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 2017/II (juillet à décembre)

26 AVRIL 2018

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

1 Aperçu / sommaire

2 Éditorial

Werner Meier
Délégué à l'approvisionnement économique du pays

Chère lectrice, cher lecteur,

La numérisation offre de formidables opportunités à notre pays – mais nous confronte également à des défis de taille. Car si l'on veut pouvoir piloter et optimiser durablement les processus économiques à l'aide de moyens informatiques, ces derniers doivent être en tout temps disponibles, fiables et résistants aux perturbations ainsi qu'aux cyberattaques. En bref, la sûreté de l'information est une condition sine qua non de la numérisation à venir.

Le Conseil fédéral prend très à cœur la numérisation. Il l'a prouvé dans sa stratégie «Suisse numérique», où la «sécurité» constitue un des quatre objectifs principaux. De même, le comité consultatif que deux départements fédéraux (DEFR et DETEC) ont créé en été 2017 pour accompagner la mise en œuvre de cette stratégie a placé la cybersécurité en tête de ses priorités.

L'Approvisionnement économique du pays (AEP) a pour mandat légal de garantir en cas de crise l'approvisionnement de la Suisse en biens et services d'importance vitale. Dans ce contexte, l'informatique est non seulement en soi essentielle, elle s'avère encore une ressource indispensable au bon approvisionnement de notre pays, par exemple en énergie électrique ou en prestations logistiques. Pour atteindre ses ambitieux objectifs, l'AEP dispose depuis la révision de la loi sur l'approvisionnement du pays d'une base légale moderne, tandis que son réseau de décideurs économiques complète ponctuellement son savoir-faire.

Ces derniers mois, l'AEP a conçu des normes minimales générales pour l'information et la communication qui, dans le cadre de la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), aident à améliorer la résilience. Sur la base d'un outil créé par l'Institut national américain des normes et de la technologie (NIST Cybersecurity Core Framework), quelque 106 mesures décrivent comment les exploitants d'infrastructures d'approvisionnement d'importance vitale peuvent protéger leurs ressources informatiques. Ces normes minimales générales seront prochainement présentées au grand public et accessibles à tout le monde. Aujourd'hui déjà, l'Association des entreprises électriques suisses (AES) s'en inspire pour élaborer un pendant destiné à la branche électrique. Cette future norme, à laquelle l'AEP a largement contribué, servira à l'autorégulation de ce secteur économique. D'autres normes informatiques minimales sont en chantier pour les eaux usées ainsi que pour l'approvisionnement en eau, en gaz et en huiles minérales.

En d'autres termes, l'AEP n'apporte pas qu'une contribution active à la numérisation de la Suisse, mais encourage encore la résilience informatique de nos infrastructures d'approvisionnement d'importance vitale face aux pannes, aux perturbations et aux cyberattaques. Le présent rapport de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI vous montrera une fois de plus, à l'aide d'exemples concrets, à quel point c'est nécessaire. Il ne me reste qu'à vous souhaiter une bonne lecture.

Werner Meier
Délégué à l'approvisionnement économique du pays

3 Thème prioritaire: fuites de données

Des millions de fichiers renfermant des informations personnelles sont générés et enregistrés au quotidien dans le monde numérique. Par exemple lorsque vous présentez votre carte de fidélité à la caisse d'un supermarché, chaque fois que vous payez par carte de crédit ou effectuez des achats en ligne, que vous consultez votre messagerie ou en cas de visite médicale. La liste pourrait être développée à loisir. Chacun laisse en particulier des dizaines de traces de son passage par jour, en naviguant sur Internet.

Si ces données tombent entre de mauvaises mains, des abus sont à craindre. Les fuites de données sont hélas toujours plus fréquentes, et le deuxième semestre 2017 n'a pas fait exception à la règle. En octobre, le géant d'Internet Yahoo! a reconnu que le vol survenu en 2013, qui portait sur plus de trois milliards de données, avait touché tous ses utilisateurs et non une partie d'entre eux, comme on l'avait cru jusque-là.[1] C'est à ce jour la plus spectaculaire fuite de données de l'histoire. Le portail «have I been pwned»[2] livre lui aussi un chiffre impressionnant. Chacun peut y vérifier si son adresse électronique a déjà été piratée. Le nombre de mots de passe dérobés est dramatiquement élevé, puisqu'il s'élève aujourd'hui sur ce site à près de cinq milliards.

En Suisse aussi, des données ont été subtilisées au cours des derniers mois. Swisscom a fait savoir qu'en octobre 2017, des personnes non autorisées avaient eu accès à plus de 800 000 données de clients. En novembre, Galaxus/Digitec soupçonnait des escrocs de lui avoir dérobé des données de clients et en décembre, le Groupe Mutuel Assurances rendait publique une fuite de données. Toujours en décembre, MELANI apprenait la mise en circulation de 70 000 jeux de données qui, par la suite, ont pu être attribués à la société suisse dvd-shop.

Entre-temps, des données dérobées avec mots de passe, données de carte de crédit et autres données personnelles apparaissent régulièrement dans les portails spécialisés. Il est toutefois difficile dans de nombreux cas d'en vérifier la provenance, l'ancienneté et la qualité. Tout indique que bien souvent, la disparition n'avait même pas été remarquée.

3.1 Définition

Les fuites de données sont des incidents de sécurité, où des tiers non autorisés s'approprient des données personnelles, secrets professionnels ou d'autres types de données. Le terme fuite de données est défini de manière très ouverte et englobe également, en plus du vol de données et de l'espionnage, des défaillances lors desquelles des données sont rendues accessibles de manière involontaire. Le spectre des données concernées ne se limite pas aux mots de passe et aux données de cartes de crédit, mais s'étend au secteur de la santé et au domaine financier par exemple.

---

1 http://www.sueddeutsche.de/digital/yahoo-hackerangriff-bei-yahoo-traf-alle-drei-milliarden-konten-1.3693671 (état: le 31 janvier 2018).

2 https://haveibeenpwned.com/ (état: le 31 janvier 2018).

3.2 Chantage, collecte de données et coups politiques

Une méthode fréquente utilisée par les criminels pour s'enrichir avec des données dérobées consiste à faire chanter leur propriétaire légitime. L'un des plus anciens cas en Suisse remonte à 2014. Un groupe se faisant appeler Rex Mundi avait menacé une entreprise romande de publier des données subtilisées. Les escrocs s'en prennent parfois aussi aux clients de l'entreprise piratée.

Les données dérobées peuvent également servir à lancer des attaques ciblées. Dans le marché clandestin, des acteurs se sont spécialisés dans la compilation d'informations sur une victime potentielle. Outre les renseignements accessibles à tout le monde, ils se servent de données volées. Le cas échéant, des attaques très ciblées seront déployées. Dans la période sous revue, MELANI a notamment constaté la diffusion de courriels munis d'un maliciel qui, outre le titre, le prénom et le nom du destinataire, indiquaient encore son numéro de téléphone ou son adresse postale.

La divulgation de données à des fins politiques est un cas à part. Le cas le plus connu est la publication des fichiers Snowden. Après Edward Snowden, beaucoup d'autres acteurs ont cherché avec la même méthode à éveiller les consciences ou à transformer la société. On peut rappeler par exemple la publication des «Panama Papers» ou des «Paradise Papers». De tels documents révélaient les pratiques commerciales liées à la finance offshore de dirigeants politiques et d'autres personnalités en vue du monde entier.

3.3 Conséquences

Qu'impliquent de telles fuites pour les victimes, et quelle est la gravité des dommages? La réponse doit être nuancée, car chacun définit différemment la valeur de ses données. Dans le cas des particuliers, certains se moquent que des tiers collectent et exploitent des informations les concernant. D'autres par contre cherchent à limiter autant que possible le volume de données enregistrées à leur sujet. Ces gens jugent bien plus grave le dommage personnel subi.

La nature des données dérobées joue également un rôle. On peut à chaque fois distinguer entre les données qu'il est aisément possible de réinitialiser, et celles qui subsistent à vie. Les mots de passe et les données d'une carte de crédit peuvent être rapidement modifiés, et donc le dommage reste éphémère. Par contre, si les données divulguées concernent la santé, les préférences personnelles ou la situation financière, il n'est pas possible de les «réinitialiser» et le dommage causé sera durable. Des escrocs peuvent ainsi nuire à une victime des années après une fuite de données. Pour aggraver les choses, la victime n'est bien souvent même pas au courant que des données ont été piratées, et ne peut donc ni se défendre, ni se protéger.

Dans le cas des entreprises, les fuites de données occasionnent non seulement un lourd surcroît de travail, mais peuvent ruiner une réputation. La communication avec la clientèle est ici déterminante. Il est par conséquent primordial pour une entreprise de bien se préparer à une éventuelle perte de données. À ce titre, il faut une planification d'urgence, une communication bien rodée et une répartition précise des responsabilités. MELANI recommande de façon générale, en cas de fuite de données, d'opter pour la transparence avec les clients concernés. Il est important de les alerter au plus vite, pour limiter autant que

possible les dommages indirects. La difficulté consiste ici à communiquer de façon calme et posée.

3.4 Information des victimes

Quand une entreprise s'est fait dérober des données, la question de l'information à donner aux clients se pose rapidement. La société lésée est la mieux à même de communiquer à ce sujet. Elle seule possède la vue d'ensemble des clients touchés, de la nature et de la quantité de données subtilisées, et pourra recommander les mesures adéquates, à l'instar de la réinitialisation des mots de passe. Il faut s'assurer en pareil cas que des tiers n'en profitent pas pour obtenir des informations sur les victimes du vol de données. Quand on lui demandait si son compte était concerné, le Groupe Mutuel exigeait par exemple une copie d'une pièce d'identité avant de répondre.

Il est plus difficile encore d'informer les victimes d'une fuite de données dont on ignore l'origine. Des portails comme «Pastebin» signalent régulièrement des combinaisons de nom d'utilisateur et de mot de passe dont la provenance n'a pu être déterminée. Dans le passé, MELANI a déjà reçu plusieurs listes de jeux de données dérobés. Dans de tels cas, les internautes ont été priés de vérifier eux-mêmes à l'aide de l'outil MELANI Checktool s'ils étaient concernés ou non. Les retours de la population permettent fréquemment d'identifier l'origine de la fuite. Une fois celle-ci établie, il incombe selon MELANI à l'entreprise concernée d'en informer sa clientèle et le grand public.

3.5 Protection des données

La protection des données personnelles est régie par la loi fédérale sur la protection des données (LPD). Cette loi vise à protéger la personnalité et les droits fondamentaux des personnes physiques et morales qui font l'objet d'un traitement de données. Une distinction y est faite entre les données personnelles et les données sensibles. Relèvent de la seconde catégorie les données personnelles sur les opinions ou activités religieuses, philosophiques, politiques ou syndicales, la santé, la sphère intime ou l'appartenance à une race, des mesures d'aide sociale, ainsi que des poursuites ou sanctions pénales et administratives. Le consentement explicite de la personne est requis pour leur traitement. La LPD tient également compte de l'aspect de la sécurité, en prévoyant que les données personnelles doivent être protégées contre tout traitement non autorisé par des mesures organisationnelles et techniques appropriées.

La révision totale de la loi fédérale sur la protection des données suit son cours. Tout indique qu'elle reprendra différentes nouveautés du règlement général de l'UE sur la protection des données, que tous les États membres de l'UE sont tenus d'appliquer au 25 mai 2018, soit dans un délai de deux ans à compter de son adoption. Toutes les entreprises suisses y sont soumises, même sans avoir d'établissement dans l'UE, dès lors qu'elles offrent des biens ou services à des personnes se trouvant dans l'UE (condition remplie à partir du moment où leur site Web ou une boutique en ligne renferme de telles offres), qu'elles traitent des données de personnes domiciliées dans l'UE ou qu'elles analysent le comportement de personnes se trouvant dans l'UE. Les principaux changements apportés par le règlement sont les suivants: droit à l'oubli; traitement des données exclusivement avec le consentement explicite de la personne concernée; droit à la portabilité des données (transfert gratuit d'un prestataire de services à un autre); droit des intéressés d'être informés en cas de violation de données à caractère personnel, et enfin sanctions plus sévères en cas d'infraction au règlement.

Concrètement, une entreprise s'expose à des amendes en espèces jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent.

Cette dernière prescription en particulier pourrait amener les entreprises à revoir leur attitude face aux fuites, afin de privilégier la sécurité des bases de données et du traitement de leurs données. Les cybercriminels seront toutefois encore plus incités à monnayer les fuites de données. Une offre d'un montant inférieur à l'amende encourue inciterait sans doute l'une ou l'autre des victimes à céder à leur chantage.

3.6 Causes des incidents et protection

Les fuites de données peuvent avoir de multiples causes, allant du vol de données par des collaborateurs aux sauvegardes mal protégées, en passant par les serveurs oubliés ou dont la maintenance laisse à désirer.[3]

3.6.1 Attention aux cimetières de données

Chacun a tendance à sauvegarder toutes les données qu'il a collectées un jour ou l'autre, même si elles sont inutiles ou périmées depuis longtemps. On trouve ainsi dans le carnet d'adresses de chaque téléphone mobile des contacts périmés depuis longtemps. Ces données «oubliées» font que le moindre incident prend sans raison des proportions spectaculaires. En cas de migration de serveur notamment, on veillera à ce que les données des anciens systèmes soient ensuite effacées. De même, une durée de vie devrait être assignée à chaque jeu de données, afin que sa validité soit périodiquement contrôlée. Il ne faudrait par ailleurs extraire et enregistrer que les données réellement nécessaires. Outre qu'il s'agit d'une exigence de la loi fédérale sur la protection des données (art. 4, al. 2, LPD, proportionnalité), on réduit ainsi fortement l'ampleur des fuites de données, puisque peu de données sont enregistrées.

3.6.2 Protéger l'accès / réduire le trafic

Les accès externes devraient être limités au strict minimum, et spécialement protégés et surveillés. Chaque entreprise doit se demander qui a besoin d'accéder à quelles données, et comment cet accès peut être sécurisé. Les ports inutilisés devraient par exemple être impérativement bloqués.

Le trafic sortant devrait être limité aux connexions nécessaires. De nombreuses attaques nécessitent que le système infecté télécharge du code depuis Internet. Ceci se déroule souvent de manière automatisée. L'interdiction du trafic sortant complique ainsi grandement la tâche de l'attaquant.

Qu'il s'agisse d'une application professionnelle ou au contraire d'un formulaire de contact peu sensible, les données fournies par l'utilisateur devraient être redirigées vers un serveur backend n'étant pas atteignable depuis Internet.

Il est fortement recommandé de prévoir un deuxième facteur d'authentification pour l'accès externe. En cas d'utilisation très large, les procédures basées sur un mot de passe à usage

---

[3] Les pièges les plus courants sont documentés dans un Top 10 du projet OWASP (Open Web Application Security Project). Cette liste est régulièrement actualisée. https://www.owasp.org/

unique (one time password, OTP), à l'instar de l'application Google Authenticator téléchargeable sur le smartphone, ont fait leurs preuves.

Tous les logiciels ou applications serveurs doivent être tenus à jour. S'il n'existe pas de rustine pour remédier à une lacune de sécurité ou à défaut de pouvoir l'installer, des mesures adéquates réduiront les risques. Il est recommandé d'utiliser un pare-feu d'applications (Web application firewall): il existe toutes sortes de produits commerciaux ou gratuits pour mieux protéger les applications Web. La plupart de ces produits proposent également des règles contre les vulnérabilités les plus courantes (OWASP Top 10).

