Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

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

SÛRETÉ DE L'INFORMATION

SITUATION EN SUISSE ET SUR LE PLAN INTERNATIONAL

Rapport semestriel 2019/2 (de juillet à décembre)

30 AVRIL 2020

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

1 Aperçu / sommaire

2 Éditorial

Le délégué de la Confédération à la cybersécurité

Florian Schütz est le délégué de la Confédération à la cybersécurité et le directeur du NCSC.

MELANI devient le Centre national pour la cybersécurité. Tel était le titre d'un article publié sur le site de MELANI début 2020. Il s'agit là d'une étape supplémentaire vers la répartition, au sein de la Confédération, des responsabilités définies par le Conseil fédéral le 30 janvier 2019 (voir fig. 1). L'organisation détaillée du Centre national pour la cybersécurité (NCSC) est en cours. Ce qui est certain, c'est que MELANI en constitue un élément clé et fera l'objet de mesures de renforcement et de développement. Je profite donc de cet éditorial pour retracer mon expérience avec MELANI au cours du second semestre 2019, et pour exposer trois défis à relever.

Premier défi: depuis la création de MELANI le 1er octobre 2004, les technologies de l'information et de la communication ont continué de pénétrer l'économie, la recherche et la société. Désormais présentes dans tous les domaines de la vie ou presque, elles sont au cœur des processus numériques. Dresser un bilan général de la situation ne suffit plus à identifier la grande variété des menaces qui pèsent sur ces outils. Il faut des analyses spécifiques pour chaque secteur de l'économie, de la politique, de la recherche et de la société. C'est dans cet esprit qu'un projet pilote teste, en ce moment, un bilan spécifique de la situation pour le secteur financier.

Deuxième défi: l'explosion du nombre d'incidents. Pendant la première année de fonctionnement de MELANI, il y a 15 ans, la centrale a reçu moins de 500 signalements. Cette année, elle en a reçu plus de 500 rien qu'en janvier. Afin de traiter ce volume, elle a mis en place au deuxième semestre 2019 un guichet national chargé de recevoir les signalements, de les analyser et de confier leur prise en charge au service qui convient.

Troisième défi: améliorer l'automatisation de l'analyse et du traitement et l'intégration des services concernés (les autorités de poursuite pénale, p. ex.).

«Vous avez été pesé, vous avez été mesuré, et on vous a jugé insuffisant.» Cette réplique est tirée du film *Chevalier* (*A Knight's Tale*) de Brian Helgeland. Malgré l'excellente réputation dont jouit MELANI sur le plan international, nous entendons de temps à autre dire, dans des discussions publiques, qu'elle est insuffisante. S'il est incontestable que la centrale peut mieux faire, cette critique à l'emporte-pièce est injuste pour l'excellent travail des équipes. Pour nous, elle tient au fait que l'absence d'indicateurs clés de performance (ICP) empêche d'avoir une bonne vue d'ensemble, d'où le risque de tirer des conclusions erronées de certaines situations. Nous allons donc établir des ICP afin de permettre une critique mieux informée et une meilleure mesure des résultats.

S'agissant des critiques, nous avons reçu l'une d'elles cinq sur cinq: certains déploraient en effet le côté trop peu technique du rapport semestriel de MELANI. Aussi, pour continuer d'intéresser non seulement le groupe cible que forment les politiques, les dirigeants et certains particuliers, mais aussi les spécialistes, avons-nous rédigé pour la première fois une annexe technique. Nous serions d'ailleurs très heureux que vous nous fassiez part de vos remarques

et suggestions à ce propos. Merci de nous écrire pour nous dire si vous souhaitez que nous développions à l'avenir cette annexe[1].

En 15 ans, MELANI a réalisé un travail considérable, comme en témoigne le présent rapport. L'avenir lui réserve sans aucun doute de nouveaux défis de taille. Mais j'ai la conviction que nous saurons les relever, et que la nouvelle organisation du CNCS se révélera un solide atout.

