurs d'attaque classiques comme les courriels ou pages Web infectés, le détournement de publicités en ligne à des fins criminelles s'avère une méthode fructueuse pour diffuser des maliciels d'e-banking. Il devient toujours plus difficile pour les internautes de repérer de telles attaques. Il incombe donc en premier lieu aux exploitants de sites Web de contrôler systématiquement leurs annonces publicitaires et leurs autres contenus dynamiques – a fortiori ceux de sociétés tierces. Par ailleurs, la prudence reste de mise avec les courriels, même quand ils paraissent sérieux et sont personnalisés. Il est donc recommandé de cliquer plutôt une fois de pas assez qu'une fois de trop sur un lien ou une annexe. Autre tendance frappante, les fraudes à l'e-banking se multiplient contre les PME qui, en plus d'être souvent moins bien protégées que les grandes sociétés, génèrent des transactions bancaires plus élevées qu'un simple particulier. Les PME suisses sont donc confrontées à des défis croissants dans le domaine de la sécurité informatique. Pour les aider à prendre les mesures internes utiles, MELANI a récemment publié une mise à jour de son aide-mémoire pour les PME sur la sécurité de l'information. Ce document renferme des conseils et astuces utiles à toute entreprise soucieuse d'améliorer sa cyber-résilience.

Sécurité de l'information: aide-mémoire pour les PME
https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/securite-informatique--aide-memoire-pour-les-pme.html

5 Situation internationale

5.1 Espionnage

5.1.1 Incidents divers attribués à Sofacy

Sofacy, aussi connu sous les noms d'APT28, Fancy Bear et Tsar Team, reste un des groupes d'espionnage les plus actifs et les plus connus du monde. Tous les vecteurs d'infection possibles et imaginables sont bons pour Sofacy, les courriels d'hameçonnage ciblé («spear phishing») comportant une annexe ou un lien malveillants, voire les attaques dites du point d'eau («watering hole»). Cette campagne repose sur une véritable armée de serveurs de commande et de contrôle. Les concepteurs de Sofacy n'adaptent pas seulement leurs maliciels à leurs victimes. Ils déploient encore de gros efforts pour mener des attaques ciblées d'ingénierie sociale[28]. Or outre les cyberattaques raffinées de la première heure, on constate entre-temps la présence d'opérations lancées à plus grande échelle, afin d'atteindre un maximum de victimes potentielles. Dans les cyberattaques reposant sur Zebrocy, un programme de téléchargement (downloader) chargé d'installer une porte dérobée (backdoor), les destinataires (adresses électroniques) ont été choisis de manière non pas ciblée mais aléatoire: il suffisait par exemple d'un moteur de recherche pour les repérer. Une telle approche, atypique pour une campagne APT, fait plutôt penser à des cybercriminels. Ce genre de stratégie[29] rend certes une infection plus probable, mais le risque d'être découvert augmente à son tour. Autre constat frappant, les attaques sont en pleine expansion vers l'Extrême-Orient[30], avec une prédilection pour les structures militaires, pour la politique de défense et les organisations diplomatiques. La grande variété des objectifs et des tactiques choisis complique le travail d'attribution, ce qui pourrait d'ailleurs être la motivation réelle sous-jacente à l'évolution en cours de Sofacy.

En 2018, le maliciel Olympic Destroyer a fait les gros titres durant les épreuves olympiques de Pyeongchang (Corée du Sud). Ce ver s'est attaqué à l'infrastructure des jeux d'hiver et à celle de plusieurs partenaires. Bien que le commanditaire de la cyberattaque n'ait pu être clairement identifié, le spécialiste de la sécurité informatique Kaspersky a mis en évidence les similitudes avec le mode opératoire de Sofacy (voir chapitre 4.1.1).

Le 10 janvier 2018, le Fancy Bears Hack Team a publié des données qui auraient été dérobées à la fin de 2016 ou au début de 2017 au Comité olympique international ainsi qu'au Comité olympique américain. Là encore, les soupçons se sont dirigés vers le groupe Sofacy[31].

---

28 https://securelist.com/a-slice-of-2017-sofacy-activity/83930/ (état: le 31 juillet 2018).

29 https://researchcenter.paloaltonetworks.com/2018/06/unit42-sofacy-groups-parallel-attacks/ (état: le 31 juillet 2018).

30 https://www.kaspersky.de/about/press-releases/2018_sofacy-erweitert-sein-operationsgebiet-in-richtung-fernost (état: le 31 juillet 2018).

31 https://www.wired.com/story/russian-fancy-bears-hackers-release-apparent-ioc-emails/ https://www.mid-day.com/articles/russia-apparently-hacking-winter-olympics-emails-report/18923160 https://www.eclecticiq.com/resources/russian-hacking-group-fancy-bear-prepares-to-attack-winter-olympics-u-s-senate (état: le 31 juillet 2018). (état: le 31 juillet 2018).

5.1.2 VPN Filter – au moins 500 000 appareils concernés

Le 23 mai 2018, les experts en cybersécurité de l'équipe Talos de Cisco ont publié des données sur VPN-Filter[32], réseau de zombies formé d'au moins un demi-million de routeurs et NAS. Il suffirait d'un ordre de l'agresseur pour que le maliciel efface les 5000 premiers octets de leur premier bloc mémoire et qu'aucun de ces appareils ne puisse ensuite redémarrer. La panne simultanée d'un demi-million de systèmes serait lourde de conséquences. Les appareils se trouvent dans 54 pays, à commencer par l'Ukraine. De tels agissements rappellent le maliciel NotPetya. À l'époque déjà, l'épicentre de la cyberattaque était situé en Ukraine, et ses retombées s'étaient fait sentir dans le monde entier.

Tous les appareils infectés étaient reliés à Internet et présentaient des lacunes de sécurité connues, ou alors n'étaient protégés que par un mot de passe standard. VPN-Filter a été découvert sur des appareils variés, dont ceux des fabricants de routeurs MikroTik, Linksys, Netgear et TP-Link – mais les appareils NAS produits par QNAP étaient aussi concernés. Le maliciel agit en trois temps. Seul le module de base est installé en permanence sur l'appareil infecté, le maliciel proprement dit et ses fonctions étant téléchargés plus tard, en deux étapes.

Au départ, la seule possibilité d'éliminer le maliciel consistait à rétablir les réglages d'usine. Toutefois, l'existence de ce réseau de zombies venait d'être rendue publique quand le FBI a réussi à s'emparer du serveur qui, après le redémarrage des appareils, aurait fourni les informations nécessaires à la deuxième phase – soit où et comment le maliciel devait être activé. Concrètement, les instructions nécessaires à une réinstallation du maliciel figuraient dans les métadonnées d'une image sauvegardée sur la plateforme Photobucket.com. Même si un redémarrage ne supprime pas de l'appareil infecté le maliciel, ce dernier ne pourra plus ensuite télécharger les fonctions des deux étapes suivantes. Les mesures adoptées par le FBI ont donc permis de neutraliser le maliciel, et aussi d'identifier les appareils infectés. Au cours de son analyse, l'équipe Talos de Cisco a découvert une erreur caractéristique, survenue lors de la mise en œuvre de l'algorithme de chiffrement RC4, qui avait déjà été observée pour le maliciel BlackEnergy.

5.1.3 Cyberattaque contre le réseau du gouvernement fédéral allemand

À la fin de février 2018, on a appris que le Ministère allemand des affaires étrangères avait été victime d'une cyberattaque. L'intrusion[33] se serait produite au passage de l'an 2016 à 2017. Les escrocs auraient ainsi eu accès au réseau de données central de l'administration fédérale, l'IVBB (Informationsverbund Berlin-Bonn). Il s'agit d'une sorte d'Intranet à l'usage du Parlement fédéral, de la Chancellerie fédérale, des ministères fédéraux, de la Cour des comptes allemande ainsi que de divers organismes de sécurité. Après l'intrusion subie en 2015 par le Parlement fédéral, c'est la deuxième attaque[34] de grande envergure subie par

---

32 https://blog.talosintelligence.com/2018/05/VPNFilter.html (état: le 31 juillet 2018).

33 https://www.zeit.de/politik/2018-04/hackerangriff-bundesregierung-russland-verfassungsschutz-hans-georg-maassen (état: le 31 juillet 2018).

34 https://www.zeit.de/digital/datenschutz/2018-03/hackerangriff-bundesregierung-outlook-auswaertiges-amt (état: le 31 juillet 2018).

l'infrastructure informatique du gouvernement allemand et officiellement reconnue comme telle.

L'attaque se serait notamment produite à travers une plateforme d'enseignement et d'apprentissage en ligne, utilisée à des fins de formation à l'école supérieure fédérale d'administration publique.[35] Rien n'a toutefois filtré sur les failles de sécurité dont les pirates auraient pu tirer parti.[36] Divers médias ont émis l'hypothèse d'une attaque du groupe Sofacy. Ce n'est que plus tard que les soupçons se sont reportés sur le groupe Snake/Turla, qui a également sévi en Suisse. C'est lui d'ailleurs qui a piraté l'entreprise d'armement Ruag.

5.1.4 Attaques contre des fournisseurs d'énergie

Le 15 mai 2018, la Süddeutsche Zeitung a révélé que Netcom BW, une entreprise de télécommunication filiale du fournisseur d'énergie EnBW, avait été victime d'une cyberattaque[37] durant l'été 2017. Même si le piratage a été déjoué de bonne heure, il aurait été brièvement possible aux intrus, selon l'article de ce quotidien, d'épier le trafic Internet. Les attaquants ont accédé au routeur à partir du compte d'utilisateur d'un prestataire externe. Ils auraient notamment tiré parti de failles de sécurité du logiciel des routeurs Cisco. Aucun détail n'a toutefois été donné sur cette vulnérabilité. Après avoir pris le contrôle du routeur, ils ont été en mesure de charger des programmes et de s'emparer de données. Il n'y aurait eu aucun risque de sabotage, le réseau d'approvisionnement étant séparé de celui de Netcom. En outre, l'attaque aurait été découverte très tôt. Il n'a pas été possible d'identifier clairement les agresseurs. Le groupe Sandworm, qui serait responsable des attaques lancées contre le réseau électrique ukrainien durant l'hiver 2015/2016, a bien été soupçonné. Mais le nom de Dragonfly a également été évoqué, ce groupe ayant multiplié en 2017 ses attaques[38] contre le secteur énergétique, dans tout le monde occidental.