3.6.3 Sauvegardes mal protégées

Les sauvegardes de données (backups) constituent une véritable assurance-vie pour toute entreprise, et à ce titre doivent satisfaire aux mêmes exigences de sécurité que les données du système de production. Les données archivées sur des discs durs externes devraient également être chiffrées.

3.6.4 Mots de passe non protégés

Si des mots de passe figurent parmi les données dérobées, il convient de veiller à ce qu'ils ne puissent pas être aisément déchiffrés. Cela suppose l'emploi d'une fonction de hachage (hash function)[4] et d'un sel (salt). Lors du salage (salting), une donnée supplémentaire que le système est seul à connaître est ajoutée au mot de passe avant le hachage. Ce sel ou chaîne de caractères aléatoires, que l'on choisira aussi long que possible, est généré à nouveau à chaque création de mot de passe. On veillera encore à utiliser une fonction de hachage lent. De cette manière, le calcul des mots de passe hachés est encore plus complexe et s'effectue au ralenti. L'utilisateur ordinaire ne remarque guère que la procédure d'enregistrement demande quelques millièmes de seconde en plus. Mais pour le pirate qui doit effectuer des millions de calculs, le temps requis pour casser le code devient décourageant.

3.6.5 Vols internes

Les données sont parfois aussi dérobées par d'anciens ou d'actuels collaborateurs mécontents, qui cherchent à nuire à leur employeur ou s'octroyer un avantage personnel. Pour y remédier, il convient de créer un climat de travail ouvert et agréable, où chacun puisse parler franchement des problèmes. Il est également important de s'assurer que les collaborateurs n'aient accès qu'aux données nécessaires à l'exécution de leur travail. Il faut immédiatement retirer tous les accès aux anciens collaborateurs, ce qui suppose une politique adéquate d'accès au réseau.

[4] Une fonction de hachage est une fonction mathématique associant à des données (ici un mot de passe) une empreinte de taille fixe, qui permet d'en vérifier l'intégrité.

4 Situation nationale

4.1 Espionnage

4.1.1 La Confédération à nouveau victime d'une cyberattaque

Le logiciel d'espionnage Turla a été découvert en juillet 2017 sur certains serveurs du Département fédéral de la défense, de la protection de la population et des sports (DDPS). Ce maliciel n'est pas inconnu dans l'administration fédérale. C'est également Turla qui, en décembre 2015, avait attaqué le groupe technologique proche de la Confédération RUAG, responsable notamment d'assurer l'équipement de l'armée. À l'époque, les pirates avaient réussi à subtiliser plus de 20 gigaoctets de données. Dans le cas actuel, le maliciel a été découvert de bonne heure, avant d'avoir pu dérober des données sensibles ou infecter d'autres systèmes raccordés au réseau. L'agresseur avait pourtant renforcé son infrastructure, étoffé sa gamme d'outils et son mode opératoire dénotait une sophistication grandissante. Les services fédéraux compétents ont procédé à temps aux vérifications nécessaires et adopté les mesures utiles. La collaboration entre les services fédéraux concernés a été très fructueuse et a livré de précieuses informations sur les méthodes d'attaque et les indicateurs techniques. Les échanges à ce sujet sont déterminants au niveau national comme sur le plan international, afin de détecter les attaques en cours ou en préparation. Le Conseil fédéral, les membres de la Délégation du Conseil fédéral pour la sécurité ainsi que les présidents des commissions compétentes ont été aussitôt informés, comme l'usage le veut lors de tels incidents. À la suite de cette cyberattaque contre ses serveurs, le DDPS a en outre adressé une dénonciation contre inconnu au Ministère public de la Confédération.[5]

4.2 Systèmes de contrôle industriels

La presse fait régulièrement état des graves menaces subies par des systèmes de contrôle industriels (Industrial control system ICS) reliés à Internet, comme des systèmes de commande d'usine ou des pompes de centrales hydroélectriques[6], ou encore des appareils médico-techniques[7]. De tels systèmes sont vulnérables, par exemple si une de leurs composantes présente une faille de sécurité, ou s'ils n'ont pas été configurés de manière suffisamment sûre.

Bien souvent, quand de tels cas sont découverts, les exploitants des infrastructures attaquées se voient reprocher de ne pas avoir effectué à temps les mises à jour. Or il peut parfois y avoir de bonnes raisons qui retardent voire empêchent la reprise des programmes correctifs. Par exemple, lorsque la mise à jour d'une composante risque de faire perdre sa certification à tout le système. Il est donc bien plus important de planifier et d'exploiter dans un souci de robustesse le paysage système et le réseau où se trouvent ces appareils, afin que d'éventuelles failles ne mettent pas en danger les fonctions essentielles.[8] Même dans la liste

---

5 https://www.vbs.admin.ch/fr/actualites/communiques.detail.nsb.html/68135.html (état: le 31 janvier 2018).

6 http://www.spiegel.de/netzwelt/web/so-bedrohen-hacker-wasserversorgung-stromnetz-und-kliniken-a-1181325.html (état: le 31 janvier 2018).

7 https://nakedsecurity.sophos.com/2018/02/01/hospital-mri-and-ct-scanners-at-risk-of-cyberattack/ (état: le 31 janvier 2018).

8 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf (état: le 31 janvier 2018).

de contrôle de MELANI «Mesures de protection des systèmes de contrôle industriels (SCI)», on constate que la gestion des correctifs n'est qu'une des onze mesures à prendre. Plusieurs des dix autres mesures sont propres à atténuer les risques: une architecture réseau robuste garantit par exemple que dans la zone du réseau dont fait partie l'appareil vulnérable, il n'y ait au mieux que les systèmes nécessaires pour communiquer avec lui. Les accès et sorties de la zone seront réduits au strict nécessaire et soigneusement surveillés. Les collaborateurs ne devraient avoir en tout temps que les droits dont ils ont réellement besoin pour exécuter les tâches confiées. L'analyse centrale des fichiers journaux (log) permet par ailleurs de contrôler si tous les systèmes fonctionnent comme ils devraient. Et si malgré toutes ces précautions une cyberattaque devait être constatée, le processus de gestion des incidents de sécurité s'avère ici utile. En effet, si la réaction à un incident de sécurité a été définie et a fait l'objet d'exercices avec toutes les personnes impliquées, il devient possible de réduire au minimum les dommages potentiels.

On trouve dans la littérature spécialisée le concept de défense en profondeur («defense in depth»)[9], qui consiste à maîtriser un risque inévitable en déployant une ou plusieurs autres stratégies de défense. La fig. 1 montre un exemple d'architecture réseau d'un système de contrôle industriel.

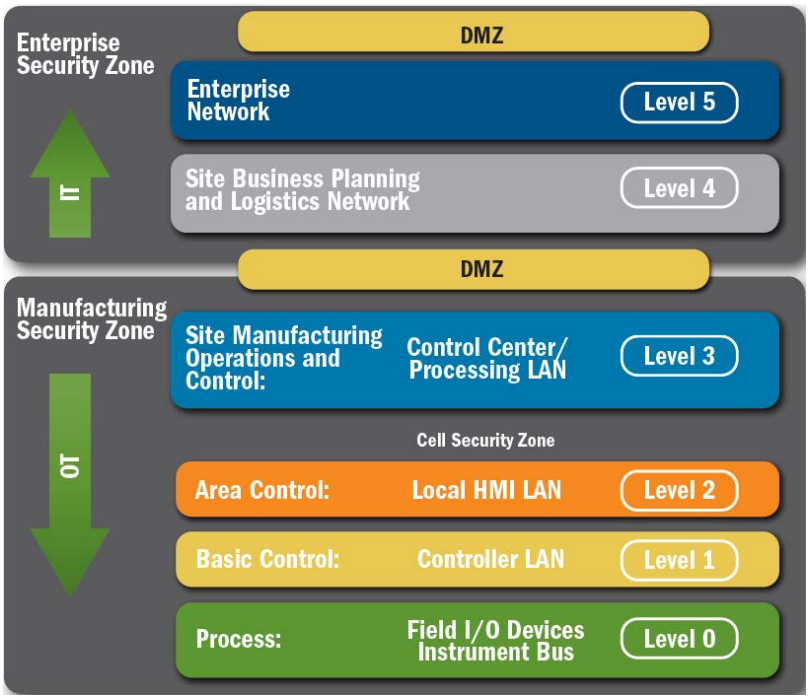

Fig. 1: Architecture d'un réseau interne de SCI découpé en deux zones, préconisée par l'ICS-CERT

Ces recommandations ont beau aller toutes de soi et être aisément réalisables quand on les envisage isolément, leur mise en œuvre dans des systèmes complexes requiert souvent des ressources dont on ne dispose pas. On a également tendance à faire primer l'achèvement d'un projet dans les délais ou la simplicité opérationnelle des processus sur la sécurité. Il est dès lors indispensable, pour faire un usage optimal des ressources limitées, de mettre en place

9 https://ics-cert.us-cert.gov/Abstract-Defense-Depth-RP (état: le 31 janvier 2018).

une gestion globale des risques, où les risques résiduels soient reconnus et assumés par l'équipe dirigeante.

Recommandation:

Si vous découvrez des systèmes de contrôle ouverts au premier venu ou mal protégés, veuillez nous indiquer 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

4.2.1 Stimulateurs cardiaques à la merci des pirates

Un stimulateur cardiaque, ou pile cardiaque, est un appareil similaire à un mini-ordinateur, dont les composants mémorisent et analysent le rythme cardiaque, et déclenchent une impulsion électrique lorsqu'il devient insuffisant. Beaucoup de ces engins qui prolongent la vie disposent d'une interface radio, afin de rendre superflue toute nouvelle intervention chirurgicale à des fins d'analyse des valeurs cardiaques ou d'adaptation de la configuration.

L'ICS-CERT du département américain de la sécurité intérieure (DHS), qui surveille de près les systèmes de contrôle, a publié le 29 août 2017 une mise en garde[10] sur les failles de sécurité de plusieurs modèles de stimulateurs cardiaques de la société Abbott Laboratories. Les vulnérabilités découvertes par MedSec Holdings Ltd permettraient de manipuler les données échangées à l'interface radio avec l'implant. À condition d'être directement placé sur le corps du patient lors d'un examen médical de routine, l'émetteur du pirate pourrait ensuite effectuer toutes les opérations de lecture et d'écriture. En effet, l'authentification de l'appareil de programmation n'était pas conforme à la norme prévue en la matière. Selon une publication[11] de l'agence fédérale américaine des aliments et des médicaments (FDA), qui réglemente aussi les appareils médicaux, une telle attaque exploitant les failles de sécurité n'a pas eu lieu à ce jour.

Le fabricant a publié entre-temps des mises à jour[12] pour les appareils concernés. Elles peuvent être activées lors de la visite trimestrielle au médecin traitant. En Suisse, les

10 https://ics-cert.us-cert.gov/advisories/ICSMA-17-241-01 (état: le 31 janvier 2018).

11 https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm (état: le 31 janvier 2018).

12 https://www.sjm.com/~/media/galaxy/patients/heart-vascular/arrhythmias/resources-support/cybersecurity/pacemaker-firmware-update-patient-guide-aug2017-us.pdf (état: le 31 janvier 2018).

5000 patients[13] concernés, soit pratiquement un septième des porteurs de stimulateur cardiaque, ont dû se soumettre à cette procédure.

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 Menaces d'attaques DDoS au nom de hackers illustres

L'extorsion est actuellement une des méthodes favorites des cybercriminels visant un rapide gain financier. Outre l'usage de rançongiciels (ransomware) et la menace de divulguer les données préalablement subtilisées, les escrocs n'hésitent pas à menacer d'une attaque DDoS imminente, alors même que beaucoup d'entre eux ne sont pas en mesure de lancer une telle attaque. Cette rhétorique agressive vise à faire peur aux victimes.

Bien souvent, les pirates cherchent à se faire passer pour les auteurs de cyberattaques ayant fait grand bruit. Ils se contentent d'envoyer un courriel de chantage, sans se donner la peine de lancer une attaque. Ils espèrent que la victime introduira le nom dans un moteur de recherche et leur versera ensuite la rançon demandée, par peur des agissements du groupe criminel ayant sévi dans le passé.

Le groupe de maîtres-chanteurs se faisant appeler Fancy Bear, apparu en été 2017 et ayant sévi en novembre en Suisse aussi, a recouru à cette méthode. Curieusement, ce nom n'appartient pas à un collectif responsable d'attaques DDoS, mais au groupe d'espionnage probablement le plus célèbre du monde. Fancy Bear, dont l'alias Sofacy est plus connu, serait un acteur étatique qui a notamment utilisé des failles «zero day». Comme à ce jour Sofacy ne s'est jamais illustré dans le chantage DDoS, tout indique qu'on a affaire à un groupe utilisant le nom de Fancy Bear et mû par l'espoir de réaliser des gains plus élevés, grâce à l'aura de son illustre modèle.

4.4 Social Engineering et phishing

Les attaques les plus fructueuses sont celles qui inventent une histoire crédible pour inciter l'utilisateur à effectuer une action spécifique. 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 deuxième semestre 2017. 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

[13] https://www.blick.ch/news/wirtschaft/sicherheitluecke-bei-herzschrittmachern-5000-schweizer-in-gefahr-id7255939.html (état: le 31 janvier 2018).

respectables, de tels courriels usurpent souvent les logos d'entreprises connues ou du service concerné.

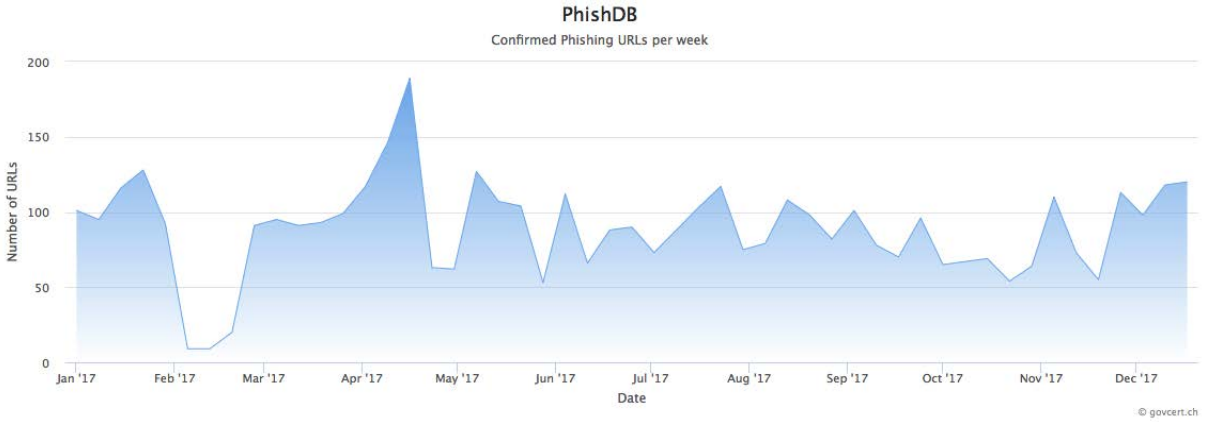

Fig. 2: Sites de phishing annoncés et confirmés par semaine sur le site antiphishing.ch en 2017

Au total, 4587 sites de phishing ont été dénoncés en 2017 sur le portail antiphishing.ch exploité par MELANI. La fig. 2 indique le nombre d'annonces hebdomadaires de pages de phishing, qui fluctue beaucoup au cours de l'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 Escroquerie par échange de factures électroniques (bill swap)

Outre les données des cartes de crédit, les cybercriminels s'en prennent surtout aux données d'accès des comptes de messagerie. Comme tout service en ligne offre la possibilité de réinitialiser le mot de passe, et donc d'obtenir un nouveau code, l'adresse électronique personnelle constitue entre-temps le pivot de presque toutes les prestations Internet. Le compte de messagerie offre toutefois bien plus de possibilités aux escrocs. Aujourd'hui, ils prennent le temps d'analyser méthodiquement la correspondance d'un compte compromis pour repérer du matériel utilisable. Une méthode plusieurs fois signalée à MELANI au deuxième semestre 2017 consiste à parcourir le compte de messagerie à la recherche de factures électroniques. Si les escrocs y découvrent une facture actuelle, ils la copient depuis la boîte de réception, puis l'effacent. Ils ont ensuite assez de temps pour manipuler la facture PDF annexée au courriel. Ils y modifient les coordonnées bancaires de l'émetteur, qu'ils remplacent par leur propre numéro IBAN. Le document ainsi modifié est ensuite replacé dans le compte de messagerie. Il suffit alors à l'escroc de falsifier l'adresse de l'expéditeur pour indiquer à la place l'adresse électronique de l'entreprise émettrice de la facture. Rien ne permet ensuite de détecter la manipulation.