Florian Schütz

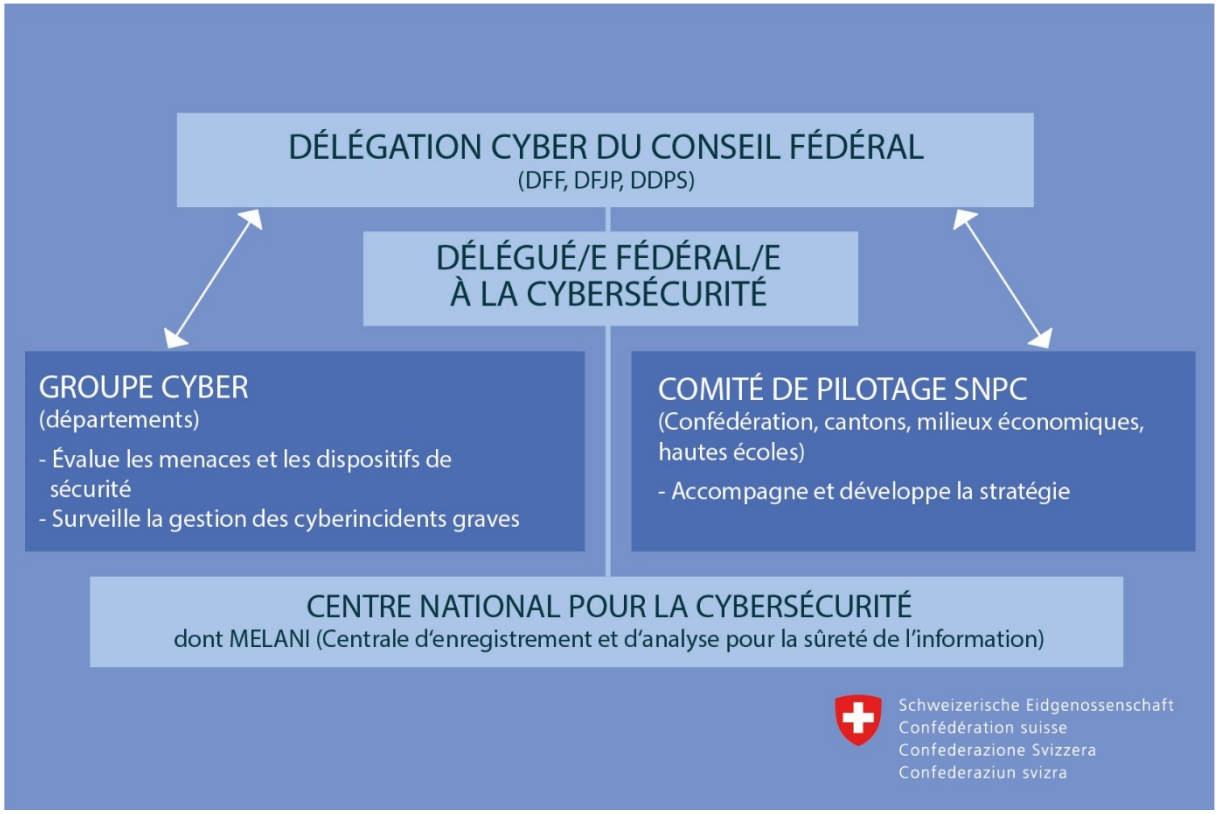

Fig. 1: Organisation de la Confédération en matière de cybersécurité

[1] Nous vous invitons à remplir l'évaluation du rapport sur notre page web : https://www.melani.admin.ch/melani/fr/home/documentation/rapports/evaluation-halbjahresbericht.html

3 Thème prioritaire: les données personnelles sur Internet

3.1 Introduction

L'essentiel du traitement de données se fait aujourd'hui par voie électronique, sur des appareils plus ou moins directement connectés à Internet. Bon nombre de données sont enregistrées sur un «nuage», où on peut les consulter.

«Nos données», ou plus exactement «des données nous concernant», sont enregistrées dans une multitude d'endroits par une multitude d'acteurs sans que personne sache au juste qui dispose de quelles données sur sa personne, et où celles-ci sont traitées.

Les données font l'objet de collectes, d'échanges et d'agrégations, mais aussi de vols (le terme «vols» prêtant à confusion puisqu'il s'agit de simples copies; le propriétaire n'est pas dépossédé). Il en va de même pour la «vente» de données. Les données sont souvent «vendues», dupliquées puis revendues. Cela brouille considérablement les pistes si l'on veut remonter à la source de certaines données.

L'autodétermination en ce qui concerne ses propres données est presque impossible, et poursuivre les infractions à la protection des données est extrêmement complexe pour les services compétents comme pour les personnes concernées.

Les fuites de données ou la divulgation de données par suite d'erreurs de configuration font presque quotidiennement la une des médias[2]. Pour les affaires les plus graves, on estime actuellement que plus d'un milliard de lots de données sont concernés[3]. MELANI a fait des fuites de données le thème prioritaire de son rapport semestriel 2017/2[4].