L'Office fédéral de protection de la constitution (Bundesamt für Verfassungsschutz, BfV) a mis en garde les entreprises allemandes du secteur énergétique, dans une publication parue le 7 juin 2018, contre les cyberattaques en cours du groupe APT Dragonfly. Celles-ci prenaient pour cibles l'approvisionnement énergétique, l'approvisionnement en eau et le traitement des eaux, ainsi que les technologies de l'information et de la télécommunication. Autre constat fait durant les mois précédents, les opérations[39] se concentraient sur des éléments d'infrastructure, comme les routeurs. Les outils utilisés sont le plus souvent accessibles au public, et les attaquants cherchent à prendre le contrôle des systèmes mal sécurisés. Pour y accéder, ils commencent en général par inspecter la zone de réseau d'une victime potentielle, à l'aide d'un programme de balayage automatique des ports («portscan»). L'Agence allemande de cybersécurité (Bundesamt für Sicherheit in der Informationstechnik, BSI) a lancé

---

35 http://m.faz.net/aktuell/politik/inland/hacker-angriff-war-gezielter-angriff-auf-das-auswaertige-amt-15476826.html (état: le 31 juillet 2018).

36 https://www.tagesschau.de/inland/hackerangriff-bundesregierung-101.html (état: le 31 juillet 2018).

37 https://www.sueddeutsche.de/digital/enbw-tochter-hacker-haben-deutschen-energieversorger-angegriffen-1.3980625 (état: le 31 juillet 2018).

38 MELANI, rapport semestriel 2/2017 https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2-2017.html (état: le 31 juillet 2018).

39 https://www.verfassungsschutz.de/de/oeffentlichkeitsarbeit/publikationen/pb-spionage-und-proliferationsabwehr/broschuere-2018-06-bfv-cyber-brief-2018-01 (état: le 31 juillet 2018).

à son tour, le 13 juin 2018, une mise en garde contre les cyberattaques lancées contre le secteur énergétique – mais aussi contre d'autres secteurs.[40]

De son côté, le département de la Sécurité intérieure des États-Unis (Department of Homeland Security, DHS) a fait savoir en juillet 2018 qu'au cours des dernières années, le réseau électrique américain avait été infiltré à des centaines d'emplacements. Les attaquants[41] s'étaient apparemment frayé un chemin jusqu'aux centres de contrôle, et avaient suffisamment progressé pour pouvoir «actionner les commutateurs» et ainsi endommager ou interrompre l'approvisionnement électrique. Les agresseurs s'introduisaient généralement à partir du réseau moins bien sécurisé d'entreprises tierces. À cet effet, ils envoyaient par exemple des courriels de phishing pour se procurer les informations de connexion requises. Une fois dans le réseau de leurs victimes, ils se concentraient sur leur cible première, soit les fournisseurs électriques[42].

5.1.5 Smart Install de Cisco dans le viseur des pirates

Depuis 2016 déjà, il est souvent fait état de cyberattaques lancées contre les commutateurs (switch) de Cisco, au moyen de la fonction de télémaintenance Smart Install (SMI). Le problème vient des appareils directement reliés à Internet sans la moindre protection, car cet outil ne prévoit pas d'authentification. Il incombe donc à l'exploitant d'installer une telle solution[43]. Cisco avait publié dès février 2017 une information à ce sujet[44]. Compte tenu du fonctionnement irréprochable de ses appareils, Cisco n'avait pas parlé de faille, tout en insistant sur la responsabilité des utilisateurs de veiller à la protection de leurs appareils. Le problème vient des propriétaires qui omettent de configurer ou de désactiver le protocole. Le cas échéant, le client attend constamment en arrière-plan des ordres de configuration ou d'installation. Un pirate pourra par conséquent modifier les paramètres du serveur, lire et modifier les fichiers de configuration, remplacer le système d'exploitation et créer de nouveaux comptes, ou encore exécuter toutes les commandes qu'il veut.

Entre-temps, plus de 200 000 appareils vulnérables sont accessibles depuis Internet, et il serait en théorie possible de les reconfigurer ou d'en prendre le contrôle. En Suisse, près de 1500 adresses IP de systèmes potentiellement menacés étaient connues.[45] Cisco dispose depuis la fin de 2017 d'indices montrant que les pirates explorent systématiquement les ports réseau des appareils, à la recherche de cette vulnérabilité. Comme le montre un graphique de Cisco, le trafic a explosé depuis lors sur le port de télémaintenance TCP 4786.

---

40 https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2018/Cyber_Angriffe_auf_deutsche_Energieversorger_13062018.html (état: le 31 juillet 2018).

41 https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110 (état: le 31 juillet 2018).

42 https://www.nzz.ch/international/russische-hacker-sitzen-schon-an-den-hebeln-der-amerikanischen-stromversorgung-ld.1406263 (état: le 31 juillet 2018).

43 https://www.bsi.bund.de/SharedDocs/Warnmeldungen/DE/CB/warnmeldung_cb-k17-0274_update_1.html (état: le 31 juillet 2018).

44 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170214-smi (état: le 31 juillet 2018).

45 Etat: May 2018

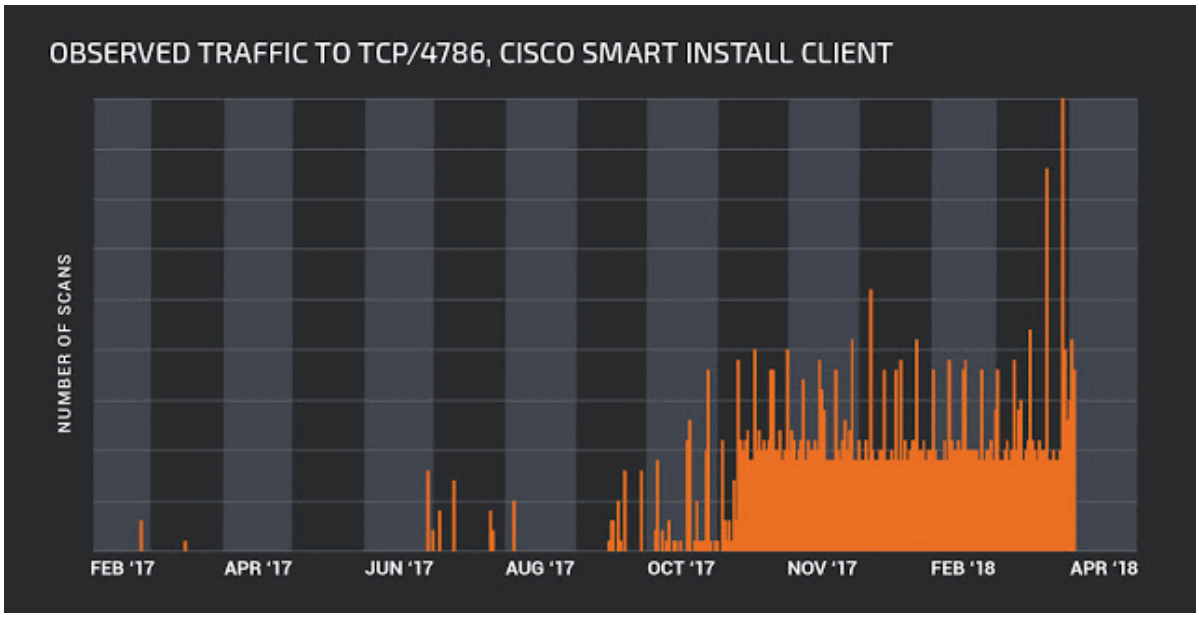


Figure 8: Nombre de cas de balayage des ports de commutateurs Cisco configurés avec la fonction Smart Install Client, entre février 2017 et avril 2018 (source: Talos, https://www.talosintelligence.com/)

Au début d'avril 2018, Cisco Talos a encore signalé une recrudescence des attaques lancées à l'aide du protocole SMI contre des infrastructures d'importance vitale[46]. Concrètement, le groupe d'espionnage Dragonfly a été évoqué. Le CERT américain avait auparavant lancé une mise en garde contre des «acteurs russes» ayant attaqué et infiltré les réseaux d'entreprises du secteur énergétique, et d'autres secteurs d'importance vitale aussi.[47]

Toujours en avril, des experts de Kaspersky ont découvert une cybercampagne visant principalement les appareils Cisco situés en Iran et en Russie. Cette vague d'attaques était apparemment due à un réseau de zombies en quête de ports 4786 ouverts et non protégés. Elle consistait à s'emparer de la fonction Smart Install, pour récrire la configuration réseau et rendre le commutateur inutilisable. Puis un message s'affichait, avec un drapeau américain et le slogan «Do not mess with our elections» [48].

La publication à la fin de mars de deux vulnérabilités permettant à un agresseur de paralyser ou contrôler les appareils Cisco a encore accru l'attention des médias. La coïncidence temporelle entre les attaques et ces deux lacunes a provoqué de nombreuses spéculations sur un possible lien de causalité. Cisco a donc tenu à préciser que les attaques observées n'avaient pas tiré parti de failles de sécurité. C'est seulement parce que les appareils avaient été mal configurés, voire pas du tout, que de tels incidents[49] s'étaient produits.

---

46 https://blog.talosintelligence.com/2018/04/critical-infrastructure-at-risk.html (état: le 31 juillet 2018).

47 https://www.us-cert.gov/ncas/alerts/TA18-106A (état: le 31 juillet 2018).

48 https://www.kaspersky.fr/blog/cisco-apocalypse/10246/ (état: le 31 juillet 2018).

49 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180409-smi (état: le 31 juillet 2018).

Appréciation / Recommandations

Les routeurs sont toujours plus dans le collimateur des cybercriminels, et cela pour trois raisons. Premièrement, il s'agit généralement du maillon le plus faible de la chaîne, faute de mises à jour rapides et systématiques. Deuxièmement, les routeurs constituent la porte d'entrée au réseau d'une entreprise: toute la communication transite par eux. Enfin, ils sont souvent directement reliés à Internet, et donc particulièrement exposés à une cyberattaque.

Comme le protocole Smart Install de Cisco n'exige pas d'authentification, un agresseur peut s'en prendre à tout appareil non protégé et accessible depuis Internet. Il est donc urgent de protéger de tels appareils des intrusions provenant de l'extérieur. En outre, il faudrait à chaque fois reprendre rapidement les mises à jour.

5.2 Systèmes de contrôle industriels

5.2.1 Piratage du système d'infodivertissement de voitures VW et Audi

En avril, des chercheurs en sécurité hollandais ont rendu publiques leurs recherches portant sur l'exploitation d'une vulnérabilité du système d'infodivertissement de certains modèles VW et Audi. Le vecteur d'attaque utilisé par les chercheurs est la connexion wifi du véhicule, par le biais de laquelle ils ont accédé à un port leur permettant de compromette le système IVI («in-vehicle infotainment» ou infodivertissement) du véhicule. Derrière ce terme assez générique se cache différents services audio et vidéo interactifs, permettant par exemple d'écouter de la musique, de recevoir des informations ou de téléphoner à l'intérieur de son véhicule. Les chercheurs ont expliqué que la compromission leur a permis d'écouter des conversations effectuées au moyen du kit mains libres, d'accéder au carnet d'adresses ou encore de suivre les déplacements du véhicule. Les chercheurs ont décidé de stopper leurs travaux[50] avant de tenter d'accéder à des systèmes d'importance vitale comme les freins ou l'accélérateur,

Ce n'est pas la première fois que la sécurité des voitures connectées se retrouve au centre des préoccupations. Il s'agit même d'un thème de recherche récurrent depuis le piratage célèbre d'une Jeep Cherokee en 2015.[51] La séparation entre les systèmes d'infodivertissement, souvent la cible des attaquants, et les systèmes d'importance vitale est centrale. Et cette recherche n'a pas permis de démontrer une porosité entre ces deux systèmes. En réponse à la divulgation d'une vulnérabilité, la mise à jour de l'ensemble d'une flotte à distance, respectivement des logiciels correspondants, serait dans tous les cas souhaitable, mais n'est pas toujours possible. Souvent, seuls les systèmes des nouveaux véhicules sont à jour, même si la possibilité pour le client de faire appliquer le correctif chez son concessionnaire existe également.