Recommandation:

Lors de chaque virement, des informations sur le compte du destinataire s'affichent. Le nom du destinataire apparaît dans le meilleur des cas, et sinon celui de son établissement bancaire. D'où l'importance de toujours vérifier la plausibilité des informations. Par chance, les escrocs ont peu d'agents financiers (mules) sous la main et ne peuvent donc pas toujours indiquer un compte adéquat. Il se peut ainsi que l'argent doive être envoyé à l'étranger, alors même que la facture émane d'une entreprise suisse. La méfiance est de mise en pareil cas.

4.4.3 Vague de phishing sur Office 365, ou la clé du bureau

Depuis juin 2017, des courriels de phishing s'en prennent à Office 365. Il n'est guère surprenant qu'avec plus de 100 millions d'utilisateurs mensuels, les comptes Office 365 soient devenus une proie attrayante pour les pirates.[14] L'attaque commence par un banal courriel signalant par exemple que l'espace de stockage est saturé, et qu'une connexion au lien indiqué permettra de régler le problème. L'internaute imprudent aboutit à un site frauduleux. Les escrocs en possession de ses données d'accès à Office 365 peuvent procéder de diverses manières. Le scénario le plus fréquent consiste à introduire dans le compte piraté une règle de redirection des messages. Le courrier électronique tant interne qu'externe sera ensuite redirigé vers un compte défini par les escrocs, qui en prennent connaissance. Les comptes d'entreprises sont particulièrement prisés ici. Les informations ainsi collectées serviront à lancer des attaques contre d'autres employés. Comme les pirates ont accès au carnet d'adresses de leurs victimes, ils peuvent choisir de façon ciblée leurs correspondants. Ils envoient des messages qu'ils ont interceptés et manipulés afin de prier par exemple le destinataire de télécharger un document. Ce dernier doit d'abord réintroduire le mot de passe d'Office 365 (sur un site manipulé). Les escrocs se rapprochent ainsi, dans l'entreprise infiltrée, des personnes intéressantes pour eux.

Une fois le contact établi avec la personne souhaitée, l'arnaque au président (CEO fraud) devient possible à l'aide des données volées. La communication dérobée peut également servir de moyen de chantage, ou les données subtilisées être revendues à d'autres escrocs. Cette méthode peut également être mise en œuvre à des fins d'espionnage économique.

Recommandation:

Si la société a opté pour une solution en nuage (cloud) basée sur Office 365, les escrocs ayant dérobé des données d'accès pourront s'emparer de tous ses documents. Il est donc très imprudent à l'heure actuelle de se contenter du nom d'utilisateur et de son mot de passe pour protéger ce genre de données. L'authentification à deux facteurs sera privilégiée partout où c'est possible.

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

[14] https://betanews.com/2017/08/30/office-365-phishing/ (état: le 31 janvier 2018).

4.5 Failles de sécurité

4.5.1 Utilité de contrôler au terminal de paiement les ordres des clients

La plateforme globale Smartvista conçue par BPC Group, société suisse de solutions de paiement électronique, a été temporairement vulnérable aux attaques par injection de commandes SQL[15]. En formulant au moment opportun des requêtes spécifiques sur l'interface de transaction concernée (SmartVista Front-End, SVFE), un escroc aurait pu obtenir une liste de tous les utilisateurs de la base de données du système, avec leurs mots de passe. Selon un communiqué de BPC, le chercheur Aaron Herndon du blog de l'entreprise de sécurité Rapid7 aurait attiré son attention en mai 2017 sur cette lacune de sécurité. Dès le 19 juillet, l'entreprise avait mis au point un programme pour remédier au problème.

4.6 Pertes de données

Comme indiqué dans le thème prioritaire, il est souvent arrivé que des données aient fuité au deuxième semestre 2017. Le présent chapitre résume les principaux incidents connus survenus en Suisse.

4.6.1 70 000 données d'accès à dvd-shop dérobées

Au début de décembre 2017, MELANI a reçu une liste avec des combinaisons de noms d'utilisateur et de mots de passe. Une analyse a révélé qu'il s'agissait de 70 000 données d'accès dérobées en Suisse. Sur le moment, il était impossible d'en connaître l'origine. D'où la décision de les intégrer à l'outil MELANI Checktool[16], afin que chacun puisse vérifier si son nom d'utilisateur y figurait. Grâce aux retours de la population, MELANI a pu identifier le service concerné. Il s'agissait du commerce en ligne dvd-shop.ch, que MELANI a aussitôt alerté. L'administrateur du site a réinitialisé tous les mots de passe et désactivé son service. Même si les jeux de données étaient anciens, il a dûment informé tous les clients concernés.

Recommandation:

MELANI rappelle qu'il faut choisir des mots de passe 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.

4.6.2 Perte de données d'un assureur-maladie suisse

Le Groupe Mutuel, leader romand de l'assurance-maladie, a signalé dans un communiqué que le 19 décembre 2017, des pirates avaient réussi en usurpant une identité à s'introduire sur sa plateforme informatique externe ePremium Health, lancée en 2012, pour y dérober des fichiers

---

15 https://blog.rapid7.com/2017/10/11/r7-2017-08-bpc-smartvista-sql-injection-vulnerability/ (état: le 31 janvier 2018).

16 https://www.checktool.ch Pour une vérification, il suffit d'indiquer son adresse électronique ou son nom d'utilisateur. Ces derniers ne sont ni transmis en texte clair à MELANI, ni enregistrés (état: le 31 novembre 2017).

informatiques. Cette plateforme destinée au réseau de vente du Groupe Mutuel permet d'établir des offres et des propositions d'assurances. Selon l'assureur, aucune donnée de gestion (par ex. polices d'assurance, rapports médicaux, factures de primes et de prestations) n'a été dérobée. À aucun moment, le système de gestion informatique des 1,4 million de clients du Groupe Mutuel n'aurait été en danger. Après la cyberattaque, l'assureur a porté plainte contre inconnu. La police cantonale valaisanne est rapidement parvenue à identifier l'un des auteurs présumés et à l'interpeller, le 28 décembre 2017. Un second individu a été arrêté le lendemain dans le canton de Thurgovie. Il s'agit d'un Suisse de 29 ans et d'un Macédonien de 30 ans. Tous deux ont été placés en détention provisoire. Des investigations sont toujours en cours, selon la police.[17]

Le Groupe Mutuel a publié en février 2018 un formulaire servant à vérifier si la fuite de données nous concerne. Les victimes potentielles sont les personnes ou entreprises ayant demandé à un agent ou à un courtier, entre 2012 et aujourd'hui, une offre d'assurance du Groupe Mutuel.[18]

4.6.3 Fuite de données d'assurance, due à la société de recouvrement EOS

À la fin de décembre 2017, la Süddeutsche Zeitung[19] a fait état d'une fuite de données dans la branche helvétique d'une société de recouvrement de créances. Le groupe EOS détient 55 entreprises actives dans 26 pays. Trois gigaoctets de données auraient été transmises lors de cet incident. Outre le nom des débiteurs, leur adresse et le montant des créances, d'autres données très sensibles y figuraient, dont des dossiers médicaux indiquant les affections préexistantes et le détail des traitements suivis. Des pièces d'identité et des relevés complets de cartes de crédit faisaient encore partie de la fuite de données. Les plus anciens jeux de données dérobés remontaient à l'année 2002.

Des médecins ont manifestement eu la possibilité de télécharger des dossiers médicaux complets sur un portail d'EOS. On ignore dans quel but et à quelles conditions ils l'ont fait. Mais une société de recouvrement n'a certainement pas besoin de données aussi sensibles que les données médicales pour remplir ses tâches.

La fuite serait due à une attaque ciblée remontant à avril 2017 et rendue possible par l'exploitation d'une faille d'Apache Struts. Selon EOS, des indices de piratage avaient été découverts à l'époque, sans qu'il soit possible de les vérifier. Le serveur avait néanmoins été entièrement reconfiguré à l'époque. On ignore si les données sont réellement liées à cet incident, ou s'il y avait encore une autre faille de sécurité.

4.6.4 Fuite de données également chez Digitec

Le 6 novembre 2017, Digitec a admis qu'une ancienne base de données avait été pillée. À sa connaissance, seules les données de clients de 2001 à la mi-2014 étaient potentiellement touchées. Mais la faille de sécurité présumée avait été corrigée entre-temps, et la nouvelle

---

17 https://www.policevalais.ch/communiques-pour-les-medias/martigny-attaque-informatique-aupres-dun-groupe-dassurances/ (état: le 31 janvier 2018).

18 https://www.groupemutuel.ch/fr/clients-prives/page/cyberattaque.html (état: le 31 janvier 2018).

19 http://www.sueddeutsche.de/digital/it-sicherheit-schwerwiegendes-datenleck-legt-zehntausende-schuldnerdaten-offen-1.3805589 (état: le 31 janvier 2018).

boutique en ligne Digitec n'était pas concernée. On ignore quand exactement s'est produite la fuite de données.[20]

4.7 Logiciels criminels (crimeware)

L'expression «crimeware» désigne un logiciel malveillant déployé par des cybercriminels dans le cadre d'attaques motivées par l'argent. D'un point de vue légal, les conséquences de son utilisation seront la détérioration de données et l'utilisation frauduleuse d'un ordinateur. De nombreuses infections dues à des logiciels criminels ont été constatées au deuxième semestre 2017. La statistique présentée ci-dessous utilise des données issues de serveurs auxquels les machines infectées se connectent. Il y a également des maliciels très problématiques qui n'apparaissent pas dans la statistique (par exemple le logiciel malveillant Retefe). 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 et déjà comblée à l'époque. Il est suivi en deuxième position par Gamarue[21], nouveau venu également connu sous le nom d'Andromeda, un programme de téléchargement (downloader) qui peut ensuite introduire n'importe quel autre virus sur l'ordinateur infecté. Puis viennent en troisième et quatrième position les maliciels Spambot et Cutwail, qui se sont spécialisés dans la diffusion de pourriels et de maliciels. Mirai, maliciel formant des armées de *zombies* à partir d'appareils vulnérables de l'Internet des objets, célèbre pour avoir paralysé le prestataire de services Internet Dyn, a reculé de la quatrième à la septième place du classement. Le premier cheval de Troie bancaire, Dyre, ne vient qu'en neuvième position.

20 https://www.digitec.ch/de/page/statement-zum-digitec-leck-6265 (état: le 31 janvier 2018).

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

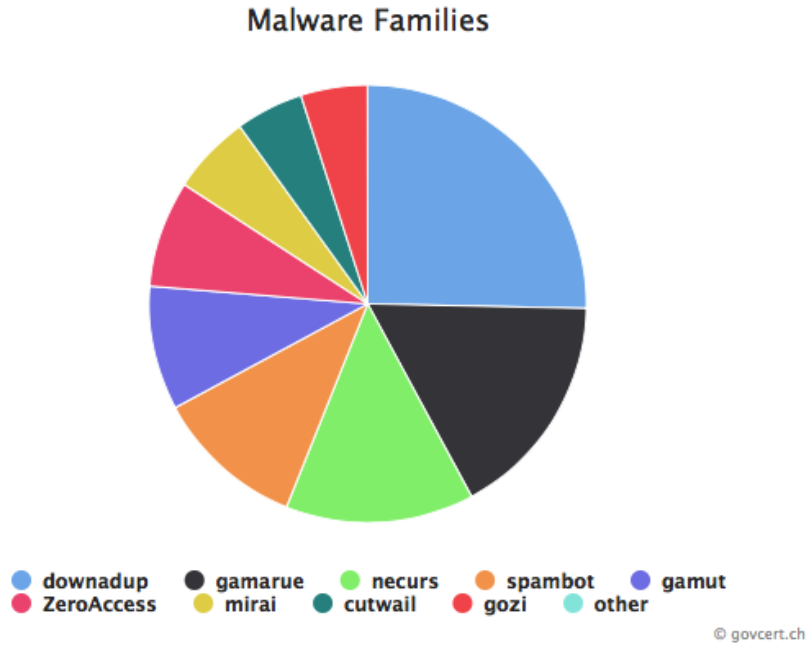

Fig. 3: Répartition des maliciels en Suisse, selon les informations en possession de MELANI. La date de référence est le 31 décembre 2017. Des données actuelles sont publiées sous: http://www.govcert.admin.ch/statistics/dronemap/

4.7.1 Rançongiciels

Durant la période sous revue, de nombreux cas de chevaux de Troie chiffrant les données, ou rançongiciels, ont été signalés à MELANI. Il est donc fondamental de procéder à une sauvegarde en bonne et due forme sur un support externe, hors de portée du rançongiciel. Mais il vaut mieux encore agir à titre préventif, afin d'éviter d'en arriver là. En effet, le chiffrement et donc la perte temporaire des données ne sont que la pointe de l'iceberg. Il faut encore s'attendre, le cas échéant, à ce qu'une grande partie de l'entreprise soit paralysée pendant leur restauration à partir de la copie de sauvegarde. Aujourd'hui où la plupart des entreprises ont besoin d'une informatique efficiente, une telle interruption risque d'entraîner une lourde perte financière. En outre, un dysfonctionnement peut avoir des conséquences fatales, dans le cas d'infrastructures d'importance vitale.

Recommandation:

INFO

Informations de MELANI concernant les rançongiciels
https://www.melani.admin.ch/melani/fr/home/themen/Ransomware.html

4.7.2 Succès non démenti du cheval de Troie Retefe

Divers chevaux de Troie bancaires sont plus ou moins répandus en Suisse. On trouve parmi eux Dridex, capable de compléter ses fonctionnalités pour lancer des attaques ciblées contre des clients commerciaux. Dridex analyse les systèmes infectés, pour y repérer des logiciels

de paiement hors ligne.[22] Le cheval de Troie Gozi ISFB se répand aussi bien par des pages Web infectées que par des annexes de courriels. Quant à Trickbot sévissant dans le monde entier, les établissements bancaires suisses figurent depuis 2017 sur son tableau de chasse. Trickbot possède une structure modulaire et s'enrichit constamment de nouvelles fonctions. Emotet, à l'origine un cheval de Troie bancaire, est également utilisé pour propager d'autres types de maliciels, par exemple des rançongiciels. Il utilise principalement pour se répandre de fausses factures.

