Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

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

SÛRETÉ DE L'INFORMATION

SITUATION EN SUISSE ET SUR LE PLAN INTERNATIONAL

Rapport semestriel 2016/II (juillet à décembre)

20 AVRIL 2017

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

1 Aperçu / Sommaire

2 Éditorial

Philippe Vuilleumier, Head of Group Security, veille depuis septembre 2015 à la sécurité logique et physique de Swisscom.

Chère lectrice, cher lecteur,

Un responsable de la sécurité se posait autrefois la question suivante: «Que dois-je faire pour mettre mon organisation à l'abri des cyberattaques?» Aujourd'hui, on a déchanté et on se demande plutôt: «Quand serai-je victime d'une cyberattaque?» En raison de la professionnalisation croissante des agresseurs, des nouvelles possibilités techniques et donc du degré de perfection atteint par de nombreuses attaques, on ferait bien de partir de l'idée que son propre environnement est déjà compromis, ou du moins que cela ne saurait tarder.

C'est une chose d'accepter cette réalité, mais c'en est une autre d'en tirer les bonnes conclusions et de prendre des mesures adéquates. De prime abord, devoir présumer l'existence de vulnérabilités – «assume breach» – semble révolutionnaire à bien des gens, mais que faut-il faire ensuite? Quel doit être le rôle d'une organisation dans son ensemble, et que peut faire aux avant-postes son équipe responsable de la sécurité?

Chez Swisscom, nous avons conclu qu'il fallait veiller à trois points essentiels:

1. Notre sécurité de base doit être préservée! À ce titre, il nous incombe de tenir à jour nos inventaires de l'infrastructure, des données et des collaborateurs, d'effectuer à intervalles rapprochés les mises à jour nécessaires de nos systèmes et applications, de gérer rigoureusement nos risques et de rationaliser toutes nos activités en la matière.

2. Il faut prévoir des solutions de sécurité simples! Et qui soient simples pour l'utilisateur final. En veillant à la simplicité et à la transparence des solutions techniques, la sécurité peut apporter une contribution majeure à l'agilité exigée de l'entreprise.

3. Il faut miser sur la détection et la réaction! La prévention reste naturellement très importante (elle relève de la sécurité de base). Mais comme les cyberattaques évoluent en permanence, elle a forcément ses limites. Pour détecter rapidement les cyberattaques, pour en limiter l'impact et les repousser, il faut des compétences spécifiques, que nous cherchons à améliorer en permanence. Je cite volontiers ici MELANI, qui constitue sur ce terrain un partenaire important et efficace de Swisscom.

Le thème prioritaire du présent rapport est l'Internet des objets. Dans ce contexte et avec les défis qui s'ensuivent, les trois priorités susmentionnées que sont la sécurité de base, la simplicité et la détection sont plus que jamais d'actualité.

Je vous souhaite une agréable lecture.

Philippe Vuilleumier

3 Thème prioritaire: Internet des objets

À l'avenir, tout ce qui peut être relié le sera à Internet. Cette affirmation un peu excessive indique bien dans quelle direction Internet va évoluer ces prochaines années. Au-delà de tous les agréments procurés, de nombreuses discussions sur la sécurité sont également à prévoir. Toujours plus d'objets quotidiens seront reliés à Internet. De premiers fabricants parlent donc déjà de l'Internet of Everything (IoE) où les personnes, les processus, les objets et les données seront tous connectés à un réseau intelligent. Le cas souvent cité du réfrigérateur qui commande automatiquement le lait n'est qu'un exemple parmi beaucoup d'autres. Ces dernières années ont été marquées par un véritable boom dans la gestion des bâtiments et dans la commande d'éclairage.
L'Internet des objets est appelé à se développer par rapport à aujourd'hui. Selon les analystes de Gartner[1], plus de 6 milliards d'objets étaient reliés au réseau en 2016. La barre des 20 milliards devrait être franchie d'ici 2020. Et les possibilités qu'offrent les objets reliés à Internet sont loin d'être épuisées. Ces objets se glisseront toujours plus dans notre quotidien pour l'influencer. Certains développements s'annoncent déjà: même si les «wearables», applications conçues pour être intégrées à un vêtement ou à un accessoire et restituant une foule d'informations n'en sont qu'à leurs débuts, ils vont bien au-delà des moniteurs d'activité physique (fitness tracker) entrés dans l'usage. Dans le secteur médical, il faut s'attendre à l'apparition de nombreuses applications, qui permettront d'établir en permanence de meilleurs diagnostics. On peut ainsi imaginer que le smartphone indique en tout temps l'état de tous les organes vitaux. Les véhicules sans chauffeur constituent un autre créneau important. Les premiers essais ont déjà eu lieu. Pour pouvoir garantir un fonctionnement sûr et fiable, il faudra toutefois installer de nombreux capteurs tant à l'intérieur qu'à l'extérieur des automobiles. Indépendamment de la mise au point de tels véhicules, les routes seront elles aussi équipées de nombreux capteurs, afin de maîtriser le flux croissant du trafic. D'où l'importance de la collecte des données: des capteurs autonomes et fonctionnant en autarcie enverront leurs données par Internet à un serveur, aideront à prendre les bonnes décisions, déclencheront des actions et identifieront de bonne heure les risques, afin de les éviter le cas échéant.

3.1 Définition

La notion d'«Internet des objets» désigne la tendance croissante des objets et appareils présents dans le monde réel à communiquer par Internet. Le terme est apparu à la fin des années 1990, où le pionnier de la technologie Kevin Ashton avait entrevu le potentiel de deux appareils intelligents à échanger des données entre eux.[2] Il n'existe toutefois pas à ce jour de définition uniforme. On peut donc également prendre ce terme dans son sens large, comme synonyme de la connexion entre le monde réel et le monde virtuel.[3] Entre autres

1 http://www.gartner.com/newsroom/id/3598917 (état: le 28 février 2017).
2 http://www.rfidjournal.com/articles/view?4986 (état: le 28 février 2017).
3 http://www.computerwoche.de/a/industrie-4-0-ist-das-internet-der-ingenieure,2538117 (état: le 28 février 2017).

applications concrètes, l'identification d'objets matériels à l'aide de puces RFID, de codes QR ou de codes-barres peut être citée ici à titre d'exemple. Un scanner établit la liaison avec Internet. Un simple objet devient ainsi un objet intelligent, enrichi d'informations et de services. Et quand de nombreux objets intelligents ou capteurs interviennent dans l'industrie, il est souvent question d'industrie 4.0, notion désignant la quatrième révolution industrielle, rendue possible par la numérisation.

3.2 L'Internet des objets, facteur d'insécurité ?

Les risques et les effets secondaires de l'Internet (des objets) nous occuperont toujours plus, au fur et à mesure de l'extension des possibilités proposées. Il faudrait par exemple toujours s'assurer que ce soit le réfrigérateur qui passe la commande de lait, et que le lait ne puisse pas commander de réfrigérateurs. Les questions fondamentales à régler ne concerneront pas seulement la maintenance et les normes de sécurité, mais aussi la protection des données. L'Internet des objets vise à prendre des décisions optimales, automatisées au moyen des capteurs. Des millions de données sont ainsi enregistrées et doivent être globalement protégées. Pour en rester à l'exemple souvent cité du réfrigérateur, les données collectées offrent un aperçu intéressant non seulement de la consommation de lait du ménage, mais de l'usage fait de tout le réfrigérateur. De telles données pourront par exemple servir à des fins de marketing. Dans des cas extrêmes, on pourra déterminer si les habitudes alimentaires d'un ménage sont saines ou non, ce qui pourrait servir d'indicateur aux caisses-maladie en vue du calcul de leurs primes.

Au deuxième semestre 2016, l'Internet des objets a fait les gros titres à cause du réseau de zombies Mirai. De nombreux appareils mal protégés ont été piratés. Le 21 octobre, une cyberattaque menée contre le fournisseur d'infrastructures Dyn a provoqué la panne de nombreux services populaires sur Internet comme Amazon, Spotify et Netflix. Cette attaque a montré pourquoi il faut dûment veiller à la sécurité des objets reliés à Internet. Plusieurs centaines de milliers d'appareils piratés avaient été programmés pour se connecter simultanément aux serveurs de la victime. Avec son débit avoisinant 1,2 térabit par seconde, il s'agit d'une des plus violentes attaques DDoS observées à ce jour.

L'Internet des objets diffère sur des points essentiels de l'informatique conventionnelle: à la différence des ordinateurs, les appareils d'usage courant reliés à Internet ne sont souvent protégés que de manière limitée contre un accès non autorisé, et donc des pirates peuvent les infecter avec des maliciels. D'une part, il est fréquemment possible d'accéder à ces appareils à l'aide de leurs mots de passe standard. En outre, bien souvent, ces mots de passe ne sont pas modifiés après l'installation, pour autant qu'il soit possible d'en changer. D'autre part, la mise à jour des logiciels utilisés s'avère problématique: le processus de mise à jour n'est réglé que dans une petite minorité de cas, et son automatisation est encore plus rare. D'où de nombreux défis, qui vont encore s'exacerber durant les années à venir: car à la différence des appareils informatiques conventionnels, qui ne sont souvent exploités que quelques années, les objets connectés peuvent parfaitement être utilisés une bonne dizaine d'années.

3.3 Conséquences pour l'avenir

Les attaques DDoS lancées depuis des réseaux d'objets connectés ne devraient toutefois pas être à l'avenir le principal risque pour la société. Les manipulations de ce genre de sys-

tèmes sont potentiellement bien plus dangereuses. Dans la branche logistique notamment, toujours plus d'appareils sont reliés à Internet. Or de mauvaises manipulations sont susceptibles de causer d'énormes dégâts. Si par exemple la logistique de distribution de médicaments a été déréglée et livre au mauvais endroit des remèdes indispensables, il peut très vite s'agir d'une question de vie ou de mort. Les escrocs pourraient tenter d'extorquer de l'argent avec de telles attaques. Et des terroristes chercher à effrayer et déstabiliser la société par ce biais.

La vulnérabilité de l'Internet des objets tient surtout à la culture de sécurité des exploitants, qui laisse à désirer. L'expert en sécurité Lucas Lundgren a rappelé, à la dernière conférence RSA de San Francisco, les failles du protocole de communication Message Queue Telemetry Transport (MQTT).[4] Ce dernier est souvent utilisé pour garantir la communication entre objets à l'aide de capteurs. Le problème n'est pas dû au protocole MQTT. Il tient en réalité aux exploitants, qui renoncent à la légère à la protection d'un mot de passe et au chiffrement. Dans le cas des capteurs fonctionnant sur pile, on peut encore expliquer une telle absence par le souci de diminuer la charge du processeur, et donc la charge de courant; or bien souvent, l'ignorance ou la commodité sont seules en cause.[5] Le problème des capteurs non protégés communiquant par le réseau touche notamment les automobiles, les capteurs sismiques, les distributeurs de billets, les appareils de climatisation, les luminaires ainsi que les appareils médicaux.

3.4 Directives et mesures de précaution

Les diverses applications possibles de l'Internet des objets dans chaque branche concernée, ainsi que la croissance fulgurante du nombre d'appareils rendent très difficile l'élaboration de directives. L'organisation Cloud Security Alliance a néanmoins publié en octobre 2016 un rapport de plus de 80 pages sur la question.[6] Ce document offre notamment un aperçu des fonctions de sécurité disponibles dans les différentes plateformes de développement de solutions logicielles. Il renferme également des directives pour le processus de conception et de production, ainsi qu'une liste de contrôle que les ingénieurs consulteront dans le cadre de leurs activités de développement.[7] MELANI a également publié sur son site quelques mesures visant à rendre plus sûr à l'usage l'Internet des objets.[8]

---

4 https://www.rsaconference.com/events/us17/agenda/sessions/6671-lightweight-protocol-serious-equipment-critical (état: le 28 février 2017).

5 https://www.heise.de/newsticker/meldung/MQTT-Protokoll-IoT-Kommunikation-von-Reaktoren-und-Gefaengnissen-oeffentlich-einsehbar-3629650.html (état: le 28 février 2017).

6 https://cloudsecurityalliance.org/download/future-proofing-the-connected-world/ (état: le 28 février 2017).

7 http://www.inside-it.ch/articles/45282 (état: le 28 février 2017).

8 https://www.melani.admin.ch/melani/fr/home/themen/internet_of_things.html (état: le 28 février 2017).

Recommandations:

Tous les appareils reliés à Internet doivent être dûment protégés (mot de passe individuel, accès restreint) et faire l'objet d'actualisations régulières. Il est important de reprendre rapidement les mises à jour disponibles. Or à la différence des ordinateurs de bureau et des smartphones, presque personne ne songe à effectuer, le cas échéant, les mises à jour requises par son interrupteur intelligent ou par son réfrigérateur.

Les objets ou appareils accessibles par Internet avec des données d'accès standard (nom d'utilisateur et mot de passe) présentent un potentiel de risque accru. De tels appareils pouvant être détectés par n'importe qui (notamment grâce à un outil d'exploration des ports (portscan) ou à un moteur de recherche comme Shodan), il s'agit d'une cible facile pour les cyberattaques.

MELANI a publié des informations sur la manière de se protéger face à ce genre de menaces:

Sécurité de l'Internet des objets (Internet of things, IoT)

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

4 Situation nationale

4.1 Espionnage

4.1.1 La Suisse comme cible indirecte possible d'activités d'espionnage

Le 11 août 2016, Anonymous Pologne annonçait avoir piraté les réseaux de l'Agence mondiale antidopage (AMA) et du Tribunal arbitral du sport (TAS). Ce groupe parlait également d'une attaque DDoS menée contre le TAS. Basé à Lausanne, le TAS est une institution internationale proposant un arbitrage ou une médiation dans des cas issus du monde du sport. Des affaires de dopage lui sont régulièrement soumises. Des zones d'ombre persistent quant aux faits exacts et au rôle d'Anonymous Pologne. Il n'en demeure pas moins que l'intérêt pour ce type d'institution fait sens dans le contexte de l'exclusion d'athlètes russes pour cause de dopage, décision politiquement sensible. [9] La Suisse se retrouve en ligne de mire du simple fait qu'elle héberge le TAS sur son territoire; alors même qu'elle ne paraît nullement être ciblée par cette opération, et que les enjeux sous-jacents ne la touchent qu'indirectement. L'incident confirme que la grande densité d'organisations internationales ayant leur siège sur notre sol constitue un facteur de risque sur le terrain des cyber opérations. La Suisse doit en tenir dûment compte en protégeant son territoire par des moyens adéquats.

[9] Voir chapitre 5.1

La Suisse a été impliquée dans un autre cas, soit la publication le 13 août 2016 par un groupe se faisant appeler The Shadow Brokers de listes de domaines et d'adresses IP compromises et potentiellement utilisées lors d'attaques menées par *Equation Group*[10]. Dans ce lot figuraient en effet trois adresses de serveurs basés à l'Université de Genève. Switch, qui offre différents services réseau aux hautes écoles helvétiques, confirme que trois serveurs ont bel et bien été compromis entre 2001 et 2003, en précisant que deux d'entre eux ont été désactivés dès 2009 et que le troisième n'est pas accessible de l'extérieur[11]. Même si l'affaire est déjà ancienne et si les mesures requises ont été prises depuis lors, elle démontre que notre pays n'est pas uniquement une cible attractive, et qu'il peut très bien aussi servir de relais et héberger de l'infrastructure utilisée à des fins d'espionnage. Il arrive que cette infrastructure soit hébergée par des prestataires peu regardants[12], mais elle peut également être administrée par le biais de serveurs légitimes préalablement compromis.

Les rapports précédents ont régulièrement exposé les raisons faisant de la Suisse une cible de choix[13]. Nous avons également rendu compte par le passé de cas concrets où un savoir-faire ou des informations sensibles spécifiques à notre pays étaient ciblés. Le cas le plus emblématique recensé récemment est l'attaque ayant touché l'entreprise d'armement RUAG[14]. Or les deux cas rapportés ci-dessus nous rappellent que notre pays peut également être la victime collatérale d'activités ne ciblant pas nécessairement directement des informations s'y trouvant.