3.2 Les données du cybermonde

Nous vivons à l'ère du tout connecté. Internet est définitivement ancré dans notre quotidien. Nous utilisons le réseau mondial pour commander des produits et des services, rechercher des informations, échanger des points de vue, des photos et bien d'autres choses encore. Nous ouvrons ainsi, presque sans y penser, une multitude de comptes auprès d'une multitude de fournisseurs, que nous oublions parfois aussi rapidement que nous les avons créés. Chacun de ces comptes est associé à une adresse de messagerie et à un mot de passe. Certains exigent en plus notre nom, notre adresse, notre date de naissance, notre numéro de téléphone, des photos, voire un numéro de carte de crédit. Les exploitants de ces services possèdent vraisemblablement des informations sur les éléments que nous avons consultés ou télétransmis en utilisant le compte ouvert chez eux. Les réseaux sociaux sont particulièrement bien informés: ils savent qui sont nos amis et nos contacts, qui nous suivons, ce que nous

---

2 https://www.helpnetsecurity.com/2019/11/14/breaches-2019/ ; https://www.immuniweb.com/blog/stolen-credentials-dark-web-fortune-500.html

3 https://securityaffairs.co/wordpress/94275/breaking-news/elasticsearch-social-information-1-2b-people.html (en); https://www.wired.com/story/billion-records-exposed-online/

4 MELANI, rapport semestriel 2017/2, chap. 3.

aimons, ce que nous partageons et le temps que nous consacrons à tel ou tel sujet. Ces renseignements permettent d'établir des profils de personnalité très détaillés.

Rien qu'en nous promenant sur la toile, nous laissons derrière nous une trace numérique sous forme de données qui s'enregistrent sur les serveurs des prestataires de services, des réseaux publicitaires et autres fournisseurs de contenus, ou sur nos propres appareils, par exemple sous la forme de *cookies*. Certaines extensions de navigateur (*add-ons* ou *plug-ins*) recueillent aussi des données pour les enregistrer ou les transmettre[5]. Celles-ci ne se rattachent pas forcément au nom d'une personne, mais à un pseudonyme. Elles permettent elles aussi de créer un profil de personnalité en vue de proposer des publicités ciblées ou d'autres contenus susceptibles de nous intéresser. Lorsqu'elles sont associées à un identifiant personnel (adresse de messagerie ou compte de réseau social, p. ex.), elles peuvent être extraites du contexte où elles ont été recueillies afin d'être traitées et exploitées de manière personnalisée.

3.3 Les données du monde analogique

L'apparition de l'informatique a entraîné l'enregistrement des données du monde analogique sous une forme numérique, initialement sur des ordinateurs ou des réseaux d'entreprise isolés, puis de plus en plus sur des appareils plus ou moins directement connectés à Internet. La correspondance, les plannings, les fichiers de clients, la comptabilité et la gestion des ressources humaines sont largement passés au numérique. Notre carnet d'adresses privé, par exemple, n'existe souvent plus que sur notre ordinateur, sur notre smartphone ou sur un nuage.

La transformation numérique a accéléré le traitement électronique des données dans un nombre croissant de domaines: la santé, avec le dossier électronique du patient ou les applications de remise en forme, la mobilité, avec les billets de transports publics achetés en ligne ou les applications de location de vélo, le logement avec les appareils domestiques «intelligents», la consommation, avec les commandes en ligne, et la liste est encore longue.

Les autorités aussi ont adopté il y a belle lurette les bases de données électroniques et l'interconnexion généralisée, et développent les services de cyberadministration. Lorsque des acteurs non autorisés parviennent à accéder aux systèmes d'une autorité, une grande partie, voire la totalité de la population est potentiellement touchée[6].

3.4 Cas particulier des bases de données et des registres publics

S'agissant des registres publics traditionnels qui ont été mis en ligne, il faut tenir compte de certains aspects propres à Internet. Des renseignements qu'on recevait naguère sur papier, en un seul exemplaire, ou qu'on ne pouvait consulter qu'en se déplaçant dans un service donné, sont désormais accessibles de n'importe quel endroit du monde, et enregistrables lo-

---

5 https://www.washingtonpost.com/technology/2019/07/18/i-found-your-data-its-sale/

6 Équateur https://www.zdnet.com/article/database-leaks-data-on-most-of-ecuadors-citizens-including-6-7-million-children/;
Chili https://www.zdnet.com/article/voter-records-for-80-of-chiles-population-left-exposed-online/;
Bulgarie https://www.inside-it.ch/articles/55013

calement. Certes, les ordonnances correspondantes imposent que les systèmes soient protégés «contre les appels en série[7]» ou que certaines données «soient gratuitement accessibles sur Internet pour des consultations individuelles[8]», mais selon le degré de technicité de la mise en œuvre, un *hacker* patient et inventif finira par parvenir à pirater un registre complet. Il y a donc un équilibre fragile à trouver entre la publication (y compris électronique) des données prévue par la loi et la protection de ces données contre les abus. Les bases légales sont muettes quant à la possibilité de consulter les données de manière anonyme. Pour empêcher efficacement les consultations de masse malveillantes, ou du moins les détecter, il faudrait pouvoir identifier les utilisateurs et enregistrer leur historique de consultation pour une période déterminée, ce qui nécessite de nouvelles bases légales.