Un des maliciels les plus agressif en Suisse reste toutefois Retefe. Il a exclusivement sévi à ce jour en Autriche, en Suède, au Japon, en Grande-Bretagne et en Suisse. Retefe avait déjà été décrit il y a trois ans, dans un précédent rapport semestriel de MELANI. À la différence d'autres maliciels, qui misent sur les infections de sites Web pour se répandre, Retefe se diffuse uniquement par courriel. Il s'agissait surtout au début de fausses factures de boutiques en ligne, comme Zalando ou Ricardo. Ses versions les plus récentes tendent plutôt à imiter des services fédéraux ou des entreprises proches de la Confédération, comme l'Administration fédérale des contributions (AFC) ou la Poste.

Dès qu'un système est infecté, Retefe modifie les paramètres du navigateur pour que certains sites Web – dont les portails d'e-banking de certains établissements financiers suisses – soient redirigés par un serveur mandataire (proxy server) vers un site malicieux. En outre, Retefe installe un certificat lui permettant d'émettre des certificats pour n'importe quel établissement financier. Le maliciel évite par ce subterfuge qu'un message d'erreur ne soit généré et ne rende la victime méfiante. Lorsque cette dernière s'annonce au moyen de l'ordinateur infecté sur un prétendu portail d'e-banking, elle voit s'afficher un *code QR*. Ce code mène vers un site malveillant, qui l'invite à télécharger et installer une application pour «améliorer la sécurité» – en réalité un maliciel pour Android (cheval de Troie SMS). Si la victime installe l'application Android proposée, tous les SMS envoyés par la banque pour l'identification à deux facteurs seront transférés aux malfaiteurs via un serveur Web situé à l'étranger. Ceux-ci contrôlent dès lors les accès e-banking de leur victime, et pourront vider son compte.

Les escrocs ont élargi leur mode opératoire au semestre dernier, en cherchant à se procurer la lettre contentant les données d'activation. En règle générale, la banque envoie par poste à ses clients ce genre de lettres, qui contiennent une mosaïque à numériser à l'aide d'une app, la première fois qu'un appareil ouvre une session d'e-banking. L'appareil utilisé est dès lors reconnu par la banque comme autorisé à se connecter au compte d'e-banking grâce aux moyens d'authentification mobiles. Les escrocs ont tenté d'obtenir les données d'activation en manipulant leurs victimes et en les incitant à en faire une copie numérique ou une photographie qui devait leur être transmise.

En septembre, le maliciel Retefe a été complété par l'exploit EternalBlue. Il peut ainsi s'engouffrer à son tour dans la faille de sécurité exploitée en mai par le rançongiciel WannaCry, dont le déferlement avait causé de lourds dégâts dans le monde entier. En intégrant EternalBlue, Retefe cherche apparemment surtout à se répandre dans les réseaux d'entreprises. Si un collaborateur ouvre par mégarde une annexe infectée, le maliciel se

[22] Rapport semestriel 2016/2, chapitre 4.6.1 https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/halbjahresbericht-2016-2.html (état: le 31 janvier 2018).

déplace jusqu'au poste où l'entreprise effectue ses paiements par e-banking. Ce mode opératoire ne fonctionne naturellement que si la lacune n'a pas encore été corrigée.

Durant la période sous revue, MELANI a régulièrement reçu des annonces au sujet de courriels contenant en annexe Retefe, qui comportaient à la fois une formule d'adresse correcte et le n° de téléphone du destinataire à la rubrique Objet. Dans la plupart des cas, l'expéditeur était censé être l'Administration fédérale des contributions (AFC), qui aurait eu des questions à propos de la déclaration d'impôts. Il y avait certes suffisamment d'indices qui auraient dû mettre la puce à l'oreille des destinataires. Mais en voyant leur propre numéro de téléphone, certains auront peut-être été incités à ouvrir l'annexe.

Von: Eidgenossische Steuerverwaltung ESTV [redacted]
Gesendet: Mittwoch, 21. Februar 2018 11:32
An: [redacted]
Betreff: Fragen zu der Steuererklarung (die Nummer 043 [redacted] ist unzuganglich)

Sehr geehrte(r) Herr/Frau [redacted]

Mein Name ist [redacted], ich bin Finanzinspektor und bin zuständig für Ihren Bezirk.

Es gibt einige Fragen zu Ihrer Einkommensteuererklärung.

Dieses Dokument beinhaltet die Liste von Fragen über Ihre Steuererklärung, sowie auch meine Kontaktnummer.

Freundliche Grüsse

[redacted]

Das Gemeindesteueramt

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Fig. 4: Exemple de courriel contenant Retefe et mentionnant à la rubrique objet un n° de téléphone

Le mystère de la source ayant fourni aux escrocs à la fois l'adresse électronique, les prénom et nom et le numéro de téléphone de cibles potentielles n'a pu être résolu. MELANI a toutefois des indices accréditant une fuite de données.

5 Situation internationale

5.1 Espionnage

5.1.1 Convoitises au Proche-Orient

Les campagnes de cyberespionnage peuvent être sommairement classées en deux catégories. Les unes sont dues à des raisons économiques, tandis que les autres visent à obtenir des informations stratégiques, militaires ou politiques. Quelques campagnes sont exposées ci-dessous. Les tensions politiques au Proche-Orient, ainsi que l'abondante

production locale de pétrole et de gaz naturel, font notamment des pays de la région d'attrayantes cibles du cyberespionnage.

5.1.2 Exemple APT33

«Nos rivaux politiques ou économiques ne sont pas seuls à détenir des données intéressantes – les informations de nos partenaires sont souvent tout aussi précieuses.» Tel pourrait être le slogan de la campagne de cyberespionnage APT33[23], qui selon l'entreprise de sécurité états-unienne FireEye serait due à un groupe iranien. APT33 a débuté au plus tard en 2013, et ses cibles principalement basées en Arabie saoudite, aux États-Unis et en Corée du Sud travaillent soit dans l'aéronautique militaire ou civile, soit dans la production d'énergie. Du milieu de l'année 2016 aux premiers mois de 2017, APT33 aurait compromis une organisation américaine et un conglomérat saoudien actif dans le secteur aéronautique. APT33 diffuse ses maliciels par des courriels incitant les victimes à répondre à des offres d'emploi. Les noms de domaine créés à cet effet ressemblaient à s'y méprendre à ceux de sociétés aéronautiques saoudiennes ou d'organisations occidentales ayant des partenariats avec elles, dans le secteur tant civil que militaire. Les analystes de FireEye pensent que les attaques visaient à récolter des informations militaires sur les forces aériennes saoudiennes, afin d'améliorer l'état des connaissances des forces aériennes iraniennes, et donc de permettre à Téhéran de prendre les meilleures décisions militaires et stratégiques.

La campagne d'espionnage s'est encore attaquée à la même époque à une raffinerie de pétrole sud-coréenne. Des employés de deux sociétés pétrochimiques, l'une saoudienne, l'autre sud-coréenne, ont reçu en mai 2017 le même genre de messages. Un courriel renfermant de prétendues offres d'emploi d'une société pétrochimique installée en Arabie Saoudite téléchargeait en réalité un programme d'espionnage sur le système de la victime.

FireEye aurait identifié une personne mêlée à ces incidents, apparemment un ancien membre du gouvernement iranien. Par ailleurs, certains des programmes malveillants utilisés contenaient des mots en farsi, langue officielle de l'Iran. De même, le timing des attaques coïncidant avec les horaires de travail en Iran, et l'utilisation de multiples outils de piratage fournis par des sites cybercriminels iraniens tendent à accréditer l'hypothèse d'une attaque menée pour le compte du gouvernement iranien.

Pour rappel, Shamoon, la campagne de cyberespionnage supposée iranienne la plus connue à ce jour, qui s'en est prise dès 2012 à des organisations du golfe Persique, se concentrait déjà sur le secteur pétrochimique.

5.1.3 Mue technologique et stratégique de Copy Kittens[24]

Le 29 mars 2017, l'Agence allemande de cybersécurité BSI (Bundesamt für Sicherheit in der Informationstechnik) a révélé que le site Internet du quotidien Jerusalem Post avait été manipulé pour diffuser des maliciels. Cette découverte serait probablement liée à des

---

[23] https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html (état: le 31 janvier 2018).

[24] http://www.clearskysec.com/tulip/ (état: le 31 janvier 2018).

anomalies non précisées du trafic réseau du Parlement allemand apparues en janvier 2017.[25] Le même mois, la société de cyberintelligence israélienne ClearSky a confirmé la compromission survenue au Jerusalem Post, tout en signalant d'autres compromissions subies par divers sites israéliens et par celui du Ministère de la santé palestinien. Elle a attribué la responsabilité de l'attaque au groupe d'espionnage CopyKittens.[26] Entre octobre 2016 et la fin janvier 2017, les sites compromis renfermaient un code Javascript qui téléchargeait, à partir d'un domaine enregistré par les pirates, un outil procédant à des tests d'intrusion des navigateurs Web. Le Javascript n'était toutefois pas délivré pour chaque visiteur, mais seulement pour des victimes dûment choisies.

CopyKittens est un groupe de cyberespionnage sévissant depuis 2013 au moins. Son nom vient de son habitude de copier sur les forums en ligne des fragments de code malveillant, utilisés pour lancer des cyberattaques. Ce groupe s'en prend principalement à Israël, à l'Arabie saoudite, à la Turquie, aux États-Unis, à la Jordanie et à l'Allemagne, mais aussi aux fonctionnaires des Nations Unies. Ses cibles comprennent notamment les institutions étatiques ou académiques, les entreprises de défense, les sous-traitants du Ministère de la défense et les grandes entreprises informatiques.

La campagne en question combine différentes tactiques d'infiltration: les attaques par point d'eau (watering hole) décrites ci-dessus sont complétées par l'envoi ciblé de courriels renfermant une annexe ou un lien malveillants. Des employés de nombreuses institutions gouvernementales ont ainsi reçu, à fin avril 2017, un courriel expédié d'un compte de messagerie compromis. Le titre du document infecté se référait aux relations internationales entre l'Iran, la Corée du Nord et la Russie. Dans deux autres cas, le groupe avait réussi à s'introduire dans le compte de messagerie de personnes en contact avec la cible visée. Les pirates ont ainsi pu s'immiscer dans les discussions du propriétaire légitime du compte, afin d'expédier un courriel muni d'un lien à un site malveillant spécialement créé.

Depuis 2013 déjà, le groupe crée et gère de faux profils Facebook. Il parvient ainsi à gagner la confiance de ses victimes potentielles et à collecter des informations à leur sujet pour de nouvelles attaques. Ces faux profils ont également envoyé des liens à une page Web compromise. Afin d'être crédibles, les profils publiaient aussi des contenus anodins et possédaient un nombre respectable d'amis.

Conclusion:

En 2015, Copy Kittens était encore considéré comme un agresseur au potentiel de nuisance ordinaire. Ses récentes cyberattaques révélées montrent toutefois que cet acteur a semble-t-il considérablement évolué, sur le plan technologique et stratégique. En plus des outils commerciaux existants, Copy Kittens utilise désormais ses propres programmes malveillants.

[25] https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2017/Cyber-Angriff_auf_den_Bundestag_Stellungnahme_29032017.html (état: le 31 janvier 2018).

[26] http://www.clearskysec.com/wp-content/uploads/2017/07/Operation_Wilted_Tulip.pdf (état: le 31 janvier 2018).

5.1.4 Nouveaux systèmes d'attaque du groupe OilRig[27]

Dans le passé, les campagnes d'espionnage d'OilRig étaient dirigées contre des entreprises publiques ou privées d'Amérique du Nord et d'Europe, et s'intéressaient tout particulièrement à la production de pétrole et de gaz naturel et aux transactions correspondantes effectuées au Proche-Orient. Durant le semestre sous revue, le groupe OilRig a complété son arsenal par de nouveaux chevaux de Troie, et continue de s'en prendre au Proche-Orient. Deux nouveaux instruments ont été déployés en juillet et août 2017: ISMAgent crée des portes dérobées, tandis qu'un injecteur installe ce virus. L'injecteur (dropper) possède une structure complexe, et use de techniques qui retardent sa découverte sur les ordinateurs infectés.

Le 23 août 2017, OilRig a attaqué un service gouvernemental des Émirats arabes unis, en lui envoyant un courriel d'hameçonnage avec deux annexes ZIP et une photo dans le texte. Comme la photo était téléchargée d'un serveur externe, elle servait probablement à vérifier l'ouverture du courriel par le destinataire. L'attaque comportait encore d'autres astuces techniques intéressantes. Ainsi l'adresse de l'expéditeur interne n'était pas falsifiée. OilRig avait probablement réussi à se procurer par phishing les données d'authentification d'un compte de messagerie du même domaine, pour expédier à partir de là le courriel décrit plus haut. Les deux fichiers ZIP contenaient un document Word. La macro malveillante dissimulée dans le premier permettait à l'injecteur d'installer la porte dérobée susmentionnée. Les escrocs utilisaient des méthodes d'ingénierie sociale pour amener les destinataires à exécuter leur macro. Le second document cherchait à exploiter une faille de sécurité de Microsoft Word[28], dont le correctif logiciel venait d'être publié. Les escrocs s'efforcent ainsi d'exploiter les défaillances tant techniques qu'humaines.

Après s'être introduits dans le système, les pirates utilisent des programmes vendus au marché noir, comme Mimikatz, pour se procurer les données d'authentification nécessaires et se mouvoir librement, de machine en machine, dans le réseau de l'entreprise. Selon le prestataire de sécurité Palo Alto, OilRig mènerait aussi des attaques exploitant la chaîne d'approvisionnement[29]. Au lieu de s'en prendre directement à sa cible, la méthode consiste à faire le détour par un de ses prestataires. Sachant qu'ils ont accès aux réseaux de la victime, voire qu'ils lui livrent des logiciels et du matériel, la victime subit ainsi une attaque indirecte. Et comme toute entreprise possède généralement plusieurs fournisseurs, la méthode laisse à l'agresseur un large «choix» de possibilités (ou de vulnérabilités) pour opérer. La méthode rencontrerait même un succès croissant, comme indiqué au chapitre «Attaques internationales» du rapport semestriel 1/2017[30]: selon les prévisions annuelles en matière de sécurité informatique de Kaspersky, cette menace va même s'aggraver en 2018[31].

---

27 https://researchcenter.paloaltonetworks.com/2017/10/unit42-oilrig-group-steps-attacks-new-delivery-documents-new-injector-trojan/ (état: le 31 janvier 2018).

28 CVE-2017-0199 Microsoft Word Office/WordPad Remote Code Execution Vulnerability

29 https://researchcenter.paloaltonetworks.com/2017/12/unit42-introducing-the-adversary-playbook-first-up-oilrig/ (état: le 31 janvier 2018).

30 https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2017-1.html (état: le 31 janvier 2018).

31 https://www.kaspersky.com/about/press-releases/2017_kaspersky-labs-threat-predictions-for-2018 (état: le 31 janvier 2018).

Conclusion:

La Suisse ne fait certes pas partie des cibles du groupe OilRig. Mais comme de nombreux fournisseurs de l'industrie pétrochimique y ont pignon sur rue, de telles attaques seraient également envisageables en Suisse.

5.1.5 «Publicités» prorusses diffusées dans Facebook[32]

Le précédent rapport semestriel avait examiné l'ingérence de pays tiers dans les élections présidentielles américaines, par le biais de cyberattaques ciblées. Leurs cibles ne se sont toutefois pas limitées aux systèmes de décompte des voix (il n'y a à ce niveau pas de signe de manipulations réussies) et à la correspondance du parti démocrate: les services de renseignement américains ont expliqué que des campagnes de désinformation avaient été menées en parallèle, sur les réseaux sociaux notamment. On sait entre-temps qu'une entreprise qui pourrait être russe a mené pendant les élections présidentielles américaines une véritable campagne de propagande sur Facebook. L'Internet Research Agency aurait acquis sur Facebook des espaces publicitaires, afin de diffuser les idées politiques des cercles dirigeants russes. Plus de 3300 annonces publicitaires seraient dues à cette campagne russe.[33] Elles ont été diffusées et promues à partir de 470 faux profils. Même si les noms des deux candidats à la présidence américaine apparaissent dans plusieurs posts, ces messages diffusaient surtout des considérations socio-politiques sur des thèmes aussi sensibles que le partenariat enregistré entre personnes de même sexe, l'immigration ou le droit à la détention d'armes. Certains posts ne cherchaient même pas à susciter le débat d'idées, mais à semer un vent de panique et le chaos dans le réseau. La Washington Post mentionne ainsi une fausse rumeur de fuite de produits chimiques en Louisiane. La propagande était ciblée, et donc ces contenus n'étaient visibles que pour la population de certaines régions.

En janvier 2017 déjà, les services de renseignement américains avaient accusé la Russie[34] de se mêler des élections présidentielles. Ils lui reprochaient d'avoir payé des trolls, afin de propager de fausses rumeurs sur les réseaux sociaux et d'influencer ainsi l'opinion publique. Suite à ces reproches Mark Zuckerberg, CEO de Facebook, a promis de déclarer la guerre à la désinformation sur sa plateforme.

5.2 Fuites d'information

La période sous revue a encore une fois été marquée par plusieurs cas de vols de données massifs, qui ont fait la une des médias.

---

32 https://www.washingtonpost.com/politics/facebook-says-it-sold-political-ads-to-russian-company-during-2016-election/2017/09/06/32f01fd2-931e-11e7-89fa-bb822a46da5b_story.html?utm_term=.936611ed98fb (état: le 31 janvier 2018).

33 http://www.wired.co.uk/article/facebook-twitter-russia-congress-fake-ads-2016-election-trump (état: le 31 janvier 2018).

34 http://www.zeit.de/politik/ausland/2017-01/hacker-angriff-us-wahl-russland-barack-obama-geheimdienste (état: le 31 janvier 2018).

5.2.1 Equifax

L'un des plus spectaculaires est sans conteste la mésaventure d'Equifax, l'une des principales agences américaines d'évaluation de crédit. Le 7 septembre 2017, l'entreprise a annoncé avoir découvert une intrusion sur ses réseaux en juillet déjà. Apparemment, une faille connue d'Apache Struts, pour laquelle Equifax n'avait pas installé le correctif, serait à l'origine de la compromission. Les données personnelles de 143 millions de clients pourraient avoir été compromises aux États-Unis. Pour aggraver les choses, cette société a accès à quantité d'informations personnelles et financières pour calculer les risques de crédit, dont le numéro de sécurité sociale («Social security number, SSN»)[35]. L'incident a mis en exergue les enjeux sécuritaires liés à ce numéro unique, initialement prévu pour l'identification des individus dans le contexte de la sécurité sociale et devenu au fil du temps un identifiant unique, utilisé dans différents domaines comme les soins médicaux, les impôts ou l'octroi de crédit. Le vol de ce numéro, a fortiori s'il est complété par d'autres informations personnelles sur son détenteur, ouvre de vastes perspectives en termes de fraude et d'usurpation d'identité.

5.2.2 Sociétés d'audit et de conseil

Le soufflé médiatique était à peine retombé que le 25 septembre 2017, le Guardian rendait public un autre incident concernant une grande compagnie américaine[36]. Selon les informations du journal anglais, le service de messagerie électronique de Deloitte, l'un des quatre grands («big four») cabinets d'audit au niveau mondial, aurait été compromis dès octobre ou novembre 2016. Un compte administrateur insuffisamment sécurisé aurait permis d'accéder aux courriels échangés entre Deloitte et ses principaux clients, stockés sur la plateforme en nuage (cloud) Azure de Microsoft. Les critiques du piètre niveau de sécurité de l'entreprise ont redoublé après les révélations concernant des éléments sensibles de son infrastructure réseau visibles sur Internet (accès RDP ouvert, identifiants d'un service VPN notamment)[37]. Entre autres activités, Deloitte fournit des conseils en cybersécurité à des entreprises dans de nombreux secteurs d'importance vitale. En juin 2017, ce cabinet d'audit avait été élu par Gartner, pour la cinquième année consécutive, n° 1 mondial dans le domaine du conseil en sécurité.

5.2.3 Chantage sur la base de données de conducteurs et passagers

La Silicon Valley n'est pas non plus épargnée par les vols de données. En novembre, Uber confirmait avoir été victime d'un vol des données personnelles de 57 millions de clients et chauffeurs. L'entreprise était au courant des détails de l'incident depuis fin 2016. Selon Bloomberg[38], une page privée publiée sur le site GitHub, utilisée par des ingénieurs d'Uber, serait à la base de l'incident. Les auteurs ont pu y récupérer des identifiants leur permettant d'accéder à des informations sensibles que l'entreprise héberge sur le service Cloud d'Amazon. Ils ont alors exercé un chantage couronné de succès, puisque l'entreprise aurait

---

35 https://www.edoeb.admin.ch/edoeb/fr/home/protection-des-donnees/statistik--register-und-forschung/numero-avs.html (état: le 31 janvier 2018).

36 https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails (état: le 31 janvier 2018).

37 https://www.theregister.co.uk/2017/09/26/deloitte_leak_github_and_google/ (état: le 31 janvier 2018).

38 https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data (état: le 31 janvier 2018).

payé 100 000 dollars en échange des données et de la non-divulgation de l'incident. Mais le paiement et la destruction annoncée de données furent loin de marquer la fin de l'incident: le cas a fini par être rendu public. En faisant le choix de n'informer ni les autorités, ni les victimes après avoir pris connaissance des faits, l'entreprise n'a pas respecté ses obligations légales. Différentes procédures judiciaires ont été engagées. On ne sait pas si l'entreprise a fait l'objet d'un autre chantage après le premier paiement.

5.2.4 Perte de support de données

Un incident survenu en Grande-Bretagne montre toutefois que les fuites de données ne sont pas uniquement dues à des failles de sécurité ou à des systèmes mal configurés. En octobre 2017, un passant a trouvé par terre à Londres une clé USB contenant 2,5 gigaoctets de données non chiffrées, dont des informations sensibles sur l'aéroport de Heathrow, par exemple sur l'emplacement des caméras de surveillance et des issues de secours, ou sur les horaires des patrouilles de police. L'auteur de la découverte a remis sa trouvaille à un journal, qui s'est empressé de publier l'incident. On ignore comment cette clé USB a pu se retrouver dans la rue.

Conclusion:

La réduction au minimum des cyberrisques est un processus global, qui exige aussi des mesures de sécurité physique. Il faut clairement définir quelles données peuvent être enregistrées sur des médias externes, et quelles sont les mesures de sécurité à prendre (par ex. niveau de chiffrement).

De plus amples informations sur le thème des fuites de données sont disponibles dans le thème prioritaire de ce rapport.

5.3 Systèmes de contrôle industriels

5.3.1 Espionnage par Dragonfly de l'infrastructure des fournisseurs d'énergie

Le New York Times a signalé en juillet 2017 que depuis le mois de mai, des pirates tentaient de s'infiltrer dans une centrale nucléaire située dans le Kansas[39]. Par la suite, plusieurs cyberattaques menées dans le secteur énergétique ont été révélées aux États-Unis et en Europe[40,41]. Même si les comptes rendus dans les médias donnent l'impression que les attaques se multiplient dans le secteur énergétique et s'il a été question d'un nouveau groupe se faisant appeler Palmetto Fusion, toutes ces opérations semblent pouvoir être attribuées à un seul et même acteur, Dragonfly, qui sévit depuis 2011.[42] À partir de 2013 Dragonfly (aussi connu sous les noms de Havex, Energetic Bear, Crouching Yeti, etc.) s'en est pris au secteur

39 https://www.nytimes.com/2017/07/06/technology/nuclear-plant-hack-report.html (état: le 31 janvier 2018).

40 https://www.wired.com/story/russian-hacking-teams-infrastructure/ (état: le 31 janvier 2018).

41 https://www.independent.ie/irish-news/news/exclusive-eirgrid-targeted-by-state-sponsored-hackers-leaving-networks-exposed-to-devious-attack-36003502.html (état: le 31 janvier 2018).

42 https://www.symantec.com/connect/blogs/dragonfly-western-energy-companies-under-sabotage-threat-energetic-bear (état: le 31 janvier 2018).

énergétique, aux États-Unis comme en Europe. En 2017 toutefois, la nouvelle vague d'attaques rebaptisée Dragonfly 2.0 a redoublé d'intensité, tout en s'améliorant sur le plan technique.

Dragonfly 2.0 repose sur des courriels d'hameçonnage ciblé (spear phishing)[43] avec des annexes ou liens compromis, ainsi que sur des pages Web légitimes piégées selon la technique du point d'eau (watering hole) pour infecter les visiteurs du même domaine d'intérêt[44]. Les sites ainsi compromis révèlent le public-cible de Dragonfly, soit les entreprises du secteur énergétique, les négociants en énergie, les cabinets d'avocats spécialisés dans le secteur énergétique et les producteurs de solutions informatiques destinées à l'industrie tant européenne qu'américaine. Les agresseurs cherchent de cette façon à s'emparer des données d'accès à des réseaux d'importance vitale. Symantec signale dans son rapport sur Dragonfly 2.0 qu'outre les victimes basées aux États-Unis et en Turquie, une société se trouvait en Suisse. MELANI n'a jusqu'ici pas pu vérifier cette information. Il n'a donc pas été possible d'identifier d'entreprise en Suisse.[45]

Conclusion:

L'espionnage des réseaux informatiques du secteur énergétique peut avoir plusieurs objectifs. D'une part, l'agresseur peut se procurer un accès aux réseaux et dérober ainsi des informations, afin d'en tirer un avantage stratégique et économique. D'autre part, en contrôlant les ordinateurs de réseaux d'importance vitale, il peut le cas échéant manipuler des processus et en altérer le fonctionnement.

On ne connaît à l'heure actuelle aucun cas de sabotage dû aux versions successives de Dragonfly. Mais il n'est pas dit que Dragonfly s'abstienne toujours d'agir, a fortiori si la situation politique devait changer. Et comme ses tentatives d'espionnage actuelles lui auront servi à identifier toutes les possibilités, il sera paré à toute éventualité. Les attaques du groupe Sandworm, autre acteur au mode opératoire similaire ayant saboté en 2015/2016 le réseau électrique ukrainien, ont montré qu'il faut des mois entiers de préparatifs, afin de comprendre comment les systèmes de contrôle attaqués sont configurés et quelles sont les combinaisons de commandes nécessaires aux actes de sabotage envisagés. Le problème tient à ce que même de simples opérations de reconnaissance peuvent provoquer des dégâts collatéraux, en cas de maladresse. Les tentatives d'attaques observées montrent à quel point il est crucial, dans la pratique, d'adopter une panoplie de mesures comme celles décrites au chapitre 4.2.

5.3.2 Tentatives de sabotage visant les systèmes de contrôle de la sécurité

En décembre 2017, plusieurs entreprises de sécurité ont publié des rapports sur un logiciel baptisé Triton/Trisis, qui s'en prend aux solutions de sécurité des processus conçues pour les systèmes de contrôle industriels. Ce maliciel découvert à la mi-novembre 2017, qui sévissait depuis août au moins, attaque expressément certaines configurations du système Triconex de

[43] http://blog.talosintelligence.com/2017/07/template-injection.html (état: le 31 janvier 2018).

[44] https://www.riskiq.com/blog/labs/energetic-bear/ (état: le 31 janvier 2018).

[45] https://www.watson.ch/Digital/Schweiz/472496967-Droht-ein-Blackout--Hacker-attackieren-Schweizer-Energiesektor (état: le 31 janvier 2018).

la société française Schneider Electric. Une de ses cibles au moins se trouvait au Proche-Orient.

Les cyberattaques antérieures s'en prenaient directement au pilotage du processus principal. Une solution de sécurité des processus surveille et contrôle par contre l'exploitation d'une installation. Si par exemple la pression ou la température du processus à surveiller dépassent un seuil critique exposant l'installation à des dommages, des contre-mesures sont automatiquement mises en place (par ex. en désactivant une opération ou en la rendant impossible). Si les pirates parviennent à manipuler son système de sécurité pour empêcher toute mise hors tension automatique en cas de défaillance, une installation risque d'être endommagée voire détruite, et des personnes de subir des lésions voire d'être tuées. Dans certaines situations cependant, un opérateur doit intervenir manuellement dans le système pour adopter les mesures nécessaires.

Les attaques ciblées contre les systèmes de contrôle industriels restent rares. Triton/Trisis est le cinquième maliciel connu à s'en prendre spécifiquement aux commandes industrielles. Le plus célèbre étant Stuxnet, maliciel découvert en 2010, conçu pour perturber ou détruire les centrifugeuses des installations iraniennes d'enrichissement d'uranium. Autres exemples plus récents, les maliciels Blackenergy et Industroyer/Crashoverride avaient paralysé le réseau électrique ukrainien, en décembre 2015[46] et en 2016[47].

Conclusion:

De telles attaques ont été lancées jusqu'ici avec beaucoup de retenue. Il faut dire que ce genre d'opération comporte toujours un risque de dommage collatéral, aux conséquences imprévisibles pour l'agresseur. Dans le cas d'espèce, les attaquants en ont fait les frais. Leurs tentatives de manipulation basées sur le maliciel ont provoqué un arrêt d'urgence automatique du système piraté. L'analyse de l'incident a conduit à la découverte du maliciel. Par conséquent, de telles attaques sont généralement dirigées contre une configuration spécifique du système, et mobilisent d'importantes ressources. Une telle dépense ne se justifie pas pour un agresseur aux intérêts pécuniaires, et émane typiquement des États. Le système Triconex a beau être souvent utilisé dans l'industrie, chaque implémentation est unique et un vecteur d'attaque n'est transposable à d'autres systèmes qu'au prix de lourds efforts. L'intérêt marqué des agresseurs pour les solutions de sécurité des processus révèle toutefois leur intention de causer un maximum de dégâts matériels dans le système lui-même, ou dans le processus piloté en mode analogique.

46 MELANI, rapport semestriel 2015/2, chapitre 5.3.1, https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2015-2.html (état: le 31 janvier 2018).

47 MELANI, rapport semestriel 2016/2, chapitre 5.3.1, https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/halbjahresbericht-2016-2.html (état: le 31 janvier 2018).

5.3.3 Cyberattaque expérimentale d'un avion menée par le DHS

La conférence américaine «CyberSat – Security in Aerospace» s'intéresse aux cyberattaques dirigées contre les satellites ou la navigation aérienne. Un représentant du département de la Sécurité intérieure des États-Unis (Department of Homeland Security, DHS) a signalé à la CyberSat de novembre 2017 que les experts du DHS étaient parvenus, lors d'une expérience menée en septembre 2016, à s'introduire dans le système informatique d'un Boeing 757 stationné à l'aéroport d'Atlantic City[48]. Le véhicule avait été acheté auparavant par le DHS, afin d'en identifier les éventuelles vulnérabilités aux cyberattaques. Ce type d'avion est principalement utilisé par les compagnies aériennes américaines. Les radiofréquences de l'avion ont servi à lancer la cyberattaque, menée à distance et sans complicités en interne. Deux jours de reconnaissance ont suffi au DHS pour découvrir la faille de sécurité nécessaire à sa cyberattaque. Un incident datant d'avril 2015[49] pourrait être à l'origine d'un tel test. À l'époque Chris Robert, chercheur en cybersécurité, s'était vanté sur Twitter d'avoir découvert, dans le système de divertissement en vol (in-flight entertainment, IFE) des avions de type Boeing 757-200, Boeing 737-800, Boeing 737-900 et Airbus A-320, des failles de sécurité lui ayant permis d'accéder à des systèmes importants de l'électronique embarquée. L'expérience confirme l'importance d'une claire séparation physique entre l'avionique (aéronautique et électronique), d'une part, et les systèmes d'information et de communication accessibles de l'extérieur, d'autre part, pour que même en cas d'erreur de configuration il soit impossible à un tiers d'accéder d'un réseau à l'autre.

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. Cela comprend également les systèmes de divertissement et les accès Internet dans les avions. 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

[48] https://www.bleepingcomputer.com/news/security/dhs-team-hacks-a-boeing-757/ (état: le 31 janvier 2018).

[49] MELANI, rapport semestriel 2015/1, chapitre 5.3.3, https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2015-1.html (état: le 31 janvier 2018).

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

5.4.1 DDoS

Les attaques DDoS sont restées un outil de choix pour différents types d'attaquants au cours de la période sous revue. Le dommage ainsi causé dépend grandement de la nécessité de garder un service en ligne coûte que coûte. Les agresseurs sont bien au fait de cette réalité et vont cibler plus systématiquement certains secteurs d'activité, en particulier ceux pour lesquels une présence en ligne est un impératif économique. C'est ainsi qu'au semestre dernier, différentes attaques ont ciblé l'industrie du jeu. Une attaque ayant fait grand bruit visait la loterie nationale du Royaume-Uni. Le 30 septembre, personne n'a pu jouer en ligne ou sur l'application mobile pendant 90 minutes. Le moment de l'attaque avait été savamment choisi, puisque la perturbation a eu lieu le samedi soir, moment d'intense activité précédant le tirage. La motivation derrière l'attaque n'est pas connue, en particulier aucune demande de rançon n'a été rendue publique.

Avec l'engouement suscité par les cryptomonnaies, les différentes plateformes proposant d'acquérir et échanger ce type de devises sont également devenues des cibles de choix pour des attaques DDoS. Un bon exemple vient de l'attaque ayant touché Electroneum, cryptomonnaie conçue pour une utilisation mobile. L'incident a forcé l'entreprise à retarder le lancement de son application mobile.

Si les auteurs d'attaques DDoS sont constamment à la recherche de nouvelles cibles, ils ajoutent également de nouvelles armes à leur arsenal. Alors que 2016 avait vu l'avènement de MIRAI et l'exploitation à large échelle d'objets connectés mal sécurisés[50], c'est une méthode du nom de Pulse Wave qu'a décrit Imperva Incapsula[51] en 2017. Contrairement aux attaques traditionnelles, dont la puissance augmente progressivement avant d'atteindre un pic, une attaque de type Pulse Wave est composée de vagues successives, délivrant chacune immédiatement son intensité maximale, allant jusqu'à 350 Gbps. Ces vagues déferlent parfois pendant plusieurs jours. Le succès de ce type d'opération tire parti des spécificités des méthodes de défense hybride, qui ne font intervenir une solution basée sur le nuage (cloud) que lorsque l'attaque atteint un certain niveau et n'est plus absorbable au niveau applicatif. Les attaques de type Pulse Wave sont dévastatrices, car le niveau maximum de trafic est atteint immédiatement. Imperva Incapsula s'attend à une recrudescence de telles attaques à l'avenir.

5.4.2 Ransomware: Bad Rabbit

Fin octobre, un nouveau rançongiciel a ravivé les peurs issues de WannaCry et NotPetya. Appelé BadRabbit, il s'est propagé à travers de fausses mises à jour d'Adobe Flash. Il aurait également utilisé l'exploit Eternal Romance pour se déplacer dans le système des entreprises victimes, ainsi que Mimikatz pour capter des identifiants. Selon Group IB, le code malveillant est une version modifiée de NotPetya[52], avec un algorithme de chiffrement différent. La plupart

---

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

51 https://www.incapsula.com/blog/pulse-wave-ddos-pins-down-multiple-targets.html (état: le 31 janvier 2018).

52 https://www.group-ib.com/blog/badrabbit (état: le 31 janvier 2018).

des victimes de BadRabbit se trouvent en Russie, mais certains cas ont également été reportés en Ukraine, en Allemagne et en Turquie notamment.

5.4.3 Cryptomonnaies

L'année dernière, le grand public et les médias ont eu les yeux de Chimène pour les cryptomonnaies. Les criminels s'y sont intéressés de très près, cherchant des moyens de profiter eux aussi de l'envolée des prix. Certaines attaques ont visé les plateformes elles-mêmes. Avec l'aide de méthodes souvent sophistiquées, les criminels peuvent voler de très importantes sommes d'argent en une fois. Par exemple, la plateforme de minage NiceHash s'est fait dérober plus de 70 millions de dollars en décembre 2017, et le mois suivant l'équivalent de plus d'un demi-milliard de dollars en NEM a été volé à la plateforme d'échange Coincheck. Même si tous les détails ne sont pas connus, de tels événements montrent bien les risques associés à la centralisation d'un grand nombre de monnaies sur les mêmes plateformes. Les plateformes ne sont d'ailleurs pas seules visées, et des attaques sur mesure ciblent également les détenteurs individuels de monnaies virtuelles. Un mode opératoire particulièrement pernicieux, décrit par le New York Times[53], a visé différents investisseurs en monnaies virtuelles aux États-Unis. Les escrocs ont réussi à se faire attribuer les numéros de téléphone d'individus repérés, car détenant potentiellement de grandes quantités de monnaies virtuelles. Pour ce faire, ils ont appelé les opérateurs de téléphonie mobile de leurs cibles et, à grand renfort d'ingénierie sociale, les ont persuadés de réattribuer le numéro de téléphone mobile à un appareil contrôlé par eux. Il leur a suffi ensuite de réinitialiser le mot de passe à l'aide du numéro mobile pour accéder aux comptes liés à ce numéro. Une autre méthode pour profiter de la manne des monnaies virtuelles consiste à solliciter les ressources des utilisateurs d'Internet pour miner de la monnaie. Dans cette catégorie, l'année 2017 a vu de nombreux cas de scripts placés sur des sites web et minant directement des monnaies virtuelles à travers le navigateur. Cette tendance est décrite au chapitre 6.2 du présent rapport.

5.5 Failles de sécurité

De nombreuses failles de sécurité ont fait les gros titres durant la période sous revue. La plus sensationnelle est incontestablement la vulnérabilité Spectre/Meltdown, découverte dans les microprocesseurs de divers fabricants. De telles failles, qu'une simple mise à jour ne suffit pas à corriger, obligent les responsables de la sécurité à définir de nouvelles stratégies pour en minimiser les effets néfastes. La faille de sécurité Spectre/Meltdown fera l'objet d'une analyse détaillée dans le prochain rapport semestriel.

5.5.1 Faille de la norme de chiffrement WPA2, pourtant réputée sûre

En octobre 2017, deux chercheurs de l'Université de Louvain ont publié une faille de la norme de chiffrement WPA2. Cette vulnérabilité baptisée KRACK (Key Reinstallation AttaCK) permet de lire des données chiffrées, ainsi que d'établir l'existence d'une connexion entre deux appareils – comme un navigateur et un serveur Web. La situation semble sérieuse à première vue. Or une série de conditions doivent être réunies pour que la faille puisse être exploitée. En particulier, le pirate doit se trouver à proximité immédiate de l'appareil wi-fi et capter ses signaux radio. La vulnérabilité ne risque donc pas d'être exploitée en ligne à grande échelle.

---

[53] https://www.nytimes.com/2017/08/21/business/dealbook/phone-hack-bitcoin-virtual-currency.html (état: le 31 janvier 2018).

En outre, la faille ne livre pas le mot de passe du réseau sans fil ni ne donne accès au routeur, par exemple pour s'attaquer plus tard directement à l'appareil pris pour cible. Autrement dit, seules certaines connexions ouvertes peuvent être piratées.

Cette faille de sécurité repose non pas sur une erreur de programmation, mais sur un défaut de conception de la norme WPA2.

Évaluation:

Les services Internet importants pour la sécurité, par ex. l'e-banking, sont déjà chiffrées au niveau du navigateur, comme l'indique dans l'adresse le préfixe «https://». De telles connexions ne risquent donc pas d'être déchiffrées à cause de la faille de sécurité décrite ci-dessus. Par contre le cryptage additionnel de la liaison radio WLAN est touché.

Il est néanmoins recommandé d'installer au plus vite les mises à jour déjà proposées par les fabricants pour cette lacune.

5.5.2 ROBOT – une faille vieille de 19 ans toujours d'actualité

Les vieilles failles s'avèrent parfois difficiles à combler, comme l'attaque Bleichenbacher découverte il y a presque 20 ans. Une analyse systématique a confirmé que sur les 100 sites les plus visités, 27 étaient encore vulnérables à ce type d'attaque – dont Facebook et Paypal. La faille a par conséquent été baptisée «Return of Bleichenbacher's Oracle Threat» (retour de la menace oracle de Bleichenbacher) ou ROBOT.

Le spécialiste en cryptographie suisse Daniel Bleichenbacher avait découvert en 1998 que les messages d'erreur d'un serveur SSL livrent de précieuses informations sur les données à déchiffrer. Moyennant l'envoi d'une série de requêtes judicieusement choisies, un déchiffrement devenait possible. Or l'actuelle norme TLS 1.2 continue d'utiliser la version de chiffrement fautive, soit le standard PKCS #1 v1.5 RSA. Pour déjouer toute attaque, il faudrait que si un bloc de données n'est pas correctement formaté le serveur envoie, en lieu et place des données déchiffrées des données aléatoires, et qu'ainsi l'entrée en connexion se poursuive. Les données aléatoires renvoyées devront être produites avant même le déchiffrement, afin de prévenir des attaques de timing. L'ensemble de la procédure est si complexe que sans surprise, son implémentation n'a pas été faite correctement sur certains serveurs.[54]

En plus des messages d'erreurs mentionnés ci-dessus, d'autres messages, comme par exemples des échecs de connexions TCP, Timeouts ou erreurs de protocoles, sont utilisés par l'attaque ROBOT afin de repérer un serveur vulnérable.

Au total, des produits de fabricants différents sont concernés. La situation est particulièrement délicate dans le cas des produits parvenus à la fin de leur cycle de vie, pour lesquels il n'est plus fourni de mise à jour.

---

[54] https://www.golem.de/news/robot-angriff-19-jahre-alter-angriff-auf-tls-funktioniert-immer-noch-1712-131607-2.html (état: le 31 janvier 2018).

5.5.3 Faille des puces de sécurité fabriquées par Infineon

En octobre 2017, des chercheurs ont découvert que les puces de sécurité d'Infineon présentaient une faille de sécurité dans la génération de clés RSA, d'où la possibilité de retrouver la clé privée à partir de la clé publique. La vulnérabilité exploitée pour l'attaque baptisée ROCA provient d'une bibliothèque de logiciels utilisée par la puce. Elle sert à générer les nombres premiers RSA, visiblement trop faibles. Une clé publique RSA est formée de deux nombres. L'un d'eux est le produit de deux grands nombres premiers générés de manière aléatoire. À condition de connaître ces deux nombres premiers, il devient possible de retrouver la clé privée. L'investissement requis pour un tel calcul est toutefois considérable, ce qui relativise la gravité de la lacune. Pour casser une clé de 2048 bits, il faudrait 141 années CPU. Il est néanmoins possible d'exploiter cette faille, moyennant une puissance de calcul suffisante. Les puces concernées d'Infineon sont intégrées à divers produits, comme des cartes à puce intelligente, des terminaux mobiles et des ordinateurs portables. L'Estonie, pays pionnier dans la numérisation au quotidien, était également concernée, ou plus précisément les cartes d'identité électroniques (eID) estoniennes. Cela a amené le gouvernement à bloquer dans ses systèmes les 760 000 certificats défectueux, jusqu'à leur actualisation auprès des services compétents.

5.5.4 Système d'exploitation vulnérable avant même sa publication

Comme tout système d'exploitation, MacOS présente régulièrement des failles de sécurité. Le moment où des tiers rendent publiques les vulnérabilités est toujours mal choisi pour l'entreprise touchée. Dans le cas d'espèce, la divulgation est intervenue au pire moment. Quelques heures avant le lancement du système d'exploitation MacOS 10.13 High Sierra agendé à la fin de septembre 2017, Patrick Wardle, chercheur en sécurité et ancien agent de la NSA, a publié une faille «zero day» de ce système. Les versions antérieures sont également concernées. Cette lacune permet de dérober les identifiants et mots de passe stockés sur l'ordinateur. Plus précisément dans le gestionnaire de mots de passe, où les utilisateurs enregistrent quantité de données sensibles (numéros de carte de crédit, mots de passe de comptes de messagerie ou de boutiques en ligne). Un maliciel annexé à un courriel ou dissimulé dans une banale App peut exploiter la faille identifiée et accéder aux données sensibles. L'erreur avait été signalée au fabricant dès le début de septembre 2017. Or Apple n'a pas pu fournir à temps la mise à jour requise, et donc High-Sierra a été commercialisé avec cette vulnérabilité.[55]

Au début de septembre 2017, Wardle avait déjà publié des détails sur une fonction de sécurité de High Sierra relativement facile à contourner. La fonction SKEL (Secure Kernel Extension Loading) vise à empêcher le chargement d'extensions tierces sans l'approbation de l'utilisateur.

[55] http://www.zdnet.de/88313439/macos-high-sierra-sicherheitsforscher-macht-zero-day-luecke-oeffentlich/?inf_by=5a91d408671db898358b4e40 (état: le 31 janvier 2018).

5.6 Mesures préventives

5.6.1 Un maliciel utilisé lors d'exercices intrigue les fabricants d'antivirus

Pendant plus de trois ans, les chercheurs de l'entreprise japonaise de logiciels et services de sécurité Trendmicro[56] ont été intrigués par un maliciel qui s'intéressait ponctuellement aux personnes occupant des postes en vue dans le secteur sud-coréen de l'énergie et des transports. Ces attaques ont été appelées OnionDog. D'autres entreprises sont tombées sur ce maliciel, l'ont analysé et ont publié des rapports à ce sujet[57]. Une analyse approfondie a toutefois révélé qu'OnionDog faisait partie d'une manœuvre de cybersécurité interne.

Les appareils infectés avaient beau communiquer avec un serveur Command & Control, ils ne recevaient jamais d'instructions de sa part. Le système se contentait d'enregistrer l'infection. Toutes les adresses utilisées remontaient au centre national de cybersécurité sud-coréen (National Cyber Security Center, NCSC). Il s'est ensuite avéré que le maliciel faisait partie de l'exercice «Ulchi Freedom Guard», organisé conjointement par la Corée du Sud et les États-Unis.

Même si les exercices proches de la réalité sont les bienvenus, il faut éviter toute fuite du maliciel utilisé dans le scénario d'exercice. Sinon des acteurs mal intentionnés y puiseront de nouvelles connaissances pour déployer de futures cyberattaques. Dans le pire des cas, une telle attaque ne sera pas prise au sérieux, puisque le maliciel est familier par l'exercice effectué et qu'on le juge inoffensif. Les conclusions hâtives au sujet de l'agresseur s'avèrent également problématiques. Dans le cas d'espèce, les 200 nouvelles versions découvertes du maliciel ont alimenté toutes sortes de spéculations sur l'origine des malfaiteurs et leurs intentions. Or la situation risque de s'envenimer rapidement suite à de telles accusations. Lorsqu'un maliciel est utilisé dans le cadre d'un exercice, il faut donc s'assurer de l'absence de fuite, ou du moins que le code malveillant soit inutilisable dans un autre contexte.

---

56 https://blog.trendmicro.com/trendlabs-security-intelligence/oniondog-not-targeted-attack-cyber-drill/ (état: le 31 janvier 2018).

57 http://zhuiri.360.cn/upload/APT-C-03-en.pdf (état: le 31 janvier 2018).

Recommandation:

Une bonne sensibilisation, à intervalles réguliers, du personnel constitue un des principaux piliers de la sécurité dans Internet. Les exercices proches de la réalité s'avèrent utiles dans ce contexte. Mais pour en garantir le bon déroulement, il faudrait au moins prévenir avant un tel test tous les acteurs responsables de l'infrastructure: soit notamment le registre gérant les domaines de premier niveau (soit SWITCH pour les domaines en .ch), le registraire et le fournisseur d'hébergement, ainsi que le fournisseur de messagerie (externe) le cas échéant. Enfin, il serait judicieux d'informer MELANI, pour lui permettre de répondre aux éventuelles annonces dans l'esprit des auteurs de la campagne et de ne rien entreprendre contre la page de test.

Formulaire d'annonce MELANI

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

5.6.2 Récupérer les domaines APT

Le groupe Fancy Bear (aussi notamment appelé APT28, Sofacy ou Strontium) se sert de noms de domaines similaires aux noms d'entreprises ou de produits connus, afin que les liens ou expéditeurs affichés paraissent dignes de confiance. Les pirates appréciaient tout particulièrement, en raison de leur diffusion, des noms calqués sur les produits Microsoft comme livemicrosoft[.]net ou rsshotmail[.]com.

Microsoft n'a certes pas pu faire traduire en justice les instigateurs de la campagne. Mais les avocats du géant du logiciel ont réussi à convaincre les juges, sur le terrain du droit des marques, que les domaines litigieux renvoyaient à ses propres produits[58]. Une fois ces domaines restitués, les victimes ont cessé de se connecter à des serveurs contrôlés par les pirates, pour communiquer avec ceux de Microsoft. Les victimes ont ainsi pu être identifiées et informées de la nécessité de nettoyer leurs appareils.

5.6.3 Re:scam, assistant virtuel menant la vie dure aux escrocs

Les escroqueries à la commission, qui sévissent depuis des années, consistent à raconter aux victimes potentielles des histoires abracadabrantes pour les amener à verser de l'argent.[59] Le scénario le plus connu est celui où un prince nigérian fait miroiter une part de l'héritage du monarque, en échange d'un acompte substantiel.

Selon Netsafe[60], ONG néozélandaise pour la sécurité sur Internet, les dommages dus à de telles arnaques avoisineraient 12 milliards de dollars par an. Faute de pouvoir empêcher

58 http://www.zdnet.com/article/us-election-hack-microsoft-wins-latest-round-in-court-against-fancy-bear-phishers/ (état: le 31 janvier 2018).

59 https://www.skppsc.ch/fr/questions-frequentes/ > Thématique Internet > Fraude sur Internet + fraude en ligne > Qu'entend-on par fraude à la commission? (état: le 31 janvier 2018).

60 https://www.netsafe.org.nz/ (état: le 31 janvier 2018).

l'envoi de tels messages, Netsafe a opté pour une approche originale. Cette organisation a mis au point des assistants à intelligence artificielle, chargés de faire perdre un maximum de temps aux escrocs[61]. Il suffit de transférer les courriels suspects à une adresse e-mail. L'assistant virtuel analyse le contenu du courriel et génère des réponses sensées, jusqu'à ce que l'agresseur finisse par se lasser. En gardant occupés les escrocs le plus longtemps possible, l'assistant virtuel les empêche de sévir ailleurs. Le déroulement de certaines conversations peut être suivi sur le compte Twitter[62] de re:scam. La communication ainsi générée prête parfois à sourire et montre le désarroi des escrocs pris à leur propre piège.

6 Tendances et perspectives

6.1 Neutralité du Net

La neutralité du Net désigne le principe selon lequel toutes les données doivent être traitées de la même manière lors de leur transmission par Internet, quels que soient l'expéditeur ou le destinataire, le service, l'application ou le contenu. Ce principe prévient toute intervention discriminatoire dans le trafic des données. Les pratiques âprement débattues dans ce contexte comprennent notamment le blocage de services, la priorité accordée à certains services et le ralentissement de certains autres, ainsi que la différenciation de produits dans l'accès à Internet. La neutralité du Net garantit par exemple que des opérateurs de téléphonie mobile ne bloquent pas les services VoIP, que les fournisseurs d'accès ne privilégient pas leur propre offre groupée de télévision sur IP au détriment des services de diffusion en continu, que les protocoles réseau pair à pair et les transmissions vidéo ne subissent aucun ralentissement, ou encore que les services de messagerie et de diffusion en continu soient mis sur un pied d'égalité pour la facturation du volume de données utilisées.

L'autorité américaine de surveillance des télécommunications (Federal Communications Commission, FCC) a publié le 14 décembre 2017 un décret[63] abrogeant ses propres dispositions de 2015[64] sur la neutralité du Net. Concrètement, les fournisseurs Internet ont été reclassés sur le plan juridique: ils cessent d'être des services de télécommunication et des «fournisseurs de base» (common carriers), redevenant de simples services d'information, et à ce titre ne sont plus soumis à la surveillance de la FCC, qui veillait jusque-là au respect de la neutralité du Net.

Plusieurs États fédéraux ainsi que le Congrès fédéral cherchent à invalider la décision de la FCC. Dans l'UE, la neutralité d'Internet a été établie en 2015, dans un règlement, en tant que «règles communes destinées à garantir un traitement égal et non discriminatoire du trafic dans le cadre de la fourniture de services d'accès à l'internet».[65] Diverses exceptions y sont toutefois définies. Ainsi des «services spécifiques», comme la télémédecine pour laquelle un niveau de qualité spécifique est objectivement nécessaire, peuvent jouir d'un traitement de faveur. Cela à condition toutefois que le service spécialisé en question ne puisse pas être

---

61 https://www.rescam.org/ (état: le 31 janvier 2018).

62 https://twitter.com/rescambot/ (état: le 31 janvier 2018).

63 Restoring Internet Freedom Order: https://apps.fcc.gov/edocs_public/attachmatch/FCC-17-166A1.pdf (état: le 31 janvier 2018).

64 Open Internet Order: https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf (état: le 31 janvier 2018).

65 RÈGLEMENT (UE) 2015/2120, http://eur-lex.europa.eu/eli/reg/2015/2120/oj (état: le 31 janvier 2018).

utilisé pour l'accès général à Internet. En outre, les mesures de gestion du trafic établissant une distinction entre des catégories de trafic objectivement différentes peuvent être admises. Néanmoins, une telle distinction ne sera autorisée que sur la base d'exigences techniques objectivement différentes en matière de qualité des services (par exemple, en termes de latence, de gigue, de pertes de paquets et de largeur de bande), et non sur la base de considérations commerciales. Il est par ailleurs permis d'exclure ou de décompter différemment le trafic de données de services spécifiques, dans le cadre de forfaits mensuels (zero rating). Les États membres restent libres d'édicter des règles plus sévères sur la neutralité d'Internet.

En Suisse, la neutralité d'Internet n'est pas ancrée dans la loi. Dans l'actuel chantier de révision partielle de la loi sur les télécommunications (LTC)[66], l'Office fédéral de la communication (OFCOM) a publié en 2014 un rapport sur la neutralité des réseaux[67], afin d'analyser le besoin de réglementation. On s'est toutefois limité à introduire, dans le projet de loi, des obligations étendues de signaler les restrictions existantes. La Suisse ne connaîtra donc probablement pas dans un proche avenir de dispositions impératives sur la neutralité des réseaux. Divers acteurs ont d'ores et déjà annoncé leur intention de revenir au Parlement sur le thème de la neutralité d'Internet, dans le débat sur la révision de la LTC.

L'avenir dira si les prescriptions sur la transparence, avec le risque réputationnel qui s'ensuit, dissuadent les fournisseurs Internet de déroger au principe de la neutralité des réseaux. Il se peut d'ailleurs que le problème ne se pose pas en Suisse avec la même acuité que dans d'autres pays, en raison tant de l'excellente infrastructure du réseau que de la manière dont les opérateurs conçoivent leur offre.

Aux États-Unis comme dans l'UE, il existe une obligation fondamentale de signaler de manière transparente les mesures restrictives. Il appartient donc à la société civile d'observer l'évolution liée à la neutralité d'Internet, pour intervenir le cas échéant.

6.2 Cyber-parasitage: quand des maliciels empruntent votre CPU

Le succès des cryptomonnaies donne des idées aux cybercriminels. Le chapitre 5.4.3 du présent rapport relate par exemple des cas de vol de Bitcoins à large échelle. Mais 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.

---

66 Aperçu publié sur le site de l'OFCOM: https://www.bakom.admin.ch/bakom/fr/page-daccueil/l-ofcom/organisation/bases-legales/lois-federales/revision-2017-de-la-ltc.html; message concernant la révision de la LTC: https://www.admin.ch/opc/fr/federal-gazette/2017/6185.pdf; projet de loi: https://www.admin.ch/opc/fr/federal-gazette/2017/6327.pdf (état: le 31 janvier 2018).

67 https://www.bakom.admin.ch/bakom/fr/page-daccueil/suisse-numerique-et-internet/internet/neutralite-des-reseaux.html (état: le 31 janvier 2018).

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[68]). Depuis lors, les attaques cherchant à utiliser la puissance de calcul d'ordinateurs à des fins de minage se sont multipliées. L'année 2017 a été particulièrement riche en la matière, à tel point que certains se demandent si ce n'est pas désormais un des modèles d'affaires les plus profitables pour les cybercriminels. D'ailleurs, certains codes malveillants ont opté pour le minage, alors que d'autres manières de rentabiliser leur intrusion étaient à disposition, comme le chiffrement de données. On peut penser à Wannamine, logiciel malveillant sophistiqué se propageant notamment à l'aide de l'exploit EternalBlue, dont les Ransomware WannaCry et NotPetya ont notamment fait usage. À ceci près que les criminels ont choisi de paramétrer leur outil pour qu'une fois installé, il mine de la monnaie virtuelle au lieu de chiffrer les données de l'utilisateur.

L'installation d'un maliciel n'est pas la seule option possible pour utiliser une machine à l'insu de son détenteur à des fins de minage. Ainsi, des sites contiennent des scripts ayant comme finalité de miner de la cryptomonnaie à travers les navigateurs des visiteurs. Si certains sites demandent l'autorisation du visiteur, qui met alors consciemment à disposition sa machine pour participer au financement d'un site web, d'autres ne s'embarrassent pas de cette précaution. Par ailleurs, dans bien des cas, des sites ont été compromis pour y placer de tels scripts, au profit de cybercriminels.

Si le fait d'utiliser les ressources d'une machine peut paraître plus bénin que d'autres types d'attaques, par exemple qu'un ransomware chiffrant des données, il ne faut pas sous-estimer le potentiel de nuisance de telles attaques. Tout d'abord, le prix du minage inopiné est celui de l'électricité consommée par les ressources accaparées. Par ailleurs si un logiciel malveillant mobilise les ressources informatiques utiles au bon fonctionnement des processus, des problèmes de stabilité ou des pannes sont à craindre, qui seront d'autant plus inquiétants pour des systèmes d'importance vitale. L'élimination d'un tel logiciel risque également de causer des interruptions de service.

Au vu de leur essor actuel, de telles attaques semblent présenter un rapport coût-bénéfice très intéressant. Pour les criminels, ces méthodes nécessitent d'être mises en œuvre à large échelle pour être profitables, les capacités de calcul de quelques machines n'étant pas suffisantes. En revanche, elles présentent l'avantage de la régularité des revenus. Pas besoin que la victime fasse le choix de payer suite au chiffrement de ses données, ou qu'il ouvre une session e-banking que l'on cherchera à détourner: une machine infectée va automatiquement commencer à générer de l'argent. Il s'agit au final du passage le plus direct entre compromission d'une machine et génération de revenu. Avantage supplémentaire, ce type de détournement est souvent difficile à détecter. Le but est ainsi de disposer d'une grande quantité de machines qui, discrètement, avec régularité et un minimum d'interruptions, rapportent chacune une petite somme d'argent. Or, et c'est peut-être le vrai problème, qu'adviendra-t-il de ces machines compromises, le jour où l'évolution du marché rendra cette activité financièrement moins attrayante? Des modes opératoires plus destructeurs sont à craindre. Il serait ainsi naïf de considérer le minage intempestif – tout au moins lorsqu'il fait suite à l'installation d'un logiciel malveillant – comme un simple parasitage bénin.

---

[68] 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).

6.3 Externalisation? La sécurité doit primer!

Dans notre monde globalisé et hautement spécialisé, rares sont les entreprises qui peuvent encore se permettre de gérer en interne tous leurs processus opérationnels. Pour rester concurrentiel il faut maximiser l'efficience de ses processus, tout en réduisant ses coûts. L'externalisation de certains services (outsourcing) peut contribuer à une telle optimisation. Or il est important de privilégier la sécurité, lors du choix d'un partenaire externe: le meilleur marché n'est pas forcément le plus sûr. En outre, on peut externaliser une prestation, mais jamais la responsabilité et le risque. Le cas échéant, chaque entreprise devrait constamment se demander quelles données peuvent être communiquées et ce qui se passerait en cas de fuite. Une entreprise ne doit jamais confier à des tiers les données dont la perte représenterait pour elle une menace existentielle.

Le Premier ministre suédois, Stefan Löfven, en a fait la désagréable expérience. En juillet 2017, il a dû reconnaître devant les médias que des données confidentielles de l'armée suédoise, du registre des permis de conduire et même du programme de protection des témoins risquaient de tomber entre des mains indélicates. Les autorités avaient auparavant externalisé leur gestion informatique au groupe IBM. Le géant américain avait alors mandaté des sous-traitants, en République tchèque et en Roumanie. Toutes les données avaient beau être stockées en Suède, les techniciens des deux sous-traitants y accédaient sans avoir reçu d'habilitation de sécurité. Les autorités suédoises ont affirmé n'avoir aucune preuve qu'un mauvais usage ait été fait des données en question.

Recommandation:

Pour s'épargner de mauvaises surprises, il faut définir en amont de ce type de projet les exigences exactes à respecter, et établir un concept de sécurité informatique pour les domaines externalisés. Il s'agit de préciser quels risques une externalisation des données pourrait entraîner, et quelles sont les mesures à prendre pour les limiter. Il est important de mettre en place une gestion des risques digne de ce nom, de ne pas minimiser les risques et de ne pas se laisser aveugler par les économies de coûts possibles. Parmi les mesures à prendre, il convient de citer la définition précise des droits d'accès, l'intervention exclusive de personnes dûment autorisées dans le processus d'installation et de maintenance, ainsi que le cryptage des données en vue de leur transport ou de leur archivage. Outre des sauvegardes régulières, il convient de veiller aux contrôles de l'accès physique aux données. Les entreprises ne devraient pas se contenter de promesses de leurs prestataires, mais exiger ponctuellement des preuves (par ex. sous forme de certificats de sécurité), et les contrôler. De même, il convient de définir les mesures à prendre dans l'hypothèse où malgré toutes ces précautions, un incident devrait surgir.

Conclusion:

La gestion des risques va devenir toujours plus complexe, notamment pour les prestations de service externalisées. On l'a bien vu quand les vulnérabilités des processeurs Spectre et Meltdown ont été publiées au début janvier. Le matériel est lui aussi sujet aux défaillances, et aucun élément d'un système informatique ne peut être considéré comme absolument sûr. Toute politique de sécurité devrait donc comporter une panoplie de mesures (organisationnelles et techniques) pour limiter autant que possible les risques, en cas d'apparition d'une telle lacune dans une composante. En l'occurrence, les vulnérabilités concernaient surtout les environnements virtualisés, et donc les prestations de service sous-traitées. Les entreprises dont des données sont traitées dans les centres de calcul de tiers doivent par conséquent s'assurer que les exploitants de tels centres aient pris toutes les précautions nécessaires pour réduire les risques liés à ce genre de lacunes de sécurité. Le cas échéant, elles peuvent exiger par contrat des garanties à propos des mesures adoptées.

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 lien
Ip	17.4285	Définir des rôles clairs pour les acteurs de la cyberdéfense et de la cybersécurité de la Suisse	Fathi Derder	15.12.2017	CN	DDPS	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174285
Ip	17.4100	Passage au numérique de la politique étrangère et de sécurité. Quels sont les risques et les opportunités pour la Suisse?	Damian Müller	13.12.201	CN	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174100
Ip	17.4004	Nécessité d'une vue d'ensemble et, le cas échéant, d'une coordination	Sylvia Flückiger-Bäni	30.11.201	CN	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174004
Ip	17.3905	Loi contre les cyberrisques	Sibel Arslan	29.09.2017	CN	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173905
Po	17.3875	Renforcer la recherche scientifique au sein de l'armée et développer des collaborations avec les institutions de recherche	Fathi Derder	29.09.2017	CN	DDPS	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173875
Mo	17.3849	Armée suisse. Comment garantir notre souveraineté et notre indépendance alors que le numérique pousse à l'interdépendance?	Claude Béglé	28.09.2017	CN	DDPS	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173849
Ip	17.3731	Pour un DDPS qui veille à la cybersécurité de tous, au-delà des seuls aspects militaires	Edith Graf-Litscher	27.09.2017	CN	DDPS	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173731
Ip	17.4296	Imposer de manière équitable les géants du	Balthasar Glättli	15.12.2017	CN	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-

		Net en prélevant une taxe d'égalisation sur le chiffre d'affaires réalisé en ligne					vista/geschaeft?AffairId=201 74296
Ip	17.4090	Mesures contre la discrimination	Nadine Masshardt	13.12.2017	CN	DFI	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=201 74090
Ip	17.3864	Offres illégales sur Internet. Réduire les préjudices et les risques	Raphaël Comte	28.09.2017	CE	DFJP	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=201 73864
Ip	17.4314	Quel rôle la Poste a-t-elle joué dans l'arrivée d'Amazon sur le marché suisse?	Regula Rytz	15.12.2017	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=201 74314
Po	17.4249	Transformer les régions de montagne en plates-formes spécialisées dans le stockage des données et dans les technologies numériques	Martin Candinas	15.12.2017	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=201 74249
Po	17.4041	Réduire les accidents de la circulation grâce aux systèmes d'assistance à la conduite? Plus de données sur ces systèmes et leurs effets sur la sécurité sont nécessaires	Jürg Grossen / Grünliberale Fraktion	07.12.2017	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=201 74041
Q	17.5619	Les réseaux sociaux doivent-ils être soumis à la loi fédérale sur la radio et la télévision?	Edith Graf-Litscher	06.12.2017	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=201 75619
Q	17.5614	Les bases juridiques contre la diffusion de fausses nouvelles sur les médias sociaux sont-elles suffisantes?	Edith Graf-Litscher	06.12.2017	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=201 75614
Q	17.5592	Cyberdéfense. Communication stratégique et opérations d'information	Priska Seiler Graf	05.12.2017	CN	DDPS	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=201 75592
Ip	17.3896	Comment créer une plate-forme numérique multimodale de transports publics?	Claude Béglé	29.09.2017	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=201 73896
Ip	17.3870	Développement du réseau de téléphonie mobile	Susanne Leutenegger Oberholzer	29.09.2017	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=201 73870
Mo	17.3847	Internet des objets. Façonner les conditions-cadres pour un écosystème national et international	Claude Béglé	28.09.2017	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=201 73847
Ip	17.3733	Drones civils. Peut-on ignorer les dangers?	Manuel Tornare	27.09.2017	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=201 73733
Ip	17.3734	Discours de haine sur les réseaux sociaux. Le laisser-faire?	Manuel Tornare	27.09.2017	CN	DFJP	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=201 73734
Ip	17.3723	Réseau mobile Swisscom. Comment interpréter les chiffres et la cartographie du taux de couverture national?	Jacques Nicolet	25.09.2017	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=201 73723

Q	17.5397	Donner une longueur d'avance à la Suisse grâce à un réseau de téléphonie mobile 5G performant	Karl Vogler	13.09.2017	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20175397
Po	17.4017	Profiter des opportunités offertes par les technologies civiques	Damian Müller	04.12.2017	CE	ChF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174017
Po	17.4295	Normes de sécurité pour les appareils connectés à Internet, qui constituent l'une des principales menaces en matière de cybersécurité	Balthasar Glättli	15.12.2017	CN	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174295
Po	17.4273	Regtech. Favoriser leur diffusion auprès des acteurs économiques et des autorités publiques	Claude Béglé	15.12.2017	CN	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174273
Ip	17.4062	Optimiser le service de validation Validator.ch	Marcel Dobler	12.12.2017	CN	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20174062
Ip	17.3854	Une seconde chance pour un impôt numérique	Géraldine Savary	28.09.2017	CE	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173854
Ip	17.3717	Défis et conséquences de la transformation numérique pour l'Office fédéral de la culture	Kathy Riklin	25.09.2017	CN	DFI	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173717
Q	17.5415	Production, utilisation, contrôle public et dangerosité des cryptomonnaies	Maximilian Reimann	18.09.2017	CN	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20175415

7.2 La Commission mondiale sur la stabilité du cyberespace (Global Commission on the Stability of Cyberspace, GCSC) appelle à protéger le «noyau public» d'Internet

Instaurée en février 2017 à l'occasion de la Conférence sur la sécurité de Munich, la Commission mondiale sur la stabilité du cyberespace réunit des représentants de haut niveau de gouvernements, d'entreprises, du domaine technique et de la société civile de divers pays. Elle a comme mission d'encourager la paix, la sécurité et la stabilité au niveau international en formulant des normes pour un comportement responsable des acteurs étatiques et non étatiques dans l'espace numérique et en lançant des initiatives à cet effet.

En novembre 2017, les représentants de la Commission ont lancé un appel pour protéger le noyau public d'Internet et ont demandé à tous les participants de respecter la norme suivante, qui vise à garantir l'intégrité et la disponibilité d'Internet:

> Non-Interference with the public core
>
> Without prejudice to their rights and obligations, state and non-state actors should not conduct or knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace.

Selon la définition de la Commission, le noyau public d'Internet comprend notamment les éléments suivants: le routage Internet, les systèmes d'adressage par domaine, les certificats et les systèmes de sécurité correspondants ainsi que la communication par câble.

Conclusions:

De plus en plus dépendantes des technologies de l'information liées à Internet, les sociétés modernes doivent pouvoir se fier à la stabilité et sécurité de ce dernier. Dans un espace numérique interconnecté à l'échelle planétaire, toute mesure touchant le noyau public de l'Internet peut avoir des conséquences involontaires dans le monde entier et entraîner des dommages collatéraux difficilement prévisibles. Il est donc dans l'intérêt général, d'une part, d'éviter toute activité qui risque d'entraver le bon fonctionnement d'Internet et, d'autre part, d'empêcher de telles pratiques ou, du moins, d'en atténuer les effets.

8 Produits publiés par MELANI

8.1 GovCERT.ch Blog

8.1.1 The Retefe Saga

03.08.2017 – Surprisingly, there is a lot of media attention going on at the moment on a macOS malware called OSX/Dok. In the recent weeks, various anti-virus vendors and security researchers published blog posts on this threat, presenting their analysis and findings. While some findings where very interesting, others were misleading or simply wrong.

➔ https://www.govcert.admin.ch/blog/33/the-retefe-saga

8.1.2 Leaked Accounts

29.08.2017 – MELANI/GovCERT has been informed about potentially leaked accounts that are in danger of being abused. MELANI/GovCERT provides a tool for checking whether your account might be affected: https://checktool.ch

➔ https://www.govcert.admin.ch/blog/34/leaked-accounts

8.2 Lettres d'information de MELANI

8.2.1 E-banking: les escrocs prennent pour cible les données d'activation

17.08.2017 – Fin 2016, MELANI a fait savoir dans une lettre d'information que les escrocs visent de plus en plus les moyens d'authentification mobiles utilisés pour l'e-banking. Depuis peu, ils vont jusqu'à inciter leurs victimes à leur envoyer une copie de la lettre de la banque contenant les données permettant d'activer l'authentification à deux facteurs.

➔ https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/e-banking--angreifer-haben-es-auf-aktivierungsbriefe-abgesehen.html

8.2.2 21'000 données d'accès à des services en ligne volées

29.08.2017 – La Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI a reçu environ 21‘000 combinaisons de noms d'utilisateur et mots de passe, ayant de toute évidence été dérobés et pouvant être utilisés à des fins illicites..

➔ https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/passwoerter-von-21000-e-mail-konten-im-umlauf.html

8.2.3 Les rançongiciels et les courriels abusifs envoyés au nom d’autorités sont de plus en plus nombreux

02.11.2017 – Le 25e rapport semestriel de la Centrale d’enregistrement et d’analyse pour la sûreté de l’information (MELANI), publié le 2 novembre, porte sur les principaux cyberincidents observés au cours du premier semestre 2017 sur le plan national et international. Les rançongiciels WannaCry et NotPetya, qui ont fait les gros titres dans le monde entier au printemps 2017, sont le thème prioritaire du rapport.

➔ https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/rapport-semestriel-1-2017.html

8.2.4 70 000 données d’accès à des services en ligne volées

05.12.2017 – La Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI a de nouveau reçu une liste avec des combinaisons de noms d'utilisateur et de mots de passe. Il s'agit cette fois de 70'000 données d'accès.

➔ https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/passwoerter-von-70000-e-mail-konten-im-umlauf.html

8.3 Listes de contrôle et instructions

MELANI n’a pas publié de listes de contrôle ou d’instructions supplémentaires durant le deuxième semestre de 2017.

9 Glossaire

Notion	Description
Adresse IP	Adresse identifiant l'ordinateur sur Internet (ou dans un réseau TCP/IP) (exemple : 172.16.54.87).
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.

App	Le terme app (abréviation anglaise d'application) recouvre tous les logiciels d'application destinés à l'utilisateur final. Dans le vocabulaire courant, il désigne surtout des applications pour smartphones modernes et tablettes tactiles.
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.)
Backup	Un backup (sauvegarde des données) désigne la duplication de données, dont la restauration permettra de retrouver les données perdues.
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.
Certificat	Un certificat numérique est l'équivalent, dans le cyberespace, d'une pièce d'identité et sert à attribuer une clé publique spécifique à une personne ou organisation. Il porte la signature numérique de l'autorité de certification.
Chiffrement RSA	Algorithme de cryptographie asymétrique (du nom de ses inventeurs Rivest, Shamir et Adleman), inventé en 1978.
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).
Ethernet	Technologie de transfert de données par réseau local câblé.
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.
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.
Injection SQL	Une injection SQL exploite une lacune de sécurité liée aux banques de données SQL, dès lors que le concepteur du site Web néglige de contrôler les variables utilisées dans les requêtes SQL. Le pirate cherche à exécuter des requêtes non prévues, pour modifier les données voire contrôler le server.
Internet des objets	Ensemble des objets branchés à Internet capables de communiquer pour collecter, transmettre et traiter des données, avec ou sans intervention humaine.
Javascript	Langage de script basé objet pour le développement d'applications. Les Javascripts sont des éléments de programmes intégrés au code HTML qui permettent d'implémenter certaines fonctions dans le navigateur Internet. Un exemple est le contrôle des indications saisies par l'utilisateur dans un formulaire Web. Il permet de vérifier que tous les caractères introduits dans un champ demandant un numéro de téléphone sont effectivement des chiffres. Comme les composants ActiveX, les Javascripts s'exécutent sur l'ordinateur de l'internaute. Outre les fonctions utiles, il est malheureusement possible aussi d'en programmer de

	nuisibles. Au contraire d'ActiveX, le langage JavaScript est compatible avec tous les navigateurs.
Kit d'exploits	Outil permettant de générer des scripts, programmes ou codes, visant à exploiter des failles de sécurité.
Malware	Programme malveillant. Terme générique employé pour tout logiciel exécutant des fonctions nuisibles sur un ordinateur (comme p.ex. les virus, les vers ou les chevaux de Troie).
Managed Service Provider (MSP)	Un fournisseur de services d'infogérance (MSP) est une société de services informatiques qui gère à distance les systèmes informatiques de ses clients, de manière proactive et sous un modèle forfaitaire.
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 valeur n'est pas inférieure à la valeur monétaire émise, acceptée comme moyen de paiement par des entreprises autres que l'émetteur.
Navigateur	Logiciel utilisé essentiellement pour afficher les différents contenus du Web. Les navigateurs les plus connus sont Internet Explorer, Opera, Firefox et Safari.
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.
Plug-Ins	Plugiciel. Logiciel complémentaire qui étend les fonctions de base d'une application. Exemple : les plugiciels Acrobat pour navigateurs Internet permettent un affichage direct des fichiers PDF.
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.
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.
RAM	Mémoire rapide d'accès, dont le contenu peut être modifié en usage normal (*random access memory*, RAM).
Ransomware	Rançongiciel. Maliciel utilisé comme moyen de chantage contre le propriétaire de l'ordinateur infecté. Typiquement, le criminel chiffre ou bloque la machine et demande de l'argent pour permettre de ré-accéder aux données ou à la machine.
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.
RootKit	Ensemble de programmes et de techniques permettant d'accéder sans être remarqué à un ordinateur pour en prendre le contrôle.
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.
Sel (salt)	Désigne en cryptographie une chaîne de caractères aléatoires que le système ajoute au mot de passe avant le hachage, pour en augmenter l'entropie.
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.
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.
Troll	Personne qui publie sans relâche des messages volontairement provocants sur Internet, dans le but de

	soulever des polémiques et de rompre l’équilibre d’une communauté donnée.
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.
Virus macro	Virus informatique modifiant ou remplaçant une macro, à savoir un ensemble de commandes utilisées par des logiciels pour exécuter des actions courantes.
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.