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'information et d'analyse pour la sûreté de l'information MELANI
www.melani.admin.ch/

SÛRETÉ DE L'INFORMATION

SITUATION EN SUISSE ET SUR LE PLAN INTERNATIONAL

Rapport semestriel 2017/I (janvier à juin)

2 NOVEMBRE 2017

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

1 Aperçu / Sommaire

2 Éditorial

Michel Buri
Chef-adjoint Service Informatique
Responsable de la sécurité informatique
Hôpital du Valais

Chère lectrice, cher lecteur,

L'infection massive, à l'échelle mondiale, du malware WannaCry (12 mai 2017) a marqué les esprits. De nombreuses entreprises, privées ou publiques, ont subi de graves préjudices. Le service de santé publique britannique (NHS) a également été lourdement touché. Chacun d'entre nous s'est probablement posé la question : « *Et si… ?* ». Car, nous le savons, sans un certain facteur chance, les effets dévastateurs auraient pu être bien plus importants. Plus fondamentalement, chacun d'entre nous s'est certainement aussi posé la question de savoir si les arbitrages entre les bénéfices et les risques liés aux technologies de l'information ont toujours été bien menés, et si le risque résiduel est bien acceptable.

Cette question est aujourd'hui une préoccupation majeure de l'hôpital. En effet, la médecine du 21ème siècle, centrée davantage encore sur la participation active du patient dans le processus de soins, va largement reposer sur ces technologies, avec une utilisation toujours croissante de dispositifs et d'objets médicaux connectés dans la prise en charge médicale. Parallèlement, les enjeux institutionnels liés à une cyberattaque du type WannaCry sont critiques (e.g. intégrité physique du patient, incapacité à assurer la continuité des activités).

La conclusion des médecins auteurs de l'article paru le 7 juin 2017 dans la revue « *The New England Journal of Medicine* » donne une première réponse à cette question d'acceptabilité du risque : « *We wouldn't accept being told to use outdated equipment on our patients, and our now-critical IT should be no different* »[1]. Au même titre qu'une seringue ou un médicament périmé ne doit plus être utilisé, un dispositif médical connecté embarquant un système d'exploitation périmé, ou ne disposant pas des derniers correctifs de sécurité, ne devrait donc également plus être utilisé. Aujourd'hui, cela n'est pas le cas !

De fait, c'est un des défis majeurs auquel est confronté aujourd'hui le secteur de la santé. Pour pouvoir raisonnablement garantir la sûreté de fonctionnement d'un dispositif ou d'un objet médical connecté durant tout son cycle de vie, sa sécurité doit être pensée différemment, dès sa conception. Sa cybersécurité doit être abordée de manière dynamique et holistique.

Répondre de manière appropriée à ce défi nécessite une collaboration étroite entre les différents acteurs concernés, porteurs de responsabilités : Les fabricants, les hôpitaux et l'autorité de régulation Swissmedic. Dans cet écosystème dédié à la sécurité des dispositifs et objets médicaux connectés, MELANI joue un rôle central de facilitateur.

Je vous souhaite beaucoup de plaisir à lire ce nouveau rapport.

Michel Buri

---

[1] R. Clarke, T. Youngstein. Cyberattack on Britain's National Health Service – A wake-up Call for Modern Medicine. In NEJM, June 2017. (état: le 31 juillet 2017).

3 Thème prioritaire: WannaCry et NotPetya – de simples rançongiciels?

Au premier semestre 2017, deux événements ont fait grand bruit dans le monde entier: le 12 mai 2017, le rançongiciel WannaCry paralysait au moins 200 000 ordinateurs situés dans 150 pays, selon Europol. Parmi les victimes figuraient l'opérateur espagnol Telefonica, des hôpitaux britanniques ou encore la Deutsche Bahn. En Suisse, MELANI a certes identifié 204 victimes potentielles; mais contrairement aux autres pays, aucun exploitant d'infrastructure d'importance vitale n'en faisait partie. Le 27 juin 2017, le maliciel NotPetya causait de graves dégâts, en Ukraine notamment. Il a notamment frappé l'aéroport de Kiev, la banque centrale ukrainienne et la station de mesure de la radioactivité de Tchernobyl. Des entreprises d'autres pays ont également été prises pour cibles, à l'instar du groupe danois Maersk – première compagnie maritime et plus grand armateur de porte-conteneurs du monde – et du groupe pharmaceutique américain Merck. En Suisse, la régie publicitaire Admeira a notamment été touchée par NotPetya. Les sous-chapitres suivants indiquent les particularités de ces deux attaques et les questions qu'elles soulèvent.

Lors de cyberattaques commises dans un but de chantage, un maliciel chiffre les données d'un système. La victime est alors invitée à payer une rançon pour récupérer ses données. Les rançongiciels sévissent depuis longtemps. Mais ces derniers temps, toujours plus de cybercriminels semblent recourir à ce vecteur d'attaque. MELANI observe de près cette évolution et a déjà évoqué dans plusieurs rapports semestriels les divers types de rançongiciels et leur mode opératoire[2] En outre, MELANI a organisé avec de nombreux partenaires, le 19 mai 2016, une journée de sensibilisation aux rançongiciels.[3] De tels incidents montrent une fois de plus à quel point la société moderne, avec ses systèmes interconnectés, peut être vulnérable.

Recommandations:

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

3.1 Déroulement des faits

Dans les deux cas, le maliciel a exploité une faille du protocole SMB pour se diffuser. SMB est un protocole réseau employé pour le partage de ressources (fichiers, périphériques) sous Windows. Réimplantation de SMB, le logiciel libre Samba permettant aux réseaux Windows d'intégrer un serveur Unix et vice-versa, dans une optique d'interopérabilité entre systèmes, a également fait les frais du maliciel.

[2] https://www.melani.admin.ch/melani/fr/home/themen/Ransomware.html (état: le 31 juillet 2017).

[3] https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/ransomwareday.html (état: le 19 mai 2016).

En amont des attaques, le groupe Shadow Broker avait publié en avril 2017 des outils de piratage baptisés DoublePulsar. Ces outils tiraient notamment parti d'Eternal Blue, la faille de sécurité susmentionnée du protocole SMB. DoublePulsar est un logiciel installant une porte dérobée, vraisemblablement conçu et utilisé par l'Agence nationale de sécurité américaine (NSA). Avec d'autres outils, DoublePulsar aurait été subtilisé aux autorités américaines en 2016 déjà.

Dans le cas de WannaCry, l'infection s'est très probablement propagée uniquement par les disques durs possédant une version périmée du logiciel SMB et repérables depuis Internet. Rien à ce jour n'indique l'existence d'autres canaux d'infection, comme les courriels. Par contre, le vecteur initial d'infection par NotPetya était une mise à jour manipulée d'un logiciel comptable du nom de MeDoc. Les entreprises basées en Ukraine sont tenues d'utiliser ce logiciel pour régler leurs impôts. Quand un ordinateur d'un réseau d'entreprise était infecté, la faille de SMB permettait à NotPetya de se déplacer latéralement dans le réseau infiltré. En outre, les agresseurs avaient prévu des possibilités alternatives de propagation latérale. Les cas sont donc différents: avec WannaCry, les pirates ont compté sur le hasard pour placer leur logiciel, tandis que pour NotPetya tout indique que des entreprises ukrainiennes ont été expressément visées.

L'organisation du paiement des rançons a manqué de professionnalisme, compte tenu du potentiel des deux cyberattaques: pour NotPetya, les escrocs ont recouru à la communication par courriel. Mais comme l'adresse indiquée a été rapidement bloquée, toute communication devenait impossible, et donc le code de déverrouillage n'a pu être envoyé aux victimes. Les médias se sont aussitôt emparés de cette information, et donc très peu de victimes ont payé la rançon exigée. Son montant, soit un peu plus de 300 dollars dans les deux cas, était d'ailleurs plutôt faible.

3.2 Mobiles criminels ou sabotage ciblé?

Dans les deux cas, les cyberexperts ne croient pas à des mobiles purement criminels. La mise en œuvre peu professionnelle de la solution de paiement amène à douter que les intérêts financiers aient été déterminants. Les acteurs mus par l'appât du gain cherchent en effet à soutirer très rapidement et efficacement une somme élevée aux victimes de leurs rançongiciels. Expérience à l'appui, ce volet de leurs attaques est le plus sophistiqué, ce qui n'était pas le cas de WannaCry et de NotPetya.

Toujours selon les experts, le code malveillant de WannaCry présentait des similitudes avec celui utilisé par le groupe Lazarus, lors de l'attaque lancée en mars 2016 contre la Banque nationale du Bangladesh. Quant à NotPetya, le choix d'un vecteur de propagation ciblé à travers le logiciel de comptabilité ukrainien MeDoc semble indiquer que la principale motivation des agresseurs était le sabotage. Et si des entreprises basées dans d'autres pays ont été touchées, c'est sans doute parce qu'elles étaient actives en Ukraine et donc tenues d'utiliser ce programme de comptabilité. On ne connaîtra probablement jamais l'identité du commanditaire. Ces incidents montrent de façon exemplaire les avantages d'une cyberattaque. Bien souvent, les enquêteurs doivent se contenter d'indices, et ne possèdent aucune preuve tangible. Tandis que le monde se perd en spéculations sur les mobiles et l'origine de l'agression, son auteur tire parti de l'anonymat d'Internet.

3.3 Problème des systèmes non actualisés

Dans les deux cas, la diffusion du maliciel a été aussi fructueuse parce que la faille de sécurité du protocole SMB lui permettait de se propager sans aucune interaction de la part de l'utilisateur. La lacune était pourtant connue depuis longtemps. Au début de mars 2017 déjà, Microsoft avait publié une mise à jour. Autrement dit, un incident du genre de WannaCry ou NotPetya n'aurait jamais dû provoquer d'infections. Pourquoi des entreprises renommées ont-elles alors fait les frais de telles attaques? Les particuliers actualisent souvent leurs appareils, en activant la fonction de mise à jour automatique. Donc si un fabricant publie des mises à jour le mardi, elles sont installées le lendemain déjà sur une grande partie des ordinateurs privés. Or il en va différemment dans le monde professionnel, où les mises à jour ne peuvent être reprises instantanément. Une mise à jour défectueuse risque de compromettre le fonctionnement d'une application stratégique, et donc de causer des pertes à l'entreprise. D'où la nécessité de procéder d'abord à des tests, pour garantir que les mises à jour fournies par les fabricants de logiciels n'auront aucun effet négatif sur les applications stratégiques. Il faut donc évaluer, avant toute mise à jour, si le risque lié à son absence l'emporte sur celui d'une application en panne. Il est bien clair que d'autres mesures visant à réduire les risques peuvent également être adoptées, à l'instar du cloisonnement des systèmes menacés.

Une mise à jour s'avère même souvent impossible dans certains secteurs, comme la santé. Toute modification, par exemple l'introduction d'une mise à jour, ferait perdre aux dispositifs médicaux leur certification, et donc l'autorisation d'utilisation correspondante. Le risque passerait ainsi du fabricant à l'exploitant. Une mise à jour défectueuse d'un dispositif médical pourrait avoir des conséquences fatales. Il est donc logique que les hôpitaux, les cabinets médicaux, les laboratoires, etc. ne veuillent pas courir un tel risque. Une nouvelle certification résoudrait certes le problème. Mais une recertification coûte cher, exige du temps et n'est pas partout possible. En ce sens, il n'est guère surprenant que WannaCry, en se diffusant au hasard dans le monde entier, ait fait des victimes dans le secteur de la santé, en l'occurrence en Grande-Bretagne.

3.4 Responsabilité des services de securité

Afin de pouvoir faire face aux défis dans le domaine de la sécurité, les autorités telles que les services de police ou les services de renseignement doivent de plus en plus souvent recourir à des méthodes électroniques pour surveiller des cibles. Dans un contexte où les communications circulant dans Internet sont désormais souvent chiffrées, ces services sont amenés à se focaliser sur les ordinateurs des cibles, afin de pouvoir accéder à l'information avant la procédure de chiffrement. Pour les services de sécurité, les vulnérabilités encore inconnues («zero day») sont un outil incontournable : lorsque les machines sont à jour et que les cibles ne se laissent pas abuser par des méthodes d'ingénierie sociale, il s'agit là d'un des seuls moyens pour accéder au système ciblé. Cependant, l'exploitation et la rétention de ce type de vulnérabilité contrevient au processus de divulgation responsable. Cette connaissance s'accompagne ainsi d'une grande responsabilité et nécessite, tout particulièrement de la part d'un Etat, une procédure d'évaluation du risque clairement réglementée, contrôlée et permettant une traçabilité.

Si l'on peut partir du principe qu'un Etat utilisera ce type d'outil en lien avec une cible ou personne bien précise, cela n'est pas forcément le cas pour d'autres acteurs. Si de tels vulnérabilités sont utilisées sans contrôle par des acteurs sans scrupules, les dégâts peuvent alors être plus élevés que les bénéfices que le service de sécurité pensait initialement obtenir. Ce

cas de figure a été démontré par WannaCry et NotPetya : la connaissance de la vulnérabilité du protocole SMB et les outils permettant de l'exploiter faisaient apparemment partie de l'arsenal de la NSA. Cette information a été publiée mi-avril par le groupe Shadow Brokers, après que ce dernier ait annoncé en août 2016 avoir dérobé à la NSA des informations concernant des failles «zero day».

Si les failles et outils utilisés par WannaCry et NotPetya proviennent effectivement de l'arsenal d'un service de renseignement et qu'ils ont été dérobés en 2016 déjà, une annonce précoce à Microsoft en vue de la mise en place d'un correctif aurait certainement permis d'éviter cette catastrophe. Au vu du laps de temps écoulé jusqu'au correctif de mars 2017, on peut douter que cela ait été le cas. Si aucune mesure de divulgation responsable avec Microsoft n'a été prise, même après la connaissance du vol et de la sévérité de la faille, le risque d'une utilisation hors de contrôle a donc été accepté.

Il ne s'agit pas du premier cas dans lequel une faille «zero day» a été dérobée pour au final être utilisée par des groupes criminels. Ainsi, la société Hacking Team a été victime d'une cyberattaque en 2015. Les données subtilisées ont été publiées par la suite dans Internet. Le 7 mars 2017, une série de révélations de Wikileaks ont commencé à paraître sous le nom de Vault 7. On y apprenait notamment l'existence de 24 failles «zero day», dont le CIA aurait eu connaissance en 2016.

3.5 Sauvegarde des données – une assurance-vie pour toute entreprise

Bien que peu de gens sachent si une assurance finira par les indemniser en cas d'incident, et dans quelle mesure, chacun espère néanmoins que le dommage subi sera entièrement pris en charge. D'où plus tard la frustration d'apprendre que la police ne couvre pas le dommage, que la couverture est insuffisante ou que la police d'assurance n'avait pas été payée. Chacun ferait donc bien d'étudier de temps à autre ses polices et, le cas échéant, de les adapter à sa situation modifiée. Il en va de même dans le domaine de la sûreté de l'information.

Les informations figurant sur leurs serveurs constituent la base du travail quotidien, sans laquelle les entreprises seraient bien en peine de gagner de l'argent. On y trouve les coordonnées des clients, la correspondance d'affaires, les commandes, la comptabilité, le site Web avec d'éventuelles bases de données et quantité d'autres informations indispensables à la bonne marche des affaires. Il est donc évident qu'il faut régulièrement sauvegarder ces données. On ne devrait toutefois pas se fier entièrement à la technique. Il faut régulièrement tester le bon fonctionnement des sauvegardes. De même, on s'assurera ponctuellement que le processus de sauvegarde englobe toutes les données pertinentes.

La perte de données que les rançongiciels risquent de causer n'est d'ailleurs pas la seule nuisance. Il faut généralement plusieurs heures afin d'installer les données sauvegardées. Les employés ne peuvent pas travailler pendant ce temps. Dans le meilleur des cas, il n'en résultera qu'un manque à gagner; des conséquences plus graves sont toutefois à craindre pour les infrastructures d'importance vitale comme les hôpitaux. Des hôpitaux britanniques victimes de WannaCry ont ainsi dû fermer leur service des urgences et leurs patients ont été obligés de se rendre dans d'autres établissements.

Recommandations:

Définissez une stratégie de sauvegarde.

Demandez-vous quelles sont les données à sauvegarder et à quelle fréquence, et aussi pendant combien de temps il y a lieu de conserver les sauvegardes effectuées.

La copie de sauvegarde devrait être stockée hors connexion, autrement dit sur un média externe (par ex. disque dur externe) qui sera ensuite retiré de l'ordinateur, de façon à être hors de portée d'un éventuel rançongiciel.

4 Situation nationale

4.1 Systèmes de contrôle industriels (SCI)

Les exploitants d'infrastructures d'importance vitale risquent eux aussi d'être victimes d'attaques par un rançongiciel, comme l'a montré le chapitre 3. En général, les rançongiciels ne s'installent pas directement dans les systèmes de contrôle industriels, mais dans leurs systèmes d'administration. Il est vrai que si ces systèmes sont déréglés, la production risque aussi d'être affectée.

À ce jour, des rançongiciels s'attaquant expressément aux systèmes de contrôle industriels n'existent que dans les travaux de recherche.[4] Aux États-Unis, le Georgia Institute of Technology a élaboré un scénario où son maliciel expérimental dénommé LogicLocker serait à même de verrouiller la logique de commande installée, dans le but d'extorquer une rançon aux exploitants.

Dans un autre cas, la société CRITIFENCE a conçu elle-même le prototype de rançongiciel ClearEnergy[5], afin de mieux commercialiser ses mesures visant à combler une vulnérabilité découverte auparavant par elle dans des produits de SCI. Le maliciel bloque l'accès à la logique de commande et menace d'en écraser les données pour la rendre inutilisable. Par bonheur, ces exemples n'ont pas quitté à ce jour leur environnement de laboratoire pour sévir dans un environnement productif.

Des attaques classiques de maliciels ont déjà été observées par contre en Suisse contre des appareils de surveillance à distance de SCI. Un système pilotant l'approvisionnement en eau potable a ainsi fait les frais d'un rançongiciel. Le maliciel s'était diffusé par le contrôle à distance relié à Internet, sans doute lors d'une attaque par force brute contre le serveur en question. L'affaire n'a toutefois pas porté à conséquence: le système a pu être restauré grâce aux sauvegardes et mieux sécurisé. Cet exemple montre bien que toute fonctionnalité supplémentaire (ici la télésurveillance des systèmes) nécessite des mesures de sécurité accrues.

---

4 http://www.cap.gatech.edu/plcransomware.pdf (état: le 31 juillet 2017).

5 http://securityaffairs.co/wordpress/57731/malware/clearenergy-ransomware-scada.html (état: le 31 juillet 2017).

Une partie du pilotage central des systèmes de contrôle industriels est toujours plus souvent transférée dans le nuage. Le chemin de fer du Gornergrat à Zermatt[6] a par exemple adopté un système de télégestion pouvant être exploité de manière virtuelle dans un nuage. De telles installations de surveillance et de télécommande sont d'autant plus sensibles qu'on parle aujourd'hui de trains sans conducteur[7]. Les systèmes de contrôle doivent donc impérativement être bien protégés.

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 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.

4.2.1 Le rootkit VENOM analysé par le CERN

Le 11 janvier 2017, l'équipe de sécurité informatique du CERN a publié une alerte concernant le programme furtif (rootkit) VENOM.[8] Un rootkit est un outil installé sur le système compromis pour dissimuler les connexions de l'agresseur et pour cacher ses processus et ses fichiers. Dans le cas de VENOM, le pirate charge automatiquement son maliciel sur le système de fichiers, puis les changements interviennent en quelques minutes. L'horloge du système est manipulée au passage pour que les fichiers annoncent de fausses heures de modification et soient d'autant plus difficiles à repérer. Dans la mesure du possible, le maliciel est directement exécuté depuis la mémoire temporaire (RAM) sur la machine attaquée, afin de ne laisser aucune trace sur les serveurs. Le maliciel s'en prend aux serveurs Linux et installe une porte dérobée (*backdoor*) sur l'appareil piraté, de façon à pouvoir donner des

6 https://www.siemens.com/innovation/de/home/pictures-of-the-future/mobilitaet-uns-antriebe/urbane-mobilitaet-gornergratbahn.html (état: le 31 juillet 2017).

7 https://www.sob.ch/medienmitteilung/news/2017/6/15/sob-treibt-automatisches-fahren-voran.html(Stand: 31 juillet 2017).

8 https://security.web.cern.ch/security/venom.shtml (état: le 31 juillet 2017).

ordres et modifier les fichiers à distance. Selon l'EGI-CSIRT[9], l'infection initiale résulterait du vol de données d'accès à distance au moyen du protocole SSH. L'attaque présentait des similitudes avec l'intrusion survenue en 2014 dans le serveur de bavardage en ligne Freenode[10]. Au CERN, le rootkit ciblait la communauté des astrophysiciens, mais n'a eu aucune conséquence.

Recommandations:

Comme Venom efface ses traces sur la machine infectée, il est recommandé d'intégrer aux serveurs un système externe de stockage du journal des événements, pour pouvoir analyser a posteriori de tels incidents.

4.2.2 Propagande en lieu et place de la température de l'eau

Les désaccords politiques s'affichent toujours plus dans le monde virtuel. Alors que dans le passé les façades d'immeubles étaient barbouillées de graffitis, les hacktivistes défigurent aujourd'hui les pages Web. L'avantage étant qu'ils n'ont plus à se déplacer et peuvent diffuser leur propagande de n'importe où. Ce découplage de toute présence locale fait que des événements internationaux peuvent avoir des retombées sur des sites Internet suisses.

À la fin de mars 2017, des activistes avaient brandi dans les rues de Berne, au cours d'une manifestation, une banderole portant le slogan «Kill Erdogan with his own weapons». Les jours suivants, MELANI a enregistré plusieurs cas de défiguration (*defacement*) de pages Web suisses[11]. Par exemple, les visiteurs du site de la piscine de Wülflingen, dans le canton de Zurich ont découvert, au lieu de la température de l'eau, des slogans nationalistes turcs.

Fig. 1: Site défiguré de la piscine de Wülflingen (ZH)

9 https://wiki.egi.eu/w/images/c/ce/Report-venom.pdf (état: le 31 juillet 2017).

10 https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2014/october/analysis-of-the-linux-backdoor-used-in-freenode-irc-network-compromise/ (état: le 31 juillet 2017).

11 http://www.tagesanzeiger.ch/digital/internet/tuerkische-propaganda-auf-schweizer-badiwebsite/story/12947804 (état: le 31 juillet 2017).

C’est un pur hasard qu’une piscine, et celle-ci en particulier, ait été touchée. Les hacktivistes recherchent des sites Web comportant des vulnérabilités. Ils seraient certainement heureux de publier leurs slogans sur des sites très consultés d’entreprises ou d’organisations connues. Mais comme ceux-ci sont généralement bien protégés, ils s’en tiennent souvent à des sites moins prestigieux.

Ce genre de propagande n’a pas seulement déferlé sur les sites Web suisses. Des comptes Twitter[12] piratés ont été transformés en outils de propagande. D’autres types de cyberattaques complétaient le répertoire des hacktivistes turcs. En mars 2017, ils ont revendiqué les attaques DDoS lancées contre le site autrichien «oe24.at»[13].

La propagande politique n’est pas toujours le premier mobile du détournement de sites Web. Comme en attestent des plateformes spécialisées[14], la soif de reconnaissance ou l’émulation entre pairs sont souvent à l’origine de tels méfaits.

Recommandations:

Il est possible de réduire drastiquement les attaques basées sur le système de gestion de contenu (CMS), en reprenant les mises à jour de sécurité dès leur publication. D’autres mesures encore peuvent contribuer à accroître la sécurité d’un CMS.

Mesures de prévention pour les systèmes de gestion de contenu (CMS):

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

4.2.3 Les médias en ligne, un canal d’infection toujours aussi prisé

Dans son rapport semestriel 2012/2[15], MELANI avait signalé les risques émanant des sites Web, toujours plus nombreux à afficher des données de sociétés tierces. Les portails d’information sont champions en la matière, proposant à la fois des vidéos, de la publicité et des contenus de réseaux sociaux. MELANI s’est régulièrement fait l’écho[16/17] de cas d’internautes dont le système avait été infecté durant la visite de tels portails.

---

12 https://www.theregister.co.uk/2017/03/15/twitter_app_hack/ (état: le 31 juillet 2017).

13 http://www.oe24.at/oesterreich/politik/Attacke-auf-oe24-Tuerkische-Hacker-bekennen-sich/273401472 (état: le 31 juillet 2017).

14 http://zone-h.com/ (état: le 31 juillet 2017).

15 MELANI, rapport semestriel 2/2012, chapitre 5.5 https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2012-2.html (état: le 31 juillet 2017).

16 MELANI, rapport semestriel 2/2015, chapitre 4.3.1 https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2015-2.html (état: le 31 juillet 2017).

Au printemps 2017, des portails d'information suisses ont subi une série d'attaques. En mars, 20min.ch[18] a fait savoir que des tiers non autorisés avaient accédé à son portail en ligne pour y placer des scripts malveillants. Un incident similaire s'est produit en avril aux dépens de pctipp.ch[19]. Un script introduit subrepticement cherchait à détourner les internautes sur des pages diffusant des maliciels.

Les portails d'information constituent une cible attrayante pour les malfaiteurs, étant donné qu'ils attirent de nombreux visiteurs et ont ainsi une portée très large. La vaste campagne de malvertising du groupe AdGholas[20] est un bon exemple de ces agissements. Par l'entremise de *kits d'exploits,* des logiciels malveillants sur mesure sont distribués aux internautes, à travers l'insertion ciblée de code malveillant.

Des instructions avec des listes de contrôle sont téléchargeables sur le site www.melani.admin.ch:

DOCU

Mesures de prévention pour les systèmes de gestion de contenu (CMS)

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

Vous y trouverez en outre des instructions avec une liste de contrôle des mesures à prendre, au cas où vous auriez déjà été victime d'une cyberattaque:

DOCU

Instructions relatives à la suppression des maliciels sur les sites Internet

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

4.2.4 Un grand merci de votre enregistrement – spams envoyés aux abonnés

Des milliards de pourriels, ou courriels publicitaires indésirables, sont expédiés au quotidien à travers le monde. Mais les filtres antipourriels des fournisseurs de messagerie ne cessent de s'améliorer et d'en réduire les effets, dans la plupart des cas, à un niveau supportable pour la grande majorité des utilisateurs. Au début de 2017, MELANI a toutefois constaté une

---

17 MELANI, rapport semestriel 1/2016, chapitre 4.4.2 https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2016-1.html (état: le 31 juillet 2017).

18 http://static01.20min.ch/ro/multimedia/stories/story/Tentative-de-piratage-de-20minutes-ch-avortee-14490421 (état: le 31 juillet 2017).

19 http://www.pctipp.ch/in-eigener-sache/artikel/drive-by-angriff-auf-pctipp-87549/ (état: le 31 juillet 2017).

20 https://www.proofpoint.com/us/threat-insight/post/massive-adgholas-malvertising-campaigns-use-steganography-and-file-whitelisting-to-hide-in-plain-sight (état: le 31 juillet 2017). https://www.proofpoint.com/us/threat-insight/post/adgholas-malvertising-campaign-using-astrum-ek-deliver-mole-ransomware (état: le 31 juillet 2017).

recrudescence de publipostages non désirés, adressés à quelques destinataires spécifiques. Des organisations et des particuliers ont ainsi été inondés de courriels concernant des lettres d'information, contributions à des forums et autres services similaires pour abonnés. Lorsqu'un programme souscrit automatiquement à la place de l'utilisateur à de tels services, on parle alors de *subscription bomb* [21].

Si les sites en question ne demandent pas de confirmation de sa part, la victime recevra tous les messages ultérieurs de ces nombreux services. On peut certes se désinscrire et utiliser des filtres adéquats. Mais si des dizaines de milliers d'abonnements ont été souscrits, cela prend énormément de temps.

4.3 Social Engineering et phishing

Outre les diverses attaques reposant sur la technique, les attaques les plus prometteuses sont celles qui inventent une histoire crédible pour mieux tromper l'utilisateur. 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. Autrefois, les agresseurs se contentaient par exemple de la liste de contacts d'un compte de messagerie. Ils écrivaient aux victimes potentielles que l'expéditeur se trouve à l'étranger, qu'il a perdu son smartphone et son portemonnaie et qu'il a un besoin urgent d'argent. Aujourd'hui, les escrocs prennent le temps d'analyser méthodiquement la correspondance d'un compte compromis pour repérer du matériel utilisable. Ils recherchent par exemple des factures électroniques qu'ils renverront à la victime, avec un numéro IBAN modifié. Les communications avec des établissements bancaires sont très prisées des escrocs. Même des données a priori inutilisables peuvent servir, comme le montre une escroquerie échafaudée à partir de la liste des participants à une foire commerciale. Les entreprises ont été informées par écrit que des contacts avaient été noués à cette occasion, qu'une «grosse» affaire y avait été discutée et qu'il fallait la traiter en toute discrétion. Une fois le climat de confiance créé, le personnel de ces sociétés était mis sous pression pour virer une somme élevée aux escrocs.

4.3.1 Hameçonnage

De nombreux courriels de phishing ont également circulé au premier 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 respectables, de tels courriels usurpent souvent les logos d'entreprises connues ou du service concerné.

[21] http://www.forbes.com/sites/leemathews/2017/05/10/secure-email-provider-attacked-with-500k-newsletter-sign-ups/ (état: le 31 juillet 2017).

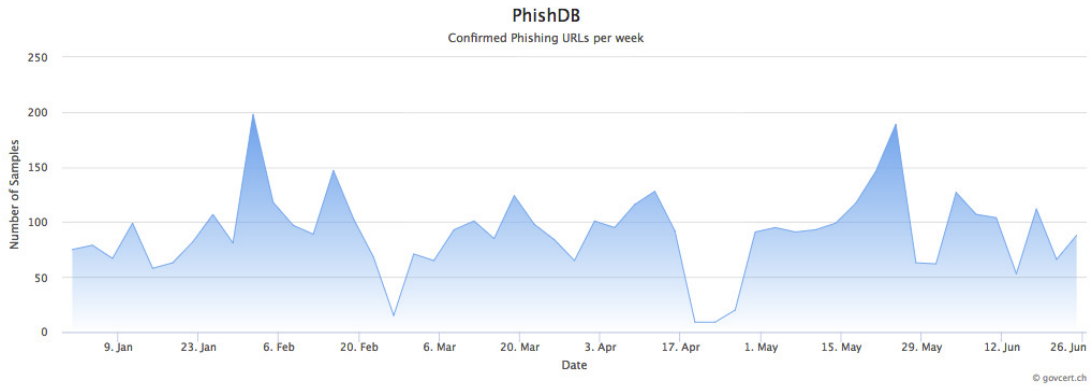

Fig. 2: Sites de phishing annoncés et confirmés par semaine sur le site antiphishing.ch au premier semestre 2017

Au total, 2343 sites de phishing avérés ont été dénoncés au premier semestre 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 en cours de semestre. 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.

4.3.2 Nouvelle méthode d'attaque ciblant les entreprises

Au premier semestre 2017, des entreprises ont reçu des appels téléphoniques où des escrocs tentaient de se faire passer pour leur établissement bancaire. Cela leur est d'autant plus facile que beaucoup de sociétés publient sur leur site Internet leurs coordonnées bancaires. Cette information peut aussi s'obtenir par téléphone ou par courriel adressé à l'entreprise.

Les auteurs des appels prétendent qu'une mise à jour de l'e-banking doit être effectuée puis testée. La présence des collaborateurs du service financier, notamment des personnes qui possèdent le droit de signature pour l'e-banking, est expressément exigée pour ce test. Soucieux d'inspirer confiance, les escrocs citent parfois les noms de collaborateurs occupant ces fonctions.

Lors du second appel, les escrocs s'efforcent d'installer un programme leur donnant accès à distance au système informatique. Une fois installé, un virement devient possible aux pirates, sous prétexte de vérifier lors d'un test les fonctionnalités du système de paiement. Comme dans le monde professionnel les paiements doivent être autorisés par signature collective au-delà d'un certain montant, ils demandent aux collaborateurs autorisés de saisir leurs données d'accès. Ce faisant, ils autorisent en réalité le détournement d'argent. Dans certains cas, les criminels ont activé un voile noir sur l'écran, afin que les victimes ne s'aperçoivent pas de leur transaction frauduleuse.

Recommandations:

Ce nouveau mode opératoire confirme que les attaques d'ingénierie sociale restent d'actualité. La sensibilisation au sein des entreprises est donc cruciale pour déjouer de telles tentatives de fraude:

- renoncez autant que possible à publier sur Internet vos coordonnées bancaires;
- ne laissez jamais des tiers non autorisés accéder à votre système;
- n'installez en aucun cas d'outils de télémaintenance (*remote tools*) à la demande de tiers non autorisés;
- aucune banque ne vous demandera de collaborer à de quelconques tests. Les banques possèdent leur propre service informatique, ou alors ont externalisé leur informatique. Dans tous les cas, les mises à jour de sécurité sont testées avant d'être mises à la disposition du public.

4.3.3 Arnaque au président – succès d'une fraude low tech

On est en présence de l'arnaque au président (*CEO fraud*) quand des escrocs ayant usurpé l'identité d'un dirigeant de l'entreprise prient en son nom la comptabilité ou le service financier de procéder à un versement sur un compte leur appartenant et situé d'ordinaire à l'étranger. La plupart du temps, la demande est effectuée depuis une adresse électronique falsifiée, mais des cas de compromission d'un compte existant ont aussi été observés. Les raisons invoquées varient, mais incluent souvent une opération financière urgente et extrêmement sensible (acquisition notamment). Le recours à un consultant ou à un cabinet d'avocat qui n'existe pas ou dont l'identité a également été usurpée peut intervenir dans le scénario. Les attaquants savent mettre une pression importante sur l'employé visé, prétextant une situation urgente, pour le contraindre à effectuer le versement et parfois à contourner les processus existants.

Cette forme de fraude a connu une croissance exponentielle, comme en témoignent les statistiques publiées au premier semestre 2017. Selon l'Office fédéral allemand de police criminelle (BKA), la fraude au président a causé en Allemagne, au cours des derniers mois, des dégâts se chiffrant en millions.[22] En mai dernier, le FBI a publié des chiffres sur l'essor spectaculaire de cette forme de fraude. Entre janvier 2015 et décembre 2016, l'arnaque au président a atteint une croissance de 2370 %. Il ressort d'un rapport que des cas ont été relevés dans 132 pays et que les dommages causés se chiffrent en milliards.[23] L'argent dérobé est généralement transféré dans des banques situées en Chine et à Hong Kong, mais des banques basées au Royaume Uni reçoivent toujours plus d'argent issu de ce genre de fraudes. Depuis longtemps déjà et malgré des moyens techniques rudimentaires, les attaques d'ingénierie sociale causent une bonne partie des dommages financiers survenant en ligne.

[22] https://www.bsi.bund.de/DE/Presse/Pressemitteilungen/Presse2017/CEO_Fraud_10072017.html (état: le 31 juillet 2017).

[23] https://www.ic3.gov/media/2017/170504.aspx#fn3 (état: le 31 juillet 2017).

Recommandations:

Les attaques d'ingénierie sociale tirent parti de la serviabilité, de la bonne foi ou de l'insécurité des personnes pour accéder par exemple à des données confidentielles ou pour conduire la victime à exécuter des actions spécifiques. Elles restent parmi les attaques les plus fructueuses, toutes catégories confondues. MELANI a publié des conseils sur la manière de se protéger de telles attaques.

Thèmes actuels: CEO-Fraud

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

Thèmes actuels: Ingénierie sociale (social engineering)

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

4.3.4 Faux support par téléphone: perfectionnement des méthodes

Depuis plusieurs années déjà, des escrocs appellent des utilisateurs suisses, la plupart du temps au nom de Microsoft, en prétextant un problème informatique nécessitant un dépannage à distance. Les escrocs cherchent à effrayer leur cible en lui faisant croire que sa machine est compromise. Ils lui demanderont par exemple d'ouvrir l'observateur d'événements (*Event Viewer*), qui signale tous les événements et activités de l'ordinateur. Selon l'âge et la configuration de l'ordinateur, la liste des messages d'erreur publiés dans le journal des événements peut être très longue, sans que le système présente le moindre problème. Suite à cela, ils chercheront à prendre la main sur la machine grâce à un logiciel d'accès à distance afin de procéder à des manipulations, et demanderont parfois un paiement pour leur soi-disant prestation. Nous avons déjà eu l'occasion de décrire ce phénomène à plusieurs reprises (la première fois dans notre rapport semestriel 2011/2, chapitre 3.1).[24]

Ces appels téléphoniques sont toujours en cours, mais désormais, les escrocs utilisent également d'autres méthodes pour entrer en contact avec leurs cibles. Dans un premier cas de figure, des appels sont effectués mais au bout du fil, la personne appelée trouvera un message préenregistré lui demandant de rappeler un numéro afin de résoudre des problèmes informatiques constatés sur sa machine.

Une tendance plus pernicieuse existe depuis quelques temps à l'étranger, et a été observée plus récemment en Suisse. Dans cette dernière, l'utilisateur naviguant sur Internet verra s'afficher un pop-up, propagé depuis des sites Internet suspects ou des publicités malveillantes. Cette fenêtre contextuelle contient un message prétendant venir de Microsoft et affirmant qu'un maliciel est présent sur la machine. Afin d'éviter des conséquences fâcheuses telles qu'un vol de données sensibles, l'utilisateur devra appeler un numéro de téléphone. Une fois l'appel effectué, on en revient au mode opératoire classique du faux support par téléphone décrit ci-dessus. Il est intéressant de noter que les escrocs ont parfois recours à des numéros suisses, depuis lesquels les appels sont vraisemblablement redirigés à l'étranger.

[24] Rapport semestriel 2011/2, chapitre 3.1
https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2011-2.html (état: le 31 juillet 2017).

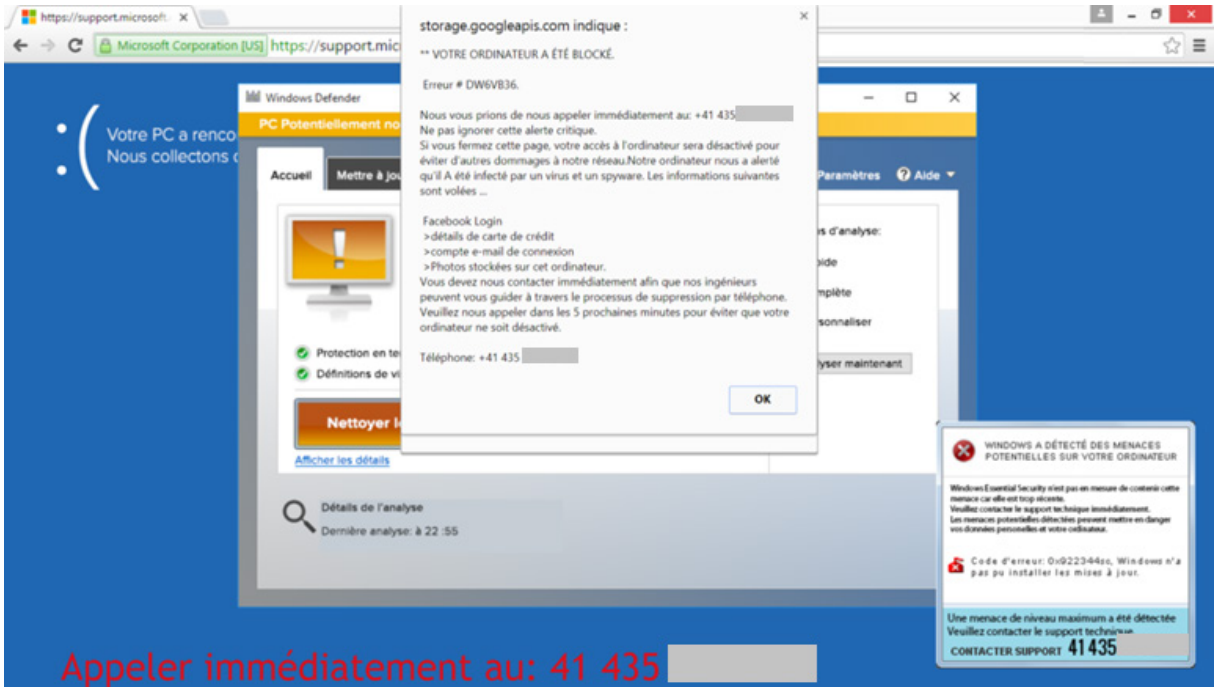

Fig. 3: Exemple de pop-up s'affichant sur l'écran. Il ne s'agit pas de la barre de navigation réelle, mais d'une simple image donnant l'illusion que l'on se trouve bien sur un site de Microsoft.

Face à ce nouveau mode opératoire, les conseils de base restent les mêmes. Il faut partir du principe que Microsoft ou d'autres entreprises n'appellent pas spontanément pour résoudre des problèmes informatiques. De tels appels doivent être immédiatement interrompus. Au cas où un accès à distance aurait été accordé aux escrocs, il est recommandé de réinstaller complètement le système et de changer les mots de passe utilisés sur la machine.

Si des messages d'alerte apparaissent sous la forme de pop-up, il est généralement possible de les faire disparaître en fermant le navigateur. En cas de pop-up persistant, il est possible de fermer le navigateur par l'intermédiaire du gestionnaire des tâches. Enfin, il faut garder à l'esprit que de tels pop-up sont généralement distribués depuis des sites peu recommandables. Il est possible de s'en prémunir dans une large mesure en naviguant sur des sites de confiance.

Recommandations:

Plus d'informations sur le site de Microsoft:

INFO

https://blogs.technet.microsoft.com/mmpc/2017/04/03/tech-support-scams-persist-with-increasingly-crafty-techniques/

https://www.microsoft.com/en-us/safety/online-privacy/avoid-phone-scams.aspx

4.3.5 Phishing basé sur la fonction Data-URL

Les escrocs sont toujours en quête de nouveaux moyens de tromper les internautes, tout en s'efforçant d'empêcher les prestataires de sécurité de désactiver leurs sites frauduleux. Une

option consiste à manipuler pour des attaques de phishing la fonction «Data-URL» du navigateur. Cette approche a beau ne pas être nouvelle, elle a servi à lancer des attaques de phishing en mars 2017. Le schéma «Data-URL» permet d'introduire directement des données dans un hyperlien, comme s'il s'agissait de ressources externes. Avec l'avantage que tout le contenu d'une page Web peut figurer dans cet hyperlien, sans qu'il faille comme d'habitude le télécharger d'un serveur. Autrement dit, la page n'est pas enregistrée sur un serveur Web, et les prestataires de sécurité n'ont pas la possibilité de la désactiver.

Une telle page incorporée dans un hyperlien diffère d'une page Web normale par son adresse URL. Elle ne commence pas par «https://», mais par «data:text/html», et elle est extrêmement longue. Or en définissant habilement le contenu de la première ligne et donc le texte apparaissant dans la barre d'adresse du navigateur, un escroc fera croire à sa victime qu'il s'agit du serveur d'un fournisseur de messagerie ou d'un institut de cartes de crédit. Concrètement, le malfaiteur doit définir le début du schéma «Data-URL» pour que seul le lien de la société en question soit visible (voir fig.4 ci-dessous). Le reste de l'hyperlien très long, qui renferme la totalité du code source de la page, disparaît dans les lignes suivantes qui ne sont pas affichées.[25]

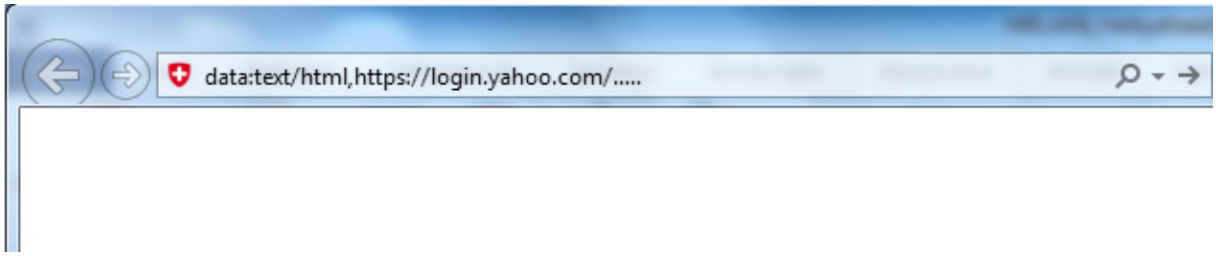

Fig. 4: Schéma «Data-URL» donnant l'illusion d'aboutir à la page d'ouverture de session de Yahoo, alors qu'il s'agit d'une page incorporée, créée par des escrocs

4.4 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 premier semestre 2017. Comme les années précédentes, la majeure partie sont imputables à Downadup (aussi appelé Conficker). Ce ver apparu il y a plus de huit ans se répand par une faille de sécurité des systèmes d'exploitation Windows, découverte en 2008 et déjà comblée à l'époque. Puis viennent en deuxième et troisième 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, est quatrième au palmarès des infections. Le premier cheval de Troie bancaire, Dyre, ne vient qu'en neuvième position.

[25] https://thehackerblog.com/dataurization-of-urls-for-a-more-effective-phishing-campaign/index.html (état: le 31 juillet 2017).

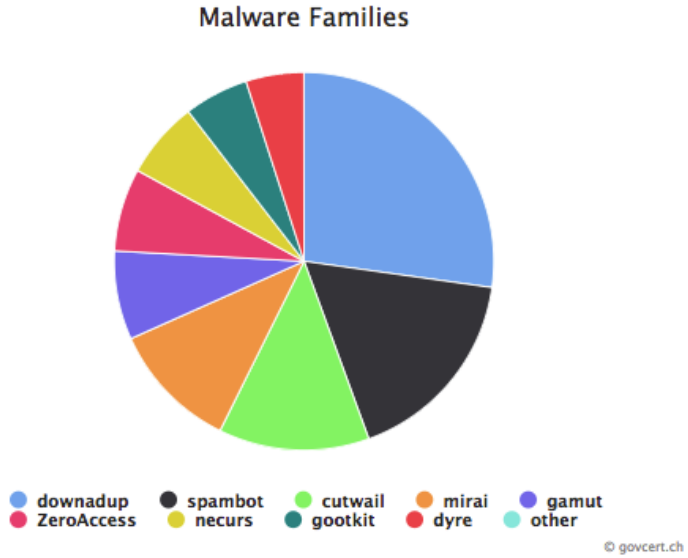

Fig. 5: Répartition des maliciels en Suisse, selon les informations en possession de MELANI (état: le 30 juin 2017). Des données actuelles sont publiées sous: http://www.govcert.admin.ch/statistics/dronemap/

4.4.1 Usurpation de l'identité d'offices fédéraux ou d'entreprises connues

Les escrocs expédient toujours plus de courriels au nom d'offices fédéraux, pour conférer une légitimité apparente à leurs courriels et accroître ainsi leurs chances de succès. Des courriels censés provenir de l'Administration fédérale des contributions (AFC) ont par exemple circulé. Ils faisaient miroiter un remboursement d'impôt au destinataire, qui devait pour cela compléter un document transmis en annexe et qui contenait un maliciel. En pareil cas, l'adresse électronique de l'expéditeur est bien entendu falsifiée.

Betreff: Fragen zu der Steuererklarung
Datum: 3. Mai 2017
An: [redacted]

Guten Tag,
mein Name ist [redacted] ich bin Steuerprüfer von Ihrem Bezirk.
Es haben sich einige Fragen zu Ihrer Steuererklärung ergeben.
Dieses Dokument enthält eine Liste von Fragen zu Ihrer Steuererklärung sowie meine Telefonnummer.

Mit freundlichen GRÜSSEN,

[redacted]

Eidgenössische Steuerverwaltung

Diese Nachricht und jegliche Anlagen sind vertraulich und unter Umständen geheim oder anderweitig vor einer Offenlegung geschützt.

Falls Sie nicht der beabsichtigte Empfänger sind, ist es Ihnen nicht gestattet, diese Nachricht oder eine Anlage zu kopieren oder ihren Inhalt gegenüber irgendwelchen anderen Personen offenzulegen.
Falls Sie diese Nachricht versehentlich erhalten haben, setzen Sie den Absender bitte umgehend davon in Kenntnis, und löschen Sie die Nachricht und jegliche Anlagen aus Ihrem System.

Fig. 6: Exemple de courriel frauduleux envoyé au nom de l'Administration fédérale des contributions (AFC)

Les escrocs usurpent aussi l'adresse d'expéditeur d'entreprises connues pour conférer une légitimité apparente à leurs courriels. Il y est fréquemment question de prétendues livraisons faites par DHL et La Poste Suisse, ou d'ordres de paiement fictifs. Un exemple connu est ici l'emploi de fausses factures censées émaner de Swisscom, par lesquelles les escrocs ont tenté de répandre le maliciel Dridex en février 2017.

Les escrocs expédient également de fausses invitations à une audience de jugement ou des courriels censés émaner de la police cantonale, dans le but de désécuriser leurs destinataires et de pousser ceux-ci à ouvrir les liens en annexe.

Conclusion:

La tactique des escrocs consiste à prendre les utilisateurs au dépourvu, à susciter leur curiosité ou à les intimider pour les amener à effectuer une action non réfléchie. Dans la plupart des cas, il s'avère rapidement que l'invitation ou le courriel sont fallacieux. Par exemple, l'AFC communique exclusivement par voie postale et jamais par simple voie électronique. Les organisations dont l'identité a été usurpée sont confrontées à un afflux de demandes d'éclaircissement, et donc à un lourd surcroît de travail.

4.4.2 Maliciels: la prudence s'impose – quel que soit le système d'exploitation

Les utilisateurs de MacOS ne sont plus à l'abri des attaques de maliciels basées sur des documents Microsoft Office: des chercheurs en sécurité ont découvert des documents Word en circulation, dotés de macros spécialement conçues pour MacOS. Au cas où l'utilisateur ouvrirait le document manipulé et autoriserait, malgré la mise en garde s'affichant à l'écran, l'activation des macros, le maliciel commence par vérifier si le logiciel de sécurité Little Snitch est actif. Si ce n'est pas le cas, le maliciel est téléchargé et une porte dérobée installée sur la machine Mac de la victime.[26]

D'autres attaques observées en Suisse contre MacOS contenaient en pièce jointe, sous la forme d'un fichier ZIP, la facture détaillée d'une prétendue commande. Ce mode opératoire visait à installer le cheval de Troie bancaire Retefe. Ce logiciel malveillant est certes bien connu en Suisse, mais à ce jour les pirates ne s'en prenaient qu'au système d'exploitation Windows.

Pour identifier le système d'exploitation utilisé par la victime et lui délivrer la version adéquate de leur maliciel, les escrocs commencent par lui envoyer un courriel anodin, qui leur transmet automatiquement cette information. En effet, ce courriel renferme une minuscule image, quasiment invisible à l'œil nu (1x1 pixel). Si elle est affichée (ce qui peut être automatique, selon la configuration de la messagerie), une communication est établie avec un serveur externe, lequel captera toute une série d'informations sur la configuration informatique utilisée, sur le système d'exploitation notamment. Les escrocs n'auront plus ensuite qu'à envoyer un courriel sur mesure à la victime pour distribuer leur maliciel.

[26] https://www.digitaltrends.com/computing/macos-suffers-first-word-macro-virus/ (état: le 31 juillet 2017).

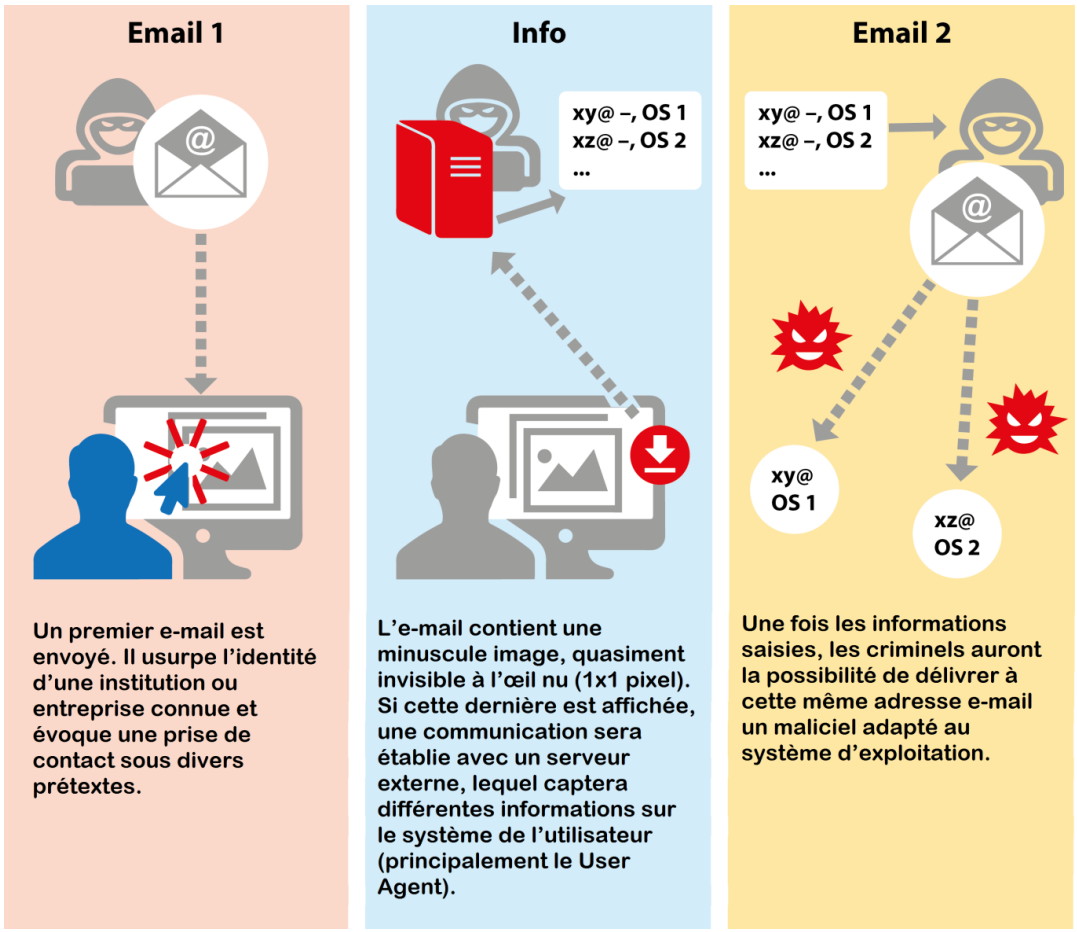

Fig. 7: Procédure utilisée par les escrocs pour identifier le système d'exploitation d'une victime

5 Situation internationale

5.1 Espionnage

5.1.1 L'infogérance prise pour cible par APT10

Depuis 2009, la campagne de cyberespionnage APT10, également connue sous les noms de menuPass, CVNX, StonePanda et POTASSIUM, s'en est prise à divers secteurs industriels ainsi qu'à des acteurs gouvernementaux. Les agresseurs semblent s'être surtout intéressés aux installations militaires de diverses nations et aux sociétés américaines.

En avril 2017, le prestataire de sécurité BAE System a publié, en collaboration avec l'entreprise d'audit et de conseil PwC et le Centre national de cybersécurité britannique (NCSC), une enquête sur les derniers méfaits d'APT10. On y apprend que depuis le deuxième semestre 2016, APT10 mène de front deux cybercampagnes: l'une contre des organisations japonaises, la seconde axée au niveau mondial sur quelques importants fournisseurs de services d'infogérance (managed service provider, MSP).

Un nouveau cheval de Troie baptisé ChChes a sévi durant la première campagne. Son certificat provenait du piratage en juillet 2015 de la société Hacking Team[27]. Selon l'état actuel des connaissances, APT10 serait le seul groupe de cyberpirates à s'en servir. Des courriels ciblés ont notamment diffusé deux types de maliciels bien connus, PlugX et Poison Ivy. Ces envois renfermaient des pièces jointes déguisées en documents Word, et le maliciel se téléchargeait en cas de clic sur l'icône affichée. Lesdits courriels, dont l'adresse de l'expéditeur avait été falsifiée et qui possédaient un en-tête accrocheur comme «The impact of Trump's victory to Japan», sont parvenus deux jours après les élections présidentielles américaines à des collaborateurs triés sur le volet de groupes pharmaceutiques japonais, ainsi qu'au personnel basé aux États-Unis d'une société japonaise.[28]

Les fournisseurs de services d'infogérance (MSP) attaqués durant la seconde campagne s'occupaient de l'infrastructure informatique de grandes organisations. Ils constituaient une cible attrayante, ayant directement accès aux systèmes et données de leurs clients. Les MSP n'étaient vraisemblablement pas un but en soi: ils auront plutôt servi de moyen d'accès aux réseaux de nombreuses grandes entreprises. Il est donc important de soigneusement choisir ses partenaires, a fortiori si la société externe s'occupe de sécurité informatique.

Les MSP ont notamment été attaqués par l'outil d'espionnage PlugX, utilisé par divers groupes criminels. RedLeaves, virus de type porte dérobée récemment développé, est également intervenu dans ce contexte.

Non seulement APT10 déploie de nouveaux outils, mais son infrastructure de commande et de contrôle (C&C) a connu une forte expansion durant la période sous revue, ce qui dénote à la fois un grand professionnalisme et des ressources financières considérables. Son champ d'action s'est également considérablement élargi par rapport aux premières années. Les cyberattaques ne se limitent plus au secteur américain de la défense ou à la branche des technologies et de la communication, mais touchent diverses autres branches industrielles, un peu partout dans le monde. Les systèmes infiltrés se trouvent en Grande-Bretagne, aux États-Unis, en Inde, au Japon et ailleurs encore.

5.1.2 16 000 personnes espionnées par un frère et une sœur

Le cyberespionnage et le vol de données sensibles de personnalités politiques sont devenus populaires depuis la cyberattaque lancée contre la direction du parti démocrate américain (voir chapitre 6.2). Des politiciens italiens ont connu les mêmes déboires. Mais cette fois l'auteur présumé n'était pas un gouvernement étranger. Le 10 janvier 2017, deux complices italiens, Giulio et Francesca Maria Occhionero, frère et sœur, étaient arrêtés.

Le maliciel utilisé est un prototype de fichier caché au format PE (*portable executable*), devant être exécuté sous Win32. Bien qu'il ait été conçu par des criminels inexpérimentés et ne se souciant guère de leur sécurité personnelle, il est passé inaperçu pendant près de trois ans et a espionné 16 000 personnes. L'affaire a été découverte quand le responsable de la sécurité de l'ENAV (établissement national pour l'assistance aux vols) s'est adressé à la police postale italienne après avoir reçu un courriel suspect, utilisé pour diffuser le maliciel. Or

---

[27] MELANI, rapport semestriel 2/2015, chapitre 5.1.1 https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2015-2.html (état: le 31 juillet 2017).

[28] https://researchcenter.paloaltonetworks.com/2017/02/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/ (état: le 31 juillet 2017).

les auteurs présumés de la cyberattaque et développeurs du maliciel avaient laissé des traces en enregistrant leurs adresses IP et lors des vols de données. La police est ainsi parvenue à identifier les responsables. Et comme le frère et la sœur communiquaient en clair par WhatsApp, le soupçon a été confirmé.

La campagne était dirigée contre des représentants du gouvernement et du monde économique. Parmi les victimes célèbres figurent Matteo Renzi, ex-premier ministre italien, Mario Draghi, président de la Banque centrale européenne, ainsi que des personnalités de haut rang du Vatican. Les comptes des membres d'une loge franc-maçonne ont également été piratés. L'entreprise de sécurité informatique Trendmicro estime que le frère et la sœur sont parvenus à dérober de cette manière 87 gigaoctets de données sensibles. Ils auraient pu exploiter à leur profit les données financières, étant propriétaires du cabinet de conseil financier Westland Securities. Il reste à savoir s'il était prévu de revendre les informations pillées, et le cas échéant à qui.

5.1.3 Arrestation en Russie pour trahison d'un dirigeant de Kaspersky

Les activités en ligne peuvent être dangereuses. Cette affirmation générale ne vaut pas que pour les victimes potentielles ou pour les criminels. Les chercheurs dans le domaine de la sécurité de l'information vivent eux aussi parfois dangereusement, quand ils analysent les informations touchant à la sécurité de certains États. Rouslan Stoïanov peut en témoigner: il dirigeait chez Kaspersky la cellule d'investigation sur les cyberattaques jusqu'à son arrestation à fin 2016 et à son inculpation de haute trahison. La célèbre entreprise de cybersécurité s'est distanciée de l'incident, en communiquant que «notre collaborateur a été arrêté pour des faits antérieurs à son activité chez Kaspersky».[29] Les autorités russes se sont abstenues de commenter l'arrestation. Il est visiblement reproché à Stoïanov d'avoir livré des informations confidentielles à des entreprises américaines, dont le prestataire informatique Verisign, qui les aurait transmises à son tour aux services secrets américains. Le même délit est reproché à Sergueï Mikhaïlov, directeur adjoint de la division cyber du FSB (ex-KGB) et à un agent s'appelant Dmitri Dokoutchaïev. Le vice-directeur de Verisign a démenti que les rapports remis aux autorités gouvernementales ou à d'autres clients aient pu contenir des secrets d'État, sans se prononcer concrètement sur le cas Stoïanov.