---

10 Voir chapitre 5.1

11 http://www.watson.ch/Digital/NSA/715933955-NSA-hackte-Uni-Genf-und-missbrauchte-drei-Server-f%C3%BCr-Cyberangriffe (état: le 28 février 2017).

12 Ce cas de figure est décrit notamment dans le rapport MELANI 2014/1, au chapitre 3.3 https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2014-1.html (état: le 28 février 2017).

13 Voir en particulier rapport semestriel 2015/2, chapitre 4.1 https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2015-2.html (état: le 28 février 2017).

14 Rapport semestriel 2016/1, chapitre 4.1.1 https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2016-1.html (état: le 28 février 2017).

Conclusions et recommandations:

MELANI joue un rôle actif depuis treize ans dans la protection contre les risques informatiques, en partenariat avec différentes entités publiques et privées. Son site Web propose un formulaire d'annonce permettant de signaler des incidents:

ANNONCER

Formulaire d'annonce MELANI:

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

Le SRC mène avec son programme Prophylax une action de prévention et de sensibilisation dans le domaine de la non-prolifération et de l'espionnage économique. Prophylax entend sensibiliser les entreprises ainsi que les institutions de formation:

DOCU

Programme Prophylax:

http://www.vbs.admin.ch/fr/themes/recherche-renseignements/espionnage-economique.detail.publication.html/vbs-internet/fr/publications/servicederenseignement/SRC-Prophylax.pdf.html

http://www.vbs.admin.ch/fr/themes/recherche-renseignements/espionnage-economique.html

4.2 Fuites d'information

4.2.1 Chantage basé sur de prétendues données de clients

Dans un communiqué du 17 novembre 2016, la banque liechtensteinoise Valartis a annoncé avoir subi une cyberattaque. Des informations concernant des ordres de paiement antérieurs à mai 2013 et essentiellement des clients commerciaux lui avaient été subtilisées. La banque excluait tout risque de manipulation des ordres de paiement au détriment de sa clientèle. La cyberattaque n'aurait pas affecté le cœur de son système. En outre, le pirate n'avait pas pu consulter l'état des comptes ou des données similaires. L'établissement a dûment informé les clients qui auraient pu être victimes de la cyberattaque.

La banque a appris l'incident quand une personne l'a contactée par courriel pour lui signaler avoir découvert une fuite de données. Elle lui proposait encore anonymement ses services pour combler les failles de sécurité, contre le versement d'une rançon. Valartis n'a pas accepté l'offre ou cédé aux revendications. [15]

[15] http://www.valartisbank.li/Download.aspx?mode=download&id=IqzI6qVOde5v%2foNBMJr8xg%3d%3d (état: le 28 février 2017).

Faute de parvenir à ses fins et d'obtenir de l'argent par ce biais, l'escroc a, selon le site d'information spécialisé inside-IT, cherché dans un second temps à contacter directement les clients de la banque par courriel. Il semblait du moins posséder quelques adresses électroniques de clients de Valartis. Dans cette lettre de chantage, il prétendait connaître le solde des comptes et d'autres données encore concernant les clients. Il menaçait de transmettre, faute de paiement, ces informations aux autorités financières et aux médias. Le maître-chanteur réclamait 10 % du solde du compte sous forme de bitcoins.[16]

Mais comme la banque avait prévenu ses clients, MELANI part du principe qu'aucun n'aura été victime de ses manœuvres. Détail piquant: l'agresseur n'aurait eu aucun moyen de vérifier si ses victimes lui versaient 10 % de leur avoir en compte ou moins, puisque selon la banque il ne disposait pas de cette information. L'escroc comptait sans doute ici sur la bonne foi de ses victimes.

Conclusions et recommandations:

En pareil cas, MELANI déconseille expressément d'effectuer tout paiement, qui rendrait la victime dépendante du maître-chanteur. Il est important par ailleurs de communiquer proactivement, afin de couper l'herbe sous les pieds des escrocs.

MELANI a connaissance de plusieurs incidents similaires, survenus durant la période sous revue. Dans la plupart des cas, une «injection SQL» avait donné accès à une base de données mal protégée, pour en dérober le contenu. Les mobiles des agresseurs sont loin d'être homogènes: certains considèrent leurs cyberattaques comme un «modèle d'affaires» et proposent de combler les failles de sécurité contre salaire. Dans d'autres cas, toute l'histoire sert de prétexte pour soutirer un maximum d'argent.

Les pirates cherchent à se différencier dans leur démarche et leurs motivations. Des catégories de chapeaux, faisant référence aux films de western, se sont imposées pour les classer: les chapeaux blancs (white hats) utilisent leurs compétences dans les limites légales. Les chapeaux noirs (black hats) déploient typiquement une grande énergie criminelle. Ils cherchent à s'infiltrer dans le système pris pour cible – parfois dans l'unique but de voir s'ils y parviennent, parfois aussi pour l'endommager ou pour y dérober des données. Entre les deux, les chapeaux gris (grey hats) enfreignent certes les lois, mais ils le font au nom d'un objectif supérieur, par exemple pour contraindre les responsables à prendre plus au sérieux la sécurité et à s'améliorer sur ce plan. Autrement dit, les chapeaux gris ont beau souvent agir de manière illégale, ils respectent généralement plus ou moins l'«éthique du hacker».

4.3 Systèmes de contrôle industriels (SCI)

Le contrôleur central d'une maison signale au propriétaire que ses stores à soleil ont été abaissés. Le propriétaire pourra au passage enclencher la climatisation, afin de trouver à

[16] http://www.inside-it.ch/articles/45798 (état: le 28 février 2017).

son arrivée une température agréable. Bien souvent, le pilotage s'effectue à partir du smartphone. Toujours plus de particuliers font appel à ses commodités et entrent ainsi en contact avec la domotique, variante des systèmes de contrôle industriels.

Or ces prestations que les ménages privés découvrent peu à peu font depuis longtemps partie intégrante de l'équipement standard des grands complexes comme les immeubles de bureaux, les fabriques ou les hôpitaux. En pareil cas, la centralisation des possibilités de contrôle d'un nombre croissant de systèmes et d'appareils s'impose, dans une optique de qualité et d'efficience. Cette centralisation aggrave toutefois l'impact potentiel d'un accès non autorisé et de manipulations du système de contrôle central.

4.3.1 Sensibilisation à la menace encourue par les SCI en réseau

Les systèmes de contrôle industriel (SCI) sont fréquemment reliés à Internet, pour tirer parti des avantages de la télémaintenance. Il est ainsi possible de surveiller l'état des appareils et de leur donner des instructions sans devoir se rendre sur place. Or si la connexion à Internet s'effectue sans mesures de protection suffisantes, des tiers non autorisés risquent de donner des instructions non souhaitées auxdits systèmes. Des moteurs de recherche spécialisés, à l'instar de Shodan[17], permettent même aux néophytes de repérer les systèmes de contrôle librement accessibles. Ce qui est bien sûr contraire à la volonté de l'exploitant.

Chaque fois que MELANI découvre en Suisse des systèmes potentiellement menacés, leurs exploitants sont contactés pour savoir s'ils sont conscients du fait que leur système est accessible à des tiers. Dans tous les cas, il leur est recommandé de sécuriser leurs systèmes de contrôle.

Des chercheurs en sécurité privés ont signalé à MELANI, à la fin de l'année dernière, un système domotique accessible au premier venu. Il était ainsi possible de modifier frauduleusement les conditions climatiques d'un bâtiment.

Fig. 1: Extrait du tableau de commande d'un bâtiment

Par chance, il s'agissait d'un système en phase de test. Le bâtiment en question n'était pas encore habité. À l'issue des tests finaux, le système a été cloisonné et depuis lors, seuls les techniciens chargés de son exploitation et de sa maintenance peuvent y accéder en ligne.

[17] https://www.shodan.io/ (état: le 28 février 2017).

Recommandations:

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

Formulaire d'annonce MELANI:

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

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

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

4.4 Cyberattaques

En Suisse, les particuliers et les entreprises continuent à faire l'objet de cyberattaques en tous genres. Les sites Internet sont souvent pris pour cibles. Les attaques par déni de service distribué (DDoS) et les défigurations de sites sont d'autant plus problématiques pour les entreprises qu'elles ont besoin d'une présence en ligne crédible.

4.4.1 DDoS et extorsion: derniers développements en Suisse

Dans le précédent rapport, il était question d'attaques mêlant tentative d'extorsion et chantage à l'attaque DDoS, de manière totalement opportuniste. La tendance à effrayer sa victime sans même se donner les moyens de mener une cyberattaque s'est confirmée au deuxième semestre. Comme on pouvait s'y attendre, des criminels n'ont pas tardé à exploiter les craintes suscitées par les attaques DDoS géantes impliquant le réseau de zombies MIRAI[18] pour tenter de soutirer des bitcoins à leurs victimes. Un groupe se faisant appeler NewWorldHacker a procédé de la sorte en fin d'année. Pour rappel, il s'agit de l'acteur ayant revendiqué les attaques massives contre le fournisseur DNS Dyn.

Malgré cette tendance, certains autres cas rappellent qu'on ne peut jamais exclure tout risque d'attaque. Le passage à l'acte ne sera pas systématique, visant plutôt à créer un précédent. Un bon exemple vient d'un groupe se faisant appeler DD-crew DDoS. Cet agresseur présente la particularité de cibler un secteur d'activité précis. Une attaque est alors menée contre un des compétiteurs. Les autres entreprises actives sur le même marché sont ensuite contactées séparément. Elles sont priées de verser une somme en bitcoins, pour s'épargner la mésaventure de leur concurrent. Il est intéressant de noter que les sommes demandées

[18] Voir chapitres 3 et 5.4

varient en fonction de la notoriété (calculée sur la base de Google Rank) et de la taille de l'entreprise.

Conclusions :

Il est probable que la combinaison entre chantage et menace d'attaque DDoS perdure. La peur engendrée par les attaques de grande ampleur rendues possibles par MIRAI sera encore exploitée. Par ailleurs, grâce aux différentes offres permettant d'acheter des services d'attaques DDoS (Voir chapitre 6.1), n'importe quel acteur est en mesure de lancer des attaques ponctuelles. Cette situation rend ce champ d'activité criminelle extrêmement mouvant, avec de nombreux acteurs aux modes opératoires proches.

4.5 Social Engineering, phishing

Outre toutes les attaques reposant sur la technique, les attaques exploitant la faiblesse humaine sont particulièrement appréciées et portent leurs fruits.

4.5.1 Tentatives d'escroquerie plus ou moins raffinées

Divers cas d'arnaque au président (CEO fraud) ont été signalés à MELANI au deuxième semestre 2016. Concrètement, 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. Les raisons invoquées varient, mais il s'agit généralement d'une opération présentée comme urgente, extrêmement sensible et confidentielle. Le degré de raffinement est lui aussi variable. Alors que dans certains cas la demande pressante de transfert d'argent est formulée en termes généraux, les malfaiteurs se documentent parfois en détail sur la société prise pour cible, afin d'inventer une histoire plausible et de personnaliser leur arnaque. Le recours à un consultant ou à un cabinet d'avocat factice ou dont l'identité a aussi été usurpée peut intervenir dans le scénario. Il arrive que des sites de banques ou de cabinets d'avocats soient copiés ou imités, afin de donner à la requête une apparence plus sérieuse[19].

Les offices fédéraux n'ont pas été épargnés durant la période sous revue. Divers services financiers de l'administration fédérale ont reçu le même genre d'instructions frauduleuses portant sur des transferts d'argent. Dans un autre cas, le site de l'Autorité fédérale de surveillance des marchés financiers (FINMA) avait même été imité pour endormir la méfiance de la victime.

Les escrocs sont toujours plus astucieux et ne négligent aucun détail, comme le montrent des cas où ils se sont même fait passer au téléphone pour un service fédéral. Ils s'étaient dit que la victime serait plus encline à exécuter l'action attendue d'elle, croyant avoir au bout du fil une autorité officielle. Le plus étonnant est que l'écran de téléphone indiquait bel et bien un numéro de l'administration fédérale, que les escrocs étaient parvenu à falsifier.

[19] Cette thématique a été traitée plus en détail dans le rapport semestriel 1/2016, chapitre 4.5.2

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.

INFO

Thèmes actuels: Ingénierie sociale (social engineering)

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

4.5.2 Phishing

De nombreux courriels de phishing ont également circulé au deuxième semestre 2016. Il s'agit toujours des mêmes types de courriels déjà connus. 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 les services Internet correspondants. Pour paraître plus respectables, de tels courriels usurpent souvent les logos d'entreprises connues ou du service concerné.

Au total, plus de 4500 sites de phishing ont été dénoncés en 2016 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 d'année. Les raisons en sont diverses: d'une part, les pages signalées sont moins nombreuses en période de vacances, d'autre part les agresseurs passent régulièrement d'un pays à l'autre.

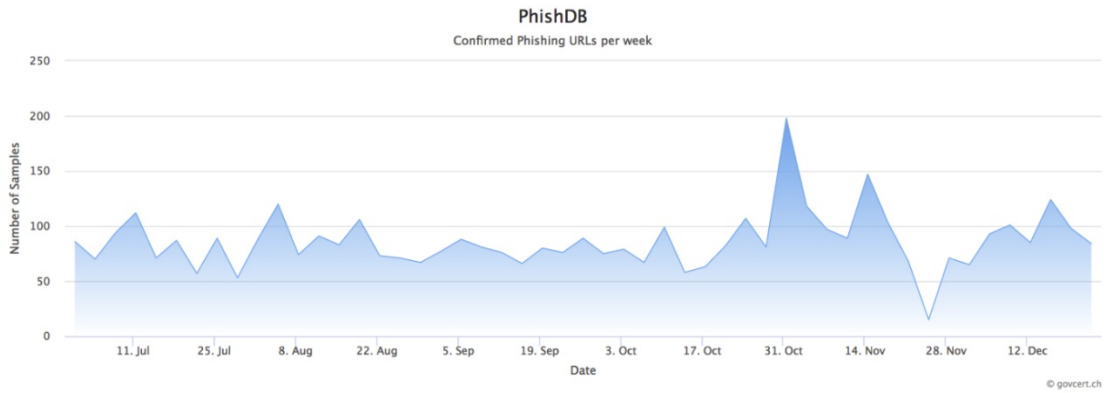

Fig. 2: Sites de phishing annoncés et confirmés par semaine sur le site antiphishing.ch au deuxième semestre 2016

4.5.3 Des pages de phishing qui n'en sont pas

Dans son rapport semestriel 1/2012[20] déjà, MELANI avait insisté sur les précautions que les entreprises devraient prendre en communiquant avec leur clientèle, à l'ère du phishing. À tout moment, des courriels authentiques laissent leurs destinataires perplexes. Durant la période sous revue, les citoyens ont été particulièrement nombreux à signaler de prétendues pages de phishing. Cela tient certainement en partie à la sensibilisation accrue de la population à cette problématique, mais témoigne aussi du fait qu'une partie des entreprises ne se conforment pas aux règles d'usage lors de l'envoi de lettres d'information (voir l'Info-Box ci-dessous).

4.5.3.1 Cas classique: modifications des conditions générales de Paypal

Les modifications de conditions générales communiquées par Paypal, eBay et consorts sont souvent prises à tort pour des pages de phishing et signalées comme telles à MELANI. Même si le message ne contenait pas de lien à une page d'ouverture de session, le simple fait de recevoir à l'improviste un courriel de Paypal a gêné certains utilisateurs. Après tout, Paypal est l'un des services Internet les plus souvent visé par des attaques de phishing, et beaucoup d'utilisateurs ont déjà reçu des courriels de phishing en son nom.

4.5.3.2 Lien caché et lien vers un serveur tiers

Des courriels de sociétés suisses légitimes peuvent parfois également déclencher des annonces pour phishing. Durant la période sous revue, une annonce publicitaire d'une société annonçait à l'utilisateur qu'il pouvait bénéficier d'un crédit. Le lien fourni, dissimulé derrière une image, ne menait cependant pas sur le site de l'entreprise mais sur celui d'une société spécialisée dans le marketing. Ceci a provoqué une méfiance justifiée chez certains utilisateurs. Dans un autre cas, une entreprise a écrit à ses clients pour leur annoncer qu'un montant allait être facturé pour couvrir des frais administratifs, en l'absence de réaction dans un délai donné. Le courriel n'était pas adressé personnellement et un lien caché menait sur un site web où un nom d'utilisateur et mot de passe étaient demandés. Là encore, le procédé a éveillé les soupçons de citoyens attentifs qui se sont ensuite adressés à MELANI. En réalité, le courriel provenait réellement de l'entreprise et le lien menait vers son site web.

[20] MELANI, rapport semestriel 1/2012, chapitre 5.4 https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2012-1.html (état: le 28 février 2017).

Conclusions et recommandations:

«Aucune entreprise sérieuse ne demande par courriel des données d'ouverture de session ou des mots de passe.» Telle est la réponse standard donnée par MELANI aux personnes lui envoyant un courriel dont elles ignorent s'il émane ou non de l'expéditeur indiqué. Cette mise en garde qui paraît simple de prime abord met souvent les entreprises dans l'embarras, à l'ère de la communication électronique avec la clientèle. Comment faut-il s'y prendre pour communiquer avec ses clients sans qu'ils s'imaginent avoir affaire à un courriel frauduleux? Surtout, une communication désinvolte risque de rendre les clients imprudents, le jour où ils recevront un courriel d'arnaque.

Les points suivants devraient être pris en compte par les entreprises, lors de tout envoi de courriels:

- Envoyer autant que possible des courriels au format texte brut, afin que les éventuels hyperliens qu'ils contiennent soient bien visibles et non dissimulés derrière un élément de texte, comme par exemple «Veuillez cliquer ici».
- N'introduire que de rares liens, et encore seulement à son propre domaine. Si possible, utiliser des liens conduisant à des pages sécurisées (https) et en informer le destinataire.
- Ne pas créer d'hyperlien vers des pages Web exigeant le nom d'utilisateur et le mot de passe, ou d'autres données encore.
- Veiller à la régularité des envois de lettres d'information.
- Signaler la lettre d'information sur la page d'accueil du site Web ou y placer directement l'hyperlien correspondant, pour que le destinataire ait la possibilité de saisir à la main l'adresse principale, puis d'y cliquer sur la lettre d'information.
- Appeler les clients par leur prénom et nom, si ces informations sont connues.

Dans le secteur financier en particulier, les informations importantes se rapportant aux comptes devraient toujours être envoyées par la poste.

4.5.4 Essor des campagnes de sensibilisation

Il est crucial de sensibiliser le personnel aux enjeux de cybersécurité au travail. À cet effet, toujours plus d'entreprises mènent des campagnes de sensibilisation à la problématique du phishing. Pendant une telle campagne, des courriels de phishing préparés sont expédiés au personnel. Une analyse révèle ensuite qui a mordu à l'hameçon. L'entreprise fait ainsi d'une pierre deux coups: en plus de sensibiliser ses collaborateurs, elle peut déterminer leur degré de prise de conscience, afin d'adopter des mesures adéquates. La page de phishing sera enregistrée sur un domaine spécialement créé à cet effet au préalable. Il est dans la nature des choses que des employés consciencieux signaleront ce genre de courriels aux services de lutte anti-phishing, à l'instar du portail «antiphishing.ch» exploité par MELANI. Or de telles démarches aboutissent à diverses mesures, comme le retrait des sites Web suspects (take down procedure) et leur annonce à des logiciels de filtrage. Ces réactions faussent logiquement le résultat du test. Car une fois la page Web bloquée ou effacée, il n'est plus possible d'évaluer le niveau de sensibilisation du personnel.

Recommandations:

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

4.6 Logiciels criminels (crimeware)

L'expression crimeware désigne tout logiciel malveillant spécialement conçu par des fraudeurs pour automatiser la cybercriminalité économique. Au deuxième semestre 2016, la plupart des infections restaient dues 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. Le maliciel Necurs, deuxième au palmarès des infections, s'est spécialisé dans la diffusion aussi bien du rançongiciel Locky, que du cheval de Troie bancaire Dridex. 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, se hisse à la troisième marche du podium.

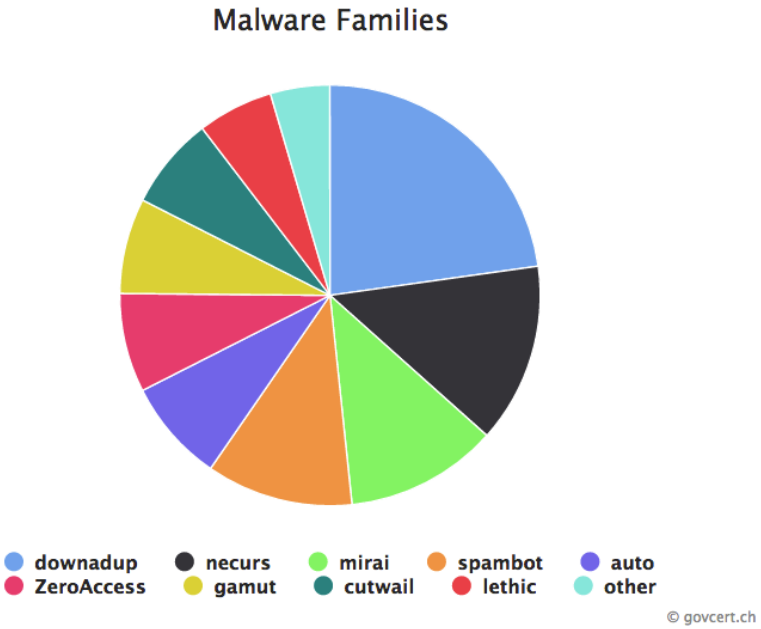

Fig. 3: Répartition des maliciels en Suisse, selon les informations en possession de MELANI. Date de référence: le 31 décembre 2016. Des données actuelles sont publiées sous: http://www.govcert.admin.ch/statistics/dronemap/

4.6.1 Chevaux de Troie bancaires – accent sur les entreprises

Il n'y a pas eu de changement majeur au dernier semestre parmi les chevaux de Troie bancaires. Ainsi, les familles de virus Retefe et Gozi continuent de sévir en Suisse. Alors que Gozi se propage aussi à travers des pages Web infectées, Retefe se répand à l'aide de courriels renfermant de fausses factures d'entreprises existantes plus ou moins connues. Le document Word annexé renferme un JavaScript ou un fichier exécutable, qui modifient les paramètres des navigateurs Internet Explorer ou Firefox pour y installer un serveur proxy appartenant aux pirates. Ils pourront ensuite, s'ils le souhaitent, rediriger n'importe quelle requête de site vers un serveur de leur choix. Retefe parvient encore à infecter les téléphones mobiles et à transmettre aux escrocs le numéro de transaction (mTAN) envoyé. Le prestataire de sécurité Trendmicro[21] a en outre constaté que les escrocs ont affiné leur maliciel conçu pour Android, qui intercepte le mot de passe unique envoyé par SMS. Ils ont conçu un maliciel indétectable aux analyses, apte à contrôler le routage et pourvu d'une fonction d'accès à distance. Il invite par ailleurs les utilisateurs à conférer à l'application divers droits, à l'instar de l'accessibilité (accessibility service), qui lui permet de simuler les interactions de l'utilisateur. Dridex est diffusé par courriel avec de fausses factures. Alors que jusqu'en juin 2016, Dridex ne s'en prenait – en Suisse du moins – qu'à la clientèle privée de l'e-banking, les escrocs ont changé de méthode en juillet 2016 pour s'attaquer aussi aux logiciels de paiement hors ligne. Beaucoup d'entreprises optent pour une telle solution afin de transmettre de grandes quantités de paiements par Internet à une ou plusieurs banques. Si les pirates découvrent, sur un système qu'ils ont préalablement infecté, la présence d'un tel logiciel de paiement, ils y chargent encore le maliciel Carbanak, spécialisé dans ce genre d'opérations. La fig. 5 représente ce mode d'infection sous forme de schéma.[22]

---

21 http://blog.trendmicro.com/trendlabs-security-intelligence/new-smssecurity-variant-roots-phones-abuses-accessibility-features-teamviewer/ (état: le 28 février 2017).

22 Le maliciel est revenu à la charge à la fin février 2017, lors d'une grande vague de pourriels: de fausses factures Swisscom avaient pour rôle d'amener les destinataires à installer le cheval de Troie. https://www.govcert.admin.ch/blog/28/the-rise-of-dridex-and-the-role-of-esps (état: le 28 février 2017).

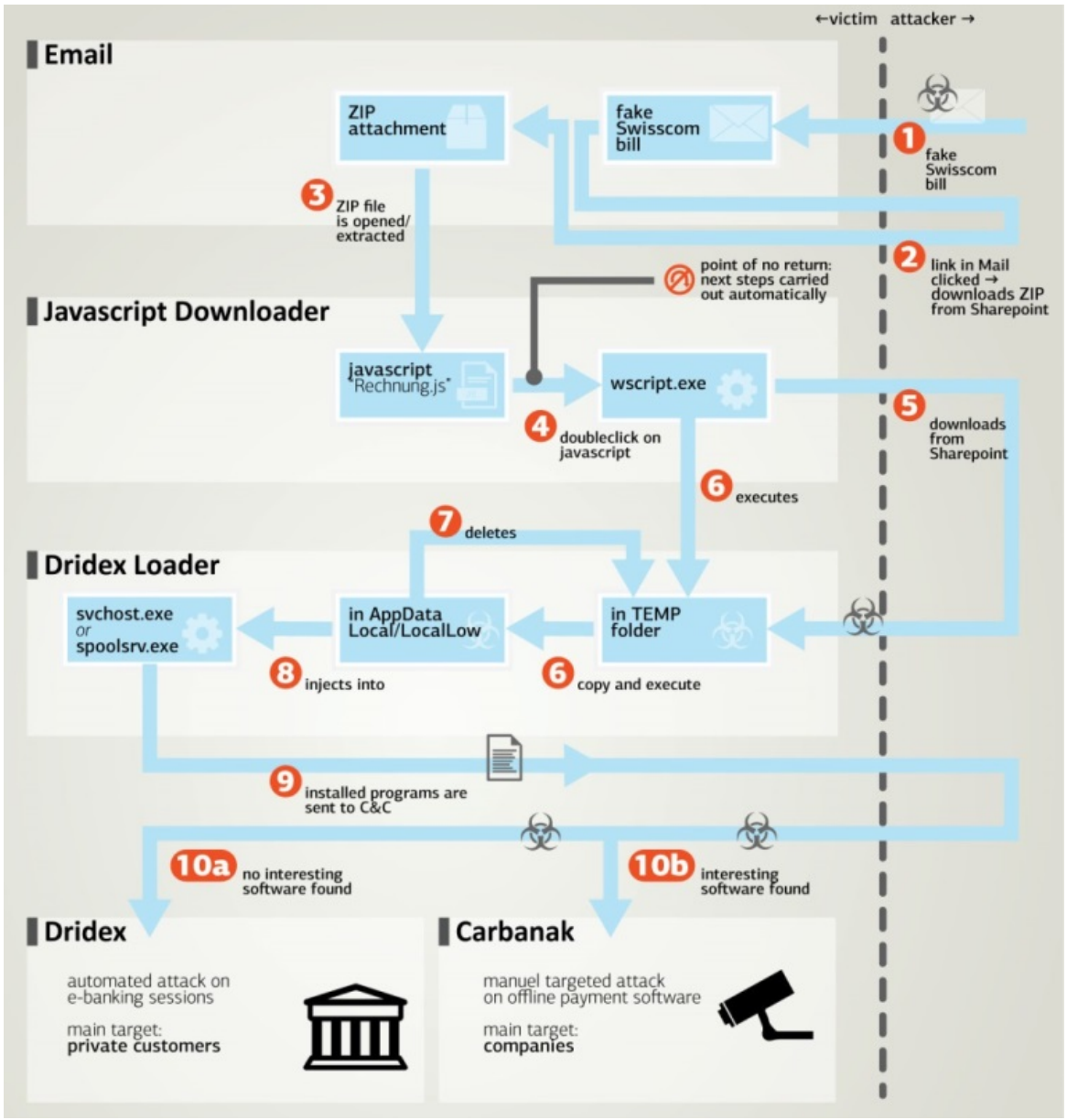

Fig. 4: Schéma du mode d'infection à l'œuvre pendant la vague de pourriels de février 2017 reposant sur de fausses factures Swisscom.

Recommandations:

Il convient de respecter les principes suivants avec les ordinateurs utilisés pour le trafic des paiements:

- Utilisez pour votre logiciel de paiement hors ligne et pour l'e-banking un ordinateur réservé à cette activité, qui ne sera pas utilisé pour naviguer sur Internet ou pour recevoir des courriels.
- Pour la validation des paiements, utilisez une signature collective à travers un deuxième canal (par ex. e-banking). Votre banque vous renseignera sur les possibilités existantes.
- Si vous utilisez un jeton d'identification physique (hardware token) tel que Smart Card ou USB Dongle, retirez-le après utilisation du logiciel de paiement.
- N'enregistrez pas vos données d'accès (numéro de contrat, mot de passe, etc.) pour l'e-banking ou pour le logiciel de paiement sur l'ordinateur ou dans le logiciel.
- Informez-vous des possibilités supplémentaires de sécurité auprès du fournisseur du logiciel de paiement, et activez les mises à jour automatiques.
- Signalez immédiatement les paiements suspects à votre banque.
- Pour prévenir dans votre entreprise une infection par Dridex ou par un autre logiciel malveillant, MELANI recommande par ailleurs les mesures suivantes:
  - Veillez à bloquer ou filtrer la réception de courriels contenant des fichiers potentiellement dangereux sur votre passerelle de messagerie ou sur votre filtre antispams. Une lettre d'information de MELANI indique une liste d'extensions de fichiers attachés qui pourraient être dangereuses: https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/offline-payment-software.html
  - Veillez à ce que ces fichiers soient également bloqués lorsqu'ils sont envoyés dans un fichier d'archive tel qu'un fichier ZIP ou RAR ou dans un fichier d'archive protégé (par ex. un fichier ZIP protégé par un mot de passe).
  - Par ailleurs, il est recommandé de bloquer tous les fichiers joints contenant des macros (par ex. fichiers Word, Excel ou PowerPoint munis de macros), s'ils ne sont pas absolument nécessaires. Le cas échéant, l'envoi et la réception de ce genre d'annexes seront limités à un cercle restreint d'expéditeurs et de destinataires.

4.6.2 Les chevaux de Troie bancaires exploitent la négligence des utilisateurs

Même l'authentification à deux facteurs moderne, comme CrontoSign, PhotoTAN ou SecureSign, n'est pas à l'abri des tentatives d'escroquerie, en dépit de la réputation de grande sécurité dont jouissent ces diverses méthodes. Dans plusieurs cas signalés à MELANI à la fin novembre 2016, des individus étaient parvenus à manipuler ces systèmes pour opérer des paiements frauduleux. Concrètement, la clientèle e-banking était amenée par des mé-

thodes d'ingénierie sociale à valider, par l'intermédiaire de PhotoTAN, CrontoSign ou SecureSign, des virements destinés en réalité aux escrocs.

Fig. 5: Mosaïque (à gauche) et code QR (à droite) servant à ouvrir une session d'e-banking et à valider les paiements.

À l'ouverture d'une session (login) ou lorsqu'il faut valider un paiement, le client voit s'afficher dans son portail e-banking un code QR ou une mosaïque (voir fig. 6). Il peut les scanner au moyen d'une application installée sur son smartphone ou sur un appareil indépendant. Puis selon le produit, il lui faut directement confirmer la connexion ou la validation du paiement dans une application, ou alors celle-ci génère un code que le client doit saisir dans le portail d'e-banking. Or bien des clients sont manipulés et amenés à valider des paiements qu'ils auraient pu reconnaître comme frauduleux, par exemple parce que le compte destinataire affiché dans l'application était manifestement erroné, ou du fait que les détails d'un paiement sont apparus dès la procédure de connexion.

Les fabricants ont réagi en améliorant la visibilité, pour que l'utilisateur puisse encore mieux distinguer entre la procédure de connexion et la validation d'un paiement.

Fig. 6: Nouvel affichage amélioré du générateur de mot de passe unique, pour les autorisations de paiement.

Recommandations:

MELANI recommande les mesures suivantes, lors de l'utilisation de méthodes d'authentification pour smartphone comme par exemple mTAN, PhotoTAN, CrontoSign ou encore SecureSign:

- Lors de la procédure de connexion au compte (login), assurez-vous que vous soyez uniquement en train de vous connecter au compte via l'appareil mobile (smartphone ou autre appareil dédié à cette activité), et non pas en train de valider un paiement.
- Si vous validez un paiement, veillez à bien lire tout le texte s'affichant sur l'appareil mobile et vérifiez encore le montant et le destinataire (nom, IBAN).
- Informez-vous des autres mesures de sécurité proposées par votre prestataire financier (par ex. exclusion par défaut des virements dans des pays avec lesquels

4.6.3 Rançongiciels

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

En Suisse, les types de rançongiciels les plus répandus sont Cerber, Locky et Mischa/Petya. Cerber s'est notamment propagé par courriel au moyen d'une promesse de gain. Les courriels renfermant des postulations alibi et adressés de manière ciblée aux services du personnel demeurent un vecteur d'infection problématique. Dans les services du personnel comme dans les services de presse, le personnel doit régulièrement ouvrir des documents de source inconnue. Il est recommandé ici de prévoir des appareils non reliés au réseau interne pour imprimer les postulations. Mais les escrocs recourent aussi à de fausses factures ou à de fausses convocations devant le tribunal. De manière générale, ils exploitent chez leurs victimes des traits de caractère comme la curiosité, la peur, leur font miroiter un gain ou promettent un grand bonheur.

Recommandations:

- Veillez à effectuer des sauvegardes régulières de vos données importantes (backup) sur un support externe (par ex. un disque dur externe). Après la sauvegarde, veillez à déconnecter de l'ordinateur le support contenant les données sauvegardées.
- Maintenez systématiquement à jour les logiciels ou plugiciels installés (par ex. antivirus, navigateur).
- N'ouvrez jamais les annexes suspectes de messages, même quand elles semblent provenir d'expéditeurs dignes de confiance. En cas de doute, demandez à l'expéditeur (connu de vous) ce que renferme au juste la pièce jointe à l'envoi reçu.
- Prévoyez, pour les fonctions impliquant de recevoir et d'ouvrir des annexes d'expéditeurs inconnus, un ordinateur spécifique et dûment isolé du reste du réseau de l'entreprise, de façon à éviter toute propagation d'une éventuelle infection.

INFO

Mesures à prendre contre les rançongiciels:

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

Dossier du BSI Ransomware: Bedrohungslage, Prävention & Reaktion:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.html

Projet No More Ransom:

https://www.nomoreransom.org/decryption-tools.html

Règles de comportement ➔ Courrier électronique:

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

4.7 Mesures préventives

4.7.1 Domaines bloqués préventivement suite à l'analyse du maliciel Tofsee

De nombreux logiciels malveillants intègrent un algorithme de génération de noms de domaine (domain generation algorithm, DGA). Grâce à cette fonction, les ordinateurs infectés (bots) sont à même de communiquer avec l'infrastructure de commande et de contrôle (C&C). L'avantage de générer dynamiquement des noms de domaines différents à intervalles réguliers, plutôt que de les définir en avance une fois pour toutes, étant que les éventuelles mesures contre la communication des bots vers l'infrastructure C&C sont beaucoup plus difficiles à mettre en place. Il faut en effet comprendre l'algorithme utilisé pour prédire les noms de domaine qui seront utilisés par les criminels après avoir été préalablement enregistrés. C'est ce type de travail auquel l'équipe de MELANI s'est attelée à la fin de décembre 2016. Une analyse de Tofsee, maliciel dont la finalité principale est l'envoi de pourriels à large échelle à travers des ordinateurs compromis, a permis de comprendre le fonctionnement du DGA. Entre autres particularités, près de la moitié des noms de domaines générés utilisaient le domaine de premier niveau national (country code top-level domain,

ccTLD) .ch. Suite à cela, MELANI a travaillé avec le registre du ccTLD .ch switch et avec Registrar of Last Resort, fondation active dans la lutte contre les noms de domaine malicieux. Cette collaboration a permis d'empêcher l'enregistrement des noms de domaine en .ch pouvant être produits par ce DGA spécifique (plus de 500), et ce pour une période de douze mois.

4.8 Autres thèmes

4.8.1 Vote électronique: code source publié sur le site Github

En décembre, le canton de Genève a publié une partie du code source de son système de vote électronique sur le site Github. Cette initiative s'inscrit dans une volonté de transparence, mais pourrait également permettre de bénéficier d'éventuelles contributions extérieures, à des fins d'amélioration du dispositif. Le système genevois est non seulement utilisé à Genève, mais également dans d'autres cantons en ayant fait l'acquisition.

4.8.2 Switch reste le registraire gérant les noms de domaine «.ch»

Au début de 2016, l'Office fédéral de la communication (OFCOM) a remis au concours la gestion des noms de domaine .ch.[23] La fondation SWITCH a obtenu le mandat, car son offre est celle qui a obtenu le plus grand nombre de points.[24] Elle s'est notamment distinguée dans le domaine important de la lutte contre la cybercriminalité. SWITCH exerce déjà aujourd'hui la fonction de registre du domaine .ch. Elle exploitera pendant au moins cinq années supplémentaires la banque de données nationale des noms de domaine .ch et assurera la liaison électronique avec le système de noms de domaine (DNS) mondial.

Le Conseil fédéral a rangé le domaine de premier niveau suisse parmi les infrastructures d'importance vitale. À ce titre, il nécessite une protection spéciale, car une panne paralyserait des pans entiers de la vie publique en Suisse. MELANI collabore étroitement avec le registre du domaine .ch, afin de garantir la sécurité et la disponibilité des noms de domaine suisses.

[23] https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-61133.html (état: le 28 février 2017).

[24] https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-63597.html; https://www.switch.ch/fr/news/SWITCH-wins-tender/ (état: le 28 février 2017).

5 Situation internationale

5.1 Espionnage

5.1.1 Attaque contre le Comité national démocrate (CND): prise de position officielle

Il a déjà été question dans le précédent rapport semestriel MELANI[25] de la cyberattaque ayant visé le Comité national démocrate (CND), attribuée dans un rapport de l'entreprise de sécurité Crowdstrike à Cozy Bear et Fancy Bear[26]. Durant la deuxième moitié de l'année, de nouvelles informations vraisemblablement issues de la même campagne ont été dévoilées sur les plateformes wikileaks et DCLeaks. Dont notamment près de 58 000 messages qui seraient issus du compte privé compromis de John Podesta, responsable de la campagne d'Hillary Clinton.

Le 7 octobre 2016, dans une prise de position commune, le département de la Sécurité intérieure (Department Of Homeland Security) et le bureau du directeur du renseignement national (Office of the Director of National Intelligence) accusent le gouvernement russe d'avoir cherché à perturber les élections à la présidence, à travers une série d'attaques visant les comptes de messagerie électronique de personnalités et d'institutions politiques[27]. Un rapport d'investigation publié le 29 décembre 2016 montre du doigt Cozy Bear et Fancy Bear[28]. Des sanctions contre des entités ou des ressortissants russes ont été annoncées dans la foulée.

Le caractère inédit de cette affaire tient sans doute à la précision avec laquelle les autorités russes au plus haut niveau sont désignées par un autre État comme instigatrices d'une cyberattaque. La cible désignée au cours de l'opération, à savoir une élection présidentielle déjà fortement conflictuelle, a amplifié encore la résonance du cas[29].

---

[25] Rapport semestriel 2016/1, chapitre 5.1.1 https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2016-1.html (état: le 28 février 2017).

[26] https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/ (état: le 28 février 2017).

[27] https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national (état: le 28 février 2017).

[28] https://www.us-cert.gov/security-publications/GRIZZLY-STEPPE-Russian-Malicious-Cyber-Activity (état: le 28 février 2017).

[29] Le chapitre 5.1 du rapport semestriel 2016/1 de MELANI est revenu plus en détail sur la thématique des méthodes d'influence, à la lumière des dernières élections présidentielles américaines.

5.1.2 APT 28 évoqué en lien avec de nombreux événements

Le groupe connu sous les noms de Sofacy, Fancy Bear, Pawn Storm ou encore APT 28[30] a été désigné comme probable responsable de nombreuses autres attaques survenues durant la période sous revue.

Le 11 août 2016, Anonymous Pologne annonce avoir piraté l'Agence mondiale antidopage (AMA) et le Tribunal arbitral du sport (TAS[31]). L'identité exacte de ce groupe n'est pas claire, ni d'ailleurs son rôle exact. Le 19 août, l'entreprise Threat Connect publie une analyse de l'opération, et fait un lien avec Fancy Bear[32]. Elle s'appuie en particulier sur la procédure d'enregistrement des noms de domaines imitant ceux de ces deux entités.

Dans le cas ayant touché l'AMA, des e-mails de spear phishing ont été observés. Ces derniers avaient pour but de rediriger l'utilisateur vers ces sites contrefaits. Les attaquants cherchaient à obtenir des identifiants leur donnant accès à «adams» (Anti-Doping Administration & Management System), système de saisie et de gestion des données liées aux contrôles antidopage des athlètes. L'attaque a été confirmée par l'agence. Elle a en particulier permis de compromettre le compte de Yuliya Stepanova, coureuse de demi-fond russe. Les révélations de cette lanceuse d'alerte avaient abouti à des sanctions contre des athlètes russes. Par la suite, en septembre, des données concernant de nombreux athlètes à travers le monde seront publiées par un groupe se faisant lui-même appeler Fancy Bears. Précisons encore que l'AMA a par la suite évoqué une possible falsification de certaines données publiées.

Le 20 septembre, la Süddeutsche Zeitung et les radios publiques allemandes NDR et WDR rapportent que des politiciens allemands ont reçu en août des courriels de spear phishing[33]. Ces derniers prétendaient provenir de services de l'OTAN. Comme lors des attaques ayant touché le Bundestag en 2015, le quotidien munichois cite des sources internes au gouvernement qui attribuent ces activités à la campagne d'espionnage Sofacy. Le 24 septembre, de nouvelles révélations précisent que l'attaque aurait également touché WDR[34].

En décembre, de nouvelles publications montrent du doigt ce même acteur. C'est tout d'abord le journal Le Monde qui révèle que l'OSCE aurait été attaquée, ce que confirme l'organisation[35]. A la fin du même mois, un rapport de l'entreprise crowdstrike fait passer les opérations menées par Sofacy dans une toute autre dimension[36]. En analysant une applica-

---

30 Ces différents noms sont ceux utilisés par les entreprises ou autorités ayant investigué ces cyberattaques.

31 Cette institution est basée à Lausanne. Ce cas est repris dans la partie Suisse du présent rapport.

32 https://www.threatconnect.com/blog/fancy-bear-anti-doping-agency-phishing/ (état: le 28 février 2017).

33 http://www.sueddeutsche.de/politik/bundesregierung-ist-alarmiert-hackerangriff-aufdeutsche-parteien-1.3170347 (état: le 28 février 2017).

34 http://www.spiegel.de/politik/deutschland/cyberattacke-russische-hacker-attackieren-wdr-journalisten-a-1113780.html (état: le 28 février 2017).

35 http://www.lemonde.fr/international/article/2016/12/28/l-osce-victime-d-une-attaque-informatique_5054744_3210.html (état: le 28 février 2017).

36 https://www.crowdstrike.com/blog/danger-close-fancy-bear-tracking-ukrainian-field-artillery-units/ (état: le 28 février 2017).

tion Android développée par un officier ukrainien et destinée aux artilleurs ukrainiens[37], crowdstrike y découvre la trace de x-Agent, maliciel exclusivement utilisé par Fancy Bear (alias Sofacy). Cette compromission aurait par exemple permis de localiser plus facilement, et potentiellement de détruire, les pièces de l'artillerie ukrainienne.

5.1.3 «Winnti» va se propager – du pillage des serveurs de jeu en ligne à l'espionnage industriel raffiné des aciéries

Au début de décembre 2016, le géant industriel allemand Thyssenkrupp a signalé à la Wirtschaftswoche[38] avoir été victime d'une attaque de cyberespionnage. Le groupe connu sous le pseudonyme de Winnti était parvenu à s'introduire dans ses réseaux en début d'année. Une fois le maliciel repéré par l'équipe de sécurité interne, il aura fallu six mois d'efforts pour en débarrasser le système. Les pirates étaient toutefois parvenus à espionner certains fichiers de données.

Outre les sites de la division Industrial Solutions basés en Europe, en Inde, en Argentine et aux États-Unis, les cibles comprenaient l'activité sidérurgique, avec les hauts fourneaux de Hohenlimburg. Il n'y a heureusement eu aucun dégât physique, les agresseurs s'en étant manifestement tenus à leurs activités d'espionnage.

L'Office fédéral allemand de la sécurité des technologies de l'information (BSI) a confirmé l'existence d'autres cas liés à Winnti. Le groupe a pour particularité d'introduire des accès à distance bien dissimulés dans les environnements système de tiers. Winnti s'est fait connaître en 2009, en pillant des serveurs de jeu en ligne pour revendre au marché au noir l'argent virtuel détourné. Son champ d'activité s'est apparemment étendu dès 2015 à l'espionnage des entreprises.

5.1.4 Netbotz: des caméras de surveillance bien indiscrètes

Les autorités et les grandes entreprises font fréquemment appel, pour leurs secteurs sensibles, à des techniques sophistiquées comme les caméras de vidéosurveillance ou les systèmes de surveillance des serveurs du fabricant américain Netbotz. Or selon le magazine politique télévisé allemand Fakt diffusé sur ARD, ces appareils disposent d'accès secrets, aménagés pour les services de renseignement américains.[39] Fakt se fonde pour le dire sur un rapport gardé secret par le Service fédéral de renseignement allemand (BND). On y apprend que depuis 2004, le BND tenait d'une source fiable que les produits Netbotz peuvent comporter une porte dérobée. Des tests techniques avaient apparemment confirmé que le système Netbotz cherchait à entrer secrètement en contact avec le serveur du Ministère américain de la défense. Netbotz avait visiblement démarché, avec des offres à prix cassés, le Ministère allemand des affaires étrangères ainsi que des clients potentiels actifs dans les segments des hautes technologies et de l'industrie d'armement, pour leur vendre ses systèmes. Le magazine de recherche reprochait surtout au BND de n'avoir informé de ses dé-

[37] Cette application, distribuée dans des forums fréquentés par les militaires, visait à accroître l'efficacité lors de l'utilisation d'un obusier (D-30 Howitzer).

[38] http://www.wiwo.de/unternehmen/industrie/spionageangriff-auf-thyssenkrupp-grossalarm-haette-die-risiken-erhoeht/14948264.html (état: le 28 février 2017).

[39] http://www.mdr.de/fakt/industriespionage-100.html (état: le 28 février 2017).

couvertes sur cet accès à distance ni l'Office fédéral de protection de la constitution (BfV), ni les entreprises prises pour cibles. Netbotz fait aujourd'hui partie de l'entreprise française Schneider Electric, qui fabrique une large gamme de produits et solutions d'automatisation et de contrôle industriel.

5.1.5 Autres campagnes ayant fait la une de l'actualité

Même si aucune campagne n'a fait autant de vagues que celle de Sofacy, de nombreuses autres révélations ont mis en lumière au deuxième semestre 2016 les pratiques de cyberespionnage sévissant partout dans le monde. Comme souvent, ces opérations ont été rendues publiques par des entreprises de sécurité, suite à des investigations menées avec des clients touchés. Etant donné leur grand nombre, il n'est pas possible ici de nommer l'ensemble des campagnes. On citera notamment la campagne d'espionnage The Dropping Elephant[40], acteur relativement peu sophistiqué qui pourrait avoir son origine en Inde selon Kaspersky, et On the StrongPity[41], qui cible particulièrement les systèmes de chiffrement. Symantec a par ailleurs rapporté les activités d'un groupe baptisé Strider[42], menant des attaques très perfectionnées contre un nombre limité de cibles (la même opération étant nommée ProjectSauron[43] par Kaspersky). Enfin, une entreprise israélienne (NSO Group) a été désignée responsable de l'exploitation, à des fins de surveillance, de failles sur iPhone corrigées entre-temps par Apple[44].

Autre événement marquant en matière d'espionnage, un collectif se faisant appeler The Shadow Brokers a publié le 13 août 2016 une série d'outils et de maliciels qu'il affirmait être issus de l'arsenal d'Equation Group. Pour rappel, Equation Group est un groupe menant des activités de cyberespionnage sophistiquées, que l'on suppose être lié à la NSA. The Shadow Brokers a souligné n'avoir publié qu'une partie de ce qu'il avait à disposition et envisager de mettre le reste aux enchères. De nombreux experts ont par la suite attesté l'authenticité des fichiers. Le 31 octobre 2016, le groupe a encore publié une nouvelle archive, contenant des noms de domaines et des adresses IP annoncés comme compromis dans le but de lancer des attaques[45]. L'identité de The Shadow Brokers et l'origine de ses informations font l'objet de nombreuses spéculations, sans qu'aucune piste n'ait pu être formellement prouvée.

---

40 https://securelist.com/blog/research/75328/the-dropping-elephant-actor (état: le 28 février 2017).

41 https://securelist.com/blog/research/76147/on-the-strongpity-waterhole-attacks-targeting-italian-and-belgian-encryption-users (état: le 28 février 2017).

42 http://www.symantec.com/connect/blogs/strider-cyberespionage-group-turns-eye-sauron-targets (état: le 28 février 2017).

43 https://securelist.com/analysis/publications/75533/faq-the-projectsauron-apt/ (état: le 28 février 2017).

44 https://motherboard.vice.com/en_us/article/nso-group-new-big-player-in-government-spyware?trk_source=recommended (état: le 28 février 2017).

45 Pour les implications suisses de cette révélation, voir chapitre 4.

L'attribution d'une attaque sophistiquée (de type APT) se base souvent sur des éléments de nature technique (typiquement: infrastructure utilisée), ou encore sur des modes opératoires spécifiques. Le niveau de confiance que l'on peut accorder à ces attributions varie selon les cas. Il est en revanche souvent nécessaire de compléter l'appréciation en y intégrant des considérations de nature politique et stratégique. En effet, les cibles des attaques ne sont pas choisies au hasard, mais selon un agenda précis. Il convient donc de se poser la question suivante: qui peut avoir intérêt à attaquer l'organisation touchée? S'il s'avère possible de répondre à la question non pas pour un cas isolé mais pour toute une constellation de cas, le processus d'attribution en sortira renforcé.

5.2 Fuites d'information

Les données constituent la matière première d'une économie et d'une société numériques. Presque chaque entreprise gère une base de données regorgeant de données personnelles (de clients), d'où la nécessité de prendre en compte de manière appropriée les questions de sécurité. Des fuites d'information, autrement dit des cas de vol de données, font néanmoins régulièrement les gros titres.

5.2.1 Yahoo data breach, spectaculaire vol de données

À la mi-décembre 2016, Yahoo a signalé une fuite de données d'une ampleur à peine imaginable. Lors d'un incident remontant à 2013, des inconnus se seraient emparés de plus d'un milliard d'enregistrements. Par chance, les données des cartes de crédit n'étaient pas stockées à cet endroit. Pourtant, même les données personnelles (nom, date de naissance, numéro de téléphone, adresse électronique) sont recherchées dans les milieux criminels, car elles servent de point de départ à de nouvelles attaques d'ingénierie sociale. Il n'est donc guère étonnant que les pirates parviennent toujours plus souvent à associer le nom de leurs destinataires à leur adresse électronique, et par là à envoyer des messages personnalisés. En septembre 2016 déjà, Yahoo avait signalé une fuite de données provenant d'un incident remontant à 2014. 500 millions de comptes étaient concernés.

5.2.2 Vol de données par des initiés

Sage Group est l'un des principaux éditeurs de logiciels de gestion et de logiciels financiers pour PME. La cyberattaque à ses dépens, probablement survenue au début d'août, porterait sur les données d'au plus 300 entreprises utilisant les logiciels financiers de Sage. Cette société enregistre diverses données de ses clients – nom, adresse, date de naissance, numéro de sécurité sociale, coordonnées bancaires et autres données financières. Comme l'intrusion faisait suite à une connexion régulière, les experts ont dès le départ cru à un délit d'initié, hypothèse s'étant confirmée par la suite. L'incident rappelle une fois de plus à tous les responsables de la sécurité que tout en se protégeant des attaques de l'extérieur, ils ne doivent pas non plus négliger les menaces internes.

5.2.3 Adultfriendfinder à nouveau visé

Le portail de rencontres Adultfriendfinder a de nouveau été victime d'une intrusion. En novembre 2016, 412 millions de données personnelles lui ont été dérobées. En 2015 déjà, le

même portail avait fait les gros titres après un incident portant sur 3,5 millions de données. Les données des portails pour adultes constituent une cible lucrative pour les escrocs. Selon le portail LeakedSource, les données pillées comprenaient les adresses électroniques et les mots de passe, ceux-ci n'étant même pas protégés parfois, les noms d'utilisateurs, les adresses IP et des informations sur le navigateur.[46] LeakedSource a reproché à ce prestataire de ne pas avoir correctement chiffré les données et d'avoir enregistré en texte clair les mots de passe, ou du moins de ne les avoir protégés qu'avec la fonction de hachage surannée SHA 1.

[46] http://www.leakedsource.com/blog/friendfinder (état: le 28 février 2017).

Recommandations:

Un coup d'œil aux adresses électroniques mises en circulation lors du piratage de ce genre de bases de données en dit long: beaucoup d'adresses professionnelles y apparaissent, alors même que le service Internet en question n'a rien à voir avec l'activité de ces entreprises. La raison tient à ce que les entreprises tolèrent souvent un usage privé de leur infrastructure, de leur accès à Internet notamment. Elles feraient toutefois bien de clairement préciser les modalités de l'utilisation à des fins privées de leur messagerie électronique, car la correspondance privée échangée au travail comporte des risques informatiques pour l'entreprise. Les internautes devraient ainsi renoncer à ouvrir toute annexe suspecte, au bureau comme chez eux.

Règles de prudence avec le courrier électronique

https://www.melani.admin.ch/melani/fr/home/schuetzen/verhaltensregeln.htm
➔ Courrier électronique

Règles de comportement adéquat pour les mots de passe

Un mot de passe devrait être changé à intervalles réguliers (tous les trois mois à peu près) mais au plus tard quand vous présumez que des tiers pourraient en avoir eu connaissance.

Autres règles:
https://www.melani.admin.ch/melani/fr/home/schuetzen/verhaltensregeln.htm
➔ Mot de passe

Si votre société gère elle-même des bases de données auxquelles les clients ont accès en ligne, vous devriez veiller à ne pas être victime de la prochaine fuite de données. La liste de contrôle publiée sur notre site Web vous y aidera.

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

5.3 Systèmes de contrôle industriel (SCI)

L'Internet des objets a été traité en détail dans ce rapport semestriel, dont il constitue le thème prioritaire. Les objets raccordés au réseau s'emploient depuis longtemps déjà. Les capteurs et les actionneurs sont coordonnés, automatisés et optimisés de façon centrale par des systèmes de contrôle. Ces commandes surveillent les réseaux électriques, les flux du trafic, le climat dans les bâtiments ou les dispositifs médicaux à l'hôpital.

5.3.1 Déjà vu à Kiev: nouvelle panne d'électricité en Ukraine

Près d'un an après la gigantesque panne électrique qui avait paralysé une partie de l'Ukraine à fin 2015 et dont l'avant-dernier rapport semestriel s'est fait l'écho[47], la banlieue nord de Kiev a été de nouveau plongée dans l'obscurité. Samedi 17 décembre 2016 peu avant minuit, les clients du fournisseur d'énergie étatique Ukrenergo approvisionnés par la sous-station de Pivnichna ont été privés de courant pendant une heure[48]. Ukrenergo a signalé à ses clients ne pas savoir si la panne était due à des composants défectueux ou à une cyberattaque. Quelques semaines plus tard Oleksandr Tkachuk, chef de cabinet des services de sécurité ukrainiens, déclarait que tant cette panne que des attaques subies par le système financier et par d'autres infrastructures avaient été orchestrées par les services de sécurité russes, en collaboration avec des éditeurs de logiciels privés et des cybercriminels[49]. Selon ses dires, les attaques étaient dues au gang ayant sévi dans le passé avec le maliciel BlackEnergy. Des spécialistes indépendants n'ont pas encore été en mesure de vérifier ses dires. À ce jour, seuls des chercheurs en sécurité ukrainiens de la société Information Systems Security Partners (ISSP) et d'Honeywell Cyber Security Labs ont repris ces accusations, lors d'un exposé présenté en janvier 2017 à la S4 ICS Security Conference[50]. Ils ont encore souligné avoir participé à l'enquête sur l'incident. Ces spécialistes ont expliqué que contrairement à l'année précédente, les unités de télégestion (remote terminal unit, RTU) n'avaient pas été rendues inutilisables par écrasement de leur microprogramme (firmware). La récente cyberattaque s'étant contentée de les déconnecter à distance, le rétablissement de l'approvisionnement électrique avait été beaucoup plus rapide. D'après ces mêmes chercheurs, les agresseurs auraient parfaitement pu causer des dégâts bien plus graves. La cyberattaque visait donc un autre but, ce qui amène à penser qu'il s'agissait plutôt d'une démonstration de force des saboteurs.

L'infiltration des cibles par le maliciel remontait à une vaste campagne électronique lancée en juillet 2016. Les agresseurs avaient ensuite circulé pendant plusieurs mois dans les réseaux, afin de les analyser et de se rapprocher des appareils les intéressant. Outre la compagnie d'électricité, le Ministère des finances, le Trésor et la caisse de retraite de l'État ukrainien figurent parmi les victimes. Le 6 décembre 2016, une attaque DDoS avait été lancée contre ces cibles, tandis que certaines composantes du réseau étaient endommagées

---

47 MELANI, rapport semestriel 2/2015 https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2015-2.html (état: le 28 février 2017).

48 https://motherboard.vice.com/en_us/article/ukrainian-power-station-hacking-december-2016-report (état: le 28 février 2017).

49 http://www.reuters.com/article/us-ukraine-crisis-cyber-idUSKBN15U2CN (état: le 28 février 2017).

50 https://www.youtube.com/watch?v=lTwsDLO3C44 (état: le 28 février 2017).

de l'intérieur et des bases de données effacées, d'où une interruption et des retards dans le trafic des paiements national.

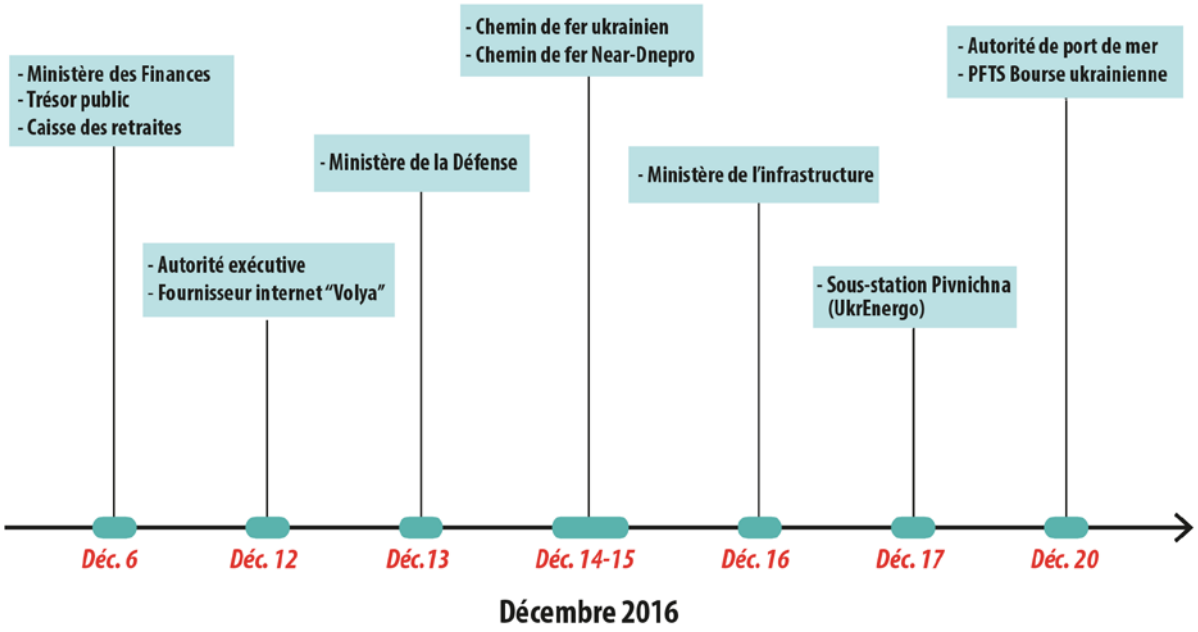

Fig. 7: Chronologie des cyberattaques (source: S4 Events)

Le 14 décembre 2016, les saboteurs s'en étaient encore pris à l'administration ferroviaire ukrainienne. Là encore, une attaque DDoS avait été lancée pour détourner l'attention de leurs agissements, prenant pour cible la vente des billets en ligne. Pendant ce temps, ils manipulaient la gestion automatisée du transport ferroviaire de marchandises. Les chercheurs ont opéré un rapprochement avec l'attaque de 2015, à propos des stratégies de propagation dans les réseaux infiltrés. Ils ont relevé des progrès au niveau des macrovirus utilisés dans l'envoi de courriels ciblés. À la différence des macros simples de 2015, seul 1 % du code avait une utilité fonctionnelle. En effet, 30 % des lignes programmées visaient à empêcher l'analyse de la macro, et les 69 % restants avaient pour unique but de dissimuler le caractère malveillant du maliciel.

Les chercheurs mandatés ont eu l'impression que l'Ukraine avait servi de base de test à la partie adverse, désireuse de mesurer ses capacités à lancer des cyberattaques. Ils précisent encore que les analyses approfondies de l'incident prendront encore plusieurs mois. D'ici là, les experts indépendants n'auront guère la possibilité de vérifier les résultats présentés.

Il importe d'éviter tout alarmisme à propos des systèmes de contrôle industriel, du fait des découvertes en apparence spectaculaires de cyberattaques. C'est ce qu'écrit Robert M. Lee, après avoir participé à l'analyse de la panne ukrainienne de 2015. Car moyennant l'adoption systématique de mesures de sécurité adéquates, il est possible de découvrir et de prévenir même les incidents aux conséquences préoccupantes. Par exemple, l'entreprise de cybersécurité SentinelOne s'est crue obligée de publier une déclaration rectificative quand la presse, s'emparant d'une de ses analyses de maliciels, avait parlé d'attaques étatiques contre le secteur énergétique américain. Un seul indice accréditait cette thèse, à savoir qu'un des systèmes pris pour victimes hébergeait un système de gestion de l'énergie. Or le mali-

ciel lui-même ne présentait aucune caractéristique visant spécifiquement les systèmes de contrôle.

5.3.2 Distributed Denial of Heating – chauffage coupé par une attaque DDoS

Les habitants de deux bâtiments de Lappeenranta, ville située à l'est de la Finlande, ont été privés de chauffage et d'eau chaude pour quelque temps. La panne résultait d'une attaque DDoS ayant mis hors service le système informatique gérant ces immeubles[51]. Le système avait vainement tenté de réinitialiser la connexion interrompue en redémarrant sans cesse, et le chauffage était resté déclenché. Les exploitants de réseaux zombies à la recherche d'appareils imprudemment configurés ou vulnérables ont repéré les solutions d'automation des bâtiments finlandais. Pour rétablir le chauffage, il a fallu une intervention humaine, consistant à couper physiquement l'accès à Internet pour déjouer l'attaque DDoS. Le fabricant du système saboté a signalé que plusieurs attaques de ce genre avaient été observées dans le pays.

Un fonctionnement sûr exigerait d'exploiter les systèmes dans un réseau cloisonné, comme le recommande MELANI. Or les systèmes sont bien souvent connectés à Internet, par confort et pour en faciliter l'utilisation.

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 industriel (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

5.4 Cyberattaques

5.4.1 Panne d'Internet subie par 900 000 clients de Deutsche Telekom

Le 27 novembre 2016, une cyberattaque a été déclenchée au niveau mondial contre de nombreux routeurs. En Allemagne, elle a privé d'Internet 900 000 clients de Deutsche Telekom. La panne était due à une nouvelle version du maliciel Mirai, qui avait déjà servi le

[51] http://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter (état: le 28 février 2017).

21 octobre 2016 contre les serveurs DNS du fournisseur Dyn[52]. Mirai est un maliciel développé pour le système d'exploitation Linux, qui s'en prend surtout aux appareils de l'Internet des objets. En l'occurrence, il recherchait une faille dans les routeurs réseau des clients finaux, afin de s'y installer. Comme les routeurs de Deutsche Telekom ont un système d'exploitation propriétaire, le maliciel n'a pas pu s'y glisser. Mais à force d'insister, il a néanmoins bloqué les routeurs. L'opérateur a fourni à sa clientèle une mise à jour logicielle.

5.4.2 Attaques ciblant les transactions financières

Diverses tentatives de détournement de transactions financières ont fait la une des médias internationaux durant la période sous revue. Les quelques cas exposés ci-dessous donnent un aperçu de la grande diversité des cibles potentielles.

Le 6 novembre, TESCO Bank annonçait que des activités malveillantes avaient eu lieu sur près de 40'000 comptes, résultant en des pertes financières pour à peu près la moitié d'entre eux. L'établissement britannique s'est vu contraint de prendre des mesures d'urgence et de bloquer les transactions financières. Plusieurs mois après les événements, il reste de nombreuses parts d'ombre quant au mode opératoire exact des attaquants. Le manque de communication à ce sujet a d'ailleurs été critiqué outre-Manche. La banque s'est engagée à rembourser les clients lésés. Par ailleurs, on ne peut pas exclure que l'incident puisse avoir des conséquences financières pour l'établissement, le régulateur britannique du secteur de la finance ayant en effet la possibilité de délivrer une amende selon la responsabilité de la banque dans l'incident.

Outre les attaques directement lancées contre les systèmes des banques, à commencer par le système de paiement SWIFT[53], les distributeurs de billets de banque constituent une cible possible pour les cybercriminels. En août, une série d'attaques a permis de dérober 12 millions de bahts (près de CHF 343'000) en Thaïlande. L'entreprise de sécurité FireEye croit pouvoir attribuer cette fraude à un maliciel qu'elle a analysé et nommé Ripper [54]. Après l'avoir installé sur le système du distributeur, les criminels le font interagir avec une carte à puce falsifiée. L'incident montre la remarquable organisation des criminels, qui doivent compromettre les machines, produire les cartes puis accéder physiquement aux distributeurs pour finaliser l'opération. En novembre, l'entreprise de sécurité Group-IB a publié un rapport sur un groupe de criminels qu'elle nomme Cobalt et qu'elle tient responsable d'une série d'incidents ayant eu lieu en Europe. Après avoir compromis les systèmes de plusieurs banques, les escrocs auraient récupéré de l'argent directement aux distributeurs, sans même avoir besoin de les manipuler physiquement[55].

---

[52] Voir le thème prioritaire traité au chapitre 3

[53] Voir notamment rapport semestriel 2016/1, chapitre 5.4.1 «Cyber-braquage: butin de 81 millions de dollars» https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2016-1.html (état: le 28 février 2017).

[54] https://www.fireeye.com/blog/threat-research/2016/08/ripper_atm_malwarea.html (état: le 28 février 2017).

[55] http://www.reuters.com/article/us-cyber-banks-atms-idUSKBN13G24Q (état: le 28 février 2017).

Rançon de leur succès, les nouvelles formes de monnaie numériques sont également la cible d'attaques, comme signalé dans de précédents rapports[56]. Lors de la période sous revue, c'est la bourse d'échange Bitfinex qui a fait l'objet d'un piratage massif. Quelque 120 000 bitcoins ont été dérobés, soit plus de 130 millions de francs suisses (au cours de février 2017). Pour arriver à leurs fins, les auteurs ont dû compromettre la fonction multi-signatures en place chez les clients de Bitfinex. L'impact sur les marchés a été important: après l'annonce de l'incident, le cours du bitcoin a chuté de 13 % en deux jours.

Enfin Carbanak, dont les attaques massives contre des banques avaient fait grand bruit en 2015[57], confirme son entreprise de diversification. Selon des chercheurs de la société Trustwave[58], le secteur hôtelier a récemment été la cible d'attaques de spear phishing faisant appel à l'ingénierie sociale. Le but final des escrocs étant de dérober des données de cartes de crédit, après avoir compromis des terminaux de pointe de vente.

Conclusion:

Les développements observés ces dernières années montrent que l'utilisateur n'est plus le seul maillon faible de la chaîne des systèmes de paiement. Les banques elles-mêmes, à travers leurs systèmes internes ou encore leurs distributeurs de billets, sont fréquemment prises pour cibles. Par ailleurs, les nouvelles monnaies, stockées exclusivement de manière digitale, sont elles aussi au centre de l'intérêt des cybercriminels.

5.4.3 Un marché des rançongiciels encore très éclaté

Sur le terrain des rançongiciels, le deuxième semestre a été très riche, comme on l'a déjà vu au chapitre consacré à la situation nationale. Les nombreux incidents signalés au niveau international témoignent de la grande diversité des attaques, des cibles et des modes opératoires. Le précédent rapport avait déjà relevé la logique entrepreneuriale des criminels. Ceux-ci améliorent leurs produits, recherchent de nouveaux débouchés et vont jusqu'à soigner leurs relations avec leurs clients (les victimes), par exemple en publiant des FAQ[59] ou en offrant la possibilité de dialoguer en direct avec les opérateurs du rançongiciel. Le marché des rançongiciels semble être encore en phase de consolidation, avec de nombreux groupes différents, des cibles et des modes opératoires très variés. La situation est tout autre pour d'autres secteurs de l'activité cybercriminelle – en particulier pour les chevaux de Troie bancaires, domaine dans lequel certaines marques bien établies paraissent se tailler la part du lion.

---

[56] Voir à ce sujet rapport semestriel 2014/1, chapitre 4.10 «Attaques visant les monnaies virtuelles» https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2014-1.html (état: le 28 février 2017).

[57] Voir rapport semestriel 2015/1, chapitre 5.1.2 «Carbanak – hold-up en ligne» https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-sur-la-situation/rapport-semestriel-2015-1.html (état: le 28 février 2017).

[58] https://www.trustwave.com/Resources/SpiderLabs-Blog/New-Carbanak-/-Anunak-Attack-Methodology/ (état: le 28 février 2017).

[59] Liste de réponses aux questions que peut se poser la victime, figurant dans le message de chantage.

Un des cas les plus spectaculaires a touché les systèmes du réseau de transports publics de San Francisco. Vendredi 25 novembre 2016, une attaque paralysait sa billetterie, obligeant la société à annoncer la gratuité de ses services le temps de restaurer les systèmes à l'aide de sauvegardes. L'attaquant a par ailleurs prétendu avoir en sa possession des données sensibles, ce que la société de transport a démenti. Quelques jours plus tard, de nouvelles révélations[60] ont permis de dresser un profil plus précis de l'agresseur, qui est apparemment responsable de plusieurs attaques du même genre. Il n'aurait toutefois pas spécifiquement ciblé les transports publics de San Francisco, se contentant de rechercher automatiquement des systèmes vulnérables.

Conclusion:

Cet exemple montre qu'une attaque, même quand elle touche des systèmes bureautiques de manière non ciblée comme cela semble être le cas ici, peut avoir des effets en chaîne et causer des dommages très concrets. Dans ce type de cas, ce n'est pas nécessairement la capacité à restaurer l'intégrité des systèmes qui est l'enjeu, mais plutôt le temps nécessaire pour le faire. En effet, durant cette période, des solutions provisoires et une véritable gestion de crise doivent être mises en place.

5.5 Failles de sécurité

Parmi les nombreuses lacunes publiées au deuxième semestre 2016, le présent rapport signale trois failles illustrant de manière exemplaire la fragilité de nos systèmes et programmes dans trois domaines différents.

5.5.1 Faille due à l'interface USB

Chacun sait qu'il n'est pas sans risque d'insérer une clé USB étrangère dans son propre ordinateur, et qu'il vaudrait mieux s'en abstenir. Les systèmes d'exploitation sont entre-temps conçus pour ne plus exécuter automatiquement les instructions des clés USB: ils demandent d'abord à l'utilisateur quelle action il souhaite effectuer. Or qu'advient-il si cet élément de sécurité est contourné? Comme l'explique dans son blog l'expert en sécurité Samy Kamkar[61], si quelqu'un branche une clé USB préparée par ses soins, lui-même pourra plus tard installer des maliciels. Il en aurait la possibilité même avec un ordinateur verrouillé. En effet, le logiciel qu'il a conçu se fait passer à l'interface USB pour un équipement Ethernet et simule ainsi une connexion à Internet par le port USB. Il pourra ainsi non seulement dérober les cookies et contrôler le trafic Internet, mais aussi installer durablement une porte dérobée. Il suffit, pour que l'attaque aboutisse, qu'un navigateur soit installé sur l'ordinateur pris pour cible.

60 https://krebsonsecurity.com/2016/11/san-francisco-rail-system-hacker-hacked/ (état: le 28 février 2017).

61 https://samy.pl/poisontap/ (état: le 28 février 2017).

Conclusions et recommandations:

Vous arrive-t-il de laisser votre ordinateur sans surveillance à une conférence, à la bibliothèque ou au café, pendant une pause de midi ou pour aller aux toilettes? Le cas échéant, des pirates auraient le champ libre pour leurs tentatives d'espionnage ciblé. Pour prévenir un tel scénario, il convient de ne jamais laisser son ordinateur sans surveillance, ou du moins de désactiver les ports USB et les autres interfaces.

5.5.2 Gestionnaire de mots de passe, risque de faille centrale ?

L'emploi de gestionnaires de mots de passe et la sécurité qu'ils confèrent sont un sujet souvent abordé. Certains ne jurent que par de tels outils, offrant la possibilité d'utiliser des mots de passe très sûrs, longs et compliqués. Divers programmes signalent même quand il y a lieu de changer ses mots de passe, ou en proposent qui sont solides. Il suffit de se souvenir de son mot de passe maître. C'est là qu'interviennent les sceptiques: à supposer qu'un pirate parvienne à dérober la base de données ou qu'il découvre le mot de passe maître, il aurait accès à tous les mots de passe à la fois. Une mine d'or pour les escrocs. Ce serait pire encore si le gestionnaire de mots de passe comportait une vulnérabilité. Une telle faille a précisément été trouvée à la fin de juillet 2016, dans le plugiciel Firefox du programme LastPass. En redirigeant l'utilisateur sur un site contrefait, les pirates pouvaient s'emparer de ses mots de passe.[62] La faille a été corrigée.

5.5.3 Faille Masque Attack d'iOS

Les premières attaques exploitant la vulnérabilité Masque Attack ont été repérées en 2014. Elles permettaient aux escrocs de remplacer une application authentique de l'App Store d'Apple par une application manipulée, signée par l'entreprise et portant le même identifiant de lot (bundle identifier, bundle ID)[63]. Les escrocs peuvent ainsi générer des contenus malveillants et leur attribuer la même bundle ID qu'à l'original. Si l'original est apprécié, la portée de l'attaque augmente logiquement, et aussi la probabilité que des utilisateurs téléchargent une application manipulée. Apple a certes comblé les failles de sécurité en cause. Trendmicro a toutefois constaté que les applications manipulées demeurent nombreuses[64]. Un rapport publié en novembre 2016 en explique la raison. Les cybercriminels exploitent une fonction du processus de signature, qui leur permet d'hériter de données existantes. La collaboration avec Apple a toutefois permis de corriger le problème dans iOS 10. Les appareils exploités sous iOS 9.3.5 ou une version antérieure restent cependant vulnérables.

---

62 https://blog.lastpass.com/2016/07/lastpass-security-updates.html/ (état: le 28 février 2017).

63 Bundle identifier, ou identifiant de lot, est le nom donné à une application à sa création pour la distinguer des autres, généralement sous la forme com.your-company.app-name. Ce nom est définitif.

64 http://blog.trendmicro.de/masque-attack-missbraucht-das-code-signing-in-ios-fuer-faelschungen/ (état: le 28 février 2017).

5.6 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.

5.6.1 Réseau Avalanche: arrestations et perquisitions

Les cybercriminels ont utilisé dès 2009 le réseaux d'envergure internationale baptisé Avalanche pour déployer leurs activités liées aux maliciels, au phishing et aux pourriels. Ils ont envoyé à leurs victimes plus d'un million de courriels hebdomadaires contenant des annexes ou des liens infectés. Le réseau Avalanche servait aussi au lancement de cyberattaques dans le monde entier, ainsi qu'au recrutement d'agents financiers. Les dégâts causés au niveau mondial sont estimés à plusieurs centaines de millions d'euros, mais les dommages effectifs restent difficiles à évaluer, ce portail servant à administrer différentes familles de maliciels. L'enquête sur la plateforme avait débuté en 2012. L'infrastructure a été démantelée le 30 novembre 2016. Des enquêteurs de 30 pays ont participé à la désactivation de la plateforme. Cinq personnes ont été arrêtées, 37 perquisitions effectuées et 39 serveurs saisis. Les procureurs ont identifié des victimes dans plus de 180 pays. À leur demande, 221 serveurs ont été débranchés par les fournisseurs d'accès compétents.[65]

Conclusion:

Cet exemple montre que les autorités de poursuite pénale parviendront à combattre d'autant plus fructueusement la cybercriminalité qu'elles collaborent à la fois au niveau international et avec le secteur privé.

5.7 Autres thèmes

5.7.1 Fin de la surveillance américaine de la gestion mondiale du réseau

Le 30 septembre 2016, les États-Unis ont cessé de jouer le rôle historique de surveillant de l'ICANN, la société de gestion des adresses Internet au niveau mondial.[66] Celle-ci est désormais dirigée par une communauté internationale, où sont représentés tous les groupes d'intérêts. Un pas important a ainsi été franchi vers une gestion internationale et multipartite du système des noms de domaine (DNS).

Depuis 1998, un contrat de l'IANA[67] entre le gouvernement américain et l'ICANN définissait la surveillance états-unienne de la gestion du système DNS. Cette surveillance consistait à

---

65 http://www.staatsanwaltschaften.niedersachsen.de/download/113197 (état: le 28 février 2017).

66 https://www.bakom.admin.ch/bakom/fr/page-daccueil/l-ofcom/informations-de-l-ofcom/ofcom-infomailing/ofcom-infomailing-43/fin-de-la-surveillance-americaine-de-la-gestion-mondiale-du-reseau.html; https://digitalwatch.giplatform.org/processes/iana (état: le 28 février 2017).

67 https://www.ntia.doc.gov/files/ntia/publications/ianacontract.pdf; https://www.icann.org/en/system/files/files/contract-01oct12-en.pdf (état: le 28 février 2017).

contrôler et valider les modifications de la banque de données centrale regroupant tous les domaines de premier niveau (par ex. .swiss, .com ou codes de pays comme .ch). Le contrat de l'IANA expirait à la fin de septembre 2016 et n'a pas été renouvelé.[68]

Le nouveau cadre institutionnel, destiné à garantir une surveillance globale et plus démocratique d'Internet, confère certains pouvoirs de contrôle aux sous-organisations de l'ICANN (y c. le comité consultatif gouvernemental GAC, où l'OFCOM représente la Suisse) par le biais du Conseil ICANN: blocage du budget, approbation des modifications des statuts et révocation du conseil d'administration ou de l'un de ses membres.

Comme l'ICANN garde son siège en Californie, il est en premier lieu soumis au droit américain et aux possibilités d'intervention des autorités états-uniennes. Une étape majeure a néanmoins été franchie vers la transformation de l'ICANN en institution globale, même si d'autres efforts devront être consentis pour renforcer sa diversité et pour mieux tenir compte des besoins et des intérêts de la communauté mondiale. L'OFCOM ainsi que les divers groupes d'intérêts concernés en Suisse encouragent et soutiendront l'évolution en cours.

Les internautes ne devraient guère s'apercevoir du changement. En effet, le fonctionnement technique ordinaire du DNS reste le même dans cette phase de transition.

5.7.2 Contrôle judiciaire des mesures de surveillance à la demande de DE-CIX

La société exploitante du nœud de routage Internet de Francfort DE-CIX a déposé plainte contre la République fédérale d'Allemagne auprès du tribunal administratif fédéral de Leipzig.[69] Sa plainte vise à soumettre à un contrôle judiciaire la surveillance stratégique des télécommunications exercée par le Service fédéral de renseignement allemand (Bundesnachrichtendienst, BND).

La plainte se fonde notamment sur une expertise[70] de Hans-Jürgen Papier, professeur de droit et ancien président du tribunal constitutionnel fédéral. Il y émet de sérieux doutes sur la légalité de la pratique actuelle, en soulignant que le secret des télécommunications doit être considéré comme un droit de l'homme. En ce sens, les personnes étrangères doivent elles aussi bénéficier de ce droit, et toute restriction dans ce domaine dûment figurer dans une loi. De son côté, le gouvernement fédéral estime ne pas avoir besoin de base légale pour surveiller des données provenant de l'étranger exclusivement.

En Suisse, la loi fédérale sur le renseignement (LRens) a introduit la base formelle nécessaire à l'exploration du réseau câblé dans le cas des télécommunications étrangères. Concrètement, toute mesure de ce type est soumise non seulement à l'aval du chef du DDPS, mais aussi à l'autorisation du Tribunal administratif fédéral, et donc fait l'objet d'un encadrement politique et d'un contrôle judiciaire indépendant.

---

68 https://www.icann.org/news/announcement-2016-10-01-en (état: le 28 février 2017).

69 https://www.de-cix.net/de/about-de-cix/media-center/press-releases/information-on-the-lawsuit-against-the-federal-republic-of-germany (état: le 28 février 2017).

70 http://rsw.beck.de/rsw/upload/NVwZ/NVwZ-Extra_2016_15.pdf; https://netzpolitik.org/2016/ex-praesident-des-bundesverfassungsgerichts-bnd-zugriff-auf-internet-knoten-wie-de-cix-ist-insgesamt-rechtswidrig/ (état: le 28 février 2017).

6 Tendances et perspectives

6.1 Cybercrime as a service et cyber extorsion: cercle vicieux

L'expression cybercrime as a service (CaaS) désigne la vaste gamme d'offres commerciales permettant d'acquérir les outils utiles au lancement d'une attaque informatique sans grande connaissance spécifique. Divers types de maliciels sont par exemple proposés, de même que la location d'un réseau de zombies (botnet), le lancement d'attaques DDoS ou des services de blanchiment d'argent. Le phénomène n'est pas nouveau, de nombreux services cybercriminels étant déjà disponibles jusqu'ici sur des forums underground. Pendant longtemps cependant, ces services restaient l'apanage du milieu cybercriminel, qui se répartissait le travail par souci d'efficacité. Une telle organisation permet en effet aux divers acteurs de se spécialiser en peaufinant des compétences bien spécifiques, qu'ils pourront ensuite vendre ou échanger.

La situation a bien changé avec le boom de la cyber extorsion. Toute une série d'offres sont venues nourrir ce marché, contribuant à la démocratisation de ce type d'attaque. Prenons le cas des attaques par déni de service, visant à contraindre la victime à un paiement en bitcoins: n'importe qui peut désormais louer un Stresser/Booter[71] afin de lancer une attaque DDoS. Il suffit de choisir sa cible et une formule d'attaque, dont le prix et l'efficacité peuvent varier. À titre d'exemple, même l'utilisation d'un botnet d'objets connectés compromis par le maliciel MIRAI est commercialisée. La situation est similaire sur le terrain des rançongiciels. Avec un minimum de compétences techniques, chacun peut acquérir clé en main et mettre en œuvre ce type d'attaque.

D'où la question de la dynamique propre à ce marché: est-ce la vigoureuse demande pour de tels services qui a amené des cybercriminels à concevoir toute une palette d'outils sur mesure ? Ou l'offre proposée a-t-elle suscité des vocations criminelles toujours plus nombreuses?

Il y a un peu des deux, et il semble s'agir d'un véritable cercle vicieux. Mais pour comprendre la dynamique à l'œuvre, il convient tout d'abord de saisir pourquoi la cyber extorsion était faite pour devenir aussi populaire. Tout d'abord, comme on l'a souvent dit, ce type d'attaque génère beaucoup d'argent, et le processus de cashout est grandement facilité[72]: un paiement en bitcoins est effectué directement par la victime, et la transaction peut être «lavée» pour devenir intraçable à travers un service de bitcoin mixing. De plus, la recherche de cible est aisée, le cercle des victimes potentielles étant quasiment illimité. Enfin, ce type d'attaque a connu une médiatisation sans précédent: de nombreuses victimes sont connues et les «success stories» criminelles sont largement relayées, alors que les arrestations de criminels semblent plus rares, entretenant un sentiment d'impunité. En conséquence, l'effet d'incitation est très fort: de nombreux auteurs potentiels, notamment issus de la petite criminalité traditionnelle, tentent leur chance dans le domaine cyber. En toute logique, la demande étant là, l'offre tend à suivre, et le marché s'adapte en proposant toute une gamme

[71] Offres de «DDoS as a service» pouvant être louées. Elles ont parfois une apparente légitimité, en proposant le service comme test de résistance (stress test) d'un service en ligne.

[72] Soit le passage entre l'activité criminelle et l'obtention d'une somme d'argent utilisable.

de services, à la portée des divers types d'auteurs. À son tour, cette offre sur mesure et facile d'accès dope le marché et permet à toujours plus de gens de s'adonner à ces pratiques.

Les concepteurs de telles offres sont bien sûr le nœud du problème. Leur nombre a beau être vraisemblablement assez limité – en 2015 Andy Archibald, directeur de la National Crime Agency (UK), estimait qu'il s'agissait de 100 à 200 personnes –, l'effet de levier est considérable.[73] En outre, la démocratisation croissante des activités cybercriminelles rend cette nébuleuse difficile à cerner, en raison du très grand nombre d'auteurs et de produits en circulation. Il va de soi que le fort éclatement de telles pratiques et la difficulté d'en avoir un bon aperçu compliquent la tâche des autorités de poursuite pénale.

6.2 Avenir de l'authentification à deux ou plusieurs facteurs

Le National Institute of Standards and Technology (NIST) américain a signalé en juillet 2016[74] que ses futures directives relatives aux identités numériques ne recommanderaient plus l'authentification par SMS, voire déconseilleraient une telle solution. Alors qu'un peu partout les efforts se poursuivent pour amener les internautes à adopter systématiquement l'authentification à deux facteurs, le deuxième facteur le plus populaire et le plus simple à l'utilisation, soit le SMS, est d'ores et déjà jugé inadéquat dans ce contexte.

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, soit souvent le téléphone mobile avec le SMS. Mais comme la plupart des téléphones mobiles sont aujourd'hui des smartphones, et donc de petits ordinateurs, ils risquent d'être infectés de maliciels capables d'intercepter des messages et de les transférer aux escrocs. En outre, les opérations bancaires s'effectuent toujours plus souvent directement sur le smartphone. Autrement dit, la connexion avec l'identifiant et la deuxième authentification se font sur le même appareil, et donc le mot de passe unique transmis par SMS cesse d'être un gage de sécurité accrue.

Or les terminaux peu sûrs ne sont pas les seuls à mettre en péril le SMS comme second facteur: de telles informations risquent déjà d'être interceptées ou détournées sur les réseaux. Cela fait plusieurs années que des chercheurs en sécurité ont signalé les problèmes de sécurité du protocole SS7[75], qui permet notamment l'itinérance entre divers opérateurs de téléphonie mobile. L'appareil peut s'annoncer en dehors des frontières nationales à des réseaux étrangers; l'exploitant du réseau contacté le signale au réseau domestique de l'abonné, qui lui transmettra ensuite les appels et les SMS. Or il est possible de simuler une telle opération sans que le téléphone mobile se trouve à l'étranger. Les SMS seront alors déviés vers les opérateurs à l'étranger, qui pourront en prendre connaissance. C'est possible 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 cer-

---

73 https://www.connectinternetsolutions.com/cyber-crime/ (état: le 28 février 2017).

74 https://pages.nist.gov/800-63-3/sp800-63b.html (état: le 28 février 2017).

75 https://www.blackhat.com/presentations/bh-europe-07/Langlois/Presentation/bh-eu-07-langlois-ppt-apr19.pdf (état: le 28 février 2017).

taines 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.

Parallèlement à ces possibilités technologiques, des cas peuvent faire appel à l'ingénierie sociale. Dans un cas concret, des escrocs ont su convaincre des collaborateurs serviables du service à la clientèle d'un opérateur Télécom d'envoyer une carte SIM de remplacement à l'adresse de leur choix[76], ce qui leur a permis par la suite de prendre le contrôle de plusieurs comptes en ligne.

L'authentification à plusieurs facteurs comprend au moins deux composantes. Elle peut faire appel à un élément que l'on connaît (par ex. mot de passe), que l'on détient (par ex. carte-clé) ou qui nous est propre (par ex. empreinte digitale). En raison de la convergence de la téléphonie et de l'informatique et de la fusion des réseaux de communication, le réseau mobile ne peut plus être considéré comme un canal autonome et indépendant d'Internet. Le SMS ne correspond donc plus que de façon limitée à la composante de l'«élément détenu». Autrement dit, les services en ligne – particulièrement ceux dont la compromission entraînerait un dommage important – feraient bien d'opter pour d'autres méthodes d'authentification. Les applications pour smartphone décodant le mot de passe unique chiffré d'un prestataire de services représentent, moyennant une utilisation correcte, un bon exemple de méthode sûre basée sur la téléphonie mobile. Autre alternative fiable, la fonction Mobile ID chiffre déjà sur la carte SIM les éléments d'authentification. Et comme les services sont toujours plus souvent utilisés sur le smartphone même, il est recommandé de prévoir pour l'authentification des éléments indépendants comme des jetons de sécurité autonomes, dont de nombreux services en ligne proposent déjà l'usage[77].

Conclusion:

Si votre service en ligne s'en tient encore à des SMS pour l'authentification ou pour la réinitialisation des mots de passe, il ne faut pas pour autant céder à la panique. Car même si cette méthode présente entre-temps des failles et ne constitue plus la meilleure variante en matière de sécurité, la présence d'au moins deux facteurs demeure bien plus sûre qu'une protection limitée à un nom d'utilisateur et à un mot de passe.

6.3 Technologies de sécurité sous pression permanente

Au-delà des produits de sécurité usuels tels que les antivirus, la technologie de micro-virtualisation et les systèmes de détection et de prévention d'intrusions, il est souvent fait appel pour accroître la sécurité aux ressources Windows embarquées, comme AppLocker et EMET[78]. Ces deux programmes renforcent sensiblement la sécurité des systèmes Windows. Ainsi, AppLocker permet de déterminer précisément quels programmes ont le droit d'être

[76] http://www.forbes.com/sites/laurashin/2016/12/20/hackers-have-stolen-millions-of-dollars-in-bitcoin-using-only-phone-numbers/#42981a5c22db (état: le 28 février 2017).

[77] http://fc16.ifca.ai/preproceedings/25_Lang.pdf (état: le 28 février 2017).

[78] L'outil de sécurité de Microsoft EMET (Enhanced Mitigation Experience Toolkit) comporte notamment les fonctions Address Space Layout Randomization (ASLR) et Data Execution Prevention (DEP).

exécutés dans quel répertoire. Il est donc bien plus difficile aux pirates de causer une infection initiale. De son côté, EMET sert de rempart face à l'exploitation des vulnérabilités.

Les programmeurs de maliciels cherchent naturellement à contourner ces mécanismes de sécurité. Même si le phénomène n'est pas nouveau et a déjà été décrit à maintes prises[79,80], ce type d'attaque a enregistré une forte progression l'automne dernier. Les agresseurs glissent par exemple dans des documents Office une macro renfermant un script PowerShell, profitant du fait que la plupart des environnements tolèrent ces scripts. D'autres approches misent sur l'outil regsvr32 et sur des scriptlets pour parvenir aux mêmes fins. Le kit d'exploits Angler permet en outre maintenant de lancer des exploits qui déjouent l'effet de protection d'EMET. En effet, les agresseurs font appel à des routines d'allocation de mémoire appartenant directement aux programmes pris pour cible (par ex. Flash).[81]

Conclusions et recommandations:

Les nouvelles technologies de protection sont toujours plus répandues et opèrent contre de nombreux vecteurs d'attaque existants. Les attaquants sont néanmoins aptes et disposés à trouver pour chaque mécanisme de sécurité une possibilité de contournement. L'usage de tels mécanismes reste néanmoins judicieux, car ils compliquent la tâche aux agresseurs et rendent inopérants un grand nombre de vecteurs d'attaque actuellement utilisés. Nous recommandons toutefois de garder à l'esprit les possibilités que PowerShell offre aux escrocs et d'introduire par exemple des mesures de sécurité adéquates, comme une signature numérique pour tous les scripts et macros. On trouve également différents outils de blocage basés sur les comportements (behavior blocking engine), qui permettent d'identifier une partie au moins de ces attaques. Enfin, Microsoft a introduit dans le mode DeviceGuard de Windows 10 des fonctions qui compliquent la vie aux attaquants.

79 http://subt0x10.blogspot.ch/2016/04/bypass-application-whitelisting-script.html (état: le 28 février 2017).
80 http://leastprivilege.blogspot.ch/2013/04/bypass-applocker-by-loading-dlls-from.html (état: le 28 février 2017).
81 https://www.fireeye.com/blog/threat-research/2016/06/angler_exploit_kite.html (état: le 28 février 2017).

7 Politique, recherche et politiques publiques

7.1 Suisse: Interventions parlementaires

Objet	*N°*	*Titre*	*Auteur*	*Date de dépôt*	*Conseil*	*Dép.*	*État des délibérations et lien*
Ip	16.4115	Identité électronique	Rosmarie Quadranti	16.12.2016	CN	DFJP	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164115
Mo	16.4089	Renforcement des instruments de politique de sécurité à l'étranger	Damian Müller	15.12.2016	CE	DDPS	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164089
Po	16.4073	Cyberrisques: pour une protection globale, indépendante et efficace	Roger Golay	15.12.2016	CN	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164073
Po	16.3706	Économie numérique et marché du travail	Beat Vonlanthen	27.09.2016	CE	DEFR	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163706
Ip	16.3694	Sommes-nous armés pour répondre aux exigences du monde du travail 4.0?	Stefan Müller-Altermatt	22.09.2016	CN	DEFR	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163694
Ip	16.4161	Julian Assange, un défenseur des droits de l'homme à protéger?	Jean-Luc Addor	16.12.2016	CN	DFAE	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164161
Ip	16.4131	Comment la Suisse peut-elle participer aux recherches sur l'intelligence artificielle de façon à assurer une bonne représentation des valeurs morales universelles au travers du numérique?	Claude Béglé	16.12.2016	CN	DEFR	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164131
Ip	16.4012	Formation duale. Comment rester les champions du monde?	Claude Béglé	14.12.2016	CN	DEFR	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164012
Ip	16.4001	Airbnb and Co. Règles en matière de responsabilité. Règles des plates-formes Internet ou lois suisses?	Carlo Sommaruga	14.12.2016	CN	DFJP	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164001
Ip	16.3960	Adapter notre système éducatif à la nouvelle représentation du monde qu'impose le numérique	Claude Béglé	08.12.2016	CN	DEFR	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163960
Po	16.3914	Comment introduire de l'éthique dans les algorithmes?	Claude Béglé	28.11.2016	CN	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163914
Mo	16.3902	Interdire les contrats léonins des plates-formes de réservation en ligne dont l'hôtellerie fait les frais	Pirmin Bischof	30.09.2016	CE	CER-E	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163902
Ip	16.3861	Création d'un comité consultatif "Suisse numérique"	Fathi Derder	30.09.2016	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163861
Ip	16.3837	Drones civils. Mieux protéger les infrastructures sensibles	Manuel Tornare	30.09.2016	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163837
Ip	16.3829	Réseau Internet invisible et service de la Confédération	Christian Imark	29.09.2016	CN	DFJP	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163829

		chargé de la cyber-sécurité					
Qu	16.1058	Développement du marché publicitaire. Fuite des fonds vers l'étranger et finance-ment des médias	Jacque-line Badran	28.09.2016	CN	DFJP	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20161058
Ip	16.4003	Ne pas compro-mettre l'attractivité de la Suisse dans le domaine du numé-rique	Marcel Dobler	14.12.2016	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164003
Ip	16.4002	Perspectives d'évolu-tion du transport 2040. Quid de la numérisation dans le scénario de réfé-rence?	Thierry Burkart	14.12.2016	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164002
Po	16.3918	Révolution numé-rique. Comment intégrer les "offli-ners"?	Claude Béglé	29.11.2016	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163918
Po	16.3789	Numérisation dans le secteur des trans-ports publics. Le défi de la protection des données	Evi Allemann	29.09.2016	CN		https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163789
Qu	16.1059	Attaques terroristes. Qu'en est-il de la sécurité des cen-trales nucléaires?	Balthasar Glättli	28.09.2016	CN	DETEC	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20161059
Ip	16.4050	Numérisation dans les douanes suisses. Réduction du travail administratif	Viola Amherd	15.12.2016	CN	DFF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164050
Po	16.4078	Vote électronique. Pour une procédure de vote intégrale-ment sans papier	Marcel Dobler	15.12.2018	CN	ChF	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164078
Mo	16.4011	Numérisation. Eviter les récoltes de données en parallèle	Daniela Schnee-berger	14.12.2016	CN	DFI	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20164011
Qu	16.5429	TISA Leaks. Des menaces sur pour protection des données, la neutralité du net et les logiciels à source ouverte	Balthasar Glättli	21.09.2016	CN	DEFR	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20165429

7.2 Stratégie «Suisse numérique»

Le Conseil fédéral a adopté en 2016 la stratégie «Suisse numérique», qui remplace la stratégie du Conseil fédéral pour une société de l'information en Suisse de 2012.

Selon les principes d'un cyberespace libre, ouvert et sécurisé (free, open and secure Internet), ce document fixe pour les volets «free and open Internet» les objectifs stratégiques que la Suisse souhaite atteindre.

De son côté, la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC) se concentre sur le volet «secure Internet» et fixe les objectifs stratégiques à atteindre sur le terrain de la sécurité, de la confiance, de la fiabilité et de la capacité de résistance (résilience).

La stratégie «Suisse numérique» vise en priorité à saisir les possibilités qu'offre la numérisation, afin de positionner la Suisse comme un espace de vie attractif et un pôle économique et scientifique innovant tourné vers l'avenir. Le Conseil fédéral a défini comme objectifs princi-

paux «Innovation, croissance et prospérité dans le monde numérique», «Égalité des chances et participation de tous», «Transparence et sécurité» et «Contribution au développement durable», définissant au passage les principes selon lesquels la transformation numérique devra s'effectuer.

7.3 Participation suisse à l'exercice Cyber Europe 2016

Cyber Europe, dont c'était la quatrième édition en 2016, fait désormais partie des exercices de sécurité informatique les plus amples et les plus complexes au monde. Cet exercice biennal organisé par l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) se concentre sur les aspects tant techniques qu'opérationnels d'une cybercrise. Quelque 29 États membres de l'UE et de l'AELE, dont la Suisse, participaient à l'édition de l'année dernière. La première phase technique, débutant en avril, a permis aux acteurs de la sécurité d'analyser des incidents complexes, innovateurs et techniquement réalistes. Puis les 13 et 14 octobre, la phase opérationnelle a réuni des experts de plus de 300 organisations – opérateurs de télécommunications, fournisseurs de services en nuage, de logiciels de cybersécurité et de services, départements de la cybersécurité, ou encore ministères et institutions européennes. De nombreux thèmes (Internet des objets, drones, informatique en nuage, logiciels malveillants mobiles, rançongiciels) ont été abordés par Cyber Europe 2016. Pour la première fois, le scénario tout entier incluait des acteurs, des journalistes, des entreprises fictives et des médias sociaux, afin de tenir dûment compte de la dimension des relations publiques. «Stronger together», la devise de Cyber Europe, montre bien que la maîtrise des cyberincidents supranationaux passe par une étroite collaboration à tous les niveaux.

8 Produits publiés par MELANI

Outre ses 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'informations, listes de contrôle, instructions et fiches d'information parus durant la période sous revue.

8.1 GovCERT.ch Blog

8.1.1 Tofsee Spambot features .ch DGA - Reversal and Countermesaures

22.12.2016 - The malware, which MELANI / GovCERT identified as Tofsee, has tried to spam out hundreds of emails within a couple of minutes. However, this wasn't the reason why it popped up on the radar. The reason why this particular sample caught our attention were the domains queried by the malware. The domains appear to be algorithmically generated, and about half of the domains use the country code top level domain (ccTLD) of Switzerland.

➔ https://www.govcert.admin.ch/blog/26/tofsee-spambot-features-.ch-dga-reversal-and-countermesaures

8.1.2 When Mirai meets Ranbyus

15.12.2016 - In the past weeks, MELAN / GovCERT has seen a rise of malicious Microsoft office documents that are being spammed out to Swiss internet users with the aim to infect them with a malicious software (malware) called Dridex. Dridex is an ebanking Trojan which is already around for some time now.

➔ https://www.govcert.admin.ch/blog/23/dridex-targeting-swiss-internet-users

8.1.1 SMS spam run targeting Android Users in Switzerland

13.07.2016 - MELANI / GovCERT.ch received several reports today about malicious SMS that have been sent to Swiss mobile numbers. The SMS is written in German and claims to come from the Swiss Post. But in fact, the SMS has been sent by hackers with the aim to infect Smartphones in Switzerland with a Trojan horse.

➔ https://www.govcert.admin.ch/blog/24/sms-spam-run-targeting-android-users-in-switzerland

8.1.2 Dridex targeting Swiss Internet Users

08.07.2016 - In the past weeks, MELANI / GovCERT has seen a rise of malicious Microsoft office documents that are being spammed out to Swiss internet users with the aim to infect them with a malicious software (malware) called Dridex. Dridex is an ebanking Trojan which is already around for some time now. The attackers are operating various botnets with Dridex infected computers. While most of these botnets do have a strong focus on financial institu-

tions from abroad (such as US or UK), one particular botnet is also targeting financial institutions in Switzerland.

➔ https://www.govcert.admin.ch/blog/23/dridex-targeting-swiss-internet-users

8.2 Lettres d'information de MELANI

MELANI a publié au deuxième semestre 2016 les lettres d'information suivantes:

8.2.1 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

8.2.2 E-banking: des attaques ciblent les moyens d'authentification mobiles

Ces dernières semaines, MELANI a eu connaissance d'attaques lors desquelles des criminels ont réussi à manipuler des utilisateurs à l'aide d'ingénierie sociale, afin que ces derniers acceptent de valider des paiements frauduleux.

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

8.2.3 La cyber-extorsion: thème prioritaire du rapport semestriel de MELANI

Le 23e rapport semestriel publié aujourd'hui par la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) présente les principaux cyber-incidents du premier semestre 2016 aux niveaux national et international. Le rapport est consacré à la multiplication des cas de cyber-extorsion. Il porte en outre sur différentes affaires de fuites de données.

➔ https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/rapport_semestriel-2016-1.html

8.2.4 Les logiciels de paiement hors ligne ciblés par des pirates : des entreprises suisses touchées

25.07.2016 - Ces derniers jours, MELANI a observé plusieurs cas dans lesquels le maliciel Dridex est dirigé contre des logiciels de paiement hors ligne. Ce type de logiciel est utilisé

par les entreprises, afin de transmettre un grand nombre d'ordre de paiements à une ou plusieurs banques. Si la machine sur laquelle un tel logiciel est installé est compromise, les dommages potentiels sont très importants. MELANI recommande fortement de protéger les ordinateurs utilisés pour le trafic de paiement en conséquence.

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

8.2.5 Vagues de courriels contenant des documents Office malicieux

08.07.2016 - Ces dernières semaines, un grand nombre d'annonces concernant des documents Office malicieux ont été effectuées auprès de la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI. Ces documents sont diffusés par e-mail et ont comme finalité d'infecter la machine de l'utilisateur avec un logiciel malveillant (maliciel). MELANI recommande fortement de ne pas ouvrir ce type de documents, de faire preuve d'une prudence accrue dans le traitement des documents Office en général et de ne pas exécuter les macros dans ces derniers.

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

8.3 Listes de contrôle et instructions

MELANI n'a pas publié de listes de contrôle ou d'instructions supplémentaires durant le deuxième semestre 2016.

9 Glossaire

Terme	Définition
Accessibility Service	Application dotée d'une interface utilisateur pour aider les personnes handicapées ou dans l'impossibilité d'interagir normalement avec leur appareil.
Advanced Persistent Threat (APT)	Menace pouvant infliger de sérieux dommages à une organisation ou à un pays. L'agresseur est disposé à investir beaucoup de temps, d'argent et de savoir-faire dans ce genre d'attaque ciblée et furtive, et dispose d'importantes ressources.
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»).
Bundle Identifier	Identifiant de lot; nom donné à une application à sa création pour la distinguer des autres, généralement sous la forme com.your-company.app-name. Ce nom est définitif.
Code à barres	Le terme code à barres (en anglais barcode) désigne la représentation d'une donnée numérique sous forme

	d’une succession de traits et d’espaces parallèles de largeur variable, pouvant être décodés au moyen d’un lecteur optique.
Code QR	Le code QR (quick response code) est un code en deux dimensions constitué de modules noirs disposés dans un carré à fond blanc. L’agencement de ces points définit l’information que contient le code.
Cookies	Témoin de connexion. Petit fichier texte enregistré sur l'ordinateur de l’internaute à l'occasion de sa visite sur une page Web. Les témoins permettent par exemple de mémoriser les réglages personnels pour un site Internet. Il est cependant aussi possible de les utiliser abusivement, notamment pour établir un profil détaillé des habitudes de l'internaute.
Defacement	Défiguration de sites Web.
Domain Generation Algorithm (DGA)	Les algorithmes de génération de noms de domaine sont notamment utilisés par de nombreuses familles de logiciels malveillants. Ils permettent de générer des noms de domaine à travers lesquels les serveurs de commande et de contrôle (C&C) pourront être contactés.
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.
Éthique du hacker	Valeurs morales et philosophiques prépondérantes dans la culture des hacker. Elles s’inspirent en particulier des principes de liberté, coopération, libre arbitre et partage.
Fast Flux	Technique basée sur le protocole DNS dont les réseaux de zombies (botnets) se servent pour dissimuler derrière diverses machines hôtes des sites de phishing ou renfermant des maliciels.
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.
Google-Rank	Le PageRank est l’algorithme d’analyse des liens concourant au système de classement des pages Web utilisé par le moteur de recherche Web. Il mesure quantitati-

	vement la popularité d'une page web.
Grey-Hat	Chapeau gris: hacker malfaisant avec une certaine éthique, n'agissant pas par intérêt personnel.
ICANN	Internet Corporation for Assigned Names and Numbers (ICANN) L'ICANN est une organisation de droit privé à but non lucratif dont le siège est à Marina del Rey, petite ville côtière de Californie. Elle fixe les standards de base pour la gestion des domaines de premier niveau. Ainsi, l'ICANN coordonne les aspects techniques d'Internet, sans édicter de droit contraignant.
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 connectés 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.
Lacunes de sécurité	Lacunes de sécurité Erreur inhérente au matériel ou aux logiciels, permettant à un pirate d'accéder au système.
Logiciel de paiement hors ligne	Logiciel de saisie des paiements installé en mode local.
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).

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.
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.
Ransomware	Rançongiciel. Maliciel utilisé comme moyen de chantage contre le propriétaire de l'ordinateur infecté. Typiquement, le criminel chiffre ou bloque la machine et de-

	mande de l'argent pour permettre de ré-accéder aux données ou à la machine.
RFID (puce)	La radio-identification ou RFID (radio frequency identification) est une technique qui permet d'identifier et de suivre des objets, des véhicules, des animaux ou des personnes au moyen d'un radio-identifiant.
Routeur	Dispositif intelligent assurant la connexion physique entre plusieurs réseaux (informatique, télécommunication, Internet). Un routeur s'utilise par exemple dans un réseau domestique, où il optimise la transmission de l'information entre le réseau interne et Intranet.
Scanneur de ports	Logiciel d'analyse conçu pour détecter les ports TCP et UDP ouverts sur un serveur de réseau.
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).
SHA	Le préfixe SHA (secure hash algorithm) est associé à plusieurs fonctions de hachage cryptographiques.
Carte SIM	La carte SIM (de l'anglais: subscriber identity mo-dule) est une petite carte à puce que l'on insère dans un appareil de téléphonie mobile et qui contient des données identifiant l'abonné.
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
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.
Systèmes de contrôle industriels (SCI)	Les systèmes de contrôle-commande sont formés d'un ou plusieurs appareils qui pilotent, règlent et/ou surveil-

	lent 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	Expression utilisée lorsqu'un fournisseur de service retire une page frauduleuse du réseau.
Texte en clair	Texte d'origine, immédiatement intelligible et pouvant donc être exploité directement, sans recours au déchiffrement.
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.
WLAN	Un WLAN (Wireless Local Area Network) est un réseau local sans fil.