Les annuaires téléphoniques ont été numérisés dès la fin des années 1980 pour être proposés à la vente sur CD. Ces données ont été rapidement rendues disponibles sur Internet, ce qui était autorisé puisqu'elles étaient déjà accessibles publiquement. Quoique les annuaires contiennent peu de numéros de téléphone mobile ou d'adresses de messagerie, leurs données peuvent servir à constituer une base, en particulier pour les acteurs se souciant peu de légalité.

Les informations du répertoire «domain whois», qui étaient jadis publiquement accessibles, constituent à cet égard un exemple parlant. Elles indiquent notamment le détenteur d'un nom de domaine. Ces données ne sont plus accessibles aussi facilement. Initialement, ce répertoire devait permettre de retrouver le propriétaire et l'exploitant d'un site afin de pouvoir les joindre. Dans l'Internet des débuts, pétri d'idéaux, la transparence allait de soi. Mais l'usage frauduleux des données qui s'est fait jour progressivement a vite généré des débats sur la forme, le but et la nécessité de ce registre. La mise en œuvre du règlement général de l'UE sur la protection des données (RGPD) a donné lieu à des mesures, et les indications relatives aux noms de domaine sont désormais largement anonymisées[9]. L'accès aux informations «whois» sur les noms de domaine suisses devrait quant à lui être réduit dans le cadre de la révision prochaine du droit des télécommunications.

3.5 Législation sur la protection des données

Le traitement de données et le commerce de données personnelles sont autorisés selon les circonstances et selon le droit applicable. Mais les prescriptions en matière de protection des données varient considérablement d'un pays à l'autre. Avec son RGPD, l'UE impose une protection uniforme des données de ses citoyens partout dans le monde. Même s'il laisse en suspens de nombreuses questions quant à la mise en œuvre internationale de ces prescriptions, le règlement a déjà produit des effets. Depuis son entrée en vigueur en mai 2018, quantité d'acteurs prennent beaucoup plus au sérieux la protection des données.

---

7 Art. 27 de l'ordonnance sur le registre foncier (ORF), RS **211.432.1**: https://www.admin.ch/opc/fr/classified-compilation/20111142/index.html#a27

8 Art. 12 de l'ordonnance sur le registre du commerce (ORC), RS **221.411**: https://www.admin.ch/opc/fr/classified-compilation/20072056/index.html#a12

9 https://www.icann.org/resources/pages/gtld-registration-data-specs-en

Selon de nombreuses prévisions, les fuites de données causeront dans un avenir proche des dommages plus importants, et la sécurité des données fera l'objet d'investissements renforcés[10]. En effet, depuis l'entrée en vigueur du RGPD, les entreprises qui portent atteinte à la protection des données sont sanctionnées par de lourdes amendes. L'estimation des dommages inclut notamment les amendes susceptibles d'être infligées aux entreprises, lesquelles peuvent atteindre 20 millions d'euros ou 4 % du chiffre d'affaires annuel si ce pourcentage dépasse 20 millions d'euros.

La révision de la loi suisse sur la protection des données (LPD) prévoit des dispositions pénales permettant de punir non pas des entreprises, mais des particuliers, c'est-à-dire des employés de celles-ci. Une entreprise ne peut être condamnée à payer que lorsque l'amende envisagée est inférieure à 50 000 francs, si l'identification de l'auteur des faits condamnables risque d'occasionner des efforts démesurés. L'avenir dira dans quelle mesure ces dispositions créeront des tensions dans les entreprises, selon que la direction prendra ou non des décisions et émettra ou non des prescriptions dont les conséquences devront être assumées par les responsables de la protection des données ou par de simples collaborateurs.