50 https://www.bleepingcomputer.com/news/security/volkswagen-and-audi-cars-vulnerable-to-remote-hacking/ (état: le 31 juillet 2018).

51 https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (état: le 31 juillet 2018).

5.2.2 «Cryptominer» parasitant une station européenne de traitement d'eau

Le succès des cryptomonnaies donne des idées aux cybercriminels. En plus des cas de vol de Bitcoins à large échelle, les criminels ont également investi le marché des cryptomonnaies par un autre biais, en détournant un processus propre à ce type de monnaie: le minage («mining»). Le minage est le processus par lequel les transactions dans une cryptomonnaie sont validées par les participants au réseau. Il consiste en calculs complexes, mobilisant des ressources informatiques importantes, et est rétribué par un certain montant de la monnaie «minée», proportionnel à la participation au calcul. Au final, le minage participe à la création monétaire. Étant donné que ce processus est lucratif, des acteurs ont cherché de bonne heure à le détourner (scénario évoqué dans notre rapport semestriel 2013/2[52]). Depuis lors, les attaques cherchant à utiliser la puissance de calcul d'ordinateurs à des fins de minage se sont multipliées. L'entreprise de cybersécurité PaloAltoNetworks a découvert plus de 470 000 échantillons de maliciels dont le but est de profiter de la puissance de calcul de la victime[53]. De plus, ce ne sont pas toujours des ordinateurs personnels, systèmes bureautiques ou encore serveurs Web qui sont touchés. En effet, selon un article de Newsportal SecurtyWeek, un exploitant d'infrastructure d'importance vitale, actif dans le traitement de l'eau au sein d'un pays européen a observé un «cryptominer» sur le réseau de production («Operational Technology network»)[54]. Dans ce cas, le maliciel ralentissait le réseau à cause de l'utilisation de la puissance de calcul et de la bande passante du réseau[55]. Bien que cette infection n'ait pas eu d'impact néfaste sur le fonctionnement du réseau, elle a coûté à l'entreprise la facture d'électricité et de la bande passante. De plus, l'infection aurait pu nuire durablement au fonctionnement de l'infrastructure, avec des conséquences pour les clients

5.2.3 Hide'n Seek – réseau de zombies P2P dans l'Internet des objets

Les réseaux de zombies qui détournent de leur fonction première des appareils dans l'Internet des objets (IdO) sont familiers au grand public, depuis le maliciel Mirai. Au début de janvier 2018, des chercheurs en cybersécurité ont découvert dans l'IdO un nouveau réseau de zombies baptisé Hide'n Seek, qui possède un mécanisme d'auto-propagation similaire à celui des vers. Le maliciel dresse une liste aléatoire d'adresses IP de victimes potentielles, avec lesquelles il communique. Si les appareils en question possèdent des ports ouverts, il cherche à établir une connexion au moyen de mots de passe standard ou de termes tirés du dictionnaire; il teste encore différentes failles de sécurité. Ce réseau de zombies possède une structure de pair à pair (P2P) décentralisée, atypique pour l'IdO. Ainsi, certains appareils échangent entre eux des informations sur leurs fructueuses tentatives de connexion et apprennent les uns des autres. À la différence de Mirai, Hide'n Seek ne se concentre pas sur les attaques par déni de service distribué (DDoS), mais privilégie l'espionnage à des fins de chantage. Ses fonctions vont de l'exfiltration de données à la mise hors service d'appareils,

---

52 MELANI, rapport semestriel 2013/2 https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2013-2.html (état: le 31 janvier 2018).

53 https://researchcenter.paloaltonetworks.com/2018/06/unit42-rise-cryptocurrency-miners/ (état: le 31 juillet 2018).

54 https://www.securityweek.com/cryptocurrency-mining-malware-hits-monitoring-systems-european-water-utility (état: le 31 juillet 2018).

55 https://radiflow.com/case-studies/detection-of-a-crypto-mining-malware-attack-at-a-water-utility/ (état: le 31 juillet 2018).

en passant par l'exécution de code à distance. Mais comme ce code malveillant n'est pas parvenu jusqu'ici à s'implanter durablement, il suffit d'un redémarrage pour nettoyer les appareils infectés.

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. Le constat vaut aussi pour l'électronique de divertissement et pour l'accès à Internet dans les transports (voitures, avion, etc.). Il faut toutefois se garder d'ignorer les risques qui s'ensuivent. Car les nouvelles possibilités induisent toujours de nouveaux risques, à prendre en compte dès le stade de la conception (security by design).

Mesures de protection des systèmes de contrôle industriels (SCI)

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

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

5.3.1 Attaque DDoS via Memcached

La cyberattaque lancée le 28 février 2018 contre la plateforme collaborative Github a été, avec sa bande passante de 1,35 Tb/s, l'une des plus virulentes attaques DDoS jamais enregistrées. L'intervention du fournisseur de services Akamai a toutefois permis d'en venir à bout rapidement[56,57]. Cette redoutable attaque DDoS reposait sur la fonction Memcached utilisée par les serveurs. Memcached est un logiciel ouvert destiné au stockage temporaire («caching») des données. Comme ces dernières sont enregistrées dans la mémoire vive, l'accès s'y fait rapidement et donc la performance, par exemple celle des applications Internet, tend globalement à s'améliorer (voir aussi chapitre 3). Le serveur écoute sur les ports TCP et/ou UDP 11211, où il est accessible à tous les internautes. À côté de TCP, le mode non connecté UDP intervient également. Les agresseurs ont ainsi la possibilité d'utiliser les services Memcached non protégés par les mesures d'usage – comme un pare-feu – pour lancer contre d'autres participants à Internet des attaques DDoS par amplification. Le problème tient à ce qu'avec un seul paquet UDP envoyé au serveur Memcached vulnérable, les attaquants peuvent atteindre un facteur d'amplification de l'ordre de 51 000, et donc générer un volume de trafic supérieur à 1 Tb/s.

Il y avait au monde 95 000 systèmes vulnérables au moment de l'attaque[58]. De nombreux exploitants ont été contactés par la suite et priés de protéger leurs systèmes. La démarche a

56 https://githubengineering.com/ddos-incident-report/ (état: le 31 juillet 2018).

57 https://blog.apnic.net/2018/03/26/understanding-the-facts-of-memcached-amplification-attacks/ (état: le 31 juillet 2018).

58 https://blog.apnic.net/2018/03/26/understanding-the-facts-of-memcached-amplification-attacks/ (état: le 31 juillet 2018).

porté ses fruits, puisque leur nombre a chuté depuis lors. En Suisse, MELANI a informé à diverses reprises des exploitants de systèmes vulnérables, dont le nombre a également diminué.

Recommandation

Le port UDP de Memcached (11211 UDP) n'est généralement pas utilisé par les systèmes d'exploitation serveur. Nous vous recommandons donc de désactiver complètement UDP en cas d'utilisation de Memcached. Il suffit de compléter le fichier de configuration de Memcached (/etc/memcached.conf) par la ligne suivante:

-U 0

Utilisez un pare-feu pour restreindre l'accès au serveur Memcached. Seuls les systèmes ayant réellement besoin d'accéder au serveur Memcached doivent pouvoir le faire.

En outre, nous vous recommandons les mesures à caractère général destinées à protéger les services en ligne. En particulier:

- Veillez à installer rapidement les mises à jour, et donc à toujours utiliser la version la plus récente de Memcached.
- Configurez Memcached de façon à ce que ce service fonctionne sous un port autre que 11211 TCP/UDP. Mais n'oubliez pas qu'à elle seule, cette mesure n'est pas suffisante. Elle ne fait que camoufler le problème, sans le résoudre.
- Surveillez votre serveur pour détecter rapidement une éventuelle utilisation abusive.

En consultant les sites suivants, vous apprendrez comment sécuriser le service Memcached.

https://www.digitalocean.com/community/tutorials/how-to-secure-memcached-by-reducing-exposure

https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Aktivitaeten/CERT-Bund/CERT-Reports/HOWTOs/Offene-Memcached-Server/Offene-Memcached-Server_node.html

5.3.2 Les systèmes internes des banques restent la cible des cybercriminels

Les systèmes internes des banques ont à nouveau été ciblés par les criminels au cours de la période sous revue. En février 2018, la banque centrale russe annonçait qu'une attaque dirigée contre un établissement du pays avait permis de dérober 339,5 millions de roubles l'année dernière (ce qui correspondait à environ 6 millions de dollars au moment de l'annonce). Pour arriver à leurs fins, les criminels ont réussi à prendre le contrôle d'une machine, sur laquelle étaient effectués des transferts d'argent par l'intermédiaire du système interbancaire SWIFT. Ni l'identité exacte de la victime, ni le mode opératoire des attaquants n'ont été communiqués.

Une attaque encore plus spectaculaire a été rendue publique en août 2018. Elle a abouti au vol de 13,5 millions de dollars à la banque indienne Cosmos. Selon les informations disponibles, cette attaque aurait compromis à la fois l'infrastructure contrôlant les distributeurs automatiques de billets de la banque et son infrastructure SWIFT. Les criminels ont ainsi pu procéder à des retraits d'argent à des distributeurs automatiques dans 28 pays différents pour

une somme totale de 11,5 millions de dollars, et effectuer des transactions via le système SWIFT pour 2 millions de dollars. Après une compromission initiale, des mouvements latéraux ont permis aux criminels d'accéder aux systèmes d'importance vitale de la banque. La sophistication des méthodes utilisées et le niveau de coordination d'une attaque se déroulant dans différents pays semblent être le signe d'un niveau avancé. L'entreprise Securonix a investigué sur l'incident et attribue l'attaque au groupe Lazarus, connu pour avoir attaqué les systèmes de différentes banques par le passé[59].

