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/I (janvier à juin)

28 OCTOBRE 2016

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

1 Aperçu / Sommaire

2 Éditorial

Martin Sibler est actif depuis 2001 chez Swiss Re dans diverses fonctions liées à la sûreté de l'information.

Chère lectrice, cher lecteur,

L'information constitue dans la branche de l'assurance un enjeu central de la chaîne de valeur ajoutée. Au-delà des formules mathématiques, l'évaluation des risques à assurer nécessite des informations historiques sur l'événement en question – par exemple un ouragan en Floride –, de façon à pouvoir calculer sa probabilité de survenance. Ce genre d'analyse exige encore fréquemment des données spécifiques aux clients, notamment sur l'emplacement des bâtiments à assurer. Il faut veiller ici à maintenir l'intégrité, la confidentialité et la disponibilité des informations. En particulier, leur disponibilité au bon moment aide grandement à mieux comprendre le risque, et jusqu'à un certain point à le prévoir.

Le contexte initial est similaire pour l'évaluation des cyberrisques. À ceci près que divers facteurs dynamiques rendent l'appréciation du risque plus complexe. D'abord, il est rare de disposer d'informations complètes sur les incidents survenus. Ensuite, ces informations ne sont bien souvent plus pertinentes, la technologie et le type d'attaques ayant évolué dans l'intervalle. En cas d'ouragan, les conditions-cadres ne changent guère: la force du vent et la trajectoire ont beau varier, diverses caractéristiques peuvent être prises en compte. Alors qu'en cas d'événement dans le cyberespace, non seulement la force du vent et la trajectoire varient, mais au lieu d'un ouragan on a parfois affaire à un tremblement de terre. La comparaison est sans doute un peu boiteuse, mais elle montre bien qu'en matière de cyberrisques, il faut s'adapter aux situations inattendues. En effet, les informations sur les cyberattaques des 20 dernières années sont d'une utilité limitée pour évaluer la menace.

Par conséquent la cyber intelligence, soit les échanges en temps réel au sujet des attaques en cours, s'avère très utile pour savoir si l'on doit se protéger face à un ouragan ou à un tremblement de terre. Dans ce domaine, MELANI fournit de précieux services, qui aident l'économie suisse à mieux se mettre à l'abri de tels risques.

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

Martin Sibler

3 Thème prioritaire: Cyber-extorsion – Tendance criminelle sur le net

Cryptolocker, Armada Collective, Rex Mundi: Qu'est-ce que ces menaces, qui ont toutes fait la une de l'actualité à un moment donné ont en commun? Il s'agit dans tous les cas de cyber-extorsion! En effet, depuis plusieurs années, les criminels se tournent de plus en plus vers ce mode opératoire extrêmement profitable et, plutôt que de tenter de dérober de l'argent directement, cherchent un moyen de pression pour contraindre la victime à effectuer elle-même un versement. De récentes expressions concrètes de ce mode opératoire sont traitées aux chapitres 4.6.2/3 (*rançongiciels*) et 4.4.1 (*DDoS* et extorsion), mais il est utile tout d'abord de s'interroger sur les raisons de ce succès et sur les dynamiques à l'œuvre.

3.1 Les recettes d'un succès

Du point de vue des criminels, cette méthode présente de nombreux avantages. Tout d'abord, nul besoin de cibler uniquement des systèmes sur lesquels de l'argent transite. Le cercle de cibles potentielles est en effet quasiment illimité, puisqu'il suffit d'atteindre des données ou des systèmes suffisamment importants pour un utilisateur ou une entreprise, qui seront prêts à payer pour en regagner le contrôle. Ce mode de fonctionnement simplifie également grandement le passage entre l'acte criminel et des fonds utilisables par l'auteur («cash out»). Nul besoin ici de blanchir de l'argent par l'intermédiaire de tiers, il suffit de se faire payer directement, dans une monnaie qui est difficilement traçable. Ce n'est d'ailleurs pas un hasard si le développement de ces méthodes est intimement lié à l'essor de nouveaux moyens de paiement permettant de masquer l'identité réelle du bénéficiaire tels que le *Bitcoin*. Grâce à des services de mixage, les criminels peuvent désormais rendre quasiment impossible l'identification des destinataires des paiements en BitCoins.

Les différentes attaques recourant à l'extorsion sont très représentatives du mode de fonctionnement des groupes criminels actuellement à l'œuvre sur Internet. C'est bien souvent une approche entrepreneuriale qui domine, entre opportunisme, recherche d'efficacité et capacité à s'adapter. Tant qu'un modèle d'attaque présente un retour sur investissement positif, il sera conservé et souvent amélioré. L'exemple typique de cette logique nous est donné par les *rançongiciels*. Si le fonctionnement de base de ce type de maliciel est connu depuis maintenant plusieurs années, cette menace se multiplie en de nombreuses variantes et se réinvente sans cesse, en intégrant de nouvelles fonctionnalités la rendant encore plus efficace. Il semble malheureusement s'agir d'un cercle vicieux: les sommes d'argent payées par les victimes alimentent le pouvoir monétaire de ces entreprises criminelles, leur permettant de renforcer leurs infrastructures et de financer leur département recherche et développement. Elles peuvent ainsi gagner en efficacité grâce à de nombreuses innovations, et donc continuer à extorquer suffisamment de victimes malgré les mesures de protection mises en place.

3.2 Dynamisme de l'écosystème criminel

Ce dynamisme et cette recherche d'efficacité obéissent à des principes communs à de nombreuses entreprises mues par l'appât du gain, qui contribuent à leur prospérité. En premier lieu, les criminels se doivent de garder une longueur d'avance au niveau technologique. Dans ce domaine, l'inviolabilité des méthodes de chiffrement est primordiale, puisqu'il s'agit de la clé de voûte d'une telle entreprise criminelle. Les opérateurs se doivent donc d'être

extrêmement réactifs, en améliorant les méthodes de chiffrement si une faille est trouvée pour une version de rançongiciel. Deuxième aspect central pour les criminels: ils doivent constamment veiller à accroître le cercle potentiel de leurs victimes. Il s'agit notamment d'améliorer les méthodes utilisées pour infecter les victimes. Des subterfuges sont trouvés pour permettre aux courriels préparés de déjouer les filtres, par exemple en étant envoyés directement depuis le compte compromis d'un contact, ou au nom d'une autorité officielle. De nouveaux modes de compromission ont aussi été observés. Dans certains cas, le rançongiciel est directement installé à travers un accès RDP (*Remote Desktop Protocol*, permettant de se connecter à distance à un serveur Windows) compromis par une attaque par *force brute*. Toujours dans cette optique, les criminels cherchent aussi à élargir leur surface d'attaque, par exemple en ne chiffrant plus seulement les données d'utilisateurs ou d'entreprises, mais aussi en visant directement les contenus de sites web. Un effort tout particulier sera parfois consenti pour attaquer des cibles particulièrement profitables, pour lesquelles les conséquences d'une attaque sont souvent dramatiques. On pense ici aux attaques ayant touché des hôpitaux. Avec l'Internet des objets et la mise en réseau de nombreux appareils n'étant jusqu'ici pas connectés, le terrain sur lequel les rançongiciels peuvent encore s'exprimer semble d'ailleurs sans limite. Une fois un système compromis, il est important de s'assurer de maximiser le profit réalisé sur un cas. En bon commerciaux, les criminels appliquent ainsi un approche «orientée client», en établissant des canaux de communication directe (des chats en-direct) avec leurs victimes, afin d'expliquer à ses dernières comment s'acquitter de leur rançon. Par ailleurs, ils cherchent des moyens d'augmenter la pression sur la victime, ne se contentant pas de rendre des données illisibles, mais en menaçant également de dévoiler les plus sensibles d'entre elles.

3.3 Une réussite qui suscite des vocations

Ces attaques sont si profitables qu'elles suscitent malheureusement de nombreuses vocations. Ainsi, les variantes de rançongiciels ne se comptent plus. Ce dynamisme s'observe aussi dans un autre type de cyber-extorsion, s'appuyant cette fois sur des attaques DDoS. Dans ce cas, c'est même tout un environnement aux contours peu clairs qui est apparu. Tout d'abord, de nombreux «copycats», imitant les dépositaires du modus operandi d'origine, ont vu le jour. Ces derniers s'appuient notamment sur l'extrême facilité avec laquelle il est désormais possible de louer un «service» d'attaque DDoS (*booter* ou *stresser*). Plus récemment, d'autres acteurs purement opportunistes se sont montrés particulièrement actifs. Ils se contentent de «surfer sur la vague» en envoyant des courriels de chantage, sans même se donner la peine de procéder à des attaques ni vraisemblablement avoir les capacités de le faire. Usurpant le nom de groupes connus et largement médiatisés (comme Armada Collective), ils espèrent ainsi que la crainte d'une attaque suffira à déclencher un paiement.

Nous sommes ainsi face à des phénomènes extrêmement profitables, attirant différents acteurs criminels, dont certains savent faire preuve d'une très grande inventivité. En conséquence, il est à craindre que ces attaques s'inscrivent dans la durée, en se réinventant continuellement. Mais tout ce marché s'appuie au final sur une unique condition: il est nécessaire d'avoir une masse critique de victimes prêtes à payer, pour que ces groupes trouvent le financement nécessaire au développement de leur activité. Sans cette source de revenu, le système s'écroule. On ne rappellera ainsi jamais assez combien il est important que les victimes ne cèdent pas au chantage opéré. Mais répéter ce message ne suffit pas, il faut en parallèle rappeler les moyens de se prémunir contre ces attaques. Chaque entreprise doit mener une réflexion individuelle, en se posant notamment les questions suivantes: quels systèmes ou informations sont suffisamment sensibles pour m'exposer à un chantage s'ils

sont atteints? Par quelles méthodes est-il possible de les atteindre? Comment ces systèmes ou informations sont-ils protégés? Quelles procédures sont en place pour réagir à une attaque faisant usage d'extorsion? Insuffisamment préparés à ces éventualités, certains utilisateurs ou entreprises prendront malheureusement la décision de payer.

Recommandations:

MELANI propose différents guides en vue d'aider à se protéger contre ces menaces, notamment:

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

Mesures contre les rançongiciels
https://www.melani.admin.ch/melani/fr/home/themen/Ransomware.html

4 Situation nationale

4.1 Espionnage

4.1.1 Turla dans une entreprise d'armement

Selon un communiqué publié le 4 mai 2016 par le Département fédéral de la défense, de la protection de la population et des sports (DDPS)[1], le Service de renseignement de la Confédération (SRC) avait informé en janvier 2016 le Ministère public de la Confédération que des ordinateurs de la société RUAG avaient été infectés par un logiciel espion. Le Ministère public a ouvert une enquête pénale contre inconnu le 25 janvier 2016. Le communiqué du DDPS a rencontré un large écho parmi les médias, et le volet politique du dossier n'est pas encore refermé. La Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) a publié le 23 mai 2016, sur mandat du Conseil fédéral, un rapport technique sur la cyberattaque contre RUAG. Cette mesure visait à donner à d'autres entreprises la possibilité d'analyser leur propre réseau et d'adopter les mesures de protection utiles.[2,3]

Les agresseurs ont utilisé un maliciel de la famille Turla, un cheval de Troie en circulation depuis plusieurs années. La variante observée dans le réseau de RUAG n'avait pas d'outil de dissimulation d'activité (*rootkit*), mais utilisait du code impénétrable pour ne pas être détectée. Les attaquants ont fait preuve de beaucoup de patience pendant l'infiltration et le

1 https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-61618.html (état: le 31 août 2016).
2 https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-61788.html (état: le 31 août 2016).
3 https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-techniques/technical-report_apt_case_ruag.html (état: le 31 août 2016).

mouvement latéral. Ils se sont uniquement attaqués aux cibles qui les intéressaient, en recourant à diverses mesures.

Parmi les principales cibles figurait le service d'annuaire (*Active Directory*). Ce service centralisé permet d'accéder à d'autres applications ou appareils renfermant des données intéressantes, en tirant parti des droits et des groupes d'appartenance. Attentif à dissimuler autant que possible les communications établies, le maliciel s'est servi du protocole HTTP pour transférer les données à plusieurs *serveurs Command & Control (C&C)*. Ces serveurs confiaient de nouvelles tâches aux appareils infectés, comme le téléchargement de nouveaux codes binaires ou fichiers de configuration, ou des travaux par lots (*batch jobs*). Une architecture hiérarchique a ainsi été mise en place, au sein de laquelle les dispositifs infectés ne communiquaient pas tous avec les serveurs C&C. Dans cette répartition des tâches, l'exfiltration incombait à certains systèmes, appelés drones de communication. Les autres, soit les drones de travail, servaient uniquement à dérober les données et à les transmettre aux drones de communication.

Il est difficile d'évaluer les dégâts survenus, et d'ailleurs ce n'était pas l'objet du rapport publié par MELANI. L'analyse des journaux proxy (*proxy logs*) a toutefois montré que les données n'étaient pas accédées en permanence. Les phases de très faible activité, en termes de requêtes et de données exfiltrées, alternaient avec d'autres phases caractérisées par d'incessantes requêtes et de grandes quantités de données exfiltrées.

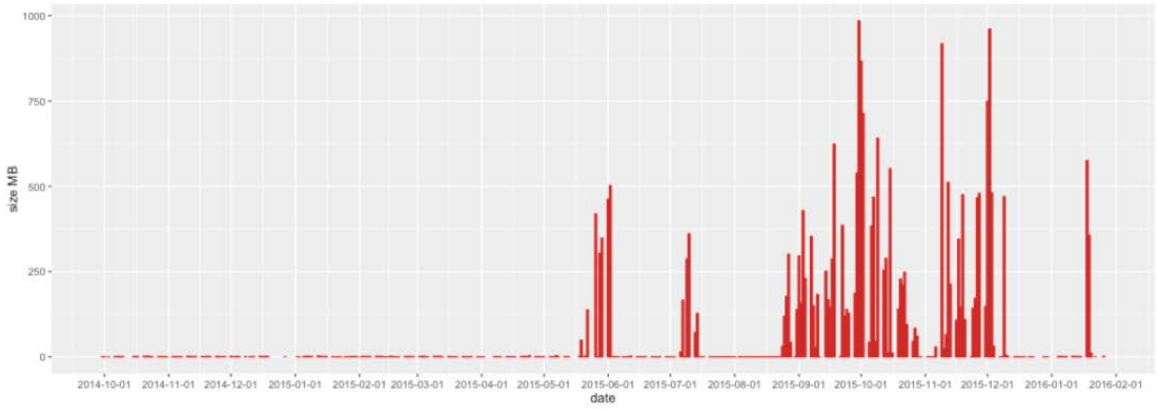


Fig. 1: Quantités de données exfiltrées par jour

Il est difficile d'assurer à une organisation une protection totale contre des attaques aussi sophistiquées. Pourtant, beaucoup de contre-mesures sont peu onéreuses, et leur mise en œuvre implique une charge de travail raisonnable. En particulier, il devient possible de détecter un incident lorsque l'agresseur commet une erreur. D'où l'importance de sensibiliser les collaborateurs, afin qu'ils parviennent à repérer dans les systèmes tout dysfonctionnement ou comportement suspect, à bien l'interpréter et à réagir en conséquence. Une liste des mesures à adopter figure dans le rapport technique publié en anglais par MELANI/GovCERT sur l'affaire d'espionnage de RUAG[4].

Il s'agit également de sensibiliser à l'importance des échanges d'expériences et d'informations avec d'autres entreprises, avec son propre secteur économique ou encore avec l'administration fédérale. Le cercle fermé de MELANI, dont font entre-temps partie plus de 190 exploitants choisis d'infrastructures critiques, est une enceinte privilégiée pour

[4] https://www.melani.admin.ch/melani/fr/home/documentation/rapports/rapports-techniques/technical-report_apt_case_ruag.html, pp. 27 ss (état: le 31 août 2016).

échanger de telles informations entre entreprises, au besoin sous forme anonyme. Le réseau international de MELANI est lui aussi précieux pour identifier les cyberattaques, sachant que les cyber-incidents ne s'arrêtent pas aux frontières. Tous les jours, les indices glanés en Suisse ou à l'étranger peuvent déboucher sur des découvertes capitales. Dans le cadre de ses tâches et de la stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), MELANI favorise l'échange d'informations entre exploitants d'infrastructures critiques, pour qu'à l'avenir toujours plus d'attaques ciblées soient détectées et si possible déjouées.

Le graphique ci-dessous présente la chronologie des événements:

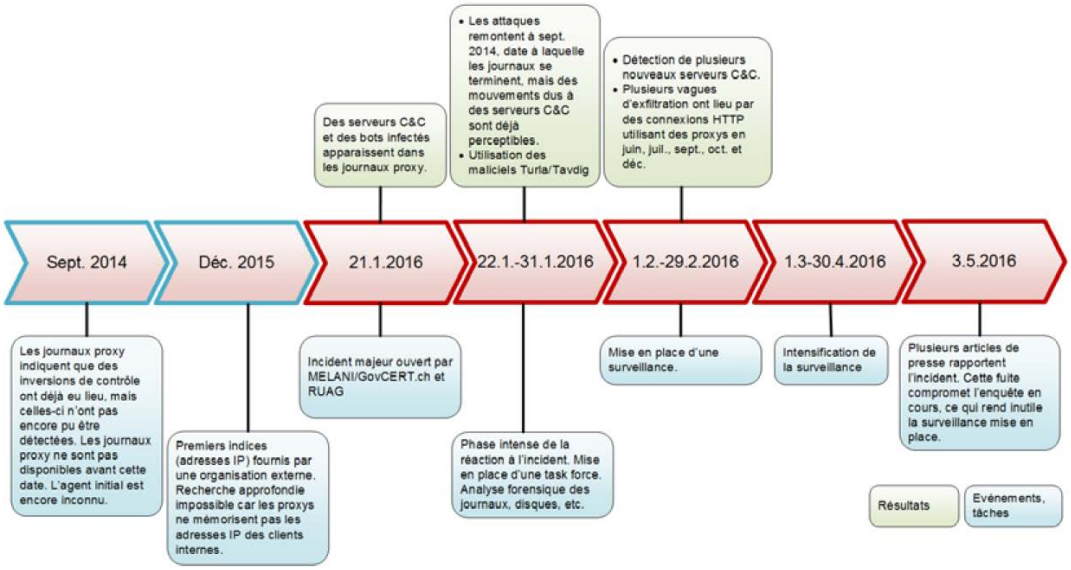


Fig. 2: Étapes de l'élucidation de la cyberattaque

Conclusions et recommandations:

Le cyber-espionnage est une réalité. Il a déjà été question de plusieurs cas dans de précédents rapports semestriels de MELANI. Le rapport annuel du Service de renseignement de la Confédération (SRC) donne également un aperçu de la situation. La prévention est la meilleure protection possible contre des tentatives d'espionnage. Pour une entreprise, la première étape nécessaire consiste à reconnaître l'existence d'un danger bien réel et non hypothétique. Les nombreux cas portés à la connaissance de MELANI attestent de cette prise de conscience. Pour combattre efficacement le cyber-espionnage, il faut que les informations circulent et donc que les cas soient annoncés. Cette démarche permet aux autorités compétentes de prendre des mesures et de tirer les enseignements nécessaires au niveau législatif ou politique. Mais plus encore, en signalant ce type d'informations, les victimes permettent à d'autres organisations de détecter d'éventuelles intrusions dans leur réseau. Le traitement strictement confidentiel de telles informations est ici primordial aux yeux des autorités.

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

Formulaire d'annonce de 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:

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 Mots de passe standard de router

Les *routeurs* de la société UPC sont fournis avec des mots de passe pré-générées par le fabricant. Le nom de réseau sans fil, ou identifiant *SSID*, comprend un nombre aléatoire à sept chiffres. Le mot de passe est généré pour chaque routeur, et donc donne l'impression d'être fortuit. Cependant grâce à une publication qui circule sur Internet depuis le début de l'année, il existe une méthode afin d'établir à partir du nom de réseau sans fil, pour certains appareils UPC, une liste de huit à douze mots de passe pour la clé de cryptage *WPA2*. Il convient de noter que les utilisateurs ayant changé leur mot de passe avant la mise en service n'étaient pas touché par la faille. Outre cette publication, plutôt destiné aux experts, le chercheur a publié sur Internet, quelques jours plus tard, un outil en ligne dont l'utilisation est

à la portée de tout le monde. Il visait par là à montrer que certains fabricants négligeaient la sécurité en générant leurs mots de passe. La faille de sécurité utilisée n'était pas vraiment nouvelle: elle se basait sur une recherche scientifique menée aux Pays-Bas, publiée au début de 2015 et présentée durant l'été à Las Vegas, à une conférence sur la sûreté de l'information.

L'histoire s'est répétée au début de juillet 2016. Le nouvel incident concernait le routeur Ubee EVW3226, également utilisé en Suisse. En l'occurrence, il fallait connaître non pas l'identifiant SSID, mais l'*adresse MAC* de l'appareil. Divers outils permettent de l'établir sans grande difficulté, dans le rayon de couverture d'un réseau sans fil. Concrètement, il était possible de retrouver à partir de cette information le mot de passe ainsi que l'identifiant SSID pré-générés. Dans ce cas aussi, uniquement les utilisateurs n'ayant pas changé leur mot de passe initial alors que cela était recommandé étaient touchés.

Conclusions et recommandations:

Les mots de passe standard sont à éviter spécialement dans l'environnement informatique. Cela d'autant plus lorsque l'accès aux appareils se fait depuis Internet ou par signal radio. Bien des fabricants ont réagi en remplaçant la combinaison usuelle «123456» par un mot de passe pré-généré individuel. Il est d'autant plus irritant que ce code individuel préréglé puisse être reconstitué par des tiers, et qu'il en résulte une faille de sécurité. La règle consistant à modifier respectivement individualiser le mot de passe lors de la mise en service d'un appareil et avant son raccordement à Internet reste par conséquent d'actualité. La plupart des appareils possèdent d'ailleurs une fonction de réinitialisation en cas d'oubli du mot de passe. Mais pour cela, il faut être présent sur place et le plus souvent appuyer sur un bouton de réinitialisation situé sur le boitier. Il est recommandé de changer le mot de passe standard tant pour les appareils que pour les logins afin d'accroître sa sécurité personnelle. Ce n'est pas seulement plus sûr mais aussi plus simple pour l'utilisation quotidienne.

4.2.2 Mots de passe de 6000 comptes de messagerie suisses mis en circulation

Le 16 mars 2016, MELANI a reçu une liste de 6000 combinaisons d'adresses électroniques et de mots de passe piratées par des escrocs. Ces comptes auraient pu être utilisés à des fins illégales (escroquerie, chantage, phishing, etc.), si leur propriétaire n'avait pas aussitôt modifié son mot de passe. MELANI a donc publié un outil en ligne, permettant à chacun de vérifier si son compte de messagerie était concerné. Pour le savoir, il suffisait d'entrer l'adresse électronique. Cette dernière était transmise sous forme chiffrée, sans être enregistrée.

Les réactions à cette action ont été le plus souvent positives. Mais des voix critiques se sont aussi élevées, et un certain nombre d'internautes ont voulu savoir si la page visait un but légitime et si elle émanait bien de MELANI. On ne peut que se féliciter d'une telle réaction, dans une optique de sensibilisation et de prévention. Une saine prudence est indiquée dans ce contexte et il est certainement utile de poser des questions pour vérifier l'authenticité d'un site. Dans le cas présent, MELANI a jugé que la publication rapide de cet outil en ligne constituait la solution la plus pratique et la plus efficace pour que les personnes potentiellement concernées puissent en avoir le cœur net.

4.2.3 Piratage de la base de données de l'UDC

À la mi-mars 2016, une cyberattaque lancée contre une banque de données de l'Union démocratique du centre (UDC) a permis de copier 50 000 adresses électroniques. Un groupe se dénommant NSHC a revendiqué l'attaque. Comme il l'a confié au magazine inside-channels.ch, il souhaitait montrer que la Suisse n'est pas suffisamment protégée contre les cyberattaques.[5] Le groupe se réclame des *grey hats*, pirates bafouant la loi sans vouloir pour autant causer de dommage direct. Il a également revendiqué les attaques *DDoS* lancées durant la même semaine contre Interdiscount, Microspot et les CFF. Là encore, ses motifs semblent avoir été de réveiller les responsables de la sécurité informatique. On ignore toutefois si ce groupe a réellement les compétences requises pour lancer des attaques DDoS ou s'il n'a revendiqué que par opportunisme quelques-unes des attaques DDoS particulièrement nombreuses survenues en mars. Le groupe NSHC ne s'était pas manifesté jusque-là et n'a plus fait parler de lui par la suite.

4.3 Systèmes de contrôle industriels

Aujourd'hui, lorsqu'une page Internet ou un service en ligne ne sont pas accessibles, on pense immédiatement à une cyberattaque. Pourtant, les dérangements techniques restent parmi les principales causes de défaillance des *systèmes de contrôle industriels (SCI)*. L'incident suivant, qui remonte à longtemps déjà, en est la preuve éclatante. Le réseau électrique des CFF s'est effondré le 22 juin 2005. Des travaux de construction avaient abouti à la mise hors service de deux des trois lignes électriques transalpines, et on avait surévalué la capacité de transport de la troisième. Après son déclenchement pour des raisons de sécurité, les réseaux électriques au Nord et au Sud des Alpes se sont retrouvés séparés. Sans avoir la même ampleur, les événements du premier semestre 2016 ont été lourds de conséquences et ont bien montré notre dépendance des moyens de communication modernes.

4.3.1 Terminaux de paiement hors service

Le 20 juin 2016, les paiements sans argent liquide ont été entravés. Les prestataires utilisant un *terminal de paiement* fourni par l'entreprise SIX ont été touchés, dans toute la Suisse et en Autriche également. L'identification de la panne a été d'autant plus compliquée que le problème n'était présent ni partout, ni en permanence. Une erreur au niveau du réseau était en cause.

4.3.2 Clientèle commerciale privée d'accès à Internet

Un mois plus tôt, Swisscom avait rencontré des problèmes. Une grave panne a affecté ses clients commerciaux. Le 24 mai 2016 à midi, divers clients ont été privés d'accès à Internet. Des distributeurs de billets ont aussi été touchés. Le dérangement a finalement pu être attribué à l'accès à la plateforme Ethernet de Swisscom, dans la région lausannoise.

4.3.3 Incendie criminel de câbles des CFF

La panne qui a paralysé le trafic ferroviaire entre l'aéroport et le centre-ville de Zurich était par contre due à un acte de sabotage commis près de Zürich Oerlikon. Le 7 juin au petit ma-

[5] http://www.inside-it.ch/articles/43272 (état: le 31 août 2016).

tin, des inconnus ont bouté le feu à deux endroits : ils avaient réussi à pénétrer sur un terrain appartenant aux CFF, et les flammes ont endommagé des câbles enterrés parallèles aux voies. C'est uniquement grâce à l'effort manuel considérable que les câbles ont pu être réparé au fur et à mesure dans la journée. Mais la ligne ferroviaire pour l'aéroport de Zürich est restée fermée jusqu'au soir.

Conclusion:

Outre les attaques électroniques, il ne faut pas perdre de vue le risque de sabotage physique d'équipements électroniques. En particulier, il n'est que ponctuellement possible de protéger les câbles électriques et de télécommunications sur une bonne partie de leur parcours. Les interventions physiques n'ont certes généralement qu'un impact local. Il ne faut pas pour autant se limiter à protéger sur le plan électronique les points ou systèmes névralgiques, il faut également le faire sur le plan physique.

4.4 Cyberattaques

Les citoyens comme les entreprises suisses restent en butte à différents types d'attaques, ayant notamment pour cible leur site web. 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

Le modus operandi intégrant chantage et menace d'attaque DDoS s'inscrit dans la tendance large de l'extorsion, thème prioritaire du présent rapport. Les groupes DD4BC et Armada Collective ont déjà fait l'objet de chapitres dans de précédents rapports semestriels (2015/1 et 2015/2). Ces criminels procédaient selon un mode opératoire désormais largement connu et documenté: après une première attaque DDoS faisant office de démonstration, les attaquants effectuent un chantage auprès de la victime. Si une somme en BitCoins ne leur est pas versée dans un délai donné, ils menacent de procéder à une deuxième attaque nettement plus forte que la première.

L'année 2016 a débuté par une information majeure sur le plan de la poursuite pénale. En effet, Europol a annoncé en janvier avoir procédé à l'arrestation de deux membres de DD4BC[6]. Dès lors, aucune attaque au nom de Armada Collective ou DD4BC et répétant le modus operandi «d'origine» tel qu'il est décrit ci-dessus n'a été observée. Ce constat accrédite la thèse selon laquelle Armada Collective et DD4BC seraient une seule et même entité, dont des membres importants sont désormais derrière les barreaux.

[6] https://www.europol.europa.eu/content/international-action-against-dd4bc-cybercriminal-group (état: le 31 août 2016).

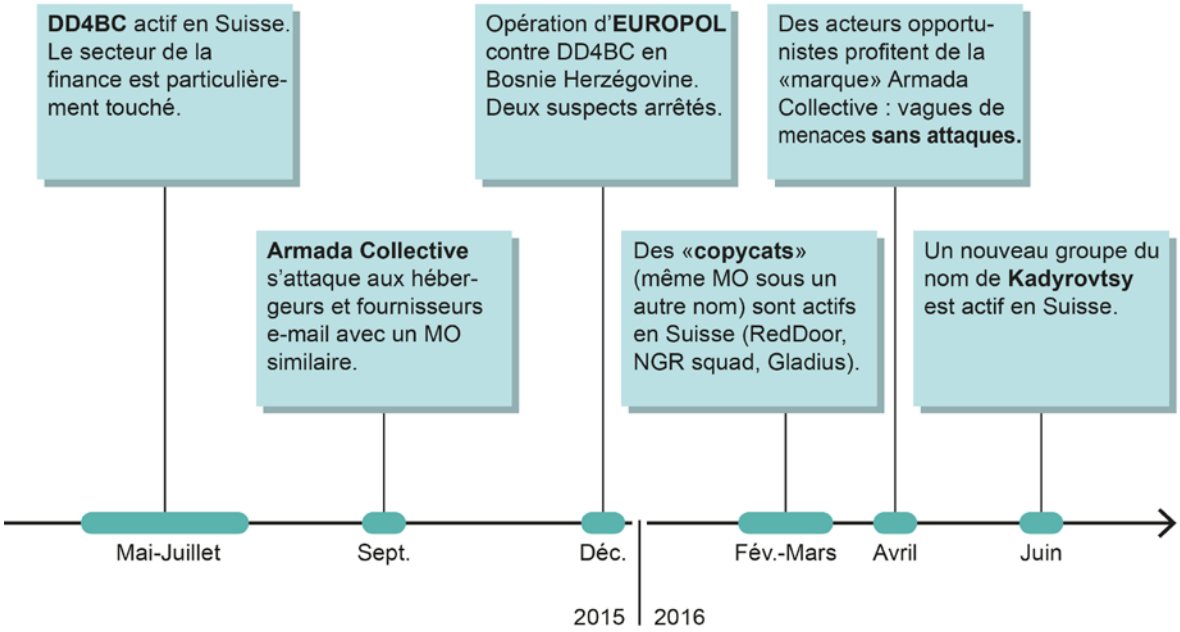


Fig. 3: DDoS et extorsion: timeline

Si ce coup de filet a changé le visage de la menace, d'autres groupes empruntant en partie les mêmes méthodes sont par la suite entrés en scène. Tout d'abord, différents groupes ont mené des attaques selon le modus operandi typique de DD4BC/Armada Collective, à savoir une attaque DDoS de démonstration suivie d'un chantage. Ces groupes ont opéré entre mars et juin sous les noms de RedDoor, NGR Squad, Gladius et Kadyrovtsy. On peut les considérer comme des «copycats», reprenant une méthode ayant fait ses preuves. Mais le phénomène le plus marquant des six premiers mois de l'année est l'apparition de groupes purement opportunistes, empruntant le nom d'Armada Collective pour diffuser des courriels de chantage en menaçant de mener des attaques DDoS. En réalité, ces groupes n'avaient ni la capacité ni l'intention de mener ce type d'attaques, même à des fins de démonstration. En revanche, comme différents articles avaient paru sur Armada Collective, ils cherchaient à profiter de la crainte suscitée par ce groupe pour récolter de l'argent. Bien souvent, les adresses BitCoin attribuées aux victimes étaient identiques. D'où l'impossibilité de savoir qui a payé ou, faute d'avoir payé la rançon, doit être attaqué. Par ailleurs, un grand nombre de cibles étaient fréquemment menacée d'attaques à une même date. En pareil cas, l'hypothèse d'un acteur purement opportuniste est la plus probable. Il est amusant de constater qu'une personne se réclamant du groupe Armada Collective a même écrit à MELANI pour se plaindre de l'usurpation éhontée de la marque Armada Collective:

> I'm member of original Armada Collective and I have just noticed your report on Twitter. Armada Collective is dead. We have stopped all operations, because it wasn't profitable enough and risk was too big. When I realized that somebody is using our name I got mad. It is obviously an amateur copycat using our name who copied our text (maybe from your site) and is probably not even capable of launching DDoS attacks. Good luck with your investigation.

Fig. 4: Message reçu par MELANI à travers son formulaire d'annonce

L'augmentation de ces différentes activités montre à quel point l'extorsion est une méthode rentable pour les criminels. Les derniers développements prouvent par ailleurs que les criminels peuvent s'appuyer sur des attaques concrètes, mais également sur la crainte des dommages causés par une attaque hypothétique. Dans quelle mesure les rapports détaillant

l'activité de ces acteurs représentent-ils une source d'inspiration? De notre point de vue, il est nécessaire d'informer sur ces modes opératoires. On ne peut cependant pas exclure qu'un «bruit médiatique» intense ne suscite également des vocations, et surtout ne permette aux attaquants de s'appuyer sur la notoriété publique acquise par un groupe ou un mode opératoire. Quoi qu'il en soit, dans de telles situations où un grand nombre d'entreprises reçoivent simultanément des courriels de chantage similaires, il faut rappeler l'importance du partage d'information et du signalement des incidents. En effet, en faisant remonter l'information auprès d'une unité comme MELANI, on rend possible l'établissement d'une vue d'ensemble, permettant de mieux évaluer la situation au regard d'autres cas similaires. C'est alors que des éléments comme les adresses BitCoins ou les dates d'attaques annoncées ont une grande valeur. Enfin, rappelons que la protection contre les attaques DDoS doit rester une priorité, puisqu'il s'agit d'une arme à laquelle de nombreux attaquants aux motivations variées peuvent recourir.

Recommandations:

Lorsqu'une attaque DDoS prend une entreprise au dépourvu, il est généralement trop tard pour y réagir de manière rapide et efficace. Les entreprises pour lesquelles Internet est le principal canal de vente devraient en priorité garantir ce processus de gestion sensible. D'où l'importance d'élaborer en amont une stratégie spécifique face aux attaques DDoS. Les services tant internes qu'externes compétents, ainsi que les autres personnes habilitées à agir en cas d'attaque doivent être connus. Dans l'idéal, une entreprise devrait prendre des mesures de prévention avant même d'avoir subi une attaque DDoS. Ces mesures s'inscriront dans la gestion générale des risques au niveau de la direction. Un certain niveau de préparation aux attaques DDoS s'impose encore sur le plan de l'exploitation. Toute organisation peut être la cible d'une attaque DDoS. Nous vous conseillons donc de parler avec votre fournisseur Internet de vos besoins et des mesures préventives proposées. Le site MELANI propose une liste de contrôle, avec des instructions sur les mesures à prendre contre les attaques DDoS, à l'adresse suivante:

DOCU

Mesures à prendre contre les attaques DDoS:

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

4.4.2 Infection du site 20min.ch[7]

Au semestre dernier déjà, le cheval de Troie bancaire Gozi ISFB s'était propagé sur divers portails d'information en ligne du groupe Tamedia. Le précédent rapport semestriel MELANI

[7] http://www.srf.ch/news/schweiz/nach-malware-attacke-auf-20-minuten-was-sie-jetzt-tun-koennen
http://www.20min.ch/digital/news/story/20minuten-ch-erneut-Ziel-von-Malware-Attacke-15457508
http://www.nzz.ch/digital/malware-auf-20minch-tamedia-gab-zu-frueh-entwarnung-ld.12431
http://www.tagesanzeiger.ch/digital/internet/Erneut-ein-Trojaner-auf-20minutench/story/19684342 (état: le 31 août 2016).

s'est fait l'écho de cet incident.[8] L'incident s'est répété au début d'avril, mais sur le site du quotidien gratuit 20 minutes, lui aussi propriété du groupe Tamedia. L'administration fédérale et diverses entreprises ont provisoirement bloqué l'accès au site 20min.ch dès le 7 avril, et la mesure a été signalée à Tamedia. L'incident découvert par MELANI provenait d'un élément *JavaScript*, introduit dans un fichier multimédia (*fichier d'animation SWF)* de ce site d'information web. Lors de sa consultation, le script s'activait et redirigeait le visiteur vers le *kit d'exploits* Niteris, qui téléchargeait automatiquement le cheval de Troie Gozi sur l'ordinateur de la victime. Or à peine nettoyé de l'infection, le site était à nouveau compromis quelques jours plus tard. Dans ce second cas, la cible n'était pas directement le site 20min.ch, mais le réseau d'un démarcheur externe dont les annonces publicitaires s'affichaient sur le site Internet du quotidien. Le cheval de Troie Bedep se propageait par l'intermédiaire du kit d'exploits Angler, qui a servi à lancer des attaques similaires sur les sites nytimes.com et bbc.com.[9] Des millions d'internautes cliquent chaque jour sur l'édition électronique des journaux quotidiens. Ce sont donc des cibles idéales pour les infections par drive-by-download. Un tel mode opératoire est toujours plus fréquent en Suisse depuis le printemps 2015. [10] Selon le quotidien gratuit 20 minutes, ses propres serveurs sont attaqués à tout moment, de 20 à 50 fois par jour.[11]

Recommandations:

Pour éviter de telles infections au niveau des clients finaux, il est recommandé de mettre régulièrement à jour – si possible de façon automatique – les systèmes d'exploitation et les applications. Limitez tant que possible l'exécution de JavaScript (*active scripting*) à travers les paramètres du navigateur ou certains modules (*plugins*), voire désactivez-le complètement. En cas de désactivation, il faut cependant être conscient que de nombreux sites web ne pourront plus fonctionner correctement. Si cette mesure s'avère trop contraignante, vous pouvez assouplir les limitations progressivement jusqu'à un niveau acceptable. Suivant la solution choisie, il est par ailleurs possible de définir sur quels sites web vous autorisez l'exécution de JavaScript (*whitelisting*).

Si vous avez l'impression que votre ordinateur est infecté, faites-le examiner par un spécialiste, qui le cas échéant le nettoiera ou réinstallera le système d'exploitation.

Règles de comportement ➔ Navigation:

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

---

8 MELANI, rapport semestriel 2015/2, chap. 4.3.1.1 https://www.melani.admin.ch/melani/fr/home/dokumentation/berichte/lageberichte/halbjahresbericht-2-2015.html (état: 31 août 2016).

9 http://www.nzz.ch/digital/newssite-gesperrt-mittels-20minch-malware-verbreitet-ld.12263 (état: le 31 août 2016).

10 https://www.govcert.admin.ch/blog/21/20min.ch-malvertising-incident (état: le 31 août 2016). https://www.govcert.admin.ch/blog/13/swiss-advertising-network-compromised-and-distributing-a-trojan https://www.govcert.admin.ch/blog/18/gozi-isfb-when-a-bug-really-is-a-feature (état: le 31 août 2016).

11 http://www.20min.ch/digital/news/story/Keine-Gefahr-fuer-die-Nutzer-der-20-Min-App-10440966 (état: le 31 août 2016).

4.4.3 OpnessunDorma d'Anonymous contre les portails d'emploi au Tessin et en Italie

Quelque 37 portails d'emplois italiens et sept d'autres pays (dont quatre tessinois) ont été victimes d'une cyberattaque entre le 9 et le 11 avril 2016. Les sites web des entreprises ont été défigurés, et des millions de données pillées. Les groupes Anonymous Italia et LulzSecITA ont revendiqué le méfait. Ils ont publié les données de connexion des utilisateurs, ainsi que des informations sur la structure de différentes banques de données et les noms de documents de plusieurs milliers de curriculums vitae (sans en révéler toutefois le contenu). Les deux organisations ont justifié leur démarche par deux arguments: d'abord, il s'agissait de montrer que «les services de placement sont des parasites exploitant les travailleurs». Ensuite, les pirates voulaient révéler la fragilité et la sécurité insuffisante des plateformes informatiques sur lesquelles sont sauvegardées les données des utilisateurs.[12] ticinoonline.ch a publié une copie d'écran du portail d'emploi défiguré de l'Association des industries tessinoises (Associazione industrie Ticinesi AITI), e-lavoro.ch, victime de l'attaque au même titre que BFKconsulting.ch, helvia.com et workandwork.ch.[13] Il y est reproché aux victimes tessinoises de céder à l'idéologie xénophobe et raciste des partis suisses de droite, en publiant des offres d'emploi ne s'adressant qu'à la population résidante suisse.[14]

4.4.4 Pirate à l'EPF de Zurich

En janvier 2016, un pirate ayant subtilisé les données d'accès de tiers a sévi pendant plusieurs jours dans le réseau de l'EPF de Zurich, commandant des logiciels par l'intermédiaire du système de l'EPF et téléchargeant des données sensibles. Quand l'EPF a découvert l'utilisation abusive de son réseau, elle a alerté la procureure du centre de compétence Cybercrime à Zurich, qui a aussitôt adopté avec les enquêteurs de police de premières mesures de protection et diligenté les investigations. L'auteur présumé a été arrêté dix jours seulement après l'ouverture de l'enquête et se trouve en détention préventive. Une procédure pénale a été ouverte pour accès indu à un système informatique et soustraction de données.[15]

4.5 Social Engineering, phishing

Outre les attaques techniques en tous genres, les attaquants cherchent aussi à exploiter les faiblesses humaines.

---

12 https://share.cyberguerrilla.info/?3263d9dcba87924c#nxVUhZU/s/diAc9ZJ1v+cjkH1F+oT3K+iiljOHLLT+0= (état: le 31 août 2016).

13 http://www.rsi.ch/news/ticino-e-grigioni-e-insubria/Siti-ticinesi-hackerati-7176668.html (état: le 31 août 2016). http://www.radiondadurto.org/2016/04/12/anonymous-italia-operazione-nessundorma-e-la-violazione-della-legge-sulla-privacy/ (état: le 31 août 2016). http://www.tio.ch/News/Ticino/Cronaca/1079978/Attacco-hacker-colpiti-4-siti-ticinesi--Rubati-milioni-di-dati/ (état: le 31 août 2016).

14 Il est notamment fait mention d'un groupe actif dans la production et la vente de prothèses orthopédiques.

15 https://www.ethz.ch/de/news-und-veranstaltungen/eth-news/news/2016/02/mm-mutmasslicher-hacker-verhaftet.html (état: le 31 août 2016).

4.5.1 Statistiques de phishing

Ces dernières années, le nombre de demandes liées au *phishing* a fortement augmenté. Soucieuse de traiter plus efficacement les annonces entrantes, la centrale MELANI a mis en place le site «antiphishing.ch» en 2015, où chacun peut signaler des sites de phishing. Au total, 2343 sites de phishing uniques ont été dénoncés sur ce portail au premier semestre 2016. La fig. 5 indique le nombre d'annonces hebdomadaires de pages de phishing, qui fluctue beaucoup au fil du temps. 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.

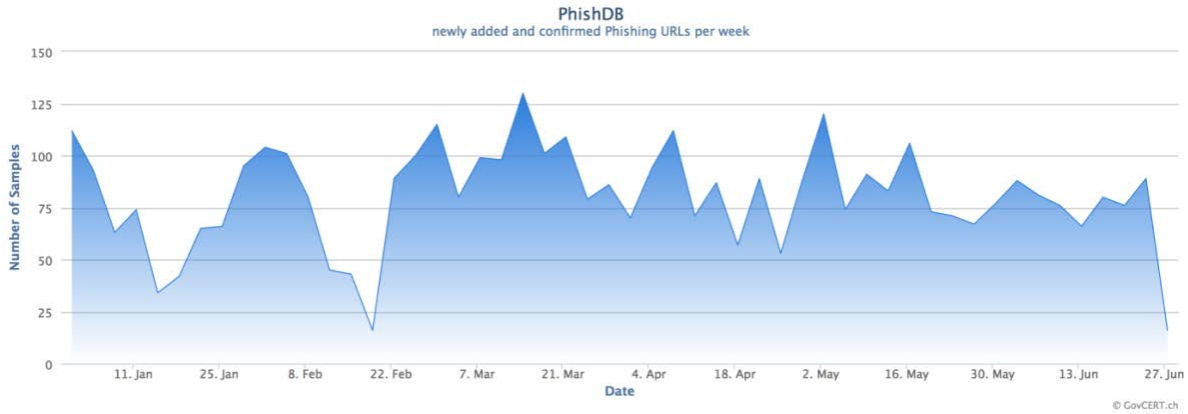


Fig. 5: Sites de phishing annoncés et confirmés par semaine sur le site antiphishing.ch

4.5.2 L'arnaque CEO Fraud se perfectionne et s'installe dans la durée

Le mode opératoire de l'arnaque au président (CEO Fraud) a déjà été plusieurs fois évoqué dans le cadre de Newsletters ou d'autres rapports semestriels de MELANI. Concrètement, l'identité d'un dirigeant d'entreprise est usurpée et le service compétent (service financier, comptabilité) est prié en son nom de procéder à un versement sur un compte (typiquement) à l'étranger. La plupart du temps, la demande est effectuée depuis une adresse courriel falsifiée, mais des cas de compromission d'un compte existant ont aussi été observés. Les raisons invoquées varient, mais incluent souvent une opération financière urgente et extrêmement sensible (acquisition notamment). Le recours à un consultant ou à un cabinet d'avocat factice ou dont l'identité a également été usurpée peut intervenir dans le scénario. Les attaquants savent mettre une pression importante sur l'employé visé, prétextant une situation urgente, pour le contraindre à effectuer le versement et parfois à contourner les processus existants.

Au cours des six mois sous revue, certains cas ont fait la une des médias à l'étranger. À l'instar de l'entreprise autrichienne active dans l'aérospatiale FACC, qui a perdu 42 millions d'euros dans une telle arnaque, avec comme conséquence de se séparer de son CEO[16]. En Suisse également, de nombreux cas ont été portés à la connaissance de MELANI. Que cela soit en Suisse ou dans d'autres pays, ce type de fraude est loin de faiblir et semble plutôt se perfectionner afin d'atteindre une plus grande efficacité et de s'installer dans la durée. C'est d'ailleurs typique des groupes criminels actifs sur Internet: lorsqu'un mode opératoire a fait ses preuves, il est conservé et amélioré encore aux différents stades de l'escroquerie.

16 http://www.reuters.com/article/us-facc-ceo-idUSKCN0YG0ZF (état: le 31 août 2016).

Les réseaux sociaux facilitent grandement la recherche initiale d'informations. LinkedIn est particulièrement intéressant pour les escrocs, qui y recherchent par exemple des informations sur les relations commerciales ou l'identité et la fonction des employés. Le registre du commerce, ou tout simplement le site web de l'entreprise, peuvent également contenir de précieux renseignements. Si les informations nécessaires à monter l'escroquerie ne sont pas disponibles en ligne, les criminels peuvent procéder à de premières prises de contact par téléphone. Des fax à l'en-tête d'une administration cantonale ont parfois été envoyés. Parmi les informations recherchées figurent notamment les coordonnées précises des employés du département comptabilité, puisque c'est au final vers eux que seront dirigées les demandes frauduleuses de virement. Ces premières prises de contact permettront d'envoyer des courriels extrêmement ciblés, présentant des situations tout à fait plausibles pour l'entreprise visée.

Pour envoyer des courriels ayant une apparente légitimité, les escrocs utilisent notamment des noms de domaines proches de celui de l'entreprise cible. Pour le seul mois de juin 2016, MELANI a eu connaissance de l'enregistrement simultané de 20 noms de domaines imitant ceux d'entreprises suisses. En envoyant des courriels depuis ces domaines, les escrocs cherchent à tromper le destinataire, qui pensera être en contact avec l'entreprise légitime. Un autre type d'courriel largement utilisé par les escrocs fait référence à une position ou profession intervenant à différents stades, selon l'identité usurpée, comme «lawyer.com», «president.com» ou «consultant.com».

Recommandation:

Il est très difficile d'empêcher ces tentatives de se produire. Les escrocs peuvent masquer leur identité et origine et facilement changer d'adresse courriel s'il le faut. En termes de prévention, il est vivement recommandé de mettre un accent particulier sur la sensibilisation du personnel à ces phénomènes, notamment aux postes clefs. Les règles de base consistent à ne fournir aucune information et à ne procéder à aucune action lors de prises de contact semblant douteuses ou inhabituelles, même lorsque l'on est mis sous pression. Il est recommandé également de contrôler quelles informations sont disponibles en ligne sur l'entreprise. Enfin, les processus doivent être définis et suivis par tous et en tout temps. Pour les transferts d'argent, une procédure de signature collectiveest recommandée.

4.6 Logiciels criminels (crimeware)

L'expression *crimeware* désigne tout logiciel malveillant spécialement conçu par des fraudeurs pour automatiser la cybercriminalité économique. Au premier semestre 2016, la plupart des infections restent 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. Des changements sont toutefois apparus dans les premières places du classement, où en pourcentage les Spambots ont supplanté les chevaux de Troie bancaires. Le maliciel lethic, à la deuxième place, diffuse des pourriels vantant des médicaments et de la publicité pour des produits de contrefaçon. Sur la dernière marche du podium, Necurs s'est spécialisé dans la diffusion aussi bien de Locky, rançongiciel opérant comme un cheval de Troie, et de Dridex, maliciel dirigé contre les logiciels de paiement hors ligne. Il est frappant de voir que le cheval de Troie bancaire Dyre a chuté du classement. Les arrestations liées à Dyre l'ont quasiment neutralisé, du moins à court terme. Des précisions figurent au chapitre 5.5.3.

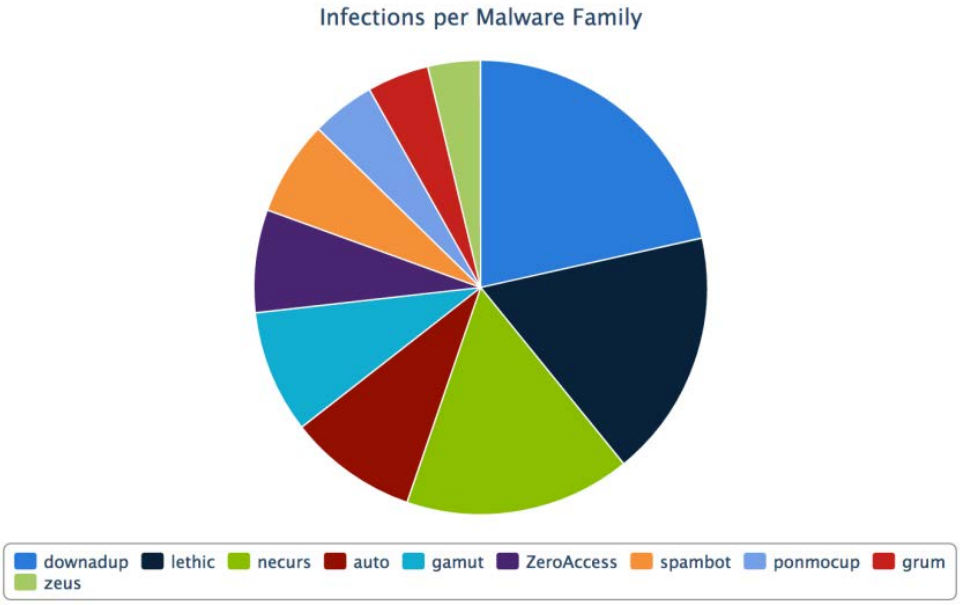


Fig. 6: Répartition des maliciels en Suisse, selon les informations en possession de MELANI. Date de référence: le 30 juin 2016. Des données actuelles sont publiées sous: http://www.govcert.admin.ch/statistics/dronemap/

4.6.1 Essor en Suisse des applications Android malveillantes

En juin et juillet 2016, des milliers de SMS envoyés à des destinataires en Suisse prétendaient provenir de La Poste, mais renfermaient un lien à un site web basé en Lettonie. En cliquant sur le lien, la victime était redirigée vers un site web piraté, où elle était priée d'installer une application Android malveillante[17]. Si elle ignorait les conseils de prudence d'Android s'affichant à l'écran et installait l'App, un maliciel infectait son appareil.

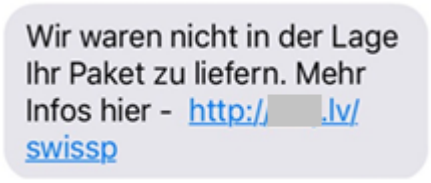


Fig. 7: SMS frauduleux indiquant comme expéditeur La Poste

Le maliciel camouflé sous le nom «*SwissPost*» utilisait le logo de La Poste. L'app copiait en arrière-plan, à l'insu de l'utilisateur, les données d'accès d'apps populaires comme Facebook, Uber ou Viber, avant de les transmettre aux escrocs.

[17] https://www.govcert.admin.ch/blog/24/sms-spam-run-targeting-android-users-in-switzerland (état: le 31 août 2016).

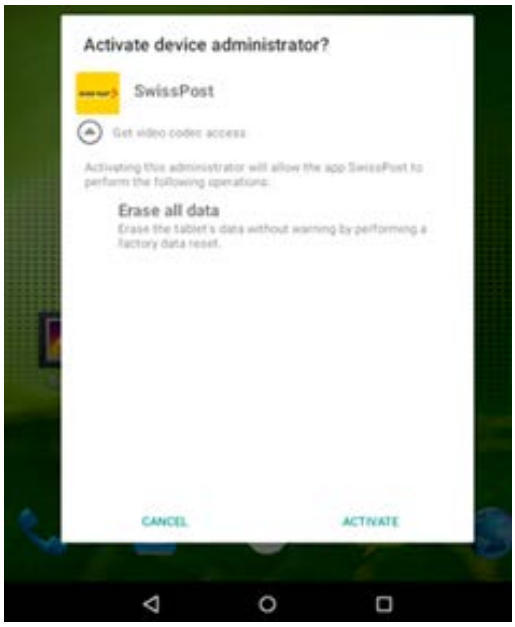


Fig. 8: Maliciel déguisé en App de la Poste Suisse

Recommandations:

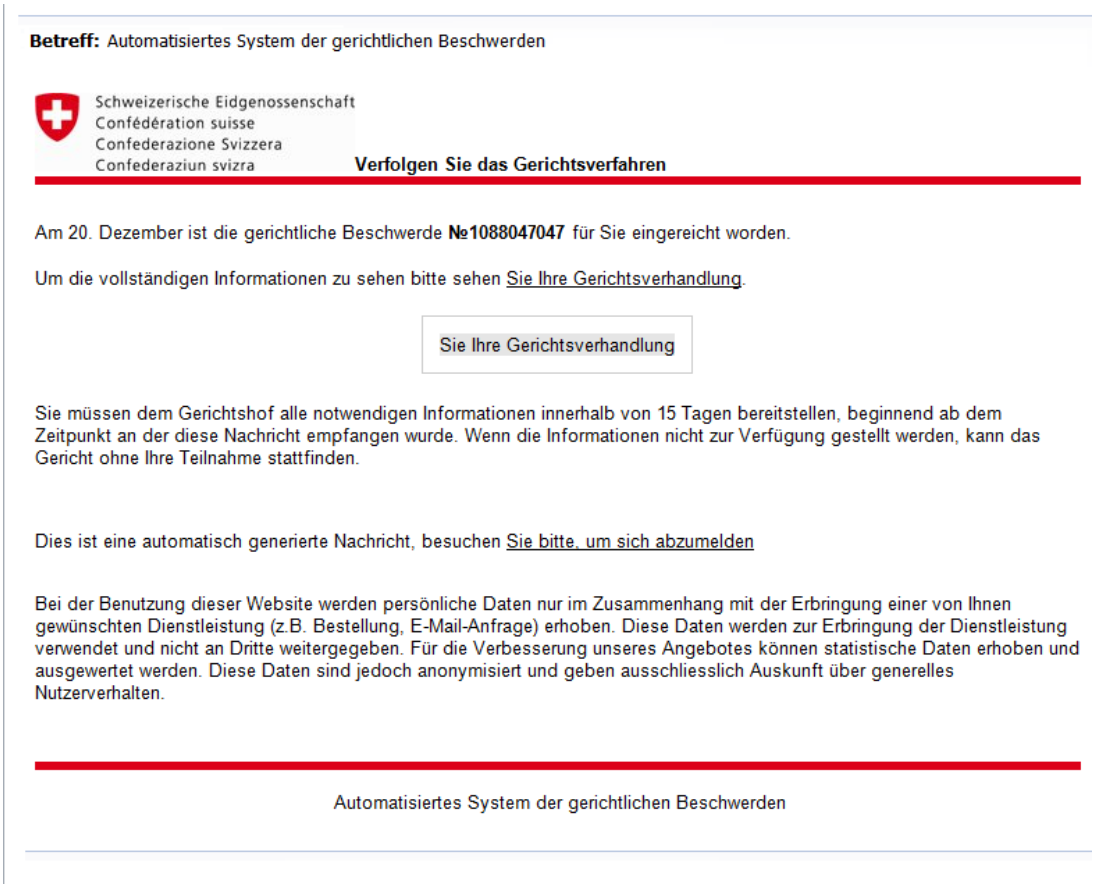
En règle générale, il ne faut jamais installer d'app provenant de sources tierces. Il est recommandé de s'approvisionner uniquement dans l'App Store officiel du fabricant.

4.6.2 Fausse convocation menant à un cheval de Troie chiffrant les données

La menace due aux *chevaux de Troie chiffrant les données* a augmenté durant la période sous revue. La simplicité de la procédure et la tentation toujours trop grande des victimes de céder aux demandes de rançon ont contribué à l'essor actuel des *rançongiciels*.

Pour amener l'utilisateur à cliquer sur un lien figurant dans un courriel ou à ouvrir des annexes et à installer ainsi le rançongiciel sur son ordinateur, l'agresseur doit rendre sa démarche plausible. Dans bien des cas, le message est censé provenir d'une institution que le destinataire connaît et qu'il juge digne de confiance. Il ne se méfiera donc pas. MELANI a signalé un tel incident en janvier 2016, dans la rubrique GovCERT Blog[18]: il était question d'une vague de courriels diffusant le rançongiciel TorrentLocker. Le courriel frauduleux indiquait au destinataire qu'une plainte avait été déposée contre lui et qu'il était convoqué au tribunal pour une audience. Pour en savoir plus, le destinataire devait cliquer sur un lien et télécharger des documents. Les escrocs misaient ici non seulement sur la bonne réputation d'une autorité, mais aussi sur la peur et l'insécurité des gens. L'intimidation constitue un bon moyen d'amener la victime à cliquer sur un lien. Or un tribunal ne se servira jamais de la messagerie électronique pour transmettre une convocation officielle.

[18] https://www.govcert.admin.ch/blog/17/torrentlocker-ransomware-targeting-swiss-internet-users (état: le 31 août 2016).



Betreff: Automatisiertes System der gerichtlichen Beschwerden

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Verfolgen Sie das Gerichtsverfahren

Am 20. Dezember ist die gerichtliche Beschwerde **№1088047047** für Sie eingereicht worden.

Um die vollständigen Informationen zu sehen bitte sehen Sie Ihre Gerichtsverhandlung.

Sie Ihre Gerichtsverhandlung

Sie müssen dem Gerichtshof alle notwendigen Informationen innerhalb von 15 Tagen bereitstellen, beginnend ab dem Zeitpunkt an der diese Nachricht empfangen wurde. Wenn die Informationen nicht zur Verfügung gestellt werden, kann das Gericht ohne Ihre Teilnahme stattfinden.

Dies ist eine automatisch generierte Nachricht, besuchen Sie bitte, um sich abzumelden

Bei der Benutzung dieser Website werden persönliche Daten nur im Zusammenhang mit der Erbringung einer von Ihnen gewünschten Dienstleistung (z.B. Bestellung, E-Mail-Anfrage) erhoben. Diese Daten werden zur Erbringung der Dienstleistung verwendet und nicht an Dritte weitergegeben. Für die Verbesserung unseres Angebotes können statistische Daten erhoben und ausgewertet werden. Diese Daten sind jedoch anonymisiert und geben ausschliesslich Auskunft über generelles Nutzerverhalten.

Automatisiertes System der gerichtlichen Beschwerden

Fig. 9: Le destinataire est informé qu'il fait l'objet d'une plainte en justice. Pour en savoir plus, il est invité à cliquer sur un lien et à télécharger des documents. Ces documents renferment un maliciel.

4.6.3 Postulations spontanées avec rançongiciel

D'autres méthodes appréciées pour amener les destinataires à cliquer sur un lien ou à ouvrir un fichier consistent à mettre l'accent sur les intérêts ou les besoins de la victime, ou à gagner sa confiance, par exemple en l'appelant par ses nom et prénom. Des courriels envoyés en mai dernier en Suisse ont précisément recouru à ces méthodes. Des victimes spécialement choisies recevaient des courriels contenant des postulations spontanées. Pour accéder au dossier complet, les destinataires devaient cliquer sur le lien indiqué. Or le lien Dropbox conduisait directement à Petya et Mischa, deux chevaux de Troie chiffrant les données. Ces derniers temps le maliciel Locky, qui continue de sévir tant en Suisse qu'à l'étranger, se dissimule derrière des postulations spontanées en apparence inoffensives.

4.6.4 Rançongiciel – aspects techniques

Sous l'angle technique, c'est surtout la version 3.1 de CryptXXX qui a retenu l'attention au premier semestre. Ce *virus* crypte non seulement les données se trouvant sur l'ordinateur de la victime, ainsi que celles enregistrées sur les supports de stockage lui étant connectés; il

est également en mesure de dérober des mots de passe et d'autres données d'accès, en téléchargeant un autre *maliciel* («stiller.dll»).[19]

CTB-Locker, rançongiciel ayant sévi principalement en été 2014, est réapparu. Il s'agit d'une nouvelle version ayant pour spécialité de crypter le contenu de sites web. On ignore encore avec quelle méthode le virus se répand. Mais des analyses de sources diverses suggèrent que l'attaque se fait par le biais de sites Wordpress vulnérables. Quand un site est infecté, un message signale la marche à suivre pour récupérer les données personnelles. Le maliciel décrypte deux fichiers choisis au hasard, pour bien montrer que les agresseurs sont en mesure de déchiffrer les données. Une vidéo d'assistance à la clientèle explique même comment se procurer les *BitCoins* nécessaires au versement de la rançon. Une fonction de communication en ligne permet encore de prendre contact avec les criminels, si l'on a besoin de plus d'informations.[20] CTB-Locker n'est toutefois pas le seul cheval de Troie chiffrant les données à faire preuve de créativité dans l'information des victimes. Le *virus macro* Cerber, également apparu en Suisse durant le semestre sous revue, est par exemple le premier à délivrer aussi la demande de rançon de manière vocale: «Attention! Attention! Attention! Your documents, photos, databases and other important files have been encrypted!», signale le haut-parleur de l'ordinateur.

Le cheval de Troie Jigsaw emploie une méthode de chantage particulièrement perverse pour mettre sous pression ses victimes: à chaque heure écoulée, le rançongiciel efface un certain nombre de documents et le montant de la rançon augmente. Tous les documents sont effacés après 72 heures.[21]

Entre-temps, même les utilisateurs de Mac ne sont plus en sécurité. Le rançongiciel KeRanger, découvert en mars, est le premier cheval de Troie chiffrant les données à s'attaquer aux plateformes OS X.[22] À l'aide d'un certificat valable pour les applications MAC, les cybercriminels sont parvenus à infecter deux programmes d'installation du client BitTorrent Transmission pour OS X (version 2.90). Le maliciel était présent sur le site web les 4 et 5 mars 2016. Toutes les personnes ayant téléchargé à cette période le programme Transmission pour OS X ont infecté leur système. Les fichiers d'installation infectés ont été effacés par la suite, et Apple a révoqué le *certificat* délivré[23].

---

19 https://www.proofpoint.com/us/threat-insight/post/cryptxxx-ransomware-learns-samba-other-new-tricks-with-version3100 (état: le 31 août 2016). Le cheval de Troie CryptXXX, dont la découverte remonte à avril, résiste à l'utilitaire de déchiffrement développé par Kaspersky Lab.

20 http://www.bleepingcomputer.com/news/security/ctb-locker-for-websites-reinventing-an-old-ransomware/ http://www.heise.de/security/meldung/Admins-aufgepasst-Krypto-Trojaner-befaellt-hunderte-Webserver-3116470.html (état: le 31 août 2016).

21 http://blog.trendmicro.com/trendlabs-security-intelligence/jigsaw-ransomware-plays-games-victims/ (état: le 31 août 2016).

22 Le rançongiciel FileCoder, découvert par Kaspersky Lab en 2014, n'était pas encore au point à l'époque et n'a donc pas pu causer de tort aux systèmes d'exploitation OS X. http://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/ (état: le 31 août 2016).

23 http://www.welivesecurity.com/2016/03/07/new-mac-ransomware-appears-keranger-spread-via-transmission-app/ (état: le 31 août 2016).

Recommandations:

Selon Kaspersky Lab, le nombre de rançongiciels a quintuplé entre avril 2015 et mars 2016. Cette croissance exponentielle fait qu'au cours des six derniers mois, diverses organisations ont publié davantage de mises en garde. L'Office fédéral allemand de la sécurité des technologies de l'information (BSI) a publié en mai un rapport complet sur le thème des rançongiciels; la police néerlandaise a créé le site web «nomoreransom.org», en collaboration avec Europol et deux entreprises spécialisées (Kaspersky Lab, Intel Security). MELANI a organisé en mai, en collaboration avec d'autres partenaires suisses, une journée de sensibilisation aux rançongiciels, tout en attirant l'attention sur quatre mesures importantes à prendre:

- Effectuer des sauvegardes régulières des données importantes (backup) : Veillez à effectuer des sauvegardes régulières de vos données importantes 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
- S'assurer que tous les logiciels ou plugiciels de navigation sont toujours actualisés.
- MELANI recommande aux internautes de ne jamais ouvrir les annexes suspectes de messages, même quand elles semblent provenir d'expéditeurs dignes de confiance.
- En outre, il faut s'assurer d'avoir installé un antivirus et le maintenir constamment à jour.

INFO

Mesures à prendre contre les chevaux de Troie verrouillant les données:

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.html

4.7 Mesures préventives

4.7.1 Ransomwareday, première journée de sensibilisation de MELANI

MELANI a organisé le 19 mai 2016, en collaboration avec de nombreux partenaires, une première journée de sensibilisation. Ce jour-là, des organisations actives dans divers secteurs, dont des fabricants de logiciels, des offices fédéraux et plusieurs associations suisses ou organismes de protection des consommateurs ont attiré l'attention de la population sur les *rançongiciels* et distribué diverses publications. Des discussions sont en cours pour savoir dans quelle mesure l'expérience pourrait être rééditée.

5 Situation internationale

5.1 Espionnage

5.1.1 Une cyberattaque perturbe la campagne électorale américaine

La veille du Congrès national du Parti démocrate américain à Philadelphie, Debbie Wasserman Schultz, présidente du Comité national démocrate (CND), a jeté l'éponge[24]. À un moment guère propice à un changement d'équipe dirigeante. Deux jours plus tôt, Wikileaks[25] avait publié près de 20 000 courriels échangés par les dirigeants du CND. Il en ressortait qu'en plus de favoriser la candidature d'Hillary Clinton, le Comité coordonnait ses efforts pour l'avantager face à Bernie Sanders, son plus dangereux concurrent.

L'histoire avait commencé un bon mois plus tôt, quand le Washington Post[26] avait signalé que l'infrastructure numérique du CND avait fait l'objet d'une cyberattaque. Depuis un an déjà, les attaquants étudiaient les analyses concernant l'adversaire républicain Donald Trump et lisaient aussi les échanges de correspondance électronique, comme l'a clairement montré la publication de Wikileaks.

À la fin d'avril 2016, alertés par des phénomènes étranges, les responsables informatiques du CND ont fait appel aux experts de la société Crowdstrike. Sa cellule de crise a alors découvert dans le réseau du Parti démocrate deux agresseurs agissant séparément, qu'elle a identifiés comme étant COZY BEAR et FANCY BEAR, deux groupes déjà connus. Le second, qui s'était illustré par son infiltration du Bundestag allemand en 2015, aurait eu accès au réseau du CND dès l'été 2015, selon Crowdstrike. Quant à COZY BEAR, sa présence n'a pu être confirmée que depuis avril 2016. Dans son rapport[27], Crowdstrike soupçonne deux services de renseignement russes différents d'être à l'origine des attaques. Or le jour même, un cyberpirate soi-disant roumain et utilisant le pseudonyme de Guccifer 2.0 a revendiqué l'attaque, prétendant l'avoir menée tout seul. Il a encore annoncé la publication sur Wikileaks d'extraits de son butin. Ce rebondissement a amené Crowdstrike à publier une mise à jour de son rapport pour démasquer l'imposteur. Deux entreprises de sécurité informatique, Fidelis Cybersecurity et Mandiant, ont abouti aux mêmes conclusions[28]. En outre Thomas Rid, professeur à King's College à Londres, a découvert que le maliciel ayant infiltré le CND possédait un serveur *Command & Control (C&C)* identique à celui utilisé contre le Bundestag allemand. Les origines roumaines de Guccifer 2.0 ont d'ailleurs été mises en doute et sa crédibilité ébranlée quand il n'a pas su parler couramment à un journaliste de langue maternelle roumaine.

---

[24] https://www.washingtonpost.com/politics/hacked-emails-cast-doubt-on-hopes-for-party-unity-at-democratic-convention/2016/07/24/a446c260-51a9-11e6-b7de-dfe509430c39_story.html (état: le 31 août 2016).

[25] https://wikileaks.org/dnc-emails/ (état: le 31 août 2016).

[26] https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html (état: le 31 août 2016).

[27] https://www.crowdstrike.com/blog/bears-midst-intrusion-democratic-national-committee/ (état: le 31 août 2016).

[28] https://www.wired.com/2016/07/heres-know-russia-dnc-hack/ (état: le 31 août 2016).

Conclusion:

L'incident montre clairement comment le cyberespace permet d'influencer les rapports de force sur le terrain politique. On a tôt fait de manipuler l'opinion publique, en espionnant des données sensibles d'un adversaire et en publiant de manière sélective certaines données pour le discréditer.

5.2 Fuites d'information

5.2.1 Registres électoraux publiquement dévoilés

À deux reprises, des fuites de données dans les registres électoraux ont fait les gros titres au premier semestre 2016. Le 30 mars, un pirate anonyme a publié un fichier contenant des informations personnelles sur 50 millions de citoyens turcs[29]. On y trouvait leurs noms et adresses, le prénom de leurs parents, leur lieu et date de naissance, ainsi que leur numéro d'identification national. Ces données ont paru avec un texte accusateur, reprochant au gouvernement Erdogan de ne pas être en mesure de dûment protéger les données des citoyens. Il s'est avéré que les données n'étaient pas actuelles, mais qu'elles remontaient à 2008. L'agence Associated Press en a confirmé l'authenticité. De telles publications sont toujours dangereuses, en rendant possibles des usurpations d'identité.

Une semaine plus tard, une fuite de données encore plus spectaculaire était rendue publique aux Philippines.[30] Suite à une intrusion dans la banque de données de la Commission électorale du pays (COMELEC[31]), des données de 55 millions d'électeurs philippins étaient publiées. Selon Trend Micro[32], fournisseur de sécurité, des informations sensibles comme des mots de passe ou 15,8 millions empreintes digitales figuraient parmi les données divulguées. L'incident remontait au 27 mars 2016, quand Anonymous Philippines avait défiguré le site de la COMELEC. Quelques jours plus tard, un utilisateur de Facebook se faisant appeler Lulzsec Pilipinas a publié en ligne les données dérobées.

5.2.2 Partages indésirables au sein du réseau professionnel

À côté des données mentionnées au chapitre 5.2.1, qui doivent être communiquées aux autorités, beaucoup d'internautes fournissent spontanément de grandes quantités de données personnelles à des entreprises privées. Or ces données ne sont évidemment pas non plus à l'abri d'une fuite. Le réseau professionnel LinkedIn a ainsi subi une cyberattaque dès 2014. À l'époque, 6,5 millions de mots de passe cryptés avaient été publiés en ligne. À la mi-mai 2016, un pirate se faisant appeler Pace a mis en vente pour cinq BitCoins (env. 2000 francs à l'époque) quelque 117 millions d'informations, y compris l'adresse électronique et le mot de passe crypté.[33] LinkedIn a confirmé l'exactitude des données. Elles avaient beau

---

29 https://www.wired.com/2016/04/hack-brief-turkey-breach-spills-info-half-citizens/ (état: le 31 août 2016).

30 http://www.theregister.co.uk/2016/04/07/philippine_voter_data_breach/ (état: le 31 août 2016).

31 COMELEC est l'une des trois commissions gouvernementales. Il lui incombe de faire appliquer les lois et réglementations, pour permettre l'organisation d'élections aux Philippines.

32 http://blog.trendmicro.com/trendlabs-security-intelligence/55m-registered-voters-risk-philippine-commission-elections-hacked/ (état: le 31 août 2016).

33 http://motherboard.vice.com/read/another-day-another-hack-117-million-linkedin-emails-and-password (état: le 31 août 2016).

remonter à quatre ans, la vente de telles données présente toujours un danger. En effet, de nombreux internautes ont tendance à ne jamais changer de mot de passe, ou alors très rarement, ainsi qu'à réutiliser le même mot de passe pour d'autres services.

Recommandations:

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

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.

Règles de comportement pour le choix d'un mot de passe

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

5.2.3 Marché au noir des données d'accès à Twitter

Les prestataires en ligne ne sont pas toujours fautifs quand des criminels s'emparent de données d'accès. En juin 2016, 32 millions de données d'accès à Twitter, mot de passe compris, ont été proposées sur le marché au noir.[34] Dans le cas d'espèce, on pense que les mots de passe auraient été copiés et transmis aux criminels par un maliciel s'étant introduit dans le navigateur des utilisateurs finaux. La copie et la revente de données d'accès procurent un revenu d'appoint aux escrocs. C'est ainsi que les maliciels conçus pour d'autres tâches, comme les escroqueries à l'e-banking ou les rançongiciels, possèdent généralement comme fonction accessoire un enregistreur de frappe (*keylogger*).

5.3 Systèmes de contrôle industriels

5.3.1 Maliciels dans une centrale nucléaire allemande

Des vérifications effectuées en amont d'une révision ont révélé, sur le site de la centrale nucléaire de Gundremmingen (Allemagne), la présence de deux maliciels sur 18 supports de données amovibles et sur un ordinateur. Selon la centrale, le système infecté faisait partie de la machine de chargement des barres de combustible et n'était utilisé que dans un but de visualisation. Autrement dit, le système n'était pas responsable de la gestion des processus. Quant au *maliciel*, il s'agissait selon divers articles de presse de Conficker, connu depuis 2008 et largement répandu. Microsoft a beau avoir fourni de bonne heure une mise à jour de

[34] https://techcrunch.com/2016/06/08/twitter-hack/ (état: le 31 août 2016).

sécurité, Conficker demeure le maliciel le plus répandu en Suisse aussi, selon la statistique de MELANI/GovCERT.ch. Le second maliciel découvert serait Ramnit, en activité depuis 2010. Europol et le prestataire de services de sécurité Symantec ont désactivé en 2015 le réseau de zombies qui le diffusait.

Il peut paraître étonnant de prime abord qu'une *vulnérabilité de Windows* connue depuis huit ans n'ait pas été corrigée dans une centrale nucléaire. Le système en question faisait toutefois partie de la zone du site déconnectée d'Internet. En outre, les équipements industriels sont souvent certifiés à l'installation; autrement dit, le fabricant en garantit le fonctionnement irréprochable dans la configuration livrée. Cette garantie s'éteint au moindre changement du système – y compris en cas de mise à jour de sécurité. Et comme les systèmes sont exploités de manière isolée, le risque de dysfonctionnement découlant d'une mise à jour dépasse de loin la menace due aux failles de sécurité. Un tel cloisonnement devrait faire en sorte que les lacunes de sécurité internes ne portent pas à conséquence. Il se peut néanmoins qu'un maliciel s'introduise dans de telles zones protégées et cause des dégâts :

- Faute de liaison à Internet, la maintenance et les contrôles des systèmes ne peuvent s'effectuer en ligne. D'où une menace pour les réseaux isolés, en cas de raccordement de systèmes externes (Notebook, *clé USB*, etc.) à des fins de maintenance, d'importation ou d'exportation de données. Une telle opération permet de contourner l'*air gap* – isolement physique dans un but de sécurité – pour infecter le système. Un exemple réel vient du virus informatique Stuxnet qui, il y a quelques années, a pénétré au moyen d'une clé USB dans une usine iranienne d'enrichissement de l'uranium.

- Le ver était d'emblée présent sur l'ordinateur, où il ne s'était pas fait remarquer jusque-là. Cela peut être le cas si lors de son installation, l'ordinateur était raccordé à Internet et n'a été isolé que par la suite, ou bien si le support de données utilisé pour le transfert des fichiers d'installation était déjà infecté.

Conclusion:

Les attaques ciblées reposent sur des maliciels spécialement programmés, dont la mise en circulation reste limitée pour ne pas attirer l'attention. Il est donc quasiment exclu que cette attaque ait été une attaque ciblée.

Une infection «accidentelle» comporte sans doute un risque de dommage collatéral: le maliciel pourrait causer des dysfonctionnements du système, qui va par exemple s'arrêter spontanément. Mais comme le pilotage des zones sensibles d'une centrale nucléaire s'effectue en mode analogique, un scénario comme celui de Gundremmingen n'aurait eu aucun impact sur les processus critiques.

5.3.2 Publication d'une cyberattaque contre un service des eaux

L'entreprise de sécurité Verizon a publié en mars 2016[35], dans son «Data Breach Report», les résultats d'une évaluation proactive menée auprès d'une société d'approvisionnement en eau potable. Verizon n'a toutefois pas divulgué l'identité de la victime, qui a reçu le nom générique de Kemuri Water Company (KWC). L'évaluation a découvert sur son site web des traces de cyberattaque. L'application web de paiement avait été compromise, les escrocs

[35] http://www.verizonenterprise.com/resources/reports/rp_data-breach-digest_xg_en.pdf (état: le 31 août 2016).

ayant tiré parti de failles de sécurité connues. Et comme les données d'accès au serveur d'arrière-plan (Back-End, un IBM AS/400) figuraient sur le serveur frontal (front-end) en clair dans un fichier *.ini*, les escrocs ont pu s'en servir. Sur le Back-End, très répandu au début des années 2000, cohabitaient non seulement la base de données servant aux opérations de paiement, mais également la comptabilité et la gestion des données de clients, ainsi que le système de contrôle industriel (*SCI*) de KWC. Ce dernier incluait des centaines d'automates programmables industriels (PLC en anglais), pilotant les soupapes et les capteurs destinés à l'approvisionnement en eau. Le système étant directement relié à Internet, les données d'accès dérobées ont permis d'accéder aux PLC et de manipuler l'ajout de produits chimiques dans l'approvisionnement en eau. L'investigation a montré que la direction de KWC était dûment informée des dysfonctionnements inexplicables des soupapes et des conduites au cours des 60 jours précédents ayant abouti à l'adjonction incontrôlée de produits chimiques, lors du traitement de l'eau potable. Mais comme la surveillance de la qualité de l'eau s'effectuait indépendamment du système, des interventions manuelles ont permis d'éviter toute mise en danger des consommateurs d'eau.

Dans un premier temps, les événements n'avaient pas été interprétés comme une cyberattaque. L'enquête subséquente a conclu que faute d'informations détaillées sur l'installation, les escrocs n'avaient pu lui infliger que des dommages limités. Mais s'ils avaient disposé de plus de temps et glané davantage de renseignements, l'attaque aurait fait bien plus de dégâts.

5.3.3 Maliciel inédit espionnant les SCI dans un but inconnu

FireEye, fournisseur de logiciels de sécurité, a publié en juin 2016 un rapport d'enquête sur IronGate[36]. Ses experts avaient découvert quelque mois plus tôt l'existence de ce maliciel menaçant les sites industriels et dont le mode opératoire est surprenant à plus d'un titre. Il possède par exemple la faculté d'enregistrer pendant cinq secondes, lors d'une attaque de l'intermédiaire (*man-in-the-middle attack*), les informations envoyées par les automates programmables industriels (PLC en anglais) à l'interface utilisateur. Ces séquences sont rejouées plus tard. Et pendant que le processus de l'opérateur prend connaissance de ce trafic anodin, le maliciel adresse des commandes manipulées aux PLC. À cet effet, il modifie une bibliothèque de liens dynamiques (*dynamic link library, DLL)*, faisant office de relais entre les API et le logiciel de surveillance. Le maliciel vérifie encore, dans l'environnement d'exécution, l'existence de bacs à sable (*sand box)* et d'autres outils répandus parmi les chercheurs en sécurité et les analystes. Certains injecteurs (*dropper*) du maliciel ne fonctionnent d'ailleurs pas dans un environnement Cuckoo ou VMware.

Le maliciel prend pour cible le logiciel S7 PLCSIM développé par Siemens et semble s'intéresser à un type d'installation spécifique. FireEye soupçonne qu'il s'agit de l'industrie du biogaz. C'est du moins ce que suggère un fichier découvert, qui porte le nom biogas.exe. L'équipe ProductCERT de Siemens a confirmé que le maliciel ne fonctionne pas dans un environnement de contrôle standard. Il est apparemment conçu pour s'activer dans un simulateur, ce qui donne à penser qu'il s'agit d'un projet de recherche ou d'un test. La grande qualité du maliciel et son évolutivité autorisent à y voir la nouvelle génération de Stuxnet. L'auteur du maliciel et sa finalité restent mystérieux. Il a été découvert par Virustotal en 2014, et donc il existait déjà au plus tard à ce moment-là.

---

[36] https://www.fireeye.com/blog/threat-research/2016/06/irongate_ics_malware.html (état: le 31 août 2016).

5.3.4 Collaboration à des fins de sécurité entre le gouvernement américain et les constructeurs automobiles

MELANI a déjà évoqué dans ses deux précédents rapports semestriels la sécurité des moyens de transport, des voitures notamment. En début d'année, le Ministère américain des transports a signé avec quelque 18 constructeurs automobiles une déclaration commune d'intention concernant la sécurité des véhicules. Cette démarche fait notamment suite à l'essor fulgurant de l'informatique embarquée, ainsi qu'aux développements dans le domaine des véhicules autonomes. Outre des déclarations générales visant à la prise en compte anticipée des risques de sécurité, à l'échange réciproque d'informations et à la collaboration dans une optique de renforcement de la sécurité routière, un point du texte porte explicitement sur l'amélioration de la cybersécurité des véhicules. L'accent y est toutefois mis sur l'intégrité physique des personnes (safety); la sécurité des systèmes (security) y est traitée de manière subsidiaire, comme cause potentielle de mise en danger des personnes.

Conclusion:

Les voitures comprennent toujours plus d'outils d'aide à la conduite, dont le fonctionnement est commandé par ordinateur. Il est toutefois indispensable que les utilisateurs puissent se fier à ces systèmes. On le voit bien avec les véhicules autonomes. Leur démocratisation présuppose que les usagers de la route leur fassent dûment confiance.

5.3.5 Vol de voitures par piratage électronique

Les fabricants automobiles prennent très au sérieux la sécurité physique des personnes (voir chapitre 5.3.4). Ce domaine a tendance à être très réglementé. Les fabricants doivent s'attendre à des demandes d'indemnisation et procéder, le cas échéant, à de coûteuses actions de rappel s'ils ont livré des produits défectueux qui causent des dégâts ou mettent des vies en danger. D'un autre côté, on trouve dans et sur les voitures des systèmes n'ayant rien à voir avec la conduite. Des clés à télécommande radio remplacent les clés traditionnelles mécaniques, voire le déverrouillage des portes qui se fait déjà par une *app* de smartphone. Beaucoup de nouveaux véhicules sont même dépourvus de serrures, leurs portes se fermant et s'ouvrant exclusivement par l'électronique (clés passives).

Dans cette évolution, certains fabricants semblent privilégier la fonctionnalité ou la vitesse de lancement sur le marché, au détriment de la sécurité des systèmes. Au début, bien des serrures électroniques étaient si simples qu'il suffisait à un voleur de voitures d'intercepter et d'enregistrer le signal émis à distance. Il n'avait plus qu'à reproduire le signal piraté pour ouvrir la porte du véhicule. Puis quand des produits déverrouillant automatiquement le véhicule dès qu'on s'en approche sont arrivés sur le marché, les voleurs de voitures ont rapidement découvert la possibilité de simuler la présence de la clé avec des appareils radio spécialement préparés. Il suffit qu'un complice s'approche du propriétaire et transmette le signal radio émis par la «clé» au voleur se trouvant à proximité du véhicule (attaque par relais). À cela s'ajoute que dans de tels systèmes, le démarrage du moteur s'effectue fréquemment par simple pression sur un bouton, quand le système a reconnu le signal radio émis par la clé à l'intérieur du véhicule. Il devient bien souvent difficile de déterminer la méthode utilisée pour dérober le véhicule. Les vols sont donc simplement déclarés et signalés à l'assurance. Tant que les assureurs rembourseront les dommages, les fabricants ne se presseront guère d'introduire des systèmes de verrouillage offrant une sécurité optimale.

L'informatisation des véhicules ne comporte pas seulement un risque de piratage et de vol. Si le smartphone sert d'interface entre le conducteur et le véhicule, une infiltration réussie du téléphone mobile ou une utilisation astucieuse de cette interface permettent de faire du sabotage. La voiture électrique Nissan Leaf en est un bon exemple: moyennant l'app requise et en y introduisant le numéro de série du véhicule inscrit sur le pare-brise, un pirate pouvait retrouver d'autres données (identité du propriétaire, derniers trajets) ou activer la climatisation. L'app ne donnait certes pas accès à l'électronique du véhicule. Elle permettait néanmoins de décharger ses batteries, en enclenchant la climatisation.

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. Car les nouvelles possibilités induisent toujours de nouveaux risques, à prendre en compte dès le stade de la conception (security by design).

Mesures de protection des systèmes de contrôle industriels (SCI)

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

5.4 Cyberattaques

5.4.1 Cyber-braquage: butin de 81 millions de dollars

Selon la Banque nationale du Bangladesh, des pirates ont dérobé les données d'accès à son système de paiement interne[37]. Ils se sont introduits dans son système informatique et y ont installé des outils logiciels spécialement programmés. Les escrocs ont manipulé la banque de données, par exemple les interfaces du logiciel client de Swift, n° 1 mondial du trafic international de paiements. Ainsi, ils ont non seulement effectué des transactions frauduleuses, mais effacé toute trace d'activité dans les journaux d'événements. Ils ont par exemple empêché l'impression des confirmations des transactions, afin qu'elles restent inaperçues le plus longtemps possible. Les 4 et 5 février 2016, des attaquants ont passé plusieurs dizaines d'ordres de transfert de fonds, depuis un compte que la banque centrale bangladaise détenait à l'antenne new yorkaise de la Réserve fédérale des États-Unis (Fed), sur des comptes privés philippins et sri-lankais. Quatre virements à destination des Philippines, d'une valeur totale de 81 millions de dollars, ont abouti. Lors de la cinquième transaction, d'un montant de 20 millions de dollars supplémentaire, une faute de frappe a attiré l'attention de la Fed. Les escrocs avaient mal orthographié le nom d'une organisation non gouvernementale basée au Sri Lanka, ce qui a amené la banque centrale américaine à demander des précisions à son homologue bangladaise. La transaction a aussitôt été bloquée. De son côté, la Fed avait constaté un nombre anormalement élevé d'ordres de paiement

[37] http://www.reuters.com/article/us-usa-nyfed-bangladesh-malware-exclusiv-idUSKCN0XM0DR (état: le 31 août 2016).

destinés à des bénéficiaires privés. Dûment alertée, la banque centrale du Bangladesh a pu annuler les transactions frauduleuses et éviter ainsi une perte supplémentaire de 850 millions de dollars. Quant aux quatre transactions fructueuses, le butin a été échangé contre des jetons de jeu dans divers casinos philippins où se perd toute trace de l'argent, les maisons de jeu étant soumises à une surveillance moins poussée que le système financier classique.

Dans cette cyber-escroquerie, la plus grave commise à ce jour contre un établissement bancaire, les autorités de poursuite pénale du Bangladesh ont accusé Swift de négligence. Il incombait selon elles à Swift, après avoir installé son système, d'analyser tout le paysage système de la banque pour y détecter des failles de sécurité. Swift a aussitôt rejeté toute responsabilité concernant la cyberattaque. Comme n'importe quel client de Swift, la Banque nationale du Bangladesh était responsable de la sécurité de ses systèmes et de l'environnement possédant des interfaces avec le système Swift. Le litige rappelle les discussions suscitées par les premières fraudes à l'e-banking. Dans quelle mesure la banque répond-elle d'un paiement frauduleux ou bien le client a-t-il manqué à son devoir de diligence, si son ordinateur est infecté par un maliciel? Les banques avaient alors renforcé la sécurité des systèmes d'e-banking. Entre-temps, Swift a aussi réagi en insistant davantage sur le respect des prescriptions de sécurité[38].

Le 12 mai 2016, un autre incident impliquant une banque commerciale au Vietnam a été découvert. Une transaction frauduleuse portant sur 1,13 million de dollars aurait été effectuée à ses dépens, via le réseau Swift utilisé pour les transactions standardisées. Un troisième cas rendu public concerne une banque équatorienne.

Le rapport du prestataire de sécurité Symantec[39] signale que la composante du maliciel supprimant toute trace d'activité (utilitaire *wipe*) avait déjà servi dans l'opération Blockbuster, à l'origine de la cyberattaque de novembre 2014 contre Sony. Des fonctions identiques de cette composante ont été découvertes dans la fraude commise au Vietnam, alors qu'elles avaient été modifiées au Bangladesh. On ignore si les systèmes bancaires ont été victimes des mêmes escrocs, ou si le code de programmation avait été vendu ou partagé dans la clandestinité.

Conclusion:

Les attaques contre la clientèle e-banking font partie depuis des années du répertoire de base des cybercriminels. On sait depuis 18 mois au plus tard, quand le maliciel Carbanak s'en est directement pris aux réseaux bancaires, que des efforts équivalents sont déployés dans le cyber-braquage et dans l'espionnage ultrasophistiqué, pour autant que les perspectives de gain le justifient. Une analyse approfondie de cette tendance figure au chapitre 6.1.

[38] http://www.theregister.co.uk/2016/06/03/swift_threatens_insecure_bank_suspensions/ (état: le 31 août 2016).

[39] http://www.symantec.com/connect/blogs/swift-attackers-malware-linked-more-financial-attacks (état: le 31 août 2016).

5.4.2 Carbanak 2.0 et autres attaques similaires

Il y a deux ans, une vaste opération appelée Carbanak avait fait grand bruit dans la communauté financière internationale. Pour la première fois, les cyberescrocs s'attaquaient non plus à un client final, mais directement à la banque. Les outils déployés, le réel professionnalisme et la ténacité rappelaient les attaques APT (*advanced persistent threats*). La logique des criminels est simple: les efforts consentis ont beau être plus grands, les gains augmentent de manière exponentielle. Le cyber gang s'est ensuite fait plus discret pendant plusieurs mois. Des indices de sa présence ont à nouveau été découverts chez une victime en septembre 2015.[40] En février 2016, l'éditeur de logiciels Kaspersky confirmait le retour de Carbanak 2.0. Dans un autre article, une équipe de chercheurs de l'entreprise de cybersécurité Proofpoint affirme avoir découvert que le gang Carbanak prépare des cyberattaques contre des banques en Europe, au Moyen-Orient et aux États-Unis.[41]

Autre particularité de Carbanak 2.0, le gang ne vise plus seulement les banques, mais a élargi son cercle de victimes au service de comptabilité d'autres sociétés. Dans un cas d'espèce, les agresseurs ont modifié les rapports de propriété d'une grande entreprise. Un homme de paille a été placé comme actionnaire de l'entreprise. On ignore toutefois quel était le but visé, car l'incident a été découvert avant qu'un dommage soit commis.[42]

Carbanak a fait des émules. Les cybercriminels apprennent vite, ils assimilent les nouvelles techniques et n'hésitent plus à s'en prendre directement aux banques. À l'instar de deux autres groupes, appelés Metel et GCMAN. Metel opère avec un style similaire à Carbanak. Dans les cas observés jusqu'ici, des escrocs vidaient la nuit les distributeurs de billets de différentes banques. Pendant ce temps, une autre équipe manipulait les comptes sur lesquels les retraits étaient effectués, afin que le solde indique à nouveau le montant d'origine. De son côté, GCMAN opère à chaque minute des virements par tranches de 200 dollars, par l'intermédiaire de services de paiement en ligne comme Bitcoin, Perfect Money ou Payza. La particularité du groupe GCMAN tient à ce que les cybercriminels étaient restés dissimulés pendant 18 mois dans le réseau.

5.4.3 Rançongiciels dans les hôpitaux

La vague de *ransomwares* observée depuis le début de l'année touche aussi des infrastructures critiques. Ces derniers temps, les hôpitaux ont fait partie des cibles privilégiées des criminels. Car avec la numérisation, le fonctionnement du service informatique d'un hôpital devient lui aussi crucial pour le traitement des patients. Plusieurs cas d'hôpitaux en Allemagne et aux États-Unis ont été publiés au premier semestre 2016. Des rançons importantes ont parfois été payées aux criminels afin de débloquer l'infrastructure. Dans le cas du Kansas Heart Hospital, les escrocs n'ont pas libéré tous les fichiers et ont demandé à ce qu'une deuxième rançon soit payée. Il semblerait que les demandes de rançons soient plus élevées pour cette catégorie de cibles. Les criminels savent qu'un hôpital doit pouvoir réagir rapidement et ne peut plus, dans certains cas, se passer de son infrastructure informatique pour sauver une vie humaine. Ces institutions peuvent donc devenir des cibles de prédilection.

---

40 https://www.csis.dk/en/csis/blog/4710/ (état: le 31 août 2016)

41 https://www.proofpoint.com/uk/threat-insight/post/carbanak-cybercrime-group-targets-executives-of-financial-organizations-in-middle-east (état: le 31 août 2016).

42 https://securelist.com/blog/research/73638/apt-style-bank-robberies-increase-with-metel-gcman-and-carbanak-2-0-attacks/ (état: le 31 août 2016).

Un défi additionnel tient à la présence d'équipements de diagnostic et d'analyse qui dépendent de contrôleurs informatiques. Ces outils sont testés et certifiés pour pouvoir être utilisés dans le domaine médical. Or dans la majeure partie des cas, le sceau d'approbation ne permet pas aux services informatiques d'un hôpital de mettre à jour le système d'exploitation, ni même les logiciels antivirus, car cela reviendrait à manipuler l'équipement qui perdrait de ce fait sa certification. De plus, les services informatiques des hôpitaux manquent de moyens ou de compétence technique pour mettre à jour ces systèmes spécifiques.

Dans le passé, de tels systèmes pouvaient être indépendants du réseau informatique d'un hôpital. Mais avec la mise en réseau des machines en vue du suivi numérique des traitements de patients, les réseaux informatiques hospitaliers comprennent de plus en plus de systèmes vulnérables, dont la sécurité ne peut être assurée. Un effort de sensibilisation et de collaboration avec les fournisseurs de matériel s'avère ici primordial.

Enfin, la numérisation des données des patients éveille aussi la convoitise des hackers. En effet, le dossier de patient d'une personne précise peut devenir une cible, à des fins d'espionnage ou de sabotage. À l'ère du Big Data, les données de traitement, les résultats ainsi que les physiologies constituent une aide précieuse dans le développement des traitements et ouvrent des voies prometteuses à la recherche. Cependant des individus et des entreprises pourraient chercher à s'en emparer de manière illégale. Il s'agit dès lors de se demander ce qui doit figurer dans les dossiers de patients, compte tenu des risques de la numérisation, et comment l'on pourrait minimiser de tels risques. En outre, il convient de définir la procédure d'annonce aux patients, en cas de perte de données sensibles.

5.4.4 Distributeurs de billets pillés au Japon

Dimanche 15 mai 2016, entre 5 et 8 heures du matin, près de 17 millions de francs ont été dérobés dans 1700 distributeurs japonais, lors d'une vaste action coordonnée. Afin d'effectuer plus de 14 000 prélèvements en un aussi bref laps de temps, près de 600 personnes avaient reçu jusqu'à 1600 clones de cartes de crédit piratées. Sur leurs bandes magnétiques figuraient les données dérobées à la clientèle de la South African Standard Bank.

Pendant longtemps, les distributeurs japonais n'ont pas accepté les cartes de crédit étrangères. Le gouvernement avait donc ordonné il y a quelque temps aux banques de s'adapter, afin de faciliter les retraits en espèces par les touristes étrangers. Or beaucoup de ces distributeurs sont apparemment trop vétustes pour lire la puce des cartes de crédit. Ils en sont restés aux cartes bancaires magnétiques, connues pour être faciles à répliquer. L'incident confirme qu'il reste des progrès à faire pour détecter les retraits frauduleux opérés avec des cartes de crédit étrangères.

La lourdeur du bilan tient à ce qu'avant cet incident, beaucoup de distributeurs de billets permettaient de retirer jusqu'à 100 000 ou 200 000 yens japonais (soit 900 ou 1800 francs). Entre-temps, les limites ont été ramenées à 50 000 yens au maximum.

5.4.5 Anonymous & Cie: #campagnes

Au premier semestre 2016, les hacktivistes ont lancé de nombreuses activités, soutenues parfois, contre une série d'organisations considérées comme au centre du pouvoir.

Dès le début de l'année, le collectif Anonymous a lancé un «appel aux armes». Une nouvelle cyberattaque, baptisée en référence à la mythologie «opération Icare», était prévue contre le

système financier mondial. «Comme Icare, les pouvoirs en place ont volé trop près du soleil, et le temps est venu de mettre le feu aux ailes de leur empire...».[43] L'opération avait été conçue au moment d'Occupy Wallstreet en 2011 – comme équivalent en ligne des protestations sur le terrain.[44] Le 4 mai 2016, une vidéo diffusée sur YouTube signalait une «campagne de 30 jours contre les sites des banques centrales dans le monde entier». Le même jour, Anonymous inondait de requêtes, avec l'aide du groupe de hackers Ghost Squad, le site web de la banque centrale grecque, dont les serveurs étaient inaccessibles pendant plusieurs heures. Durant tout le mois de mai, la campagne #OpIcarus a notamment paralysé les sites de plus de 30 banques centrales. Parmi les victimes les plus connues figuraient la Banque d'Angleterre, la bourse de New York et la Banque vaticane. La puissance d'attaque dépassait 250 gigabits par seconde.[45] Anonymous a publié la liste complète de ses cibles, qui renfermait plus de 200 sites web, en précisant sur Twitter ne pas avoir dit son dernier mot.

Les hackers de Ghost Squad, groupuscule récemment encore affilié à Anonymous[46], avaient annoncé dans la foulée l'opération #OpSilence pour le mois de juin. Il s'agissait de sanctionner les médias n'ayant pas dénoncé, ou alors seulement de manière unilatérale, la guerre en Palestine ainsi que les atrocités commises en Syrie.[47] Ghost Squad[48] n'a toutefois pas respecté le calendrier annoncé et commencé à sévir le 31 mai, en paralysant pendant plusieurs heures les systèmes des chaînes d'information CNN et FOX News. Les mêmes hackers ont encore annoncé d'autres cyberattaques contre les médias. Ils ont signalé comme cibles potentielles NBC et MSN; ces menaces n'ont toutefois pas été mises à exécution. Le groupe Ghost Squad a bien souligné dans ce contexte, et le fait mérite d'être relevé, qu'il s'agissait d'une opération autonome, n'ayant (plus) rien à voir avec Anonymous.

Conclusion:

Les liens informels au sein d'Anonymous et d'autres groupes comme Ghost Squad se traduisent par une absence de coordination au niveau tant de la communication que des cyberattaques plus ou moins spectaculaires effectuées. Comme la structure d'Anonymous ne prévoit ni affiliation ni porte-parole officiel, et que personne ne porte la responsabilité d'ensemble de ce mouvement, chacun peut en principe publier des communiqués au nom d'Anonymous pour susciter l'intérêt des médias.

---

43 https://opicarus.wordpress.com/ (état: le 31 août 2016).

44 http://www.ibtimes.co.uk/opicarus-anonymous-hacker-reveals-inspiration-behind-latest-operation-evolution-hacktivism-1561457 (état: le 31 août 2016).

45 http://thefreethoughtproject.com/anonymous-hits-york-stock-exchange-world-bank-vatican-total-corporate-media-blackout-ensues/ (état: le 31 août 2016).

46 http://thefreethoughtproject.com/not-anonymous-hacking-group-declares-war-mainstream-takes-cnn-fox/ http://anonhq.com/anonymous-opsilence/ (état: le 31 août 2016).

47 http://news.softpedia.com/news/anonymous-announces-opsilence-month-long-attacks-on-mainstream-media-504760.shtml (état: le 31 août 2016).

48 http://thefreethoughtproject.com/not-anonymous-hacking-group-declares-war-mainstream-takes-cnn-fox/ (état: le 31 août 2016).

5.4.6 xDedic: l'accès à des serveurs piratés se monnaie en ligne

En juin, Kaspersky a publié les détails d'une investigation menée avec un fournisseur de services Internet européen, sur un marché clandestin du nom de xDedic. En activité depuis 2014 déjà, xDedic proposait d'acheter les données d'accès à près de 70 000 serveurs piratés, accessibles par le *protocole RDP* («Remote Desktop Protocol», permettant de se connecter à distance à un serveur Windows). Le prix variait selon les spécificités du serveur, avec une «entrée de gamme» à six dollars. De tels serveurs peuvent être utilisés pour lancer des attaques (*DDoS, spam*, etc.), ou alors être exploités pour les données ou logiciels qu'ils contiennent. Certains serveurs particulièrement intéressants pouvant par exemple donner accès à des *terminaux de paiement*. Peu après les révélations de Kaspersky, le site a brièvement disparu avant de réapparaître, hébergé cette fois sur le *réseau TOR.*

Conclusion:

De tels cas reflètent la tendance à une division du travail toujours plus poussée dans le marché noir de la cybercriminalité. Les acteurs les moins avancés peuvent recourir à toute une gamme de services, afin de lancer des attaques en investissant un minimum de temps et de compétences techniques. Après l'étude que Kaspersky lui avait consacrée, le site a disparu pour réapparaître sur une plateforme offrant plus d'anonymat aux administrateurs, aux vendeurs et aux acheteurs. Cela confirme que lorsqu'une niche du marché est rentable, ses opérateurs savent procéder aux adaptations formelles requises pour en assurer la pérennité.

5.5 Mesures préventives

Outre la sensibilisation, la mesure de prévention la plus efficace consiste à mettre sous les verrous les cybercriminels. On a bien souvent l'impression que les arrestations dans le cyberespace sont difficiles sinon impossibles. Diverses razzias montrent toutefois que ce n'est pas le cas.

5.5.1 Razzia dans le darknet

Une razzia internationale contre des exploitants et des clients de plateformes web illégales a abouti à l'arrestation de neuf suspects. En outre, 69 logements ou sièges d'entreprises ont été perquisitionnés en Allemagne, Suisse, France, aux Pays-Bas, en Lituanie et en Russie. Les poursuites étaient dirigées contre divers forums germanophones de l'économie souterraine. Il s'y négociait des marchandises illégales, comme des armes, des stupéfiants, de la fausse monnaie ou des faux passeports, ainsi que des données de cartes de crédit ou d'e-banking obtenues par espionnage. La palette d'offres comprenait encore des services criminels, par exemple des attaques *DDoS* ou l'infection d'ordinateurs par *maliciels*.

L'exploitant principal de trois forums au total serait un ressortissant bosniaque de 27 ans. Arrêté le 24 février 2016 en Bosnie-Herzégovine, il se trouve en détention préventive.

De nombreux moyens de preuve ont pu être réunis, notamment un grand nombre d'ordinateurs et de supports de stockage, une arme à feu, des stupéfiants et des biens d'une valeur de 150 000 euros. En outre, plusieurs serveurs hébergeant des marchés en ligne ont

été saisis en France, aux Pays-Bas, en Lituanie et en Russie. Un avis de saisie a été diffusé sur les sites web correspondants.[49]

Fig. 10: Bannière publiée par la police sur les serveurs web saisis

Conclusion:

L'action décrite ci-dessus prouve une nouvelle fois que l'anonymat complet n'existe pas sur Internet. Elle rappelle encore l'importance de la collaboration internationale, dans la lutte contre la cybercriminalité.

5.5.2 Cessation d'activité des kits d'exploits Angler et Nuclear

Les deux *kits d'exploits* sans doute les plus connus ont quasiment disparu au premier semestre 2016, pour des raisons différentes. En avril 2016, l'entreprise de sécurité Check Point avait publié une analyse détaillée sur Nuclear. Les exploitants auront pris peur, au point de se cacher et d'interrompre au moins temporairement leur activité. Depuis le 30 avril, l'expert français en kits d'exploits Kafeine n'a plus constaté la moindre cyberattaque émanant de Nuclear.[50]

Toujours selon Kafeine, Angler a cessé de sévir le 7 juin. Là encore, on peut se demander ce qui a provoqué sa soudaine disparition. Une explication possible réside dans l'arrestation par les autorités russes, au même moment, de 50 présumés cybercriminels en relation avec le maliciel Lurk. Ces personnes auraient dérobé de l'argent de comptes en banque russes à l'aide d'un cheval de Troie. Or le vecteur d'infection des attaques est directement lié au kit d'exploits Angler. D'où la question de savoir si les auteurs d'Angler ont bel et bien été arrêtés, ou s'ils ont craint que les personnes sous les verrous ne dénoncent d'autres complices.

---

49 https://www.bka.de/SharedDocs/Pressemitteilungen/DE/Presse_2016/pm160229_UndergroundEconomy.pdf?__blob=publicationFile&v=1 (état: le 31 août 2016).

50 http://www.securityweek.com/exploit-kit-activity-down-96-april (état: le 31 août 2016).

Les criminels ne se sont hélas pas détournés des kits d'exploits après les déboires d'Angler. Il n'y a eu qu'un effet de substitution: le kit d'exploits Neutrino connaît un succès croissant depuis la disparition d'Angler.

5.5.3 Arrestations dans divers pays des responsables de Dyre

En février, le site d'information Forbes[51] a rapporté qu'en novembre 2015, les autorités russes auraient neutralisé le *réseau de zombies* de Dyre, cheval de Troie bancaire, et arrêté les dirigeants de cette organisation criminelle. Le cheval de Troie bancaire le plus actif en 2015 selon IBM, responsable de 25 % des fraudes bancaires survenues dans le monde, s'était propagé jusque-là de manière exponentielle, en Suisse aussi. Au début, il s'en prenait surtout aux PME. Les escrocs avaient notamment dérobé un montant à sept chiffres à une entreprise du canton de Fribourg.[52] Puis Dyre s'est également intéressé aux utilisateurs privés. Même si les autorités russes n'ont pas officiellement confirmé avoir ordonné une razzia, les activités de Dyre ont cessé, comme le montre clairement la statistique des maliciels de GovCERT.ch. Il ne reste plus que les infections des systèmes n'ayant jamais été nettoyés. Ce n'est pas pour autant la fin du maliciel Dyre, rappelle le site Forbes; son *code source* est depuis peu libre d'accès sur la toile.

6 Tendances et perspectives

6.1 Attaques sophistiquées – APT déployées par les criminels

Les cybercriminels ne reculent plus devant l'effort afin d'améliorer leurs perspectives de gain, leur approche est devenu plus ciblée et ils cherchent à optimiser leurs dépenses et leurs revenus. Outre les attaques prenant pour cible le système de messages interbancaires Swift en début d'année (chap. 5.4.1) et les opérations attribuées au gang Carbanak (chap. 5.4.2), les cyberattaques contre les clients finaux ont le vent en poupe. La division des tâches et le recyclage des maliciels dans le marché souterrain des services cybercriminels favorisent une telle tendance.

Pendant longtemps, la loi du moindre effort a poussé les pirates à rechercher les systèmes les moins bien protégés. Les cibles les plus faciles étaient principalement les ordinateurs de clients finaux utilisés par exemple pour l'e-banking. Il y a quelques années encore, personne n'aurait osé s'attaquer directement aux établissements financiers. Les efforts requis étaient jugés excessifs, et les escrocs n'avaient pas atteint le niveau de professionnalisme exigé. Mais la tendance récente aux cyber-braquages n'est pas surprenante et tient à plusieurs raisons:

- D'une part, les logiciels nécessaires à des attaques aussi complexes sont proposés entre-temps sur le marché clandestin. Les criminels ont eux aussi assimilé les connaissances nécessaires. D'autant plus que la ligne de démarcation entre les attaques bénéficiant du soutien d'États ou de nature criminelle tend à s'estomper.

---

51 http://www.forbes.com/sites/thomasbrewster/2016/02/08/russia-arrests-dyre-malware-masterminds/#5d5cf29a1e02 (état: le 31 août 2016).

52 http://www.20min.ch/digital/news/story/E-Banking-Trojaner-zielt-auf-Schweizer-Firmen-ab-23497999 (état: le 31 août 2016).

- Une autre raison importante tient à la difficulté croissante de blanchir l'argent. Par chance, les personnes assez naïves pour se faire recruter comme agents financiers (*money mules*) se font rares. À cela s'ajoute qu'un agent financier doit généralement être remplacé après une seule transaction. Les criminels recherchent donc des alternatives leur permettant de se passer d'agents financiers, ou d'en faire un usage plus rationnel. Le moyen le plus efficace de blanchir l'argent consiste ici à transférer des montants plus élevés par agent financier. Les escrocs se sont ainsi tournés vers les entreprises, où de tels virements se remarquent moins.

Les incidents décrits aux chapitres 5.4.1 et 5.4.2 montrent de manière exemplaire que d'autres approches sont recherchées et hélas trouvées pour effacer toute trace des flux financiers. Ainsi, les groupes exploitant les maliciels Carbanak et Metel ont manipulé les distributeurs de billets pour libérer des billets à une heure précise. Comme le versement s'effectue en espèces, tout blanchiment est superflu. Le groupe GCMAN s'est servi de monnaies électroniques, dont les flux sont difficiles à reconstituer. Quant au cyber-braquage contre la Banque nationale bangladaise, l'argent des quatre transactions fructueuses a été échangé contre des jetons de jeu dans des casinos philippins, où se perd toute trace du pactole. En effet, les maisons de jeu sont soumises à une surveillance moins poussée que le système financier classique. En conclusion, plus le butin est élevé, et plus les criminels peuvent recourir à des méthodes complexes et professionnelles pour le blanchir.

Il serait faux toutefois de croire que les cyberattaques professionnelles vont se substituer aux attaques plus rudimentaires. Expérience à l'appui, les anciennes formes d'attaques ne disparaissent pas, mais d'autres escrocs s'en chargent. Ainsi, les tentatives de *phishing* restent d'actualité. Elles ont beau ne plus avoir autant de succès que dans le passé, elles continuent d'avoir lieu et il faut s'en protéger. Le gâteau n'est donc pas seulement partagé différemment, sa taille a aussi augmenté.

6.2 Avenir d'Internet – perspectives techniques et sociétales

Les premières voitures étaient dépourvues de toit et ne comportaient ni ceintures de sécurité, ni le moindre dispositif de protection du conducteur. Mais comme les routes étaient désertes, on était déjà content de rouler dans la direction voulue. Il en allait de même du temps des pionniers d'Internet. Danny Hillis, ingénieur informatique américain, a bien résumé la situation dans les années 1980: «There were only two other Dannys on the Internet then. I knew them both. We didn't all know each other, but we all kind of trusted each other.»[53] Chacun appréciait le bon fonctionnement du réseau. Dans le trafic routier, au fil des ans et avec la multiplication des accidents, on a introduit des règles de circulation, construit des routes sûres et imposé aux fabricants les ceintures de sécurité, les zones de déformation, le système antiblocage ABS et les airbags. Alors que l'architecture originel d'Internet n'a guère changé et qu'on n'a pas introduit de règles contraignantes pour le trafic Internet. Les mesures de sécurité ont été laissées à la libre appréciation des utilisateurs et des services en ligne. Pour en rester à l'analogie avec la route, c'est comme si malgré le constat qu'un solide casque s'impose, son port restait facultatif.

Physiquement parlant, Internet est formé de 60 000 réseaux, ou *systèmes autonomes*. Ces systèmes sont principalement exploités par les grands opérateurs télécom, mais des organi-

[53] https://www.ted.com/talks/danny_hillis_the_internet_could_crash_we_need_a_plan_b/transcript (état: le 31 août 2016).

sations publiques ou privées de tailles diverses ont aussi le leur. Chaque exploitant de système autonome contrôle son propre réseau, alors qu'au-delà de ses frontières un corpus de règles communes s'applique, le *Border Gateway Protocol (BGP)*. Le BGP, conçu dans les années 1980 pour assurer la connectivité entre un petit nombre de réseaux, détermine aujourd'hui encore les routes empruntées par nos paquets de données. Cet héritage du passé rend la dorsale d'Internet sujette aux erreurs et aux influences indésirables. Et comme le prouvent les documents publiés par Edward Snowden, ces failles ont été largement exploitées.

Une variante consisterait à mettre en place un Internet entièrement nouveau. Les bases nécessaires sont déjà en place. Ainsi, le projet SCION de l'EPF de Zurich comporte une architecture svelte, qui permettrait de contrôler le chemin emprunté, d'identifier les erreurs et d'établir une communication de bout en bout reposant sur la confiance. Mais il faudra sans doute du temps pour qu'un tel modèle s'impose auprès des 60 000 exploitants de systèmes autonomes. Au lieu de préparer la structure de base aux défis de l'avenir, on continue de bricoler de nouvelles applications pour y ajouter des fonctions inédites. Il est surtout question aujourd'hui du Big Data ou de la technologie Blockchain. L'avenir dira si le noyau d'Internet peut être modernisé, ou si une nouvelle structure voit le jour en parallèle.

Quiconque veut faire partie du réseau doit en assumer les inconvénients. En prenant conscience des imperfections d'Internet, les utilisateurs finaux réalisent toujours mieux qu'il leur incombe de veiller à leur sphère privée et à leur sécurité. Des outils d'anonymisation comme le *navigateur TOR* sont toujours plus utilisés, et le chiffrement de bout en bout s'est répandu depuis les publications d'Edward Snowden. Les logiciels spéciaux, qui jusqu'alors nécessitaient des manipulations compliquées, se sont popularisés avec l'intégration du protocole de chiffrement Signal[54] dans le service de messagerie WhatsApp.

En définitive, la gestion des risques est du ressort de chacun – individu, organisation ou entreprise. Quelles données vais-je stocker en ligne, qui pourra y accéder, comment seront-elles utilisées et à qui procureraient-elles un avantage financier? De telles questions sont toujours plus brûlantes, alors qu'Internet est constamment tiraillé entre l'innovation, la sphère privée, la sûreté de l'information et en dernier lieu la sécurité juridique. Et comme l'innovation ne s'arrête jamais, les réponses données ne sont jamais définitives. Chacun est à tout moment confronté à de nouvelles questions. De même, l'anonymat et la sphère privée sont toujours plus difficiles à faire respecter. Le service russe FindFace en est une bonne illustration. À partir d'une photo d'une personne, il est possible de retrouver son compte dans le réseau social VK.com. L'app n'est proposée qu'en russe pour l'instant, et elle ne donne accès qu'à VK.com. Or tôt ou tard, les apps de reconnaissance faciale se répandront dans le monde entier. Il suffira d'une photo pour identifier une personne et obtenir sur Internet toutes les informations la concernant. L'anonymat dans la foule appartiendra au passé. Le progrès sur Internet représente une concurrence problématique au droit à la sphère privée.

La société devra trouver les bonnes réponses, voire un jour mettre en place des garde-fous. D'ailleurs, l'évolution d'Internet se poursuivra, et les normes sociales sont appelées à changer. D'où d'intéressantes phases de développement en perspective, au niveau d'Internet mais aussi d'un point de vue technique et sociétal, ou encore juridique et politique.

---

[54] Signal est un protocole open source moderne conçu pour la communication asynchrone, dont le cryptage est pour l'heure inviolable.

7 Politique, recherche et politiques publiques

7.1 Suisse: Interventions parlementaires

Objet	N°	Titre	Auteur	Date de dépôt	Con-seil	Dépt	État des délibérations et lien
Ip	16.3606	Qui s'occupe de la cybersécurité suisse?	Derder Fathi	17.06.2016	CN	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163606
Ip	16.3561	Élargissement de la clause de défense mutuelle de l'OTAN aux cyberattaques. Et la Suisse?	Josef Dittli	17.06.2016	CE	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163561
Mo	16.3528	Compétence en matière de cyberdéfense	Ida Glanzmann-Hunkeler	16.06.2016	CN	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163528
Ip	16.3462	Garantir la sécurité des données électroniques des patients	Edith Graf-Litscher	15.06.2016	CN	DFI	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163462
Ip	16.3413	Cyberrisques et installations nucléaires	Bea Heim	09.06.2016	CN	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163413
Ip	16.3394	Collaboration avec la Principauté de Liechtenstein dans le domaine de la sécurité	Josef Dittli	07.06.2016	CE	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163394
Qu	16.1024	Interpol, cyberrisques et cybercriminalité	Hansjörg Knecht	07.06.2016	CN	DFJP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20161024
Po	16.3382	Sécurité de l'internet des objets. Encourager l'émergence d'un savoir-faire	Claude Béglé	06.06.2016	CN	DFF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163382
Qu	16.1022	Faire toute la lumière sur la cyberattaque contre l'entreprise RUAG	Groupe PDC	02.06.2016	CN	DDPS	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20161022
Qu	16.1021	Cyberattaque contre l'entreprise RUAG et le DDPS. Il faut tirer les conséquences qui s'imposent!	Groupe des Verts	02.06.2016	CN	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20161021
Qu	16.1020	Lutte contre les cyber-risques. Institution d'un système de contrôle et d'un centre de compétences en vue de relever les défis à venir	Groupe BD	02.06.2016	CN	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20161020
Ip	16.3359	Poursuites pénales en cas d'attaques DDoS (cyberattaques). Quel soutien la Confédération fournit-elle aux cantons, qui ne disposent pas toujours du savoir-faire requis?	Marcel Dobler	31.05.2016	CN	DFJP	https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163359
Ip	16.3356	Redéployer enfin les moyens humains et financiers en faveur de la cybersécurité	Groupe socialiste	31.05.2016	CN	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163356
Ip	16.3353	A quoi sert le Réseau national de sécurité?	Werner Salzmann	30.05.2016	CN	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163353

Po	16.3348	Création d'un conseil de cyberdéfense. Une priorité pour notre souveraineté et notre sécurité	Claude Béglé	27.04.2016	CN	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163348
Mo	16.3186	Cyberrisques. Échange d'informations techniques	Corina Eichenberger	17.03.2016	CN	DFF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163186
Po	16.3058	Abandon des raccordements téléphoniques analogiques. Incidences sur les téléphones installés dans les ascenseurs et sur les autres systèmes d'alarme	Hans Egloff	08.03.2016	CN	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163058
Ip	16.3440	Quels moyens techniques pour alerter l'ensemble de la population suisse en cas de catastrophe?	Mathias Reynard	15.06.2016	CN	DDPS	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163440
Po	16.3381	Industrie 4.0. Créer une coordination au niveau suisse	Claude Béglé	06.06.2016	CN	DEFR	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163381
Ip	16.3337	Fixation dynamique des débits minimaux en vertu de l'ordonnance sur les services de télécommunication	Martin Candinas	24.04.2016	CN	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163337
Mo	16.3336	Faire passer à 10 mégabits par seconde la vitesse minimale de connexion à Internet dans le cadre du service universel	Martin Candinas	27.04.2016	CN	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163336
Po	16.3313	Examiner la mise en oeuvre de mesures contre les voyeurs qui gênent les interventions ou violent les droits de la personnalité	Bernhard Guhl	27.04.2016	CN	DFJP	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163313
Ip	16.3296	Du wi-fi partout, sauf dans les trains suisses?	Derder Fathi	26.04.2016	CN	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163296
Ip	16.3272	Fintech. Un défi pour la Suisse	Elisabeth Schneider-Schneiter	26.04.2016	CN	DFF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163272
Po	16.3245	Examiner la scission de Swisscom en une société de réseau publique et en une société de services privée	Balthasar Glättli	18.03.2016	CN	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163245
Po	16.3219	Une feuille de route pour le vote électronique	Marco Romano	18.03.2016	CN	Chf	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163219
Mo	16.3184	Numérisation et formation à l'informatique. Développement commun d'un espace numérique de formation	Jonas Fricker	17.03.2016	CN	DEFR	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163184
Ip	16.3162	Vengeance pornographique	Yvonne Feri	17.03.2016	CN	EJPD	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20163184
Mo	16.3128	Un plan national pour	Jean Chris-	16.03.2016	CN	DE-	https://www.parlament.ch/de/rats

		réduire la fracture numérique	tophe Schwaab			TEC	betrieb/suche-curia-vis-ta/geschaeft?AffairId=20163128
Mo	16.3120	Agir concrètement pour sauver et renforcer les PME	Corrado Pardini	16.03.2016	CN	DEFR	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vis-ta/geschaeft?AffairId=20163120
Po	16.3051	Abandon des raccordements téléphoniques analogiques. Incidences sur les téléphones installés dans les ascenseurs et sur les autres systèmes d'alarme	Joachim Eder	08.03.2016	CE	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vis-ta/geschaeft?AffairId=20163051
Mo	16.3007	Garantir le plus rapidement possible la modernisation des réseaux de téléphonie mobile	Commission des transports et des télécommunications CN	01.02.2016	CN	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vis-ta/geschaeft?AffairId=20163007
Ip	16.3555	Conduite autonome. Conditions-cadres et conséquences	Susanne Leutenegger Oberholzer	17.06.2016	CN	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vis-ta/geschaeft?AffairId=20163555
Mo	16.3526	Halte à la tromperie des consommateurs suisses. Pas de numéros de téléphone suisses permettant de simuler des activités économiques en Suisse	Jean-François Steiert	16.06.2016	CN	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vis-ta/geschaeft?AffairId=20163526
Mo	16.3452	Frais d'itinérance. Maintenant ça suffit!	Elisabeth Schneider-Schneiter	15.06.2016	CN	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vis-ta/geschaeft?AffairId=20163452
Qu	16.5294	Comment le Conseil fédéral compte-t-il renforcer le pilotage de la Suisse numérique?	Derder Fathi	08.01.1900	CN	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vis-ta/geschaeft?AffairId=20165294
Ip	16.3387	La facturation électronique sans signature numérique est-elle conforme au droit de la TVA?	Fabio Regazzi	07.06.2016	CN	DFF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vis-ta/geschaeft?AffairId=20163387
Mo	16.3310	Drones. Protéger la population contre les dangers potentiels	Susanne Leutenegger Oberholzer	27.04.2016	CN	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vis-ta/geschaeft?AffairId=20163310
Po	16.3260	Mettre en place une gouvernance du numérique	Claude Béglé	18.03.2016	CN	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vis-ta/geschaeft?AffairId=20163260
Qu	16.5056	Voitures sans conducteur	Susanne Leutenegger Oberholzer	02.03.2016	CN	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vis-ta/geschaeft?AffairId=20165056
Mo	16.3228	La Confédération ne doit plus être l'actionnaire majoritaire de Swisscom	Ruedi Noser	18.03.2016	CN	DE-TEC	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vis-ta/geschaeft?AffairId=20163228
Mo	16.3484	Conforter la position dominante de la Suisse dans la technologie «blockchain»	Claude Béglé	16.06.2016	CN	DFF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-vis-ta/geschaeft?AffairId=20163484
	16.044	Préservation de la valeur de Polycom. Crédit d'ensemble	Objet du Conseil fédéral	25.05.2016	CF		https://www.parlament.ch/de/ratsbetrieb/suche-curia-vis-ta/geschaeft?AffairId=20160044
Po	16.3256	Promouvoir la numérisation dans le do-	Martin Landolt	18.03.2016	CN	DFF	https://www.parlament.ch/de/ratsbetrieb/suche-curia-

		maine de la réglementation (technologies de gestion de la conformité réglementaire)					vista/geschaeft?AffairId=20163256

7.2 Directive UE sur la sécurité des réseaux et de l'information (SRI)

Au début de juillet 2016, le Parlement s'est entendu sur les termes de la première loi européenne relative à la cybersécurité. Dans sa directive sur la sécurité des réseaux et de l'information (directive SRI), l'UE vise à renforcer la capacité européenne de résistance aux cyberattaques. Les entreprises fournissant des services essentiels dans des domaines tels que l'énergie, les transports, la finance et la santé, ou les fournisseurs de services numériques (moteurs de recherche, marchés en ligne et *services en nuage*) devront adopter des mesures de sécurité pour améliorer leur cyberrésilience. Il leur incombera aussi de signaler les incidents touchant la sécurité informatique aux autorités compétentes, sous peine de sanctions. Le Parlement européen est convaincu que l'adoption de règles communes en matière de cybersécurité et la coopération accrue aideront les entreprises à se protéger face aux cyberattaques toujours plus fréquentes.

La directive SRI est en vigueur depuis août 2016 et les États membres disposent d'un délai de 21 mois à compter de cette date pour adopter les dispositions nationales nécessaires. À l'issue de cette période, ils auront six mois supplémentaires pour identifier leurs opérateurs de services essentiels.

L'adoption de la directive SRI n'aura provisoirement aucun impact sur la Suisse. Il reste à savoir dans quelle mesure la nouvelle loi européenne ainsi que la participation souhaitée au marché unique du numérique amèneront la Suisse à reprendre, dans le cadre de l'exécution autonome, des propositions telles que les normes de cybersécurité communes et le devoir d'informer les autorités des incidents. La coopération volontaire entre l'État et l'économie a fait ses preuves jusqu'ici en Suisse, dans le domaine de la sûreté de l'information. Mais il est clair qu'en cas d'adoption de normes de droit pénal accessoire obligeant à signaler les cyber-incidents, il faudrait renforcer les capacités existantes et désigner des organes de contrôle spécifiques.

7.3 France: nouvelles règles pour les opérateurs d'importance vitale (OIV)

En France, les premiers arrêtés définissant une obligation légale pour les opérateurs d'importance vitale[55] de se protéger contre les cyberattaques ont été publiés par l'Agence nationale de sécurité des systèmes d'information (ANSSI) et sont entrés en vigueur le 1er juillet 2016. Ils concernent initialement les entreprises des secteurs des produits de santé, de l'alimentation et de la gestion de l'eau, mais des arrêtés spécifiques pour les autres secteurs vont suivre. Cette base légale fait suite à la loi de programmation militaire de décembre 2013. Les infrastructures d'importance vitale devront non seulement prendre des mesures de protection, mais également annoncer les incidents qu'elles rencontrent. À noter que ce dis-

[55] MELANI parle généralement d'exploitants d'infrastructures critiques pour évoquer ces mêmes opérateurs.

positif est contraignant, puisque des sanctions sont prévues pour les infrastructures critiques ne respectant pas ces règles.

La France se dote d'un dispositif inédit en Europe, devançant ainsi les mesures qui découleront de la directive sur la sécurité des réseaux et de l'information (SRI) pour l'ensemble des pays de l'Union européenne. Notons tout de même que la SRI aura une portée plus large, s'appliquant à des entreprises non concernées par les arrêtés.

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 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, we have 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 institutions 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

8.1.3 Technical Report about the RUAG espionage case

23.05.2016 - After several months of Incident Response and Analysis in the RUAG cyber espionage case, we got the assignment from the Federal Council to write and publish a report about the findings. The following is a purely technical report, intending to inform the public about Indicators of Compromise (IOCs) and the Modus Operandi of the attacker group behind this case. We strongly believe in sharing information as one of the most powerful countermeasures against such threats; this is the main reason we publish this report not only within our constituency, but to the public as well.

➔ https://www.govcert.admin.ch/blog/22/technical-report-about-the-ruag-espionage-case

8.1.4 20min.ch Malvertising Incident

08.04.2016 - With this blog post we would like to share Indicators Of Compromise (IOCs) related to the attacks against 20min.ch, a popular newspaper website in Switzerland which got compromised and abused by hackers to infect visitors with an ebanking Trojan called Gozi ISFB. The IOCs shared in this blogpost may be used to spot infections within corporate networks.

➔ https://www.govcert.admin.ch/blog/21/20min.ch-malvertising-incident

8.1.5 Leaked Mail Accounts

18.03.2016 - MELANI/GovCERT has been informed about potentially leaked eMail Accounts that are in danger of being abused. MELANI/GovCERT provides a tool for checking whether your account might be affected: https://checktool.ch.

➔ https://www.govcert.admin.ch/blog/20/leaked-mail-accounts

8.1.6 Armada Collective is back, extorting Financial Institutions in Switzerland

11.03.2016 - A new wave of extortion emails has arrived in different Swiss Onlineshops. We have strong indications, that those extortioner are a copycat of Armada Collective.

➔ https://www.govcert.admin.ch/blog/19/armada-collective-is-back-extorting-financial-institutions-in-switzerland

8.1.7 Gozi ISFB - When A Bug Really Is A Feature

05.02.2016 - Gozi ISFB is an eBanking Trojan we already know for quite some time. Just recently, a new wave was launched against financial institutions in Switzerland. Similar to the attack we had already reported in September 2015, Cybercriminals once again compromised a major advertising network in Switzerland daily visited by a large number of Swiss internet users; they all become potential victims of the Gozi eBanking Trojan.

➔ https://www.govcert.admin.ch/blog/18/gozi-isfb-when-a-bug-really-is-a-feature

8.1.8 TorrentLocker Ransomware targeting Swiss Internet Users

21.01.2016 - On Wednesday, Jan 20 2016, we have noticed a major spam campaign hitting the Swiss cyberspace, distributing a ransomware called TorrentLocker. We have already warned about similar TorrentLocker attacks against Swiss internet users last year via Twitter. TorrentLocker is one of many ransomware families that encrypts any local file on a victim's computer and demands that the victim pays a ransom to have his files decrypted again. Since some ransomware families do not only encrypt files stored locally on the infected machine but also on any mapped network share, ransomware also represent a serious threat to corporate networks. To make sure that the malicious email goes through spam filters and gets opened by the recipient swiftly, the TorrentLocker gang is using a handful of tricks.

➔ https://www.govcert.admin.ch/blog/17/torrentlocker-ransomware-targeting-swiss-internet-users

8.2 Lettre d'information

8.2.1 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 plu-

sieurs 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

8.2.2 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

8.2.3 Rapport technique sur le maliciel utilisé lors de la cyber-attaque contre RUAG

23.05.16 - La Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) a, sur mandat du Conseil fédéral, publié un rapport avec les éléments techniques du cas ayant touché RUAG. Ce rapport est destiné aux professionnels de la sécurité, et doit les soutenir dans leur tâche d'identification des risques dans leurs réseaux et de mise en place de mesures de sécurité.

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

8.2.4 Journée suisse de sensibilisation aux rançongiciels

19.05.16 - La Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) organise jeudi prochain en collaboration avec d'autres partenaires une journée de sensibilisation aux rançongiciels (ransomware). Parmi les participants à cette journée figurent, notamment, des organisations actives dans divers secteurs telles que des fabricants de logiciels, des offices fédéraux ainsi que plusieurs associations suisses et organismes de protection des consommateurs.

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

8.2.5 22e rapport semestriel de MELANI: gestion des lacunes de sécurité, vulnérabilité des infrastructures et attaques DDoS

28.04.2016 - Le second semestre 2015 a été marqué au niveau mondial par des cyberincidents parfois spectaculaires. Les diverses attaques ont notamment été réalisées par déni de service (distributed denial of service, DDoS) ou par hameçonnage, ou ont été lancées contre

des systèmes de contrôle industriels. Publié aujourd'hui, le 22e rapport semestriel de MELANI a pour thème prioritaire la gestion des lacunes de sécurité.

➔ https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/rapport_semestriel-2-2015.html

8.2.6 Les mots de passe de 6000 comptes de messagerie suisses circulent

18.03.2016 - La Centrale d'enregistrement et d'analyse pour la sûreté de l'information a reçu une liste de 6000 adresses de comptes de messagerie ayant apparemment été piratées et qui pourraient maintenant être utilisées à des fins illicites.

➔ https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/passwoerter-von-6000-e-mail-konten-im-umlauf.html

8.2.7 Appels téléphoniques frauduleux aux PME en lien avec le cheval de Troie bancaire "Retefe"

16.02.2016 - Depuis début février 2016, la Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI et le service de coordination de la lutte contre la criminalité sur Internet SCOCI observent une augmentation des messages concernant des appels téléphoniques frauduleux. Ces appels ont pour but de préparer une fraude eBanking.

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

8.3 Listes de contrôle et instructions

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

9 Glossaire

Terme	Définition
Active Directory	Active Directory (AD) est la mise en œuvre par Microsoft des services d'annuaire LDAP pour les systèmes d'exploitation Windows.
Adresse MAC	Adresse matérielle d'une carte réseau qui en permet l'identification unique dans le monde entier. L'adresse MAC est inscrite dans la ROM de la carte par les différents fabricants (exemple : 00:0d:93:ff:fe:a1:96:72).
Advanced Persistent Threats (APT)	Menace pouvant infliger de sérieux dommages à une organisation ou à un pays. L'agresseur est disposé à investir beaucoup de temps, d'argent et de savoir-faire dans ce genre d'attaque ciblée et furtive, et dispose d'importantes ressources.

Air gap	Mesure de sécurité consistant à isoler physiquement un système à sécuriser de tout réseau informatique. Cette mesure, lorsqu'elle est correctement implémentée, rend toute tentative de piratage à distance impossible.
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.
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.
Batchjob	Traitement par lots. Enchaînement automatique d'une suite de commandes sur un ordinateur, sans intervention d'un opérateur. Une fois le processus terminé, le lot suivant est traité. Le traitement des lots s'achève quand tous les lots de la pile ont été exécutés.
Bitcoin	«Bitcoin» désigne à la fois un système de paiement à travers le réseau Internet et l'unité de compte utilisée par ce système de paiement.
Booter / Stresser	Ceux-ci sont des services permettant de lancer une attaque DDoS contre de l'argent («DDoS as a service»).
Border Gateway Protocol (BGP)	Protocole d'échange de routes utilisé notamment sur le réseau Internet, pour la connectivité entre des systèmes autonomes.
Certificat numérique	Attestation qu'une entité (personne, ordinateur) possède une clé publique (PKI).
Cheval de Troie	Les chevaux de Troie sont des programmes qui, de manière larvée, exécutent des actions préjudiciables tout en se présentant à l'utilisateur comme des applications ou des fichiers utiles.
Cloud Computing	L'informatique dans les nuages (cloud computing, cloud IT) est une notion propre aux technologies de l'information. Les TIC ne sont plus gérées et mises à disposition par l'utilisateur, mais acquises d'un ou plusieurs prestataires. Les applications et les données ne se trouvent plus sur l'ordinateur local ou au centre de calcul de l'entreprise, mais dans le nuage (cloud). L'accès à ces systèmes à distance s'effectue par un réseau.
Code source	Instructions originales d'un programme écrites dans un langage lisible par l'homme.

Crimeware Kit	Boîte à outils composée de codes malveillants personnalisables et permettant même aux débutants de lancer à grande échelle des attaques «clés en main».
Dynamic Link Library	L'acronyme DLL, en français bibliothèque de liens dynamiques, désigne une collection partageable de sous-programmes spécialisés qui peuvent être appelés depuis un programme ou une application en cours d'exécution.
Fichier binaire	Un fichier binaire n'est pas assimilable à un fichier texte et ne peut être lu directement par un éditeur de texte. Les fichiers binaires peuvent contenir du langage machine, du son, des images, etc.
Fichier d'animation SWF	Acronyme de Shockwave Flash. À l'époque, la société Macromedia commercialisait Flash sous le nom de Shockwave. Flash est une plateforme de programmation et de présentation de contenus multimédia et interactifs.
Fichier INI	Fichier de configuration dans un format de données introduit par les systèmes d'exploitation Windows en 1985. Par convention, les noms de ces fichiers texte portent l'extension «.ini».
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.
Grey hat	Chapeau gris: hacker malfaisant avec une certaine éthique, n'agissant pas par intérêt personnel.
Infection par «drive-by download»	Infection d'un ordinateur par un maliciel, lors de la simple visite d'un site web. Les sites concernés contiennent dans bien des cas des offres sérieuses, mais ont été compromis auparavant pour la diffusion de maliciels. Différents exploits, tirant parti des lacunes de sécurité non comblées par le visiteur, sont souvent testés à cet effet.
Injecteur	(en anglais dropper); programme informatique créé pour installer un logiciel malveillant sur un système cible. Il s'agit d'une forme minimaliste de cheval de Troie.
Interface utilisateur	Ensemble des outils logiciels ou matériels développés et mis à la disposition d'une personne pour dialoguer avec l'ordinateur qu'elle utilise.
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 véri-

	fier 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.
Keylogger	Appareil ou programme intercalé entre l'ordinateur et le clavier qui permet d'enregistrer toute saisie au clavier.
Lacunes de sécurité	Lacunes de sécurité Erreur inhérente au matériel ou aux logiciels, permettant à un pirate d'accéder au système.
Malicious Code	Programme malveillant. Terme générique employé pour tout logiciel exécutant des fonctions nuisibles sur un ordinateur (comme p.ex. les virus, les vers ou les chevaux de Troie).
Man-in-the-middle attack (MITM)	Attaque de l'intermédiaire. Attaque où le pirate s'immisce dans le canal de communication de deux partenaires pour lire ou modifier les données échangées.
Monnaie électronique	Valeur monétaire représentant une créance sur l'émetteur, qui est stockée sur un support électronique, émise contre la remise de fonds d'un montant dont la valeur n'est pas inférieure à la valeur monétaire émise, acceptée comme moyen de paiement par des entreprises autres que l'émetteur.
Navigateur	Logiciel utilisé essentiellement pour afficher les différents contenus du web. Les navigateurs les plus connus sont Internet Explorer, Opera, Firefox et Safari.
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.
Pipe	Canal ou tube; espace de communication interprocessus permettant à un programme d'utiliser son espace de sortie comme espace d'entrée vers un autre programme, facilitant ainsi la transmission des données.
Point-of-Sale Terminals (POS)	Terminal de point de vente acceptant le paiement sans numéraire (carte de débit ou de crédit).

Pourriel (Spam)	Désigne le courrier électronique non sollicité, constitué surtout de publicité, envoyé automatiquement. L'auteur de tels messages est qualifié de polluposteur (spammer) et ses envois de pollupostage (spamming).
Programmable Logic Controller (PLC)	Un automate programmable industriel (en angl. programmable logic controller, PLC), est un dispositif électronique programmable destiné à la commande de processus industriels par un traitement séquentiel. Depuis plusieurs années, de tels dispositifs remplacent dans la plupart des domaines le pilotage par des réseaux logiques câblés.
Ransomware	Maliciel utilisé comme moyen de chantage contre le propriétaire de l'ordinateur infecté. Typiquement, le pirate crypte ou efface des données et ne fournit la clé nécessaire pour les sauver qu'après le versement d'une rançon.
Remote Desktop Protocol, RDP	Protocole propriétaire, servant à la prise de contrôle à distance des postes Microsoft Windows.
Réseau de zombies	Réseau d'ordinateurs infectés par des programmes malveillants (bots). Un pirate (le propriétaire du réseau de zombies) les contrôle complètement à distance. Un réseau de zombies peut compter de quelques centaines à des millions d'ordinateurs compromis.
Rootkit	Ensemble de programmes et de techniques permettant d'accéder sans être remarqué à un ordinateur pour en prendre le contrôle.
Router	Dispositif intelligent assurant la connexion physique entre plusieurs réseaux (informatique, télécommunication, Internet). Un router s'utilise par exemple dans un réseau domestique, où il optimise la transmission de l'information entre le réseau interne et Intranet.
Serveur Command & Control	La plupart des réseaux de zombies reçoivent des instructions de leur créateur, qui les surveille par un canal de communication. Le cas échéant, on parle de serveur Command & Control (C&C).
SSID	Acronyme de service set identifier; chaîne de 32 caractères de l'en-tête des paquets de données d'un réseau sans fil de type Wi-Fi, utilisée comme mot de passe permettant aux connexions de s'établir.
Système autonome (AS)	(en angl. autonomous system, AS); ensemble de réseaux informatiques IP intégrés à Internet et dont la politique de routage interne (routes à choisir en priorité, filtrage des annonces) est cohérente.

Systèmes de contrôle-commande (SCI)	Les systèmes de contrôle-commande sont formés d'un ou plusieurs appareils qui pilotent, règlent et/ou surveillent le fonctionnement d'autres appareils ou systèmes. L'expression «systèmes de contrôle industriels» (industrial control systems, ICS) est entrée dans le langage courant.
Tor	Réseau informatique décentralisé permettant d'anonymiser les connexions.
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	Programme informatique d'autoréplication, doté de fonctions nuisibles, qui s'installe en annexe d'un programme ou fichier hôte pour se propager.
Virus macro	Virus informatique modifiant ou remplaçant une macro, à savoir un ensemble de commandes utilisées par des logiciels pour exécuter des actions courantes.
Wipe	Utilitaire spécialisé dans la suppression des fichiers. Une fois les données effacées, elles sont écrasées plusieurs fois avec des zéros, des séquences de bits ou des données aléatoires.
WLAN	Un WLAN (Wireless Local Area Network) est un réseau local sans fil.
WPA2	Wi-Fi Protected Access 2 Nouvelle norme de sécurité s'appliquant aux réseaux de radiocommunication conformément à la spécification IEEE 802.11i. Elle remplace le système de cryptage WPA, ainsi que WEP considéré comme peu sûr.