3.6 Risques et effets secondaires

On parle peu des dommages que causent les atteintes à la protection des données chez les personnes concernées. Il est vrai qu'ils sont difficiles à chiffrer. Certes, les données telles que nom, adresse, numéro de téléphone, adresse de messagerie, etc. ne sont pas «sensibles», mais des personnes mal intentionnées peuvent les exploiter dans un but nuisible, le moindre étant une multiplication des courriels indésirables (*spam*). Les criminels utilisent les données obtenues frauduleusement pour lancer des attaques sur mesure d'ingénierie sociale, qui visent l'installation de maliciels, l'obtention de données supplémentaires (plus sensibles), l'exécution de paiements injustifiés ou d'autres effets négatifs pour les personnes concernées[11]. Les données personnelles peuvent aussi servir à des usurpations d'identité. Les escrocs en profitent pour créer des comptes sur les réseaux sociaux, pour enregistrer des noms de domaine ou pour passer des commandes. Les contacts de personnes dont le compte de messagerie a été piraté, ou dont les données ont fuité d'une manière ou d'une autre, font aussi régulièrement l'objet d'abus.

Les conséquences de l'obtention et de la transformation frauduleuses de données sont difficiles à évaluer. À l'ère des *big data* et de l'apprentissage automatique, il est de plus en plus facile d'automatiser l'association des sources de données les plus variées. Que cela se passe dans les entreprises, pour des motifs légitimes, dans un certain flou juridique («zone grise») ou dans le milieu criminel n'importe que superficiellement. Il faut partir du principe que toute base de données sera piratée tôt ou tard, et que son contenu finira sur le marché clandestin.

---

10 https://securityintelligence.com/articles/11-stats-on-ciso-spending-to-inform-your-2020-cybersecurity-budget/; https://www.business2community.com/cybersecurity/10-cybersecurity-trends-in-2020-you-need-to-keep-an-eye-on-02275883; https://www.forbes.com/sites/gilpress/2019/12/03/141-cybersecurity-predictions-for-2020/; https://www.forbes.com/sites/gilpress/2019/12/12/42-more-cybersecurity-predictions-for-2020/

11 Voir https://www.microsoft.com/security/blog/2019/12/02/spear-phishing-campaigns-sharper-than-you-think/ (en) et les chapitres «Ingénierie sociale» des rapports semestriels de MELANI.

3.7 Conclusion

«Nos données» ou des «données nous concernant» sont enregistrées dans une multitude d'endroits par une multitude d'acteurs. La collecte de données est un modèle d'affaires tant dans les milieux illégaux que dans les milieux légaux et entraîne le négoce de ces données. Nous devons nous faire à l'idée que des entreprises, des annonceurs mais aussi des criminels possèdent des données plus ou moins nombreuses nous concernant et qu'ils peuvent les utiliser pour nous toucher directement. Lorsque ces données servent, en outre, à établir des profils de personnalité, elles leur permettent d'exercer sur nous une influence psychologique spécifique, en matière non seulement de consommation et de vulnérabilité à l'escroquerie, mais aussi de formation d'opinions et, par conséquent, de vote.

La publicité que nous voyons sur Internet est déjà largement personnalisée. Cette tendance va se poursuivre, et les acteurs politiques y adhéreront sans doute de plus en plus pour diffuser leurs arguments électoraux.

Les criminels continueront de peaufiner leurs méthodes d'attaque pour cibler plus précisément leurs victimes potentielles. Les formules de politesse personnalisées en tête des courriels ne sont plus un gage de fiabilité, tant s'en faut. Voilà longtemps que les criminels indiquent dans leurs messages les nom, adresse, numéro de téléphone et d'autres éléments personnels concernant le destinataire. Ils choisissent même régulièrement leurs adresses d'expéditeur de manière à ce que le message ait l'air de provenir d'une connaissance, quand ils ne piratent pas carrément la messagerie ou le compte de réseau social véritable, mais compromis, de l'expéditeur supposé.

Appréciation / recommandations:

S'il est vrai qu'Internet présente de nombreux avantages et facilite énormément l'accès à de précieuses informations: ne croyez pas tout ce qui s'y publie, ni tout ce qui arrive dans votre boîte de réception. Armez-vous de prudence et d'une bonne dose de méfiance lorsque vous surfez et que vous communiquez sur le Net. En cas de doute, n'hésitez pas à discuter avec vos connaissances pour faire le point sur un sujet, sur un événement ou sur une nouvelle curieuse. Et avant de cliquer sur un lien ou d'ouvrir une pièce jointe à un courriel, vérifiez auprès de l'expéditeur supposé que c'est bien lui qui vous l'a envoyé.