5.4 Fuites d'information

5.4.1 DHS Privacy Leak

Le département de la Sécurité intérieure des États-Unis (Department of Homeland Security, DHS) a annoncé en janvier 2018 avoir été victime d'une fuite interne de données. Les informations subtilisées concernaient plus de 240 000 employés et se rapportaient surtout à l'année 2014. Les données relatives aux personnes impliquées, entre 2002 et 2014, dans une enquête de l'autorité de surveillance du DHS – Office of Inspector General – étaient également touchées. Même les témoins et les plaignants apparaissaient dans les données dérobées, qui incluaient notamment le nom, le numéro de sécurité sociale, l'adresse postale et électronique, le numéro de téléphone et la date de naissance.

En l'occurrence, la fuite de données n'était pas due à une cyberattaque externe; il s'agissait d'un incident strictement interne. En mai 2017, il était apparu lors d'une enquête pénale qu'un ancien collaborateur du DHS avait effectué une copie non autorisée du système de gestion des dossiers de cette autorité.

Le DHS a informé ses collaborateurs par courrier et a créé à leur intention un service d'assistance téléphonique. Il a également offert aux personnes touchées un service de protection contre les usurpations d'identité et les fraudes à la carte de crédit, valable pendant 18 mois. Enfin, le DHS a adopté des mesures de sécurité[60] pour restreindre l'accès aux systèmes renfermant des données personnelles.

5.4.2 Fuite de données chez Exactis

Une base de données de l'entreprise américaine Exactis livrant des informations personnelles sur plusieurs millions de personnes a longtemps été accessible de l'extérieur, faute de toute mesure de protection. Exactis est une société de marketing basée en Floride, qui collecte des données sur les préférences et comportements de millions de personnes. L'ampleur exacte de la fuite n'est pas connue. Les enregistrements de 200 millions de consommateurs, ainsi que 110 millions de profils professionnels ou d'entreprises seraient concernés. Parmi les données figuraient des informations commerciales, des numéros de téléphone, ainsi que des adresses postales et électroniques. Par chance, il semblerait que la base de données ne renfermait pas d'informations financières, de numéros de sécurité sociale ou d'autres données

---

59 https://www.securonix.com/securonix-threat-research-cosmos-bank-swift-atm-us13-5-million-cyber-attack-detection-using-security-analytics/ (état: le 31 juillet 2018).

60 https://www.dhs.gov/news/2018/01/18/privacy-incident-involving-dhs-oig-case-management-system-update (état: le 31 juillet 2018).

sensibles. Même si les personnes concernées n'ont pas été directement lésées, les données pourraient servir à lancer à leurs dépens des attaques ciblées et personnalisées (voir chapitre 6.1).

L'incident a ceci de particulier qu'il ne s'agissait pas à proprement parler d'une cyberattaque. Le chercheur en sécurité informatique Vinny Troia avait recensé dans Internet, à l'aide du moteur de recherche Shodan, les bases de données gérées à l'aide d'ElasticSearch.[61] Celle d'Exactis s'était affichée dans les résultats et en l'absence de tout pare-feu et d'autres mesures de protection, n'importe qui pouvait y accéder. On ignore si Vinny Troia a été le premier à découvrir cette base de données ou si d'autres acteurs l'avaient repérée et copiée avant lui. Exactis a sécurisé sa base de données après avoir eu connaissance de la brèche.

5.5 Mesures préventives

5.5.1 Arrestation d'un membre du groupe Carbanak/Cobalt

Le 26 mars 2018, la police espagnole a procédé à l'arrestation d'un membre du groupe criminel à l'origine des maliciels «carbanak» et «cobalt», en partenariat avec Europol et d'autre polices nationales[62]. Ce groupe s'est fait connaître à partir de 2013 en s'attaquant à des banques et en utilisant notamment leurs distributeurs de billets pour empocher de l'argent (MELANI, rapport semestriel 2016/I[63]). Les victimes recevaient des courriels similaires à des courriels de phishing, qui contenaient un document piégé. Une fois téléchargé et exécuté, le document permettait aux membres du groupe de progresser dans le réseau de la banque à l'aide de mouvements latéraux. Le groupe est soupçonné d'avoir attaqué plus de 100 institutions financières à travers le monde, engendrant ainsi des pertes cumulées dépassant le milliard d'euros.

5.5.2 Cyber Europe 2018 – préparatifs en vue de la prochaine cybercrise

Imaginez la situation suivante: un jour ordinaire à l'aéroport, les bornes d'enregistrement en libre-service affichent une erreur système. Les applications voyage ne fonctionnent plus sur les smartphones. Les ordinateurs du personnel des comptoirs d'enregistrement se bloquent. Les voyageurs ne peuvent ni remettre leurs bagages, ni se soumettre aux contrôles de sécurité. Des files d'attente se forment partout. Tous les vols sont indiqués comme annulés sur les écrans d'affichage. Pour des raisons inconnues, le retrait des bagages ne fonctionne plus, et une bonne moitié des avions restent cloués au sol. Selon certaines informations, un mouvement extrémiste aurait pris le contrôle de systèmes aéroportuaires d'importance vitale, lors d'attaques numériques et hybrides. Il a déjà revendiqué la panne technique et utilise ses canaux de propagande pour lancer un appel à l'action et pour rallier à son idéologie extrémiste de nouveaux adeptes.

---

61 http://www.vinnytroia.com/ (état: le 31 juillet 2018).

62 https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain (état: le 31 juillet 2018).

63 MELANI, rapport semestriel 2016/1 https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2016-1.html (état: le 31 juillet 2018).

Tel est le scénario extrême auquel, les 6 et 7 juin 2018, plus de 900 experts européens en sécurité des réseaux et de l'information issus de 30 pays ont été confrontés durant Cyber Europe 2018 (CE2018), le plus ambitieux exercice de cybercoopération réalisé à ce jour par l'UE/AELE. Cyber Europe 2018 était organisé par l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), en collaboration avec les autorités et les offices compétents de toute l'Europe. La Suisse a pris part à l'exercice, avec divers participants issus de l'administration ou du secteur privé. La manifestation avait pour but d'aider les organisations à tester leurs plans d'urgence internes censés assurer la continuité des activités, avec les plans de gestion de crise correspondants. En outre, il s'agissait de promouvoir la collaboration entre les secteurs public et privé. Cyber Europe se veut en effet la réponse aux menaces transnationales, et mise à ce titre sur une étroite collaboration entre les divers pays ou organisations européens.

Points-clés de l'exercice Cyber Europe 2018:

- Pays participants: 30
  (Allemagne, Autriche, Belgique, Bulgarie, Croatie, Chypre, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Norvège, Pays-Bas, Pologne, Portugal, République tchèque, Roumanie, Royaume-Uni, Slovaquie, Slovénie, Suède, Suisse)
- Organisations participantes: 300
- Nombre de participants: plus de 900 experts en cybersécurité
- Nombre d'attaques: 23 222.

Huit ans après sa création, Cyber Europe constitue un événement majeur de la coopération pour la sécurité des réseaux et de l'information, auquel participent des centaines d'experts en cybersécurité venus des quatre coins de l'Europe. Il s'agit d'une expérience d'apprentissage sur mesure, chacun pouvant adapter l'exercice à ses propres exigences – les analystes individuels comme les organisations entières. L'accent y est mis sur la collaboration internationale entre l'ensemble des organisations participantes. La Suisse a d'emblée répondu à l'invitation et peut ainsi se targuer d'avoir pris part depuis 2010 à toutes les éditions bisannuelles de l'exercice Cyber Europe.

5.5.3 Prise de contrôle d'un serveur de commande et de contrôle de Lazarus

Le 25 avril le ThaiCERT a annoncé avoir saisi un serveur de commande et de contrôle dans une université thaïlandaise[64]. Selon l'institution, le serveur était utilisé par le groupe «Hidden Cobra», aussi connu sous le nom de «Lazarus Group». Ce groupe est notamment soupçonné d'avoir perpétré les attaques contre Sony Pictures en 2014 et contre la banque nationale du

[64] https://www.thaicert.or.th/alerts/admin/2018/al2018ad001.html (état: le 31 juillet 2018).

Bangladesh en 2016[65] (MELANI, rapport semestriel 2016/I[66]). Cette dernière attaque leur avait permis de dérober 81 millions de dollars.

Selon McAfee, l'opération nommée «Operation GhostSecret» visait des infrastructures d'importance vitale ou des institutions des domaines de la finance, de la santé et du divertissement dans plus de 17 pays, dont une entité en Suisse. Selon McAfee, le serveur fait partie d'une campagne qui visait des institutions financières en Turquie en février 2018[67].

L'attaquant dispose de plusieurs maliciels pour arriver à ses fins. Le US-CERT a publié différentes analyses sur les maliciels et estime que ces activités sont imputables à des attaquants nord-coréens[68]. Selon McAfee, au moment de la prise de contrôle, la campagne était encore au stade de reconnaissance, cherchant à obtenir des informations pour de futures attaques.

6 Tendances et perspectives

6.1 Attaques reposant sur des données dérobées

Comme le signalait le dernier rapport semestriel de MELANI[69], les fuites de données involontaires sont toujours plus nombreuses. La Suisse n'est pas épargnée, à en juger par les mésaventures de Swisscom, de dvd-shop ou de Epsitec.

Les cybercriminels savent se diversifier et innover dans l'emploi de telles données. La méthode la plus simple de gagner de l'argent avec les données piratées consiste à faire du chantage à la société dont elles proviennent. Leur valeur intrinsèque n'a guère d'importance. Le simple fait d'avoir égaré des données met une entreprise sous pression, d'autant plus à l'ère du règlement général de l'UE sur la protection des données (RGPD). Le plus célèbre exemple en Suisse de cette façon d'agir vient du groupe de pirates Rex Mundi. Or cette variante n'est que l'une des nombreuses possibilités dont disposent les escrocs. De façon générale, ils connaissent toujours mieux la valeur des données piratées, et parviennent à monnayer même des enregistrements en apparence sans valeur[70].

Les cybercriminels bénéficient du fait que sur le marché au noir, les données dérobées constituent des ressources en apparence inépuisables. À lui seul, le portail

---

65 https://threatpost.com/thaicert-seizes-hidden-cobra-server-linked-to-ghostsecret-sony-attacks/131498/ (état: le 31 juillet 2018).

66 MELANI, rapport semestriel 2016/1 https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2016-1.html (état: le 31 juillet 2018).

67 https://securingtomorrow.mcafee.com/mcafee-labs/analyzing-operation-ghostsecret-attack-seeks-to-steal-data-worldwide/ (état: le 31 juillet 2018).

68 https://www.us-cert.gov/HIDDEN-COBRA-North-Korean-Malicious-Cyber-Activity (état: le 31 juillet 2018).

69 MELANI, rapport semestriel 2017/2 https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2-2017.html (état: le 31 juillet 2018).

70 MELANI, rapport semestriel 2015/1 https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2015-1.html (état: le 31 juillet 2018).

https://haveibeenpwned.com/, où chacun peut vérifier si ses données d'accès ont été dérobées, renferme plus de cinq milliards de combinaisons de noms d'utilisateurs et de mots de passe. À cela s'ajoutent quantité d'autres informations provenant de fuites de données, de comptes de messagerie ou d'ordinateurs piratés. Une véritable filière a ainsi vu le jour au marché au noir, consistant à survoler les données et à les extraire le cas échéant pour constituer de nouvelles bases de données. Ces dernières seront ensuite revendues à d'autres cybercriminels. Le chapitre 4.5 indique divers usages possibles de telles données. On y constate une tendance des escrocs à personnaliser leurs attaques en tous genres.

Un exemple frappant vient de l'arnaque connue sous le nom de «sextorsion». Les escrocs essaient de faire croire à leur victime qu'ils sont en possession de photos intimes d'elle. Pour mener à bien leur coup de bluff, ils lui mentionnent des données personnelles qui proviennent d'une fuite de données (par ex. prénom et nom, adresse IP ou fournisseur d'accès, mots de passe ou numéro de téléphone mobile).

Les maliciels tendent eux aussi à être diffusés selon une approche toujours plus personnalisée. Il est même possible que les données dérobées amènent parfois les pirates à réorienter l'activité de leur maliciel. Une hypothèse est par exemple que les données soutirées à la société Epsitec, située à la Suisse Romande, aient permis au cheval de Troie bancaire Retefe, qui jusque-là ne sévissait qu'outre-Sarine, de s'attaquer également à des victimes en Romandie.

Les données recueillies sur la victime potentielle jouent également un rôle-clé dans l'arnaque au président (CEO fraud). Pour le moment, la plupart des escrocs passent encore au crible les sites Internet des entreprises ou les comptes sur les réseaux sociaux, afin d'échafauder un scénario adéquat. Or là encore, tout indique que les fuites de données revêtiront une importance croissante. Dorénavant les informations ainsi dérobées, comme dans le cas de l'entreprise Exactis dont un tiers des données proviennent d'entreprises, pourraient être à l'origine de telles attaques ciblées.

De façon générale, les informations recueillies lors de fuites de données aident les escrocs à mener des attaques toujours plus raffinées. Cette personnalisation semble augmenter sensiblement le taux de succès par rapport aux vagues de pourriels. Il faut donc s'attendre à ce qu'à l'avenir toujours plus de criminels optent pour cette manière d'agir.

6.2 Mise en réseau des appareils médicaux, des données de santé et des dossiers de patients

La numérisation avance à grands pas dans le secteur de la santé. Le terme «cybersanté» («eHealth») englobe tous les services électroniques se rapportant à la santé: des moyens électroniques servent à améliorer les processus, ainsi qu'à mettre en réseau les protagonistes. Le dossier électronique du patient (DEP) constitue ici la clé de voûte. Il s'agit d'un dossier virtuel, où figurent toutes les données médicales d'une personne. Le dossier électronique du patient vise à améliorer la qualité de la prise en charge médicale et des processus thérapeutiques, à augmenter la sécurité des patients, à accroître l'efficacité du système de santé ainsi qu'à encourager le développement des compétences des patients en matière de santé. Vous-même et les professionnels de la santé qui vous soignent pouvez consulter ces informations en tout temps, en passant par une connexion Internet sûre. Vous décidez librement qui peut visionner quels documents. Tout traitement du DEP est consigné. Les noms des personnes ayant visionné des documents, de même que la date à laquelle elles les ont consultés ou ont enregistré de nouveaux documents, figurent dans le journal d'accès. Cette consignation complète des accès instaure une «chaîne de confiance», qui permet de vérifier

de manière fiable et sur plusieurs phases de travail que les informations sont transmises correctement et sans subir de modification.

Il est indispensable de garantir pour le DEP la confidentialité, l'intégrité et la disponibilité des données, ainsi que la traçabilité de leur traitement. En effet, les données relatives à la santé constituent des données personnelles sensibles, non seulement parce qu'elles sont de nature privée, mais aussi parce qu'elles nous accompagnent toute notre vie (données concernant notre corps, antécédents médicaux, etc.).

Si un dossier médical tombe entre les mauvaises mains, les données ainsi divulguées (maladie spécifique, médicaments prescrits, etc.) conservent leur validité. Divers acteurs sont susceptibles d'en tirer parti. Au-delà d'une utilisation immédiate à des fins de chantage, il est possible de collecter à l'avance des données de patients pour en faire usage plus tard, sachant qu'elles seront toujours valables. Une personne est susceptible de constituer un jour une cible plus lucrative – si elle accède à un poste en vue dans la politique ou l'économie, ou si pour d'autres raisons elle devient plus vulnérable au chantage (ou si une plus grosse somme peut lui être extorquée). Par ailleurs, les données sur la santé ne sont pas seulement une cible directement exploitable pour les cybercriminels, elles pourront aussi être revendues à des acteurs économiques ou étatiques. Elles permettront par exemple d'afficher en ligne de la publicité personnalisée contre l'impuissance, ou alors de divulguer de manière ciblée une information précise, pour ne citer qu'un seul cas concret lié à la santé.

Sachant que même le système le mieux sécurisé n'est pas à l'abri d'une faille, il faudrait veiller à ce que les données médicales ne puissent être directement attribuées à une personne concrète. Lors de la pseudonymisation, on veillera à éviter à la fois que la santé du patient ne soit menacée, au cas où des professionnels de la santé se tromperaient de dossier, et que des tiers non autorisés ne puissent identifier la personne à partir du dossier.

Le DEP sera réalisé en Suisse sous forme de système décentralisé. Une telle approche est préférable pour la sûreté de l'information. En effet, tous les documents de la population suisse ne seront pas stockés au même endroit, ce qui permettra d'éviter une concentration des risques. Le délai d'introduction du DEP expire au début de 2020. De nombreux tests seront encore effectués, de façon à garantir d'ici là la sécurité du système et la confidentialité des données.

6.3 La rapidité prime sur la sécurité? – prudence avec la téléphonie mobile

6.3.1 Problèmes notoires des réseaux 2G et 3G liés au protocole SS7

La plupart des utilisateurs connaissent entre-temps les risques liés à l'utilisation de réseaux sans fil (wifi) publics[71]. Par contre, les réseaux de téléphonie jouissent de la confiance de la plupart des propriétaires de smartphones, pour ce qui est de la sécurité. Or comme MELANI

[71] https://www.melani.admin.ch/melani/fr/home/schuetzen/sekundaere-grundschutz.html (état: le 31 juillet 2018).

l'a signalé à deux reprises déjà[72,73], les réseaux de téléphonie mobile ne sont pas sans risque. Notamment quand ils servent de canal de confiance, par exemple sous forme de code SMS dans l'authentification à deux facteurs. La faille technique des réseaux de téléphonie mobile des 2e et 3e générations qu'exploitent les cybercriminels provient du protocole SS7, qui règle la coordination entre les opérateurs de téléphonie mobile, par exemple pour l'itinérance. Entre-temps, des opérateurs de l'Internet clandestin[74] proposent un service tirant parti de cette vulnérabilité. Même des entreprises légitimes[75] offrent des prestations analogues aux autorités[76]. Les opérateurs mobiles peuvent toutefois prévenir de tels abus dans leur réseau, en tirant parti de la technologie des pare-feux. Or dès qu'on est en itinérance sur un autre réseau, on est à nouveau à la merci de telles attaques, au cas où l'autre opérateur n'aurait adopté aucune mesure de protection.

D'où les espoirs placés dans les réseaux modernes de la 4e et surtout de la 5e générations, pour accroître la sécurité des clients de la téléphonie mobile. Même s'il n'existe pas encore de téléphones mobiles équipés de la technologie 5G, les discussions sur l'adjudication des fréquences nécessaires, ainsi que les résultats des premiers tests de bande passante ont relancé le débat sur les avantages de la toute dernière génération de téléphonie mobile. Avec son importante bande passante et ses temps de réaction courts, tout indique que la norme 5G accélérera le développement de l'Internet des objets (IdO) et de l'industrie 4.0 (Internet industriel des objets, IIdO). Les premiers essais pilotes[77] se sont avérés prometteurs pour le déploiement de la technologie de la nouvelle génération.

6.3.2 LTE marque un progrès, même si tout est loin d'être parfait

À l'heure actuelle, Long Term Evolution (LTE), soit la norme de téléphonie mobile de la 4e génération, constitue la solution la plus rapide et la plus répandue pour communiquer. Au lieu de SS7, LTE utilise le protocole Diameter. Or beaucoup d'attaques connues jusque-là demeurent possibles moyennant un effort un peu plus grand, en raison d'une configuration mal sécurisée, et aussi de la rétrocompatibilité avec les anciennes normes. Silke Holtmanns de Nokia Bell Labs a présenté au 34e Chaos Computer Congress ses conclusions à ce sujet[78]. De même qu'il était déjà possible de déjouer les attaques contre les anciennes normes, des

---

72 MELANI, rapport semestriel 2017/1, chapitre 5.4.5, https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2017-1.html (état: le 31 juillet 2018).

73 Voir MELANI, rapport semestriel 2/2016, chapitre 6.2: https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/halbjahresbericht-2016-2.html (état: le 31 juillet 2018).

74 https://www.theverge.com/2017/6/13/15794292/ss7-hack-dark-web-tap-phone-texts-cyber-crime (état: le 31 juillet 2018).

75 https://www.forbes.com/sites/thomasbrewster/2017/09/27/ability-inc-ss7-hackers-fail-to-sell-surveillance/#13d65f0d734c (état: le 31 juillet 2018).

76 https://www.techrepublic.com/article/ss7-flaws-used-by-surveillance-firms-highlight-need-for-better-vendor-due-diligence/#ftag=RSS56d97e7 (état: le 31 juillet 2018).

77 https://www.inside-it.ch/articles/50396 (état: le 31 juillet 2018).

78 https://www.heise.de/newsticker/meldung/34C3-Auch-4G-Mobilfunk-ist-einfach-abzuhoeren-und-zu-ueberwachen-3928496.html (état: le 31 juillet 2018).

mesures seraient sans doute envisageables[79] pour corriger ces vulnérabilités – mais tous les opérateurs ne les mettent pas en œuvre rigoureusement.

De nouveaux vecteurs d'attaques[80] ont été découverts au semestre écoulé. Des chercheurs des universités américaines de Purdue (Indiana) et de l'Iowa sont parvenus, lors d'attaques LTE par relais d'authentification, à intercepter des messages ou à obtenir des informations de localisation de l'utilisateur, et cela pour tous les grands opérateurs de réseaux américains. Il suffirait d'ailleurs d'un équipement revenant à moins de 4000 dollars pour expédier de faux avertissements de catastrophe à tous les abonnés au réseau d'une région.

Au prix d'un effort plus important, une équipe de chercheurs de l'université de la Ruhr à Bochum et de la New York University Abu Dhabi a mis au point trois nouveaux scénarios d'attaque[81] contre les réseaux LTE. Les deux variantes passives permettent d'identifier les utilisateurs du réseau et de retracer les pages Web qu'ils ont consultées. Quant à la variante active, elle tire parti d'une vulnérabilité de la méthode de chiffrement utilisée pour rediriger les internautes sur des pages frauduleuses, au moyen de réponses DNS manipulées. Là encore, les fournisseurs réseau ont réagi en montrant[82] comment déjouer de telles cyberattaques.

6.3.3 La norme 5G comblera-t-elle enfin les brèches?

Outre ses progrès tant vantés dans la transmission des données, la cinquième génération de la norme de téléphonie mobile promet une sécurité accrue, pour les opérateurs comme pour les participants au réseau. Mais si des améliorations sont prévues, certains défauts des normes antérieures n'ont pas disparu pour autant. Ainsi, la nouvelle norme reprend l'architecture Evolved Packet Core (EPC) pour faire converger dans le réseau le trafic vocal et celui des données. Or l'absence de mécanismes de chiffrement dans le protocole GTPv2 permettra de surveiller les flux de données mobiles, tout en rendant possibles des attaques DoS contre des composants du réseau[83].

Des satellites de télécommunication interviennent comme solution de repli de la norme 5G. La résilience du réseau aux pannes des stations au sol augmente au passage, ce qui est une excellente chose, mais il s'agit d'un nouveau vecteur d'attaque[84] contre la communication mobile. À partir du moment où des satellites font partie d'un scénario opérationnel, il faudrait dûment intégrer les risques correspondants dans les considérations touchant à la sécurité.

Même la toute dernière norme n'éliminera pas complètement les risques liés à la sécurité des télécommunications. Les opérateurs ont ici une grande responsabilité: il leur incombe de

---

79 https://researchcenter.paloaltonetworks.com/2018/02/sp-prevent-bad-signals-harming-network-availability/, (état: le 31 juillet 2018).

80 https://www.zdnet.com/article/new-lte-attacks-eavesdrop-on-messages-track-locations-spoof-alerts/ (état: le 31 juillet 2018).

81 https://alter-attack.net/media/breaking_lte_on_layer_two.pdf (état: le 31 juillet 2018).

82 https://blogs.cisco.com/security/protecting-against-the-latest-lte-network-attacks (état: le 31 juillet 2018).

83 https://www.darkreading.com/perimeter/new-4g-5g-network-flaw-worrisome-/d/d-id/1330062 (état: le 31 juillet 2018).

84 https://blog.trendmicro.com/trendlabs-security-intelligence/attack-vectors-in-orbit-need-for-satellite-security-in-5g-iot/ (état: le 31 juillet 2018).

décider du degré de priorité accordé à la sécurité dans la mise en œuvre de la nouvelle norme. Ils disposent pour ce faire d'outils, comme la modélisation des menaces[85] pesant sur leur propre réseau ou les expériences acquises avec la sécurité des réseaux informatiques classiques. Mais leur utilisation a un coût, et donc implique une disposition à investir de la part des opérateurs.

6.3.4 La sécurité du réseau n'offre pas une protection suffisante

Même avec la toute dernière génération de téléphones mobiles, les utilisateurs ne peuvent donc s'attendre à ce que la norme ou les opérateurs écartent tout risque lié à la sûreté de l'information. Il appartient donc à chacun d'adopter, dans la téléphonie mobile, des mesures de protection conformes aux risques liés à sa propre infrastructure et à ses applications.

Expérience à l'appui, les agresseurs n'opèrent pas qu'à partir du réseau, mais tentent aussi leur chance en étudiant de près les processus commerciaux et les collaborateurs impliqués. Bien souvent, l'authentification à plusieurs facteurs ou les processus de réinitialisation du mot de passe sont reliés au numéro de téléphone du détenteur du compte. Des escrocs habiles sont déjà parvenus à plusieurs reprises, en appelant le service à la clientèle de l'opérateur mobile[86], à faire transférer le numéro de leur victime à leur propre appareil, ou à se faire envoyer des cartes SIM de remplacement.

La nouvelle réglementation européenne sur les tarifs d'itinérance dans les États membres a encore confronté les opérateurs mobiles européens à des défis inédits quant à la disponibilité du réseau. Cette adaptation réglementaire fait que les utilisateurs profitent, dans les autres pays européens, des mêmes conditions que dans leur réseau domestique. Les voyageurs ont aussitôt renoncé à rechercher des réseaux sans fil (wifi) et utilisent à la place le réseau mobile pour transférer leurs données en déplacement aussi, ce qui a multiplié par six voire huit le trafic de données (roaming)[87]. Cette brusque hausse du trafic a amené les opérateurs des destinations de vacances aux limites de leurs capacités.

---

85 https://www.nccgroup.trust/us/about-us/newsroom-and-events/blog/2018/march/tackling-5g-security-with-threat-modelling/ (état: le 31 juillet 2018).

86 https://krebsonsecurity.com/2018/02/how-to-fight-mobile-number-port-out-scams/ (état: le 31 juillet 2018).

87 https://www.lightreading.com/regulation/roam-like-at-home-the-impact-after-one-year/a/d-id/744836 (état: le 31 juillet 2018).

7 Politique, recherche et politiques publiques

7.1 Suisse: interventions parlementaires

Objet	Numéro	Titre	Déposé par	Date de dépôt	Conseil	Dép.	États des délibérations et liens
Po	18.3003	Stratégie globale claire de la Confédération pour la protection contre les cyberrisques	Commission de la politique de sécurité	22.01.2018	CN	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183003
Mo	18.3249	Service centralisé pour lutter contre le "cyberstalking"	Marchand-Balet Géraldine	15.03.2018	CN	DFJP	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183249
Ip	18.3335	Cyberespace et droit international	Dobler Marcel	16.03.2018	CN	DFAE	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183335
Ip	18.3511	Développement d'un marché fiable pour les matériels électroniques. Mettre à profit les avantages stratégiques de la Suisse	Vonlanthen Beat	13.06.2018	CE	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183511
IP	18.434	Punir enfin le pédopiégeage en ligne	Amherd Viola	14.06.2018	CN	Parlement	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20180434
Ip	18.3556	Réduire les cyberrisques en sensibilisant la population et les entreprises	Glanzmann-Hunkeler Ida	14.06.2018	CN	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183556
Ip	18.3562	Prévoir une déclaration obligatoire des cyberattaques à MELANI	Groupe PDC	14.06.2018	CN	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183562
Po	18.3565	Couverture des dommages causés par les cyberattaques. Prévoir une limite par événement à partir de laquelle la Confédération prendrait financièrement le relais	Groupe PDC	14.06.2018	CN	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183565
Mo	18.3006	Eviter l'effondrement des réseaux de téléphonie mobile et assurer l'avenir numérique du pays	Commission des transports et des télécommunications	29.01.2018	CE	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183006
Ip	18.3013	La Poste respecte-t-elle l'égalité de traitement entre Amazon et les autres plates-formes d'e-commerce ?	Feller Olivier	26.02.2018	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183013
Q	18.5111	Un réseau WLAN dans les centres fédéraux pour requérants d'asile ?	Keller Peter	28.02.2018	CN	DFJP	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185111
IP	18.407	Inscrire la neutralité du Net dans la Constitution	Reynard Mathias	01.03.2018	CN	Parlement	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-

							vista/geschaeft?AffairId=20180407
Ip	18.3057	Le vote électronique, machine à casser la démocratie directe	Zanetti Claudio	01.03.2018	CN	ChF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183057
Mo	18.3062	Initiatives et référendums. Autoriser la collecte de signatures en ligne pour renforcer les droits populaires	Grüter Franz	05.03.2018	CN	ChF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183062
Ip	18.3197	Entité légale en Suisse pour les fournisseurs de service	Marchand-Balet Géraldine	14.03.2018	CN	DFJP	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183197
Ip	18.3222	Commerce en ligne. Distorsions de concurrence au détriment de la Suisse	Amherd Viola	15.03.2018	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183222
Mo	18.3306	Renforcer l'application du droit sur Internet en obligeant les grandes plates-formes commerciales à avoir un domicile de notification	Glättli Balthasar	15.03.2018	CN	DFJP	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183306
Mo	18.3349	Garantir la neutralité du réseau	Flach Beat	16.01.2018	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183349
Ip	18.3367	La science, atout diplomatique de la Suisse	Béglé Claude	16.03.2018	CN	DFAE	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183367
Mo	18.3379	Accès des autorités de poursuite pénale aux données conservées à l'étranger	Commission des affaires juridiques	23.03.2018	CE	DFJP	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183379
Q	18.5258	Quand la vitesse Internet minimale sera-t-elle augmentée à 10 mégabits par seconde ?	Candinas Martin	30.05.2018	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185258
Objet du CF	18.049	Loi sur les services d'identification électronique	Message du Conseil fédéral	01.06.2018		DFJP	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20180049
Ip	18.3443	La formation numérique des personnes âgées	Marchand-Balet Géraldine	04.06.2018	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183443
Ip	18.3448	Les "fake news" dans la démocratie helvétique	Marchand-Balet Géraldine	04.06.2018	CN	ChF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183448
Q	18.5321	CFF. Accès Internet gratuit	Derder Fathi	04.06.2018	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185321
Mo	18.3507	Mise en œuvre de la LSCPT conforme à la volonté du législateur	Molina Fabian	13.06.2018	CN	DFJP	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183507
Po	18.3590	Web 3.0 – Quelle place pour la Suisse dans un web décentralisé ?	Béglé Claude	14.06.2018	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183590

Ip	18.3591	Site ch.ch – quelle utilisation et quels éventuels développements ?	Wehrli Laurent	14.06.2018	CN	ChF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183591
Mo	18.3617	Créer une identité numérique 3.0. Pour une Suisse leader du secteur "blockchain" et une sécurité inédite des données personnelles	Béglé Claude	14.06.2018	CN	DFJP	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183617
Ip	18.3670	Connexion wi-fi dans les trains des CFF	Ammann Thomas	15.06.2018	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183670
Mo	18.3701	Vignette numérique optionnelle	Candinas Martin	15.06.2018	CN	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183701
Mo	18.3702	Smart data. Faire de la Suisse la championne d'une digitalisation durable et à forte valeur ajoutée	Béglé Claude	15.06.2018	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183702
Q	18.1044	Drones	Leutenegger Oberholzer Susanne	15.06.2018	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20181044
Po	18.3601	Adapter la législation en matière de drones	Marchand-Balet Géraldine	14.06.2018	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183601
Po	18.3478	Rapport du Conseil fédéral sur les mesures à envisager pour les drones	Brélaz Daniel	11.06.2018	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183478
Ip	18.3397	Régler l'utilisation privée de drones	Jositsch Daniel	28.05.2018	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183397
Q	18.5399	Drones en Suisse	Leutenegger Oberholzer Susanne	06.06.2018	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185399
Mo	18.3371	Encadrer l'utilisation des drones pour une meilleure sécurité aérienne	Candinas Martin	16.03.2018	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183371
Po	18.3245	Identification des drones et des engins balistiques similaires	Guhl Bernhard	15.03.2018	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183245
Ip	18.3463	Des villes intelligentes aux villages intelligents	Egger Thomas	07.06.2018	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183463
Ip	18.3445	Véhicules autonomes et responsabilité. A quand une adaptation de la législation helvétique ?	Marchand-Balet Géraldine	04.06.2018	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183445
Q	18.5220	Le géant internet Amazon est-il traité comme les autres clients de la Poste dans le domaine des tarifs de distribution des colis ?	Feller Olivier	28.05.2018	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185220

Q	18.1021	Pourquoi le Conseil fédéral ne se préoccupe-t-il pas davantage de la protection des données par Swisscom ?	Glättli Balthasar	16.03.2018	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20181021
Q	18.5209	Déploiement du réseau 5G en Suisse. Le Conseil fédéral peut légiférer par le biais de l'ordonnance	Derder Fathi	07.03.2018	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185209
Q	18.5167	Téléphonie mobile. Mise en place du réseau 5G sans augmenter les valeurs limites	Leutenegger Oberholzer Susanne	07.03.2018	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20185167
Ip	18.3044	Partenariat entre La Poste Suisse et Amazon	Reynard Mathias	28.02.2018	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183044
Ip	18.3575	Peut-on exclure que des enfants aient contribué à la fabrication des appareils informatiques de la Confédération?	Masshardt Nadine	14.06.2018	CN	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183575
Ip	18.3374	Logiciel pour l'enregistrement des cancers. L'adjudication douteuse à l'OFIT du développement d'une nouvelle solution gaspille-t-elle l'argent du contribuable ?	Weibel Thomas	16.03.2018	CN	DFI	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183374
Mo	18.3219	Numérique. Promouvoir la formation continue des travailleurs d'un certain âge	Kälin Irène	15.03.2018	CN	DEFR	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183219
Mo	18.3008	Documents internes à l'administration fédérale. Généraliser la signature électronique	Dobler Marcel	26.02.2018	CN	ChF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183008
Mo	18.3517	Programme d'incitations financières visant à renforcer les compétences numériques dans les écoles	Groupe PDC	13.06.2018	CN	DEFR	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183517
Mo	18.3664	Système de santé et numérisation. Remise de toutes les factures aux assureurs par voie électroniques	Grossen Jürg	15.06.2018	CN	DFI	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183664
Mo	18.365o	Améliorer la sécurité des patients au moyen d'une documentation électronique et d'un échange électronique de données médicales	Humbel Ruth	15.06.2018	CN	DFI	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183650
Po	18.3502	Généraliser la signature électronique pour les documents internes à l'administration fédérale	Dobler Marcel	12.06.2018	CN	ChF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183502

7.2 Développements politiques liés au cyberespace – état des lieux

Le Parlement devait examiner trois importantes interventions concernant le cyberespace déposées l'année dernière, soit les motions Eder (CE PLR-17.3508)[88], Dittli (CE PLR-17.3507)[89] et Grüter (CN UDC-17.3199)[90]. Entre-temps, les deux Chambres ont adopté à une large majorité la motion Eder, elles ont également adopté avec quelques adaptations la motion Dittli, tandis que la motion Grüter, avalisée par 134 voix contre 47 et 9 abstentions au Conseil national, vient d'être refusée par le Conseil des États. Le Conseil fédéral a ainsi été chargé de mettre sur pied un centre de compétence fédéral pour la cybersécurité, ainsi que de créer dans l'armée suisse un commandement comptant 100 spécialistes en informatique ou cybersoldats. Si la première cyberécole de recrue a débuté en août 2018, la mise en œuvre des mandats relevant du domaine civil prendra davantage de temps.

Dans la nouvelle stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC II) 2018-2022[91], adoptée le 18 avril 2018, le Conseil fédéral entend lutter activement contre les cyberrisques et prendre les mesures nécessaires afin de préserver la sécurité du pays face aux menaces provenant du cyberespace. La mise en œuvre de ces mesures, pour laquelle une claire répartition des compétences est prévue, s'effectuera conjointement avec les cantons, les milieux économiques et les hautes écoles. Quant au centre de compétence fédéral pour la cybersécurité, les travaux liés à ce mandat supplémentaire seront également planifiés et menés à bien dans le cadre de la mise en œuvre de la SNPC II.

Avant la pause estivale, le Conseil fédéral a pris de premières décisions relatives à la création d'un centre de compétence pour la cybersécurité, dans l'optique de renforcer ses efforts en matière de prévention et de lutte contre les cyberrisques. Selon ses premières décisions de principe, le centre de compétence sera rattaché au Département fédéral des finances (DFF) et assurera la coordination des tâches au sein de l'administration fédérale, il favorisera la prévention et sera l'interlocuteur principal pour répondre aux demandes des milieux économiques et des cantons. Par ailleurs, la collaboration avec la science et la recherche sera intensifiée. Le centre de compétence sera dirigé par une personne occupant un rang élevé dans la hiérarchie («Monsieur ou Madame Cyber»), mais qui ne sera pas habilité à donner des instructions comme le préconisait la motion Eder. Enfin, on ignore jusqu'à quel point toutes les instances compétentes seront regroupées dans un seul et même centre de cybercompétence.

La décision de désigner un Monsieur ou une Madame Cyber occupant un rang élevé dans la hiérarchie mais n'ayant qu'une fonction de coordination, sans la prérogative de donner des instructions, a été critiquée de tous côtés, et le Conseil fédéral a été prié, dans une lettre ouverte émanant des associations économiques[92] et dans une autre rédigée par la

---

88 https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173508 (état: le 31 juillet 2018).

89 https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173507 (état: le 31 juillet 2018).

90 https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173199 (état: le 31 juillet 2018).

91 https://www.isb.admin.ch/isb/fr/home/themen/cyber_risiken_ncs/ncs_strategie.html (état: le 31 juillet 2018).

92 https://www.satw.ch/fr/cybersecurite/detail/publication/au-sujet-des-decisions-de-principe-du-conseil-federal-concernant-la-cybersecurite/ (état: le 31 juillet 2018).

Commission de la politique de sécurité du Conseil national (CPS-N)[93], de doter la fonction de Monsieur ou Madame Cyber du pouvoir de donner des instructions. La CPS-N appelle encore, à titre de mesure immédiate pour la période transitoire, à débloquer rapidement des ressources humaines et financières supplémentaires, afin notamment de développer les compétences de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), ainsi que pour améliorer la cyber-résilience des infrastructures d'importance vitale.

Les décisions définitives du Conseil fédéral portant sur la création d'un centre de compétence sont attendues au plus tôt à la fin de 2018[94].

7.3 RGPD et loi sur la protection des données

Le nouveau règlement général de l'UE sur la protection des données (RGPD) est entré en vigueur le 25 mai 2018. Toute une série de changements majeurs ont été adoptés à cette date, à commencer par le droit à l'oubli, la nécessité d'informer et d'obtenir le consentement de la personne dont les données sont traitées, le droit à la portabilité des données, celui d'être informé de toute violation de données à caractère personnel engendrant un risque, ainsi que la menace, en cas de non-respect du règlement, d'amendes pécuniaires allant jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent. Des incertitudes subsistent néanmoins à propos de la mise en œuvre conforme du RGPD dans des cas d'espèce. Même si les vagues d'avertissements redoutées n'ont pas déferlé sur les entreprises basées dans l'UE, bien des sociétés ont eu d'autant plus de mal à s'adapter concrètement au règlement qu'il n'existe encore aucune pratique courante à ce sujet. Ainsi, beaucoup de sites Internet européens ont été désactivés après l'entrée en vigueur du RGPD, tandis que des journaux américains n'étaient provisoirement plus accessibles à la clientèle européenne. L'inquiétude était palpable à l'échelon des PME, des associations et des indépendants, ainsi que parmi les petites sociétés du secteur en ligne, comme les boutiques en ligne ou les blogueurs. Faute de satisfaire aux exigences du RGPD pour des raisons budgétaires ou organisationnelles, beaucoup ont craint que les amendes prévues ne menacent leur existence, et ont préféré limiter leur présence sur Internet voire y renoncer complètement.

Recommandation:

Le RGPD n'est en principe pas directement applicable la Suisse. Les hyperliens ci-après permettent de vérifier dans quels cas des entreprises suisses peuvent néanmoins être directement touchées par le champ d'application de la nouvelle réglementation:

https://www.edoeb.admin.ch/edoeb/fr/home/actualites/rgpd-last-minute.html

https://www.kmu.admin.ch/kmu/fr/home/savoir-pratique/gestion-pme/e-commerce/reglementation-ue-pour-la-protection-des-donnees.html

https://www.economiesuisse.ch/fr/datenschutz-online-check

93 https://www.parlament.ch/press-releases/Pages/mm-sik-n-2018-08-21.aspx (état: le 31 juillet 2018).

94 https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-71458.html (état: le 31 juillet 2018).

La Suisse continue de se fonder sur sa loi fédérale de 1992 sur la protection des données (LPD). Le Parlement ne s'est pas encore attelé à sa révision totale. La priorité a été donnée aux adaptations urgentes de la loi, liées aux accords de Schengen. Le Parlement a tenu à se donner davantage de temps pour la révision totale de la LPD. Il en résultera inévitablement une phase transitoire, où des problèmes risquent de se poser pour l'économie suisse et les acteurs suisses du monde en ligne. Ceux-ci doivent en effet se conformer au nouveau droit et ont besoin d'être au clair à ce sujet. Or le cadre juridique demeurera relativement opaque jusqu'à la fin du deuxième volet de la refonte totale de la LPD.

8 Produits publiés par MELANI

8.1 GovCERT.ch Blog

MELANI n'a pas publié des nouveaux blogs durant le première semestre de 2018.

8.2 MELANI Newsletter

8.2.1 Rapport semestriel MELANI: fuites de données, logiciels criminels et attaques contre les systèmes de contrôle industriels

26.04.18 - Le 26e rapport semestriel de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), publié le 26 avril 2018, porte sur les principaux cyberincidents observés au cours du second semestre 2017 en Suisse et sur le plan international. Il met notamment en évidence l'utilisation très répandue de logiciels criminels et les attaques contre les systèmes de contrôle industriels dans le domaine des appareils médico-techniques. Le thème prioritaire du rapport concerne la multiplication des fuites de données et ses conséquences.

https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/rapport-semestriel-2-2017.html

8.2.2 Les appels frauduleux aux entreprises se multiplient

05.07.2018 - Ces derniers jours, des appels aux entreprises durant lesquels des escrocs se font passer pour des employés d'une banque se multiplient. Les escrocs incitent l'entreprise à délivrer un paiement ou l'informent qu'une prétendue mise à jour concernant le e-banking devra être effectuée puis testée.

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

8.3 Listes de contrôle et instructions

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

9 Glossaire

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

	central d'un ordinateur, qui contient les circuits logiques exécutant les instructions des programmes.
Defacement	Défiguration de sites Web.
Domain Name System	Système de noms de domaine (Domain Name System). Le DNS rend les services Internet plus conviviaux, puisqu'au lieu de l'adresse IP les utilisateurs composent un nom (p. ex. www.melani.admin.ch).
Downloader	Programme dont la fonction est de télécharger et installer un ou plusieurs composants malveillants.
Elastic Search	Moteur de recherche et d'analyse écrit en Java et basé sur le projet Apache Lucene.
Faille de sécurité	Vulnérabilité dans un logiciel ou dans du matériel, grâce à laquelle un attaquant peut chercher à accéder à un système.
Fonction de hachage	Fonction calculant, à partir d'une donnée fournie en entrée, une empreinte servant à identifier rapidement, bien qu'incomplètement, la donnée initiale.
Force brute	La recherche par force brute (brute force) ou recherche exhaustive consiste, en informatique, en cryptanalyse ou dans la théorie des jeux, à tester toutes les combinaisons possibles pour résoudre les problèmes.
Global Positioning System (GPS)	Global Positioning System (GPS), dont le nom officiel est NAVSTAR GPS, est un système mondial de navigation par satellite, permettant de déterminer à un moment précis une position géographique.
Infection par «drive-by download»	Infection d'un ordinateur par un maliciel, lors de la simple visite d'un site Web. Les sites concernés contiennent dans bien des cas des offres sérieuses, mais ont été compromis auparavant pour la diffusion de maliciels. Différents exploits, tirant parti des lacunes de sécurité non comblées par le visiteur, sont souvent testés à cet effet.
Internet des objets	Ensemble des objets branchés à Internet capables de communiquer pour collecter, transmettre et traiter des données, avec ou sans intervention humaine.
Javascript	Langage de script basé objet pour le développement d'applications. Les Javascripts sont des éléments de programmes intégrés au code HTML qui permettent d'implémenter certaines fonctions dans le navigateur

	Internet. Un exemple est le contrôle des indications saisies par l'utilisateur dans un formulaire Web. Il permet de vérifier que tous les caractères introduits dans un champ demandant un numéro de téléphone sont effectivement des chiffres. Comme les composants ActiveX, les Javascripts s'exécutent sur l'ordinateur de l'internaute. Outre les fonctions utiles, il est malheureusement possible aussi d'en programmer de nuisibles. Au contraire d'ActiveX, le langage JavaScript est compatible avec tous les navigateurs.
Kit d'exploits	Outil permettant de générer des scripts, programmes ou codes, visant à exploiter des failles de sécurité.
LTE	Long Term Evolution (aussi appelée 3.9G); norme de réseau de téléphonie mobile de la 3e génération. Son développement LTE-Advanced (4G) garde une compatibilité descendante complète avec LTE.
Malware	Programme malveillant. Terme générique employé pour tout logiciel exécutant des fonctions nuisibles sur un ordinateur (comme p.ex. les virus, les vers ou les chevaux de Troie).
Métadonnées	Les métadonnées ou métainformations sont des données renseignant sur la nature de certaines au-tres données.
Minage	Utilisation de la puissance de calcul d'un ordinateur pour valider et sécuriser, par blocs, les transactions d'un réseau de cryptomonnaie. Cette activité est rémunérée à cause de sa forte consommation d'énergie.
MITM	Man-in-the-Middle attack, attaque de l'intermédiaire Attaque où le pirate s'immisce dans le canal de communication de deux partenaires pour lire ou modifier les données échangées.
Monnaie électronique	Valeur monétaire représentant une créance sur l'émetteur, qui est stockée sur un support électronique, émise contre la remise de fonds d'un montant dont la va-leur n'est pas inférieure à la valeur monétaire émise, ac-ceptée comme moyen de paiement par des entreprises autres que l'émetteur.
MS HTA	Une HTML Application (HTA) est un fichier exécutable de Microsoft avec une extension .hta et qui s'exécute à partir du navigateur Explorer, par un simple double-clic.

NAS	Serveur de stockage en réseau (Network Attached Storage); serveur de fichiers autonome, relié à un réseau pour permettre à ses utilisateurs de stocker et de mettre en commun leurs données.
P2P	Peer to Peer Architecture de réseau où tous les postes de travail ont les mêmes possibilités de communication (à l'inverse des réseaux client/serveur). P2P sert fréquemment aux échanges de données.
Patch	Programme qui remplace une partie de programme comportant des erreurs par une partie exempte d'erreurs et remédie ainsi par exemple à une lacune de sécurité.
Phishing	Via l'hameçonnage, des pirates tentent d'accéder aux données confidentielles d'utilisateurs Internet ne se doutant de rien. Il peut s'agir p. ex. d'informations concernant les comptes pour des soumissionnaires de ventes aux enchères en ligne (p. ex. eBay) ou des données d'accès pour le e-banking. Les pirates font appel à la bonne foi, à la crédulité ou à la serviabilité de leurs victimes en leur envoyant des courriels avec des adresses d'expéditeur falsifiées.
PKI	infrastructure à clé publique (Public Key Infrastructure) Système de gestion des clés de chiffrement et des certificats numériques.
Port (logiciel)	Dans la couche de transport du modèle OSI, la notion de port logiciel permet, sur un ordinateur, de distinguer divers interlocuteurs, soit les programmes qui écoutent ou émettent des informations sur ces ports. Un port est distingué par son numéro.
Porte dérobée	Une porte dérobée (en anglais: backdoor) désigne une fonctionnalité inconnue de l'utilisateur légitime, qui permet à un pirate d'accéder secrètement à un programme ou à un système d'exploitation, en contournant les mécanismes de sécurité en place.
Pourriel (Spam)	Désigne le courrier électronique non sollicité, constitué surtout de publicité, envoyé automatiquement. L'auteur de tels messages est qualifié de polluposteur (spammer) et ses envois de pollupostage (spamming).
PowerShell (script)	PowerShell est une suite logicielle Microsoft qui intègre une interface en ligne de commande et un langage de script, permettant d'automatiser des tâches ou de configurer et d'administrer des systèmes.

Proxy	Programme servant d'intermédiaire pour accéder à un autre réseau, en collectant les requêtes et en les transmettant vers l'extérieur à partir d'une même adresse.
RC4 (chiffrement)	Algorithme de chiffrement en continu conçu en 1987 par Ronald L. Rivest; les spécifications de RC4 (Ron's Code 4), marque déposée de RSA Security, n'ont jamais été officiellement publiées (selon le principe de la sécurité par l'obscurité).
Remote Administration Tool ou Remote Access Tool (RAT)	Un Remote Administration Tool, outil de télémaintenance, est un programme permettant la prise de contrôle totale, à distance, d'un ordinateur depuis un autre ordinateur.
Router	Dispositif intelligent assurant la connexion physique entre plusieurs réseaux (informatique, télécommunication, Internet). Un router s'utilise par exemple dans un réseau domestique, où il optimise la transmission de l'information entre le réseau interne et Intranet.
Serveur Command & Control	La plupart des réseaux de zombies reçoivent des instructions de leur créateur, qui les surveille par un canal de communication. Le cas échéant, on parle de serveur Command & Control (C&C).
Smartphone	Un smartphone est un téléphone mobile doté des fonctions d'un assistant numérique personnel (agenda, calendrier, navigation Web, consultation du courrier électronique, messagerie instantanée, GPS, etc.).
SMS	Short Message Service Service de messages courts. Service permettant d'envoyer des messages courts (max. 160 caractères) à un (utilisateur de) téléphone mobile
Social Engineering	Les attaques de social engineering (subversion psychologique) utilisent la serviabilité, la bonne foi ou l'insécurité des personnes pour accéder par exemple à des données confidentielles ou conduire la victime à exécuter certaines actions spécifiques.
Spear Phishing	Pêche au harpon. La victime aura p. ex. l'illusion de communiquer par courriel avec une personne connue d'elle.

Spearphishing-Mails	Pêche au harpon. La victime aura par ex. l'illusion de communiquer par courriel avec une personne connue d'elle.
SS7	Le système de signalisation n° 7 (signaling system #7, SS7) et un ensemble de protocoles de signalisation téléphonique utilisés dans les réseaux de télécommunication. On le trouve dans le réseau téléphonique public (ISDN, téléphonie fixe ou mobile) et toujours plus souvent aussi dans les réseaux VoIP.
SSH	Secure Shell Protocole permettant grâce au chiffrement des données d'ouvrir une session (login) sécurisée sur un système informatique accessible par l'intermédiaire d'un réseau (p.ex. Internet).
Systèmes de contrôle industriels (SCI)	Les systèmes de contrôle-commande sont formés d'un ou plusieurs appareils qui pilotent, règlent et/ou surveillent le fonctionnement d'autres appareils ou systèmes. Dans le domaine industriel, l'expression «systèmes de contrôle industriels» (Industrial Control Systems, ICS) est entrée dans le langage courant.
Take Down	Retrait de contenu frauduleux, désactivation d'adresse Web par un hébergeur ou un registraire.
TCP/IP (Transmission Control Protocol / Internet Protocol)	Ensemble de protocoles de communication conçu pour la transmission des données sur Internet.
Top-Level-Domains	Tout nom de domaine dans Internet est formé d'une série de signes séparés par des points. Le domaine de premier niveau ou de tête (TLD) désigne le dernier élément de cette série et se situe au niveau hiérarchique le plus élevé du nom. Par exemple, si le nom de domaine d'un ordinateur ou d'un site est de.example.com, le TLD sera «com».
UDP	User Datagram Protocol; protocole sans connexion, utilisé pour expédier de petits messages (datagrammes) d'une application Internet à l'autre.
USB	Universal Serial Bus Bus série permettant (avec les interfaces physiques) de raccorder des périphériques tels qu'un clavier, une souris, un support de données externe, une imprimante, etc. Il n'est pas nécessaire d'arrêter l'ordinateur pour brancher ou débrancher un appareil USB. Les nouveaux appareils sont

	généralement (selon le système d'exploitation) reconnus et configurés automatiquement.
Ver	A la différence des virus, les vers n'ont pas besoin de programme hôte pour se reproduire. Ils utilisent les lacunes de sécurité ou des erreurs de configuration des systèmes d'exploitation ou des applications, pour se propager d'ordinateur en ordinateur.
Watering Hole Attack	Attaque dite du point d'eau, attaque ciblée par un maliciel, diffusé à traversdes sites supposés être visités par un groupe spécifique d'utilisateurs.
WLAN	Un WLAN (Wireless Local Area Network) est un réseau local sans fil.
Zero-Day	Vulnérabilité, pour laquelle aucun correctif de sécurité n'est pour l'instant disponible.
Zip	zip est un algorithme et un format de compression des données destiné à réduire l'espace mémoire occupé par les fichiers lors de l'archivage ou du transfert.