5.1.4 APT32 – Espionnage en provenance du Vietnam?

Des campagnes d'espionnage viennent parfois de régions qu'on associe moins à ce genre d'incidents. Cela vaut par exemple pour le groupe OceanLotus, découvert en 2014 par SkyEye Labs. Il n'est toutefois connu que depuis peu, suite à une recherche de l'entreprise de sécurité FireEye, et porte désormais le nom d'APT32. Les pirates sont probablement actifs depuis 2013 déjà, et leurs agissements semblent servir les intérêts vietnamiens. Outre diverses entreprises ayant des intérêts économiques au Vietnam et actives dans le secteur de la santé notamment, plusieurs médias vietnamiens ou étrangers ont été pris pour cible, ainsi que des gouvernements étrangers – chinois notamment –, mais aussi des dissidents et des activistes. FireEye a constaté douze attaques de grande envergure.

[29] http://www.forbes.com/sites/thomasbrewster/2017/01/25/russia-kaspersky-treason-arrest/#1ce5f9174a68 (état: le 31 juillet 2017).

APT32 opère avec plusieurs maliciels, distribués en annexe des programmes usuels dans le commerce. Tout indique, au vu des cibles choisies, l'implication d'une organisation étatique. Le gouvernement vietnamien a toutefois déclaré ne rien savoir des activités d'OceanLotus.

Pour ses dernières attaques, le groupe APT32 a utilisé des documents Microsoft contenant des macros malveillantes, distribués par courriel aux victimes. Il s'en est pris au siège vietnamien d'une société de conseil active au niveau mondial, aux membres de la diaspora vietnamienne vivant en Australie, à des employés du gouvernement philippin, ainsi qu'au siège local de deux producteurs de biens de consommation originaires des Philippines et des États-Unis. Les agresseurs ont recouru à des techniques d'ingénierie sociale assez peu élaborées pour inciter leurs victimes à activer les macros infectées.

5.1.5 Utilisation abusive de logiciels de surveillance commerciaux

Pegasus est un programme d'espionnage (spyware) sophistiqué, conçu pour les téléphones mobiles et capable d'infiltrer les systèmes tant iOS qu'Android. Mis au point par la société de surveillance israélienne NSO, il n'est vendu qu'aux institutions étatiques, pour les aider à combattre le terrorisme et la criminalité. Pegasus permet de surveiller toutes les activités d'un appareil mobile. On sait entre-temps que le programme d'espionnage de NSO a parfois servi des intérêts économiques partisans, à l'encontre des objectifs affichés.

En août 2016 déjà, Citizen Lab et Lookout Security[30] ont toutes deux parlé d'Ahmed Mansoor. Cet éminent défenseur des droits de l'homme vivant aux Émirats arabes unis compte en effet parmi les victimes de Pegasus. Au Mexique, ce logiciel d'espionnage aurait servi dans deux opérations différentes.

Entre juillet et août 2016, Pegasus s'en est pris à un chercheur réputé de l'Institut national de santé publique (INSP) du Mexique, ainsi qu'aux directeurs de deux ONG locales s'engageant dans la lutte contre le surpoids et l'obésité. Tous trois soutenaient la taxe sur les sodas, mesure introduite en 2014 pour réduire la consommation de boissons sucrées. Comme on pouvait s'y attendre, cette taxe a plombé les ventes de tels produits, au grand dam de l'industrie alimentaire.

En juin 2017, un article de Citizen Lab a révélé l'utilisation de logiciels malveillants contre des journalistes, des avocats et des activistes qui s'engageaient en faveur des droits de l'homme, ou alors qui enquêtaient sur la corruption des autorités gouvernementales mexicaines.[31] La plupart des tentatives d'infection ont eu lieu en août 2015 ainsi qu'entre avril et juillet 2016, quand le président mexicain et son gouvernement essuyaient de vives critiques de la part de ces milieux. Il s'agissait à chaque fois d'attaques ciblées, propagées par SMS. En usant de techniques d'ingénierie sociale, les agresseurs ont essayé d'amener les destinataires de leurs messages à cliquer sur un hyperlien qui installait automatiquement leur logiciel espion. Et si la personne en question n'était pas dupe, ses proches étaient pris pour cible. L'épouse d'un militant anti-corruption a ainsi reçu un SMS lui annonçant que son mari lui était infidèle et lui proposant de cliquer sur un lien pour voir les preuves.

---

30 https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/ (état: le 31 juillet 2017).

31 https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/ (état: le 31 juillet 2017).

5.2 Fuites d'information

Après les spectaculaires fuites d'information de 2016, où plus d'un demi-milliard de données d'utilisateurs de Yahoo[32] et plus de 100 millions de données d'accès au réseau social professionnel LinkedIn[33] avaient été piratées, de nouveaux cas de vol de données personnelles ont été rendus publics au début de 2017. Nous reviendrons encore au chapitre 6.3 sur les changements juridiques prévus au niveau européen dans le nouveau Règlement général sur la protection des données (RGPD), qui amèneront à gérer différemment de tels incidents.

5.2.1 Profil des électeurs républicains américains exposé au grand jour

À la demande du parti républicain, des sociétés devaient sonder les électeurs potentiels, durant la campagne électorale américaine de 2016. Or ces entreprises n'ont visiblement pas protégé avec le soin requis les serveurs sur lesquels leurs données étaient stockées. Des chercheurs de la société Upguard[34] ont ainsi découvert les données collectées et entreposées dans le nuage, sur un serveur non sécurisé appartenant à la société Deep Root Analytics. Quelque 1,1 téraoctets de données réunies par cette entreprise et par deux autres sociétés étaient ainsi accessibles au premier venu, dans un espace de stockage loué à Amazon. À commencer par des informations personnelles telles que le nom, la date de naissance, l'adresse, le numéro de téléphone ou les détails issus des fichiers électoraux, mais aussi des données sensibles sur l'appartenance ethnique ou religieuse présumée, et cela pour plus de 198 millions de personnes, soit la quasi-totalité des électeurs américains. Deep Root Analytics a expliqué au magazine The Intercept[35] que la fuite de données était due à une erreur de configuration des droits d'accès.

5.2.2 Protection contre les attaques DDoS, mais divulgation de contenus confidentiels

La société Cloudflare s'est fait connaître par la protection qu'elle offre contre les attaques DDoS. Or suite à une erreur de configuration de son logiciel serveur, des contenus de mémoire parfois sensibles de pages de tiers ont été divulgués aux visiteurs du site d'autres clients. Tavis Ormandy, chercheur en sécurité membre de l'équipe Project Zero de Google, a remarqué que pendant plusieurs mois, quand il voulait consulter des pages Internet utilisant le réseau de diffusion de contenu (*content delivery network*, CDN) Cloudflare[36], des informations confidentielles d'autres clients y étaient également publiées. L'erreur a été appelée

---

[32] MELANI, rapport semestriel 1/2016, chapitre 5.2.1 https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2016-1.html (état: le 31 juillet 2017).

[33] MELANI, rapport semestriel 2/2015, chapitre 5.2.2 https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2015-2.html (état: le 31 juillet 2017).

[34] https://www.upguard.com/breaches/the-rnc-files?utm_campaign=RNC%20Files&utm_source=upguard_home&utm_medium=breakingnewsbanner, (état: le 31 juillet 2017).

[35] https://theintercept.com/2017/06/19/republican-data-mining-firm-exposed-personal-information-for-virtually-every-american-voter/ (état: le 31 juillet 2017).

[36] Un réseau de diffusion de contenu (content delivery network, CDN) est constitué d'ordinateurs reliés en réseau à travers Internet, qui coopèrent pour mettre du contenu ou des données à la disposition des utilisateurs.

Cloudbleed sur les réseaux sociaux, par analogie à Heartbleed, la vulnérabilité ayant touché le logiciel OpenSSL.

Ormandy est connu pour s'intéresser principalement aux entreprises promettant de protéger des risques d'Internet. Cloudflare a fait savoir que rien n'indiquait qu'en dehors du chercheur de Google, d'autres personnes aient remarqué l'erreur. Il reste toutefois un risque que les données figurant dans la mémoire cache des moteurs de recherche et des services Web ayant indiqué les pages en question continuent d'être visibles pour des tiers non autorisés.

5.2.3 eID indienne: confiance ébranlée par des fuites de données

Soucieuse d'accroître la transparence des flux monétaires sur son territoire, l'Inde aimerait inciter sa population à renoncer à payer en espèces, en optant pour les cartes de crédit. Elle mise à cet effet sur le projet d'identité numérique Aadhaar, lancé il y a huit ans, qui gère la base de données des numéros d'identité uniques (*unique identification number*, UID), utilisée pour l'authentification et l'autorisation des paiements par carte.

Le groupe de recherche indien Centre for Internet and Society (CIS)[37] a annoncé que 135 millions de données de cartes de crédit, reliées à 100 millions de comptes bancaires avaient été subtilisées. Cette fuite de données n'était pas due à la base de données Aadhaar. Le problème venait d'au moins quatre projets gouvernementaux, qui complètent les données d'Aadhaar par leurs propres informations.

L'incident montre de manière exemplaire les risques qu'implique l'usage d'identités uniques en ligne, qu'il convient de limiter autant que possible. Une négligence même minime de la part d'un des partenaires risque de porter gravement atteinte à la sphère privée des utilisateurs, et donc d'ébranler durablement la confiance accordée au projet.

5.3 Systèmes de contrôle industriels (SCI)

Ce chapitre expose tout d'abord les récentes découvertes concernant le maliciel qui, en décembre 2016, avait provoqué pour la seconde fois une panne électrique en Ukraine[38]. Il y est aussi question de téléviseurs, de sirènes d'alarme, de caméras de surveillance et de portes de chambres d'hôtels, qui tous peuvent être rangés parmi les systèmes de contrôle industriels et qui ont également subi des cyberattaques au premier semestre 2017.

Des maliciels s'attaquant aux exploitants de systèmes de contrôle industriels sont à tout moment découverts. Une étude du projet MIMICS (*malware in modern industrial control systems*)[39] de la société de cybersécurité Dragos, spécialisée dans les SCI, parvient à la conclusion que les exploitants de tels systèmes sont confrontés aux mêmes types de maliciels que les autres entreprises. Un cheval de Troie bancaire sera certes inoffensif dans un SCI.

---

37 http://cis-india.org/internet-governance/information-security-practices-of-aadhaar-or-lack-thereof-a-documentation-of-public-availability-of-aadhaar-numbers-with-sensitive-personal-financial-information-1 (état: le 31 juillet 2017).

38 MELANI, rapport semestriel 2/2016, 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 juillet 2017).

39 https://dragos.com/blog/mimics/ (état: le 31 juillet 2017).

Par contre, un rançongiciel chiffrant des fichiers nécessaires à l'exploitation paralysera l'appareil infecté, voire des systèmes entiers. Cela est récemment arrivé à Washington à des téléviseurs connectés[40] ou à des caméras de surveillance[41]. Le maliciel Brickerbot[42/43] a également causé de sérieux dégâts dans l'Internet des objets, en rendant inutilisables des appareils vulnérables connectés. Or bien qu'elles soient sérieusement embarrassantes pour les victimes, toutes ces attaques ne visaient pas expressément à perturber le fonctionnement des systèmes de contrôle.

5.3.1 Industroyer/CrashOverride – maliciel apte à communiquer avec une sous-station

Après les nombreux articles parus en début d'année[44/45], les médias se sont désintéressés de la cyberattaque présumée subie en décembre 2016 par le réseau électrique au nord de Kiev. Dans l'intervalle, les chercheurs en sécurité impliqués se sont efforcés d'identifier les causes de la panne électrique. Le 12 juin, le prestataire de sécurité ESET et Dragos, société de cybersécurité spécialisée dans les SCI, ont publié de façon concertée les résultats de leurs analyses d'échantillons, baptisant le nouveau maliciel Industroyer[46] ou CrashOverride[47]. Il s'agit du tout premier outil expressément conçu pour saboter les réseaux électriques. Après Stuxnet, Havex et Blackenergy 2, CrashOverride est le quatrième maliciel à viser les SCI. C'est encore, avec Stuxnet, l'unique maliciel capable à ce jour de modifier de son propre chef les processus physiques. Comme le montre la Fig. *8*, un dispositif de lancement lui permet d'intervenir, de façon ciblée, dans quatre protocoles de communication industrielle utilisés pour la fourniture d'électricité. D'autres protocoles adaptés à de futures cibles pourraient même en théorie s'y ajouter avec un effort raisonnable, en raison de sa conception modulaire. Dragos attribue la paternité du maliciel à un groupe ELECTRUM, qui serait lié au groupe Sandworm. Divers prestataires de sécurité[48] avaient imputé à Sandstorm les attaques ayant plongé l'Ukraine dans le noir en 2015 et en 2016.

---

40 https://www.heise.de/security/meldung/Erpresser-Botschaft-in-Dauerschleife-Smart-TV-von-LG-mit-Ransomware-infiziert-3584043.html (état: le 31 juillet 2017).

41 www.theregister.co.uk/2017/01/30/ransomware_killed_70_of_washington_dc_cctv_ahead_of_inauguration/ (état: le 31 juillet 2017).

42 https://ics-cert.us-cert.gov/alerts/ICS-ALERT-17-102-01A (état: le 31 juillet 2017).

43 http://www.zdnet.com/article/homeland-security-warns-of-brickerbot-malware-that-destroys-unsecured-internet-connected-devices/ (état: le 31 juillet 2017).

44 http://www.bbc.com/news/technology-38573074 (état: le 31 juillet 2017).

45 https://nakedsecurity.sophos.com/2017/01/16/ukraine-power-outages-the-work-of-cyberattackers-warn-experts/ (état: le 31 juillet 2017).

46 https://www.welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/ (état: le 31 juillet 2017).

47 https://dragos.com/blog/crashoverride/ (état: le 31 juillet 2017).

48 https://www.wired.com/story/russian-hackers-attack-ukraine/ (état: le 31 juillet 2017).

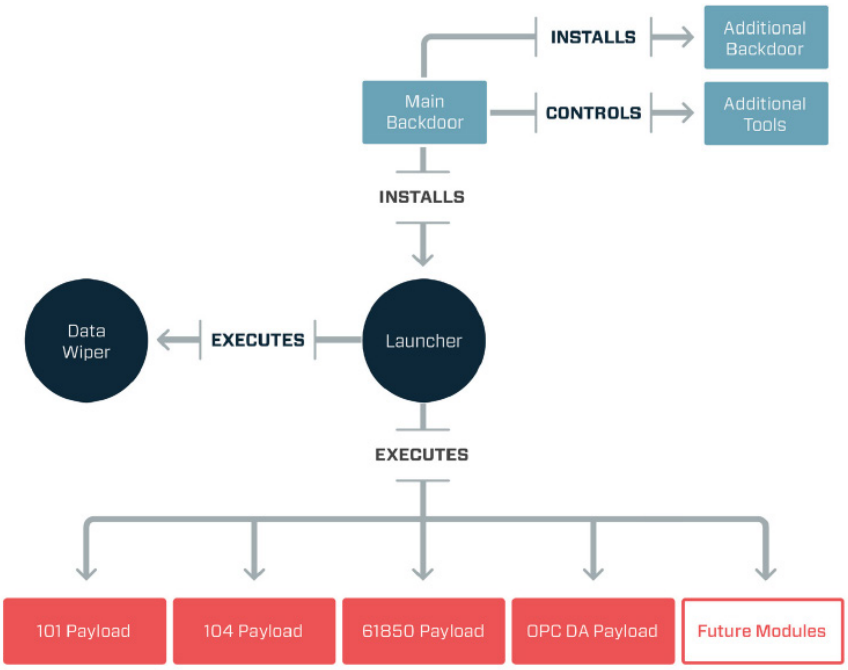

Fig. 8: Structure schématique et interaction des modules de CrashOverride (Source : https://dragos.com/blog/crashoverride/)

5.3.2 Déclenchement à minuit de sirènes d'alarme piratées à Dallas

En Suisse, le test annuel des sirènes a lieu le premier mercredi de février à midi, pour garantir qu'en cas de catastrophe, l'alarme puisse être transmise à l'ensemble de la population. Or le 7 avril 2017 peu avant minuit, quand par un ciel dégagé toutes les sirènes de Dallas ont retenti pendant 95 minutes pour mettre en garde contre une tornade, il ne s'agissait pas d'un test. On a d'abord cru à un piratage des systèmes des organisations d'urgence de la ville texane. Mais les autorités ont pu rapidement annoncer l'absence de toute intrusion dans leurs réseaux. La fausse alerte était due au fait que les sirènes sont commandées par les signaux radio que le service météorologique national émet, en cas d'incident. Or ces signaux radios sont envoyés sur des fréquences publiques, sans être spécialement sécurisés ni même chiffrés, dans le cas des vieux modèles de sirènes. Par ailleurs, les radios logicielles (*software defined radio*, SDR) capables d'émettre de tels flux radio sont toujours moins coûteuses. Et comme presque n'importe qui peut se servir de ce genre d'appareils, ce n'était qu'une question de temps pour que des abus se produisent. Il a suffi à l'agresseur de tester toutes les commandes possibles sur la fréquence correspondante. La panique qui s'est emparée des habitants de Dallas confirme le succès de cette méthode.

5.3.3 Serrures bloquées

De nombreux hôtels n'ont plus de clés classiques, mais remettent à leurs hôtes une carte sur laquelle est enregistré le code d'ouverture de leur porte de chambre. L'avantage saute aux yeux: non seulement la clé de chambre est moins encombrante, mais en cas de perte il est facile de révoquer l'ancien code pour en attribuer un nouveau à la porte. Or ce progrès a également ses inconvénients, comme l'a appris à ses dépens l'établissement autrichien Romantik Seehotel Jägerwirt. Le week-end d'ouverture de la saison d'hiver, alors que l'hôtel affichait complet, les portes des chambres sont restées closes: le système avait été infecté

par un rançongiciel[49]. Outre les systèmes de réservation et de paiement, le serveur des cartes-clés avait été pris en otage. Il n'était donc possible ni d'ouvrir les portes des chambres, ni de reprogrammer les clés. En désespoir de cause, l'hôtel a payé la rançon demandée de 1500 euros en bitcoins. Les escrocs ont alors déverrouillé les appareils infectés, tout en installant une porte dérobée pour revenir. Mais l'hôtel a rapidement remplacé une partie des appareils et mieux sécurisé son réseau, pour prévenir toute nouvelle infection. Après cette expérience désagréable, le Jägerwirt prévoit d'en revenir au système de clés traditionnel, lors de ses prochains travaux de rénovation.

Conclusions et recommandations:

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. Il faut toutefois se garder d'ignorer les risques qui s'ensuivent. En effet, les nouvelles possibilités induisent toujours de nouveaux risques, à prendre en compte dès le stade de la conception (*security by design*).

Mesures de protection des systèmes de contrôle industriels (SCI):

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

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

5.3.5 Réseaux d'établissements financiers détournés pendant sept minutes

À la fin d'avril 2017, le trafic réseau de plusieurs prestataires de services financiers, dont les sociétés de cartes de crédit Visa et Mastercard, a été détourné pendant sept minutes vers un opérateur russe. Les anomalies du protocole de passerelle frontière BGP (*Border Gateway Protocol*) sont hélas fréquentes. BGP règle le trafic entre les sous-réseaux existants, et détermine ainsi quel paquet de données sera acheminé par quel opérateur. Il est frappant de constater que l'instruction erronée de l'opérateur télécom russe Rostelecom se concentrait sur les blocs d'adresses de prestataires de services financiers ou d'entreprises de sécurité informatique. Pendant ce détournement de trafic, il lui aura été possible d'analyser le trafic réseau, et dans le pire des cas de le modifier. On ignore encore quelle manipulation a bien pu provoquer l'incident. En particulier, on n'a pas pu déterminer à ce jour si l'erreur de configuration était d'origine technique ou humaine, voire si une cyberattaque en est la cause.[50]

Dans un autre cas, ayant touché une bonne partie du réseau d'une banque brésilienne, la totalité du trafic a été détourné pendant cinq heures. Les pirates étaient parvenus à compromettre l'opérateur du serveur DNS utilisé par la banque, et donc à se faire passer pour le

[49] https://www.thelocal.at/20170128/hotel-ransomed-by-hackers-as-guests-locked-in-rooms/ (état: le 31 juillet 2017).

[50] https://arstechnica.com/information-technology/2017/04/russian-controlled-telecom-hijacks-financial-services-internet-traffic/ (état: le 31 juillet 2017).

gestionnaire de l'infrastructure bancaire auprès de la plupart des participants au réseau. Ils ont ainsi pu potentiellement espionner les transactions effectuées, intercepter les données d'accès et infecter la clientèle avec leur maliciel.[51]

5.3.6 Infection transmise par le site Web du régulateur financier polonais

Au début de février 2017, on a appris la découverte d'un maliciel sur les machines de plusieurs banques polonaises. Le vecteur d'infection était le site Web de l'Autorité polonaise de supervision financière (KNF), et les escrocs avaient utilisé la méthode *drive-by download*. Un fichier JavaScript local avait été modifié pour que les visiteurs du site chargent le fichier JavaScript malveillant, qui téléchargeait à son tour le maliciel.[52] La simple consultation de ce site Web suffisait à infecter le système des internautes. Sachant que les interlocuteurs du régulateur financier sont essentiellement des acteurs de la finance, on est en présence d'une attaque bien ciblée. Le maliciel communiquait ensuite avec des serveurs étrangers. Selon le portail BadCyber, les pirates sont parvenus dans quelques cas à prendre le contrôle des ordinateurs d'infrastructures bancaires. [53]

Il s'est avéré que l'attaque ciblée lancée contre les établissements financiers polonais s'inscrivait dans une campagne de grande envergure. Une infection analogue a été découverte sur le site Web de l'Autorité mexicaine de surveillance des banques et des bourses. Le kit d'exploits était configuré de façon à n'infecter que les visiteurs du site possédant l'une des 150 adresses IP prédéfinies. Ces adresses appartenaient à 104 organisations différentes, basées dans 31 pays. La plupart des victimes potentielles étaient actives dans le secteur bancaire, et quelques-unes dans les secteurs télécom et Internet. Selon l'état actuel des connaissances, aucune organisation suisse n'a été touchée. Les premières traces découvertes des attaques remontent à au moins octobre 2016.

Un maliciel inconnu jusque-là, baptisé Ratankba[54], était à l'œuvre: après avoir pris contact avec le serveur de commande et contrôle, il téléchargeait un outil de piratage associé à Lazarus. Le groupe Lazarus s'en prend depuis 2009 à des cibles américaines ou sud-coréennes. Le cyber-braquage de la Banque nationale du Bangladesh en 2016 lui est aussi attribué.[55] D'autres analyses de Kaspersky prouvent que le groupe Lazarus possède une cellule spécialisée dans les cyberattaques contre le système financier, qui s'est aussi fait connaître dans le passé sous le nom de BlueNoroff. La persévérance et la ténacité de cet acteur donneront certainement encore du fil à retordre aux marchés financiers internationaux.

---

51 https://www.wired.com/2017/04/hackers-hijacked-banks-entire-online-operation/ (état: le 31 juillet 2017).

52 https://badcyber.com/several-polish-banks-hacked-information-stolen-by-unknown-attackers/ (état: le 31 juillet 2017).

53 https://www.theregister.co.uk/2017/02/06/polish_banks_hit_by_malware_sent_through_hacked_financial_regulator/ (état: le 31 juillet 2017).

54 https://www.symantec.com/connect/blogs/attackers-target-dozens-global-banks-new-malware-0 (état: le 31 juillet 2017).

55 MELANI, rapport semestriel 1/2016, chapitre 5.4.1 https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2016-1.html

5.3.7 Rumeurs répandues par un réseau de zombies pour manipuler le marché

Necurs est un réseau de zombies classique spécialisé dans l'envoi de pourriels, connu pour avoir diffusé à large échelle le rançongiciel Locky ainsi que le cheval de Troie bancaire Dridex. Selon la statistique établie par MELANI, Necurs figure au septième rang des maliciels les plus répandus en Suisse.[56] Durant la période sous revue, des escrocs ont innové en envoyant des pourriels pour manipuler le cours boursier d'actions de faible valeur (*penny stocks*)[57]. Une vague de pourriels diffusés par Necurs signalait un prétendu rachat sur le marché des drones. Appâtés par un gain rapide, certains destinataires ont alors acquis des parts de la société vantée, dont le cours s'est envolé. Les pirates, qui avaient acheté des actions de cette entreprise avant d'expédier leurs pourriels, les ont alors revendues avec un coquet bénéfice. Cet exemple de fraude *pump and dump* montre que les cybercriminels sont toujours à l'affût de nouvelles tactiques pour rentabiliser leur infrastructure et leurs compétences – sans renoncer pour autant à leurs bonnes vieilles méthodes.

5.3.8 Base de données de patients aux mains de maîtres-chanteurs

Après les dommages infligés par WannaCry à des hôpitaux, en Grande-Bretagne surtout, un incident survenu dans une clinique de chirurgie plastique lituanienne rappelle à quel point les données des patients sont sensibles et doivent être protégées. Sous le pseudonyme de Tsar Team, des escrocs ont menacé les clients de cette clinique, originaires de plus de 60 pays, de publier les photos d'eux qu'ils avaient préalablement copiées dans la base de données de la clinique. Pour prouver leurs dires, ils ont mis en ligne 25 000 photos dérobées[58]. Ils avaient vainement tenté de vendre à la clinique la base de données complète pour un demi-million de livres anglaises en bitcoins, avant de contacter un par un tous ses clients dans l'espoir de leur soutirer entre 50 et 2000 euros. On ignore combien de clients leur ont versé une rançon. Tsar Team est une identité jadis utilisée par Sofacy. Or aucun lien n'a pu être confirmé jusqu'ici. Il se peut d'ailleurs que les agresseurs n'aient emprunté le nom d'un groupe connu que pour intimider leurs victimes.

5.3.9 SS7 – Norme désuète d'authentification pour l'e-banking

Outre le mot de passe, au moins un deuxième mécanisme d'authentification est utilisé pour garantir une connexion sécurisée à un service Internet comme l'e-banking. Idéalement, il s'agira d'un canal de communication indépendant. Beaucoup d'opérateurs ont opté ici pour le téléphone mobile avec le SMS. Mais comme la plupart de ces appareils sont aujourd'hui de petits ordinateurs, ils risquent d'être infectés de maliciels capables d'intercepter les messages reçus et de les transférer aux escrocs. En outre, dans bien des cas, les opérations bancaires s'effectuent directement sur le smartphone, et donc la connexion avec l'identifiant puis la deuxième authentification se font sur le même appareil. Autrement dit, l'authentification par SMS cesse d'être un gage de sécurité accrue. MELANI a déjà abordé dans son dernier rapport semestriel les problèmes soulevés par l'emploi de SMS dans ce contexte.[59]

---

[56] Voir plus haut, chapitre 4.

[57] http://blog.talosintelligence.com/2017/03/necurs-diversifies.html (état: le 31 juillet 2017).

[58] https://www.theguardian.com/technology/2017/may/31/hackers-publish-private-photos-cosmetic-surgery-clinic-bitcoin-ransom-payments?CMP=twt_gu (état: le 31 juillet 2017).

[59] MELANI, rapport semestriel 2/2016, chapitre 6.2

Au début de mars 2017, des escrocs ont exploité activement une autre possibilité d'intercepter les SMS envoyés par les banques à des fins d'authentification. Comme l'opérateur de téléphonie mobile britannique O_2 l'a confirmé à la Süddeutsche Zeitung, une faille du protocole SS7 connue depuis des années leur a servi à opérer des transactions abusives sur des comptes bancaires allemands.[60] Les escrocs ont tiré parti d'une fonction du protocole SS7, qui permet notamment l'itinérance internationale. L'appareil mobile peut s'annoncer en dehors des frontières nationales à un réseau étranger; l'exploitant du réseau contacté le signale au réseau local de l'abonné, qui lui transmet les SMS. Or il est possible de simuler une telle situation, sans que le téléphone mobile se trouve à l'étranger: les SMS seront alors déviés vers des opérateurs à l'étranger, et tomberont entre les mains des escrocs. Un tel stratagème ne fonctionne que parce qu'au départ, le protocole sous-jacent SS7 avait été conçu de manière ouverte. On partait de l'idée que fondamentalement, tous les opérateurs de téléphonie mobile se font confiance. Or avec leur multiplication dans le monde entier, il se peut entre-temps que certaines sociétés ne respectent pas toutes les règles et le cas échéant, qu'elles ne préviennent pas les activités frauduleuses, voire qu'elles collaborent avec des escrocs.

Conclusion:

Divers pays ont pratiquement éliminé les barrières à l'entrée pour les participants au marché peu recommandables. Par ailleurs, tous les opérateurs de téléphonie mobile n'effectuent pas de contrôles de plausibilité. Le problème a été régulièrement abordé depuis 2014. De solides connaissances techniques demeurent certes nécessaires pour contourner sur Internet la procédure d'authentification par SMS. Mais les groupes criminels organisés ou des acteurs étatiques possèdent d'ores et déjà les capacités requises. Aussi l'infection simultanée de l'ordinateur et du smartphone d'un utilisateur reste-t-elle sans doute la méthode la plus répandue et la plus lucrative pour les escroqueries à l'e-banking. Ne serait-ce que pour cette raison, les fournisseurs de services en ligne seront amenés à moyen terme à proposer d'autres méthodes d'authentification.

5.4 Mesures préventives

Outre la sensibilisation des utilisateurs, les arrestations constituent la mesure de prévention la plus efficace contre la cybercriminalité. On croit souvent qu'il est difficile sinon impossible d'identifier et d'arrêter les auteurs de tels abus. Or des succès sont possibles sur ce terrain.

5.4.1 Panne de Deutsche Telekom due à Mirai: arrestation

Le réseau de zombies Mirai a fait l'objet d'une analyse détaillée dans le précédent rapport semestriel.[61] Mirai est un maliciel développé pour le système d'exploitation Linux, qui s'en prend surtout aux appareils de l'Internet des objets. Le 27 novembre 2016, une attaque lan-

---

https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/halbjahresbericht-2016-2.html (état: le 31 juillet 2017).

60 https://www.theregister.co.uk/2017/05/03/hackers_fire_up_ss7_flaw/ (état: le 31 juillet 2017).

61 MELANI, rapport semestriel 2/2016, chapitre 3 https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/halbjahresbericht-2016-2.html (état: le 31 juillet 2017).

cée par Mirai avait privé d'Internet 900 000 clients de Deutsche Telekom. Suite à une erreur de programmation, la nouvelle version du maliciel utilisée avait bloqué les routeurs de Deutsche Telekom, au lieu de les infecter.

Un hacker libérien impliqué dans cette attaque a été arrêté à Londres entre-temps. Ses explications montrent à quel point les raisons d'un tel acte peuvent être complexes et multiples. Il a déclaré avoir été approché par un opérateur télécom libérien pour saboter un concurrent local. Pour mener à bien son attaque DDoS, il avait intégré dans le code librement disponible du réseau de zombies Mirai une nouvelle routine exploitant la fonction de télémaintenance de certains routeurs. Cette fonction supplémentaire aurait provoqué la panne des routeurs de Deutsche Telekom. Par ailleurs, le prévenu proposait à la location son réseau de zombies dans Internet. Il a toutefois déclaré aux juges que ce n'était qu'une manœuvre pour détourner l'attention de son donneur d'ouvrage réel, et qu'il espérait alors se faire embaucher par son mandant. Lonestar Cell, principal fournisseur Internet du Liberia, avait subi une cyberattaque en janvier 2017. Une partie de ses clients s'étaient retrouvés privés de connexion au réseau, et le câble sous-marin acheminant les télécommunications jusqu'en Afrique avait été saturé.

Le tribunal allemand s'est uniquement référé à l'attaque subie par Deutsche Telekom et n'a par conséquent condamné le hacker qu'à un an et huit mois de prison avec sursis. Il n'a pas pour autant été remis en libéré, mais placé en détention en vue d'une extradition. Les reproches formulés par les autorités britanniques sont beaucoup plus lourds. Outre l'attaque susmentionnée contre Lonestar Cell, le pirate aurait soutiré à de grandes banques britanniques des montants à cinq chiffres.

5.4.2 Arrestation de trafiquants de données de clients Apple

La police chinoise a arrêté plus de 20 employés de partenaires d'Apple, suspectés de recel et de vente au noir de données de clients du fabricant d'iPhones[62]. Principalement actifs dans la vente et le marketing, ces collaborateurs indélicats avaient récupéré dans une base de données des informations sur les détenteurs d'iPhones et d'iPads (nom, numéro de téléphone, identifiant Apple ID, etc.). Les profils étaient ensuite revendus au noir aux acheteurs intéressés entre 1,50 et 26,50 dollars pièce. Ce mode opératoire leur a permis de récolter plus de 7 millions de dollars. De tels délits d'initiés rappellent qu'il ne suffit pas, pour protéger ses données, de mettre en place des mesures préventives contre les agresseurs externes, mais que chaque organisation devrait encore prévoir des processus et systèmes internes lui permettant de repérer les attaques en cours.

62 https://www.tripwire.com/state-of-security/latest-security-news/apple-employees-detained-selling-user-data-chinese-black-market/ (état: le 31 juillet 2017).

Un bon début pour éviter de telles attaques ou d'autres similaires consiste à réaliser les mesures de l'aide-mémoire de MELANI pour les PME sur la sécurité informatique:

Sécurité informatique: aide-mémoire pour les PME

https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/aide-memoire--presentation-en-ligne-de-votre-pme.html

Portail PME de la Confédération

https://www.kmu.admin.ch/kmu/fr/home.html

6 Tendances et perspectives

6.1 Rôle des assurances dans le cyberespace

Quiconque examine l'ordonnance concernant les exigences techniques requises pour les véhicules routiers (OETV) y apprendra que les portes doivent être assurées contre une «ouverture involontaire», alors qu'un dispositif de verrouillage n'est pas explicitement exigé. De même, les systèmes d'alarme pour véhicules ne sont pas nécessaires, mais à supposer qu'un tel système soit installé à bord, l'OETV décrit précisément les exigences à respecter.

Une auto dépourvue de tout système de verrouillage aurait beau être autorisée à rouler, personne ne s'aviserait de retirer ses serrures montées par défaut. D'abord le propriétaire ne veut pas faciliter la tâche aux voleurs, ensuite l'assurance ne paierait rien en cas de vol.

On pourrait multiplier les exemples concrets où les assurances imposent le respect de normes de sécurité spécifiques, ou du moins en tiennent compte pour le calcul de leurs primes. Bien souvent, la prime due pour les œuvres d'art ne dépend pas seulement de la valeur marchande d'un tableau. D'autres facteurs interviennent, à l'instar des mesures de sécurité adoptées. Si ces dernières correspondent aux bonnes pratiques actuelles en la matière, le client paiera moins de primes.

Le cyberespace évolue très vite, avec pour effet que ce qui hier encore était à la pointe du progrès ne tardera pas à être dépassé. La promulgation de normes minimales de sécurité constitue donc une tâche permanente et dynamique. Mais comme les technologies de l'information et de la communication s'utilisent à peu près partout, les normes de sécurité du cyberespace doivent être conçues pour offrir une grande flexibilité et être dûment adaptées au but recherché. Le processus d'édiction de règles par le régulateur étatique prend cependant normalement du temps.

Par ailleurs, les assurances sont relativement libres, dans le cadre de leurs affaires, de s'adapter rapidement aux évolutions ou mutations et d'obliger leurs clients à prendre des mesures de sécurité conformes aux bonnes pratiques récentes. Ainsi, les assureurs thématisent des mesures qui, typiquement, ne sont soumises à aucune réglementation particulière.

Par conséquent, en plus d'offrir des opportunités économiques, le marché en plein essor des cyberassurances contribue plus généralement à améliorer durablement la culture de sécurité, et donc la sécurité de base dans le cyberespace.

On ne saurait pour autant s'en remettre à la branche des assurances afin qu'elle règle seule, tôt ou tard, le problème des normes de sécurité dans le cyberespace. D'abord, les autorités spécialisées peuvent la soutenir dans cette tâche, par exemple en élaborant dans leur champ d'activité des prescriptions basées sur des principes, qui puissent servir de fil conducteur à la branche. Il en va de même pour l'activité proprement dite du calcul des risques: les services étatiques peuvent apporter une contribution, grâce à leur savoir sur les menaces et leur évolution dans le cyberespace. Enfin, il existe dans le cyberespace comme dans le monde physique la possibilité hypothétique d'une «catastrophe du siècle», dont les pertes exorbitantes ruineraient n'importe quelle assurance, rendant impossible d'assurer certains cyberrisques. D'où le défi pour l'État et la branche des assurances de trouver une solution au problème, en s'inspirant par exemple de la garantie publique couvrant les dommages sismiques au-delà d'une certaine somme. En cas de succès, les assureurs bénéficieraient d'une sécurité de planification accrue et pourraient se montrer d'autant plus proactifs dans leurs polices d'assurance des cyberrisques. En définitive, la branche des assurances ne serait pas la seule gagnante: l'économie, la société et l'État profiteraient aussi de la prise en charge des risques du cyberespace, y compris des conditions édictées par les assureurs afin d'en réduire l'impact.

6.2 Cybermanipulation: les politiciens souvent pris pour cible

La cyberattaque lancée contre le comité national du Parti démocrate américain (DNC), attribuée par l'entreprise de cybersécurité Crowdstrike aux opérations d'espionnage de deux groupes, Cozy Bear et Fancy Bear[63], a été la première en date d'une longue série de cyberattaques visant des responsables politiques. Ces attaques ont montré que la publication d'informations à caractère privé tend à influencer l'opinion publique. Selon un blog du magazine en ligne The Intercept[64], l'hypothèse selon laquelle les cybercriminels cherchaient en réalité à manipuler les résultats des élections présidentielles américaines se confirme peu à peu. Le phénomène des fausses nouvelles (*fake news*), fréquentes pendant les campagnes électorales, vise lui aussi à favoriser un candidat, en entachant la réputation d'un concurrent.

Les mesures techniques de protection des réseaux gouvernementaux ou d'entreprises ne suffisent pas à protéger l'État, la société et les institutions démocratiques. On constate en effet que toujours plus de comptes en ligne privés de personnes connues, d'acteurs politiques et notamment d'élus sont la cible de cyberattaques ayant pour but de découvrir du matériel compromettant ou d'utiliser le compte piraté pour répandre des propos calomnieux ou tendancieux.

En s'inspirant d'autres pays comme l'Allemagne et la Grande-Bretagne, MELANI a conçu une liste miniaturisée, au format d'infocard, de mesures de sécurité pour aider les parlemen-

---

63 MELANI, rapport semestriel 2/2016 https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/halbjahresbericht-2016-2.html (état: le 31 juillet 2017).

64 https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/ (état: le 31 juillet 2017).

taires fédéraux à se protéger. Ces recommandations valent naturellement aussi pour les personnes n'ayant pas de mandat politique.

6.2.1 Attaques contre les programmes de vote électronique

Les cyberattaques survenues lors des élections présidentielles américaines ne visaient pas seulement les comptes de messagerie des représentants de la direction du parti démocrate. Selon le magazine en ligne The Intercept, une entreprise fabriquant des machines à voter électroniques a également été attaquée.[65]

Des courriels ont encore été envoyés de manière ciblée à plus de 100 fonctionnaires chargés d'observer les résultats des élections. Ces messages comportant un maliciel en annexe étaient bien conçus, et les membres d'organisations gouvernementales locales à qui ils étaient adressés n'ont dû se douter de rien. Les courriels étaient censés émaner d'un collaborateur d'une entreprise fournissant tant des services dans le domaine du vote électronique que des logiciels de vote en ligne. Le compte de cette société avait préalablement été compromis. Entre le 31 octobre et le 1er novembre 2016, 122 destinataires ont reçu un courriel avec en pièce jointe un document Word renfermant un cheval de Troie. La NSA est toutefois restée vague tant sur le résultat de ces cyberattaques que sur l'impact éventuel des courriels malveillants, en termes de données extraites voire manipulées.

Il faut dès lors se demander jusqu'à quel point les programmes de vote électronique sont sûrs. Les États utilisant de tels programmes devraient être bien conscients qu'il s'agit d'infrastructures d'importance vitale. Ils feraient bien de réfléchir aux processus permettant de les sécuriser de façon optimale. Et si le risque est jugé excessif, des solutions radicales doivent être envisagées. L'Allemagne et la Grande-Bretagne ont par exemple renoncé à de tels programmes.

6.2.2 Honeypots: stratégie visant à piéger les infiltrations malveillantes

En décembre 2016, les adresses e-mail des collaborateurs du candidat à l'élection présidentielle française et leader d' « En Marche » Emmanuel Macron ont été visées par une campagne de *spear phishing*. En outre, la NSA a découvert une tentative d'infiltration dans l'infrastructure française et alerté le 5 mai 2017 les autorités compétentes. Sans surprise, les attaques ont redoublé d'intensité en fin de campagne. Suite aux rebondissements des élections présidentielles américaines et en sachant bien qu'une protection complète est impossible, l'équipe technique d'«En Marche!» a alors décidé d'agir à titre préventif. Une stratégie de *cyber-blurring* (floutage numérique) a consisté à créer de faux comptes de messagerie pour piéger les attaquants, selon la technique du pot de miel (*honeypot*). Chacun de ces faux comptes regorgeait de faux documents, pour compliquer la tâche aux pirates qui devaient commencer par vérifier, en cas d'extraction de données, si les documents étaient authentiques ou non. Les agresseurs n'ont toutefois pas pris cette peine. Ils ont publié 9 gigaoctets de données, dont les faux documents. Les données ont d'abord été diffusées sur le site américain Pastebin, puis par 4Chan et WikiLeaks. En dépit des tentatives de discréditer le candidat à la présidence Macron, en lui attribuant par exemple un compte bancaire caché aux Bahamas, la stratégie a porté ses fruits. Comme les données publiées étaient en partie

[65] https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/ (état: le 31 juillet 2017).

fausses et n'avaient rien de piquant, elles n'ont guère influencé le déroulement de la campagne présidentielle.

La qualité des courriels utilisés pour cette cyberattaque a été jugée globalement bonne. Peu avant la fin de la campagne, des courriels ont circulé au nom du directeur de la campagne numérique d'Emmanuel Macron. Les destinataires étaient priés de télécharger un fichier annexé pour se protéger des cyberattaques. L'attaque a toutefois manqué de professionnalisme à certains égards, et les agresseurs ont laissé des traces. Par exemple, des noms d'utilisateurs russes apparaissaient dans les documents créés ou modifiés, ou alors ils provenaient d'une version de Microsoft disponible en Russie uniquement. Quant à l'infrastructure C&C, des indices suggèrent que les attaques s'inscrivaient dans une campagne du groupe de hackers Sofacy[66], qui s'en était déjà pris à la campagne d'Hillary Clinton.

6.2.3 L'Allemagne et la Grande-Bretagne prises pour cibles

Vers la fin juin 2017, comme l'a fait savoir l'Office fédéral allemand de la sécurité des technologies de l'information (BSI), des vagues de phishing ont pris pour cible les comptes de messagerie privés de représentants économiques ainsi que d'employés d'administrations publiques.[67] Les attaques se sont concentrées sur les comptes Yahoo et Gmail. Or les analyses de l'infrastructure des agresseurs ont révélé des similitudes avec les campagnes décrites aux chapitres 6.2.1 et 6.2.2 contre la direction du parti démocrate américain et contre la France.

Le vendredi 23 juin 2017, le Parlement anglais a lui aussi été victime d'une cyberattaque. Les comptes de messagerie de 90 parlementaires auraient été piratés. Ils possédaient apparemment des mots de passe beaucoup trop simples et non conformes aux exigences. Après avoir compromis les comptes, les escrocs ont bloqué les accès à distance, pour empêcher les propriétaires légitimes des comptes d'adopter des mots de passe sûrs.

---

66 https://www.nytimes.com/2017/04/24/world/europe/macron-russian-hacking.html?mcubz=0 (état: le 31 juillet 2017).

67 http://www.zdnet.de/88302365/bsi-warnt-vor-phishing-angriffen-auf-funktionstraeger/?inf_by=59a97d93681db8d9688b45bf (état: le 31 juillet 2017).

Recommandations:

Les administrations et les entreprises peuvent uniquement protéger leurs propres réseaux et infrastructures. Les appareils mobiles, les adresses électroniques et les autres infrastructures informatiques dont leurs collaborateurs se servent à titre privé échappent à leur sphère d'influence. Les attaques visant les réseaux privés ont donc potentiellement de meilleures chances de succès, et on ne saurait exclure la possibilité d'infecter à partir de là les réseaux gouvernementaux. Le BSI a donc publié une série de guides utiles à la prévention. Conçus pour les employés des administrations publiques et le personnel dirigeant des entreprises financières, ils s'avèrent également utiles aux particuliers. MELANI recommande en particulier les mesures suivantes, reprises des guides publiés par le BSI:

- ne pas envoyer de messages professionnels depuis un compte de messagerie privé;
- chiffrer les données confidentielles;
- mettre en place l'authentification à deux facteurs;
- changer de mot de passe au moindre soupçon de piratage du compte de messagerie.

MELANI a conçu une liste de mesures de sécurité au format d'infocard, à l'intention des parlementaires fédéraux

La liste au format d'infocardpour parlementaires peut être téléchargée sur le site de MELANI.

https://www.melani.admin.ch/melani/fr/home/documentation/Infokarten.html

6.3 Nouveau règlement général de l'UE sur la protection des données, et conséquences pour la Suisse

Le règlement général de l'Union européenne sur la protection des données (RGPD UE) uniformise au niveau européen les normes relatives au traitement des données à caractère personnel par les entreprises privées et les autorités publiques. Abrogeant la directive 95/46/CE remontant à 1995, il est entré en vigueur le 24 mai 2016, et tous les États membres doivent s'y conformer dans un délai de deux ans, soit au 25 mai 2018.

Convaincue que l'avenir numérique de l'Europe doit être basé sur la confiance, l'UE vise trois objectifs à travers le nouveau règlement: harmoniser dans toute l'Europe le droit à la protection des données, renforcer le marché intérieur en instaurant les mêmes conditions économiques dans toute l'UE, et moderniser la protection des données en réponse au progrès technique, tout en garantissant la protection des droits fondamentaux.

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.

À la différence de la directive 95/46/CE, que les États membres devaient transposer en droit national, le règlement général sur la protection des données sera directement applicable dans tout État membre à partir de mai 2018. Autrement dit, il n'est pas permis aux États membres de relativiser ou de renforcer dans leur droit national la protection des données inscrite dans le règlement. Il prévoit toutefois plus de 70 clauses d'ouverture, permettant aux États membres de traiter au niveau national certains aspects de la protection des données.

Les nombreuses exceptions prévues, source d'insécurité juridique, ont valu bien des critiques au règlement. Son objectif initial d'uniformisation serait trop abstrait, il comporterait trop d'exceptions, et des difficultés d'interprétation voire des contradictions avec le droit interne ne manqueraient pas d'apparaître. L'Allemagne en particulier craint de ne plus pouvoir appliquer sa législation sur la protection des données. Enfin, dans leur souci de neutralité technologique, les normes n'aborderaient pas de manière adéquate les risques inhérents à l'informatique et à la télécommunication.

Le règlement général sur la protection des données ne s'applique pas seulement dans l'UE, mais vaut aussi dans des États tiers comme la Suisse. 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 personnelles appartenant à des ressortissants de pays membres de l'UE ou qu'elles analysent le comportement de personnes se trouvant dans l'UE.

Recommandations:

MELANI recommande d'adapter suffisamment tôt aux nouvelles exigences légales les processus de traitement de l'information, la conservation et la sécurité des données. L'introduction du règlement, avec les sévères amendes à craindre en cas d'atteinte à la protection des données, ne préoccupe d'ailleurs pas seulement les entreprises. Les cybercriminels ne manqueront pas d'y puiser de nouveaux moyens de chantage.

La révision totale de la loi fédérale sur la protection des données suit son cours. Tout indique que la révision reprendra différentes nouveautés introduites par le règlement général de l'Union européenne sur la protection des données.

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
Motion	17.3508	Création d'un centre de compétence fédéral pour la cybersécurité	Joachim Eder	15.06.2017	Conseil des États	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173508
Motion	17.3507	Création d'un commandement de cyberdéfense dans l'armée suisse	Josef Dittli	15.06.2017	Conseil des États	DDPS	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173507

Motion	17.3497	Coordination de la lutte contre la cybercriminalité internationale organisée	Marcel Dobler	15.06.2017	Conseil national	DFJP	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173497
Motion	17.3496	Imposer une protection de base pour les infrastructures d'électricité critiques	Edith Graf-Litscher	15.06.2017	Conseil national	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173496
Postulat	17.3475	Infrastructures critiques. Prévoir une obligation de signaler les incidents graves de sécurité	Edith Graf-Litscher	15.06.2017	Conseil national	DFF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173475
Postulat	17.3433	Cybersécurité dans le domaine de la santé	Bea Heim	13.06.2017	Conseil national	DFI	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173433
Motion	17.3199	Développement des compétences en matière de cyberdéfense	Franz Grüter	16.03.2017	Conseil national	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173199
Interpellation	17.3136	Cybersécurité dans le domaine de la santé	Bea Heim	15.03.2017	Conseil national	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173136
Interpellation	17.3103	La Suisse face à la cybermenace. Que faire?	Joachim Eder	13.03.2017	Conseil des États	DDPS	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173103
Motion	17.3591	Neutralité du Net. Préserver la vitalité originelle de l'Internet	Claude Béglé	16.06.2017	Conseil national	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173591
Interpellation	17.3452	Comment soutenir les médias dans leur transition vers le numérique?	Adèle Thorens Goumaz	14.06.2017	Conseil national	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173452
Interpellation	17.3277	Les sanctions judiciaires suffisent-elles à dompter les géants d'Internet?	Jean Christophe Schwaab	02.05.2017	Conseil national	DFJP	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173277
Interpellation	17.3276	Quelle responsabilité en cas de publicité sur Internet illégale, haineuse ou générant des revenus servant à financer des activités criminelles?	Jean Christophe Schwaab	02.05.2017	Conseil national	DFJP	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173276
Interpellation	17.3254	Avantages des nouvelles technologies pour les personnes handicapées. L'exemple de HbbTV	Pascale Bruderer Wyss	17.03.2017	Conseil national	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173254

Interpellation	17.313	Vente par Internet d'animaux vivants et protection des animaux	Daniel Brélaz	15.03.2017	Conseil national	DFI	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173130
Question	17.5206	Cybersécurité. Normes destinées à empêcher que des appareils piratés connectés à l'Internet des objets ne puissent être utilisés abusivement par le biais de «botnets»	Balthasar Glättli	08.03.2017	Conseil national	DEFR	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20175206
Interpellation	17.3069	Les statistiques actuelles tiennent-elles compte du potentiel de la numérisation?	Ruedi Noser	07.03.2017	Conseil des États	DFI	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173069
Interpellation	17.3075	Quels défis et quelles chances la numérisation représente-t-elle dans le monde du travail du point de vue de l'inégalité entre les sexes?	Sibel Arslan	08.03.2017	Conseil national	DEFR	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173075
Motion	17.3592	Faire évoluer la gouvernance du numérique vers un mode de gouvernance inspiré du numérique	Claude Béglé	16.06.2017	Conseil national	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173592
Interpellation	17.3533	Renforcer la formation en informatique en Suisse	Franz Grüter	15.06.2017	Conseil national	DEFR	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173533
Interpellation	17.3341	Entre internalisations et externalisations, l'OFIT sait-il où il va?	Stefan Müller-Altermatt	04.05.2017	Conseil national	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173341
Question	17.104 0	Extension des réseaux de téléphonie mobile pour la numérisation de la Suisse	Christian Wasserfallen, Groupe libéral-radical	06.06.2017	Conseil national	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20171040
Motion	17.3498	Téléphonie mobile. Rendre sa compétitivité à la Suisse!	Yannick Buttet	16.06.2017	Conseil national	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20173498
Question	17.5303	Les drones mettent-ils en péril la sécurité des aéroports nationaux?	Priska Seiler Graf	07.06.2017	Conseil national	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20175303
Question	17.5221	Des exploitations d'alpage coupées du monde	Erich von Siebenthal	30.05.2017	Conseil national	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20175221

8 Produits publiés par MELANI

Outreses rapports semestriels, MELANI met à disposition du grand public des produits aussi nombreux que variés. Les sous-chapitres suivants passent en revue les blogs, lettres d'information, listes de contrôle, instructions et fiches d'information parus durant la période sous revue.

8.1 GovCERT.ch Blog

8.1.1 Notes About The «NotPetya» Ransomware

28.06.2017 - A new ransomware, currently named «NotPetya», has begun spreading yesterday. There are many victims, especially in Ukraine, but also large companies have been hit hard such as «Maersk» or «Merck». There are infections in Switzerland as well. As many others we have analyzed the malware and tried to harden evidence about its functioning. As there are many good papers already published, we do not want to repeat all these things but to highlight a few important facts that now can be considered being hardened evidence.

➔ https://www.govcert.admin.ch/blog/32/notes-about-the-notpetya-ransomware

8.1.2 «WannaCry»? It is not worth it!

15.05.2017 - On Friday, May 12th 2017, a ransomware called «WannaCry» hit the cyber space. Among the victims are hospitals in UK, the national telecom provider in Spain and U.S delivery service «FedEx». But WannaCry did not only hit the internet, the ransomware was also very present in newspapers worldwide. It also kept us and our partners from abroad very busy during the last weekend, analyzing the malware, reevaluating the current situation in Switzerland and world-wide, communicating with National Critical Infrastructure, and talking to the press. While we analyzed the threat as well, there are already many good papers on «WannaCry». For this reason we do for once not focus on the exact technical implementation, but try to give a comprehensive overview of this threat and the impact «WannaCry» has, with a focus on the situation in Switzerland.

➔ https://www.govcert.admin.ch/blog/31/wannacry-it-is-not-worth-it

8.1.3 When «Gozi» Lost its Head

04.04.2017 - After our automated unpacking procedure recently failed on a «Gozi» binary (MD5 c1a73ff8fb2836fe47bc095b622c6c50), we were forced to perform a manual analysis - and indeed we found some interesting new features in the first layer of the packer…

➔ https://www.govcert.admin.ch/blog/30/when-gozi-lost-its-head

8.1.4 Taking a Look at «Nymaim»

03.03.2017 - «Nymaim» is active worldwide since at least 2013 and is also responsible for many infections in Switzerland. Sinkhole Data shows that «Nymaim» is responsible for about 2% of infected devices in Switzerland that hit sinkholes the last few days. When we looked at the «Nymaim» trojan in January, we were stunned by their powerful code obfuscation techniques and wrote an «IDAPython» script to deobfuscate the code using the debugger engine.

Later we found similar tools already available in the public to do this using code emulation. Nevertheless, we decided to publish a paper about our approach, as it is a very nice case study to demonstrate how debugger orchestration works in «IDAPython», and to explain different disassembly strategies that can be used. Instrumenting the debugger means to set breakpoints in scripts and to run the code in pieces, which has a very dynamic and fascinating impact on the IDA GUI.

➔ https://www.govcert.admin.ch/blog/29/taking-a-look-at-nymaim

8.1.5 The Rise of «Dridex» and the Role of ESPs

20.02.2017 - Last week, we have warned Swiss citizens about a new malspam run targeting exclusively Swiss internet users. The attack aimed to infect them with «Dridex». «Dridex» is a sophisticated eBanking Trojan that emerged from the code base of «Bugat» / «Cridex» in 2014. Despite takedown attempts by the security industry and several arrests conducted by the FBI in 2015, the botnet is still very active. In 2016, MELANI / GovCERT.ch became aware of a handful of highly sophisticated attacks against small and medium businesses (SMB) in Switzerland aiming to steal large amounts of money by targeting offline payment software. During our incident response in 2016, we could identify «Dridex» to be the initial infection vector, which had arrived in the victim's mailbox by malicious Office Word documents, and uncovered the installation of a sophisticated malware called «Carbanak», used by the attacker for lateral movement and conducting the actual fraud. Between 2013 and 2015, the «Carbanak» malware was used to steal approximately 1 billion USD from banks worldwide.

➔ https://www.govcert.admin.ch/blog/28/the-rise-of-dridex-and-the-role-of-esps

8.1.6 «Sage 2.0» comes with IP Generation Algorithm (IPGA)

30.01.2017 - On Jan 20, 2017, we came across a malware that appeared to be a new Ransomware family called «Sage 2.0». Within a couple of days we were able to collect more than 200 malware binaries across our sensors associated with this new Ransomware. Last week, Brad Duncan also wrote a SANS InfoSec Diary entry on «Sage 2.0», noticing some strange UDP packets sent to over 7'000 different Ips.

➔ https://www.govcert.admin.ch/blog/27/sage-2.0-comes-with-ip-generation-algorithm-ipga

8.2 Lettres d'information de MELANI

MELANI a publié au première semestre 2017 les lettres d'information suivantes:

8.2.1 Logiciels malveillants : prudence recommandée, quel que soit votre système d'exploitation

15.06.2017 - Les criminels à l'origine de vagues d'e-mails malicieux cherchent de plus en plus à diversifier leurs cibles. Ainsi, ce ne sont pas uniquement les utilisateurs de Windows qui sont visés. Ces dernières semaines, la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) a observé différentes vagues cherchant à distribuer des maliciels et ciblant les utilisateurs suisses de macOS, le système d'exploitation développé

par Apple. Il est important de rappeler que la prudence s'impose pour tous les utilisateurs, quel que soit le système d'exploitation qu'ils utilisent.

➔ https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/malware---si-raccomanda-prudenza-indipendentemente-dal-sistema-o.html

8.2.2 Augmentation des cas d'usurpation de l'identité d'offices fédéraux et d'entreprises connues

04.05.2017 - Les cas d'usurpation de l'identité d'offices fédéraux et d'entreprises pour l'envoi de courriels frauduleux ont augmenté au cours des derniers mois. MELANI vous indique comment réagir.

➔ https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/zunehmender-missbrauch-der-namen-von-bundesstellen-und-firmen.html

8.2.3 Pour une utilisation sûre de l'Internet des objets

20.04.2017 - Le 24e rapport semestriel de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI), publié le 20 avril, porte sur les principaux cyberincidents observés au cours du second semestre 2016 en Suisse et sur le plan international. Le thème prioritaire du rapport est l'Internet des objets.

➔ https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/rapport_semestriel-2016-2.html

8.2.4 Ingénierie sociale: Nouvelle méthode d'attaque ciblant les entreprises

20.01.2017 - Ces derniers jours, la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) a été informée de plusieurs cas dans lesquels des escrocs se font passer pour des employés d'une banque et appellent des entreprises. Ils annoncent alors qu'une prétendue mise à jour concernant le e-banking devra être effectuée au cours d'un deuxième appel, qui aura lieu le lendemain. Ils requièrent la présence de plusieurs collaborateurs du service des finances lors de ce deuxième appel. L'objectif des escrocs est de s'assurer de la présence des personnes nécessaires afin de transmettre un paiement en signature collective.

➔ https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/social-engineering--neue-angriffsmethode-richtet-sich-gegen-firmen.html

8.3 Listes de contrôle et instructions

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

9 Glossaire

Terme	Définition

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.
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.
Booter / Stresser	Ceux-ci sont des services permettant de lancer une attaque DDoS contre de l'argent («DDoS as a service»).
Border Gateway Protocol	Protocole d'échange de routes utilisé notamment sur le réseau Internet, pour la connectivité entre des systèmes autonomes.
Content Delivery Network (CDN)	Un réseau de diffusion de contenu (CDN) est constitué d'ordinateurs reliés en réseau à travers Internet, qui coopèrent pour mettre du contenu ou des données à la disposition des utilisateurs.
Cyber-blurring	Méthode consistant à créer une quantité massive de faux documents (courriels, mots de passe, comptes) afin de ralentir le travail des hackers. Cette technique de diver-

	sion est aussi appelée floutage numérique.
Data-URL	Schéma permettant d'introduire directement des données (texte source HTML) dans un hyperlien, comme s'il s'agissait de ressources externes.
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.
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.
Launcher	Programme facilitant l'accès aux applications désirées; lanceur d'applications.
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.
mTAN	Numéro mTAN, acronyme de mobile TransAction Number. Une fois connecté à Internet, l'utilisateur d'un service e-banking reçoit par SMS sur son téléphone mobile un code numérique valable très peu de temps et non réutilisable.
Navigateur	Logiciel utilisé essentiellement pour afficher les différents contenus du Web. Les navigateurs les plus connus sont Internet Explorer, Opera, Firefox et Safari.
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.
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.
Protocole SMB	Server Message Block (SMB) est un protocole permettant le partage de ressources (fichiers, imprimantes, etc.) sur des réseaux locaux.
Proxy	Programme servant d'intermédiaire pour accéder à un autre réseau, en collectant les requêtes et en les transmettant vers l'extérieur à partir d'une même adresse.
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.
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.
Software Defined Radio (SDR)	Radio logicielle; technique qui consiste à remplacer, dans des émetteurs et récepteurs radioélectriques, des dispositifs matériels par des logiciels.
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).
Subscription Bomb	Attaque consistant à souscrire à une multitude de lettres d'information pour bloquer la boîte aux lettres de la victime ou ses dispositifs de communication.
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.

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.
Win32PE	PE (*portable executable*) est un format de fichier binaire développé pour les programmes exécutables. Les systèmes d'exploitation Win32 bits et 64 bits supportent ce format.
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.