Quiconque modifie et enregistre des données personnelles doit par conséquent veiller à les protéger contre les accès non autorisés. Les registres publics doivent pouvoir être consultés mais sans permettre les consultations de masse. S'agissant des bases de données dont l'accès est restreint (parce qu'en mode «test» ou «démonstration», p. ex.), il faut veiller à ce que les restrictions ne puissent pas être contournées, ce que tentent précisément de faire les acteurs qui se sont spécialisés dans la collecte de données, par exemple en générant automatiquement un grand nombre de comptes tests ou en faisant croire par d'autres moyens à l'existence d'un grand nombre d'utilisateurs.

4 Situation

Les particuliers peuvent utiliser le formulaire d'annonce de MELANI[12] pour nous signaler des incidents et nous poser des questions. Ces signalements nous aident à détecter des tendances en matière de cyberdangers, à communiquer à leur sujet et, le cas échéant, à recommander des mesures ou à les prendre nous-mêmes. Le graphique ci-après sur la nature et le nombre des signalements reçus au deuxième semestre 2019 donne des indications sur les sujets qui ont préoccupé la population suisse pendant cette période.

Internet est le lieu de tous les mensonges et de tous les abus. Les signalements de cas de phishing, d'escroquerie et de sextortion le confirment. Il s'agit de phénomènes relativement faciles à identifier et qui aboutissent donc fréquemment à des signalements. Il est pratiquement certain que la plupart de ces signalements proviennent d'utilisateurs qui ont détecté la menace et n'en sont pas devenus les victimes. Nous ne pouvons pas nous prononcer sur le taux de réussite de ces attaques. Pour ce qui est des signalements portant sur des maliciels, par contre, l'incident sous-jacent a parfois fait des dégâts, si minimes soient-ils. Certains maliciels agissent dans l'ombre sans être remarqués et ne sont donc pas signalés (voir la question du *drive-by download* en Suisse, chap. 4.3.2).

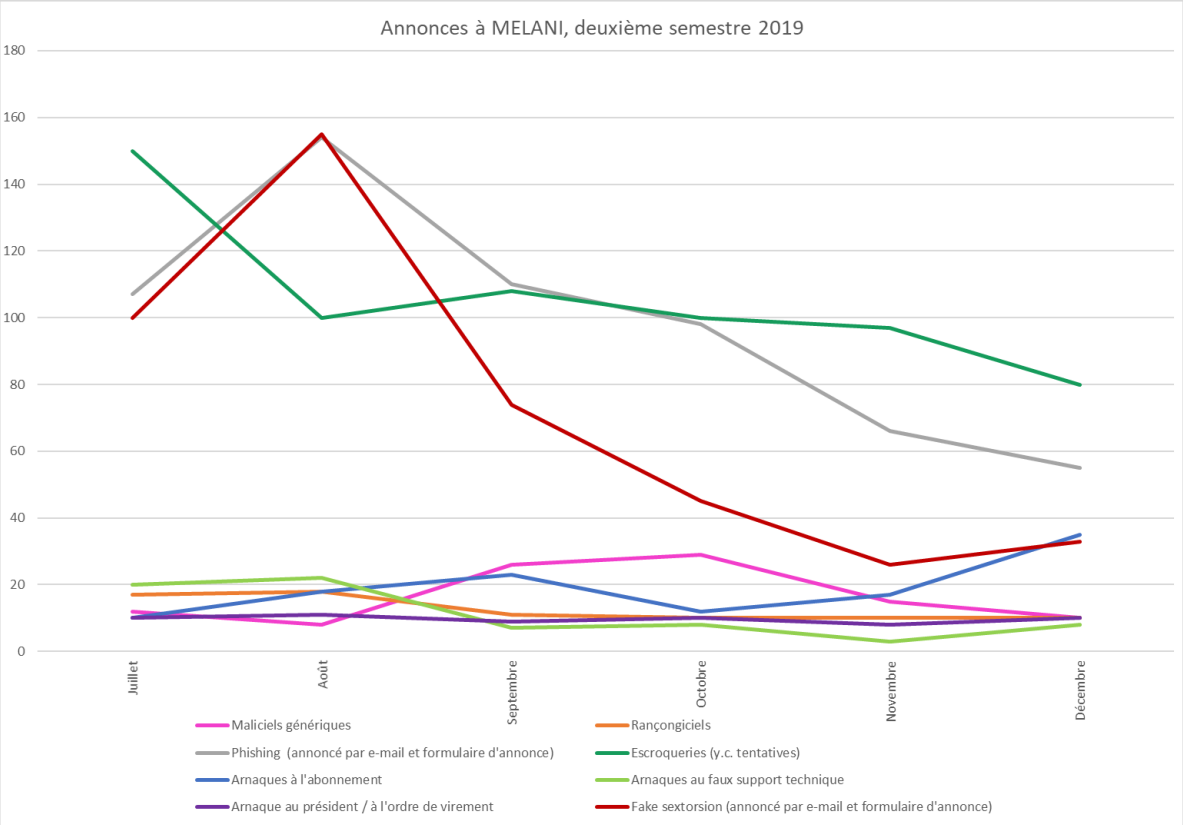

Fig. 2: Signalements effectués au moyen du formulaire d'annonce en ligne (les signalements provenant d'autres sources ne sont pas pris en compte).

12 https://www.melani.admin.ch/melani/fr/home/meldeformular/formular0.html

4.1 Espionnage

Au deuxième semestre 2019, les États ont encore beaucoup recouru au cyberespionnage pour soutenir la collecte d'informations et les vols de propriété intellectuelle. Le groupe d'analyse des menaces (Threat analysis group [TAG]) de Google a pour mission de détecter et de repousser les cyberattaques visant les utilisateurs des services de l'entreprise. Il a par exemple signalé, rien que pour le troisième trimestre 2019 (de juillet à septembre), 12 000 tentatives de phishing ciblé (*spear phishing*) dans 149 États[13], lesquelles seraient dues à plus de 270 groupes liés à des gouvernements et agissant dans au moins 50 pays. Outre les activités d'espionnage traditionnelles, le TAG a aussi repéré des campagnes de désinformation visant à promouvoir les intérêts d'un État donné ou à discriminer des mouvements politiques. Les politiques font partie, comme les dissidents et les activistes, du groupe à fort potentiel de risque. C'est ce que confirment des centaines de tentatives d'attaque contre des organisations politiques enregistrées par AccountGuard, le service de sécurité de Microsoft. Cette plateforme a été créée pour mettre en garde les services officiels et les candidats en campagne électorale menacés de cyberattaques. Les principales cibles des tentatives de cybercompromission soutenues par des États seraient toutefois les grandes entreprises. Elles représenteraient plus des trois quarts des 10 000 utilisateurs ayant fait l'objet d'un signalement de la part de Microsoft en 2019[14]. Le géant du logiciel a établi la liste des cinq groupes de menaces persistantes avancées (*advanced persistent threats [APT]*) les plus actifs de l'année 2019. Parmi ces groupes, Holmium alias APT33 serait financé, selon Microsoft et d'autres entreprises de sécurité[15], par le gouvernement iranien. Il ciblerait en priorité des organisations opérant dans les domaines de l'aviation civile et militaire et dans celui de l'énergie pétrochimique. Il a fait la une des médias pour avoir attaqué, notamment, deux entreprises d'aviation, l'une américaine l'autre saoudienne, en 2016 et en 2017[16]. Sur la liste établie par Microsoft figure aussi Strontium, alias Fancy Bear, alias APT28 ou encore Sofacy. Selon des communications officielles de plusieurs pays (notamment le Royaume-Uni et les États-Unis) et des entreprises de sécurité (telles que CrowdStrike), ce groupe serait lié au service de renseignement militaire russe (GRU). Il serait impliqué dans les attaques perpétrées contre le Bundestag allemand (en 2015), le Comité national démocrate américain (en 2016) et l'Agence mondiale antidopage (en 2016).

4.1.1 Cyberattaques contre des organisations sportives et antidopage

Les organisations sportives et antidopage sont depuis plusieurs années déjà la cible de campagnes de cyberespionnage. Comme le relate le rapport semestriel MELANI 2018/1 (chap. 4.1.1), l'infrastructure des Jeux olympiques d'hiver de Pyeongchang (Corée du Sud) a été, cette année-là, attaquée par le ver Olympic Destroyer, à propos duquel le spécialiste de

---

13 https://blog.google/technology/safety-security/threat-analysis-group/protecting-users-government-backed-hacking-and-disinformation/

14 https://blogs.microsoft.com/on-the-issues/2019/07/17/new-cyberthreats-require-new-ways-to-protect-democracy/; https://arstechnica.com/tech-policy/2019/07/microsoft-warns-10000-customers-theyre-targeted-by-nation-sponsored-hackers/

15 https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html

16 Voir MELANI, rapport semestriel 2017/2, chap. 5.1.2.

la sécurité informatique Kaspersky Lab a mis en évidence des analogies avec Sofacy. Il semble que le groupe Fancy Bears présente lui aussi des liens avec cette campagne. Il a en effet publié début 2018 des données qui avaient été dérobées entre la fin 2016 et le début 2017 au Comité international olympique et au Comité national olympique des États-Unis, parmi lesquelles figuraient des historiques de santé d'athlètes et des courriels.

Le 28 octobre 2019, le *Threat Intelligence Center* de Microsoft a annoncé avoir identifié de nombreuses attaques qu'aurait perpétrées Sofacy contre au moins 16 organisations sportives et autorités antidopage sur 3 continents. Ces attaques auraient commencé à la mi-septembre, juste avant que l'Agence mondiale antidopage (AMA) ne publie sa décision d'exclure la Russie des prochains Jeux olympiques[17].

Cette campagne est loin d'être la seule à viser les jeux d'été qui doivent se dérouler au Japon en 2021, après avoir été reportés d'une année suite à la crise du coronavirus. Le Comité d'organisation des Jeux olympiques et paralympiques a mis en garde contre des campagnes de courriels qui usurpent son identité afin de conduire les destinataires vers des pages de phishing ou d'infecter leurs appareils. Une campagne de phishing a ciblé 170 000 individus au Japon et aux États-Unis. Des détails la concernant (intention et ampleur, p. ex.) auraient été trouvés dans un chat sur le darknet[18]. Les indices dont on dispose semblent indiquer qu'on a ici affaire à d'autres auteurs que ceux de la tentative d'infiltration des organisations sportives et antidopage d'octobre dernier[19].

Qu'est-ce qui fait l'attrait de ces cibles? Avant le début des compétitions, les attaques peuvent servir à recueillir des informations sur les athlètes d'autres pays, leurs performances, leurs faiblesses et leurs projets, dans l'espoir qu'elles permettront d'élaborer des stratégies gagnantes. Les attaques peuvent aussi viser à fausser les résultats de tests de dopage. Dans certains pays, le sport est plus qu'une compétition entre athlètes. Il est un facteur de cohésion de la société et peut être employé à des fins politiques, par exemple en permettant à des dirigeants de profiter de la popularité de certains sportifs à succès. Les grandes manifestations sportives sont en outre une plateforme idéale pour faire connaître ses propres talents informatiques. De telles attaques réalisées «sous fausse bannière» (*false flag operations)* permettent en outre, potentiellement, de réorganiser l'échiquier politique international, en jetant le discrédit sur un pays concurrent. Elles peuvent, enfin, satisfaire un besoin de réparation dans un pays sanctionné.

4.1.2 Campagne d'espionnage industriel Winnti

Selon les dernières révélations en date, le nombre des multinationales allemandes victimes de cyberattaques n'a cessé d'augmenter ces dernières années. Le géant de la communication Siemens, par exemple, a confirmé récemment avoir été ciblé en juin 2016, mais apparemment sans fuite de données. La société Covestro, un fabricant de plastiques et de colles, a également été touchée mais sans subir de dommages non plus. Le géant pharmaceutique Bayer a indiqué en avril avoir été victime de cyberespionnage dès 2018. Selon différents experts en

17 https://blogs.microsoft.com/on-the-issues/2019/10/28/cyberattacks-sporting-anti-doping/

18 https://www.bleepingcomputer.com/news/security/tokyo-2020-staff-warns-of-phishing-disguised-as-official-emails/

19 https://english.kyodonews.net/news/2018/09/e2d8f3727275-phishing-scam-on-2020-olympics-tickets-spotted.html

sécurité, toutes ces attaques seraient imputables à Winnti, un nom qui désigne à la fois un groupe et le maliciel que celui-ci utilise et qui s'est notamment fait connaître pour avoir infiltré en 2016 le groupe sidérurgique ThyssenKrupp[20]. Les mêmes experts sont nombreux à considérer ces attaques comme ayant leur origine en Chine.

Au départ, le groupe s'était focalisé sur les plateformes de jeux en ligne, dans un but purement financier. Mais en 2015 au plus tard, il a étendu ses activités à l'espionnage industriel, en se concentrant apparemment sur les secteurs chimique et pharmaceutique et sur les entreprises spécialisées dans les technologies de pointe. Outre les victimes précitées, deux radios allemandes, le Bayerischer Rundfunk et le Norddeutscher Rundfunk, ont mentionné, dans le cadre d'une analyse approfondie, d'autres traces d'infection anciennes, qui n'avaient jusqu'ici pas été relayées par la presse. Elles ont par exemple signalé que Henkel, qui comme Covestro fabrique notamment des colles pour l'industrie, avait été infiltré en 2014. Parmi les victimes figurerait également BASF, l'un des principaux géants de la chimie, qui a lui aussi son siège en Allemagne, mais l'attaque subie en 2015 n'aurait pas fait de dégâts importants[21].

Une fois qu'ils se sont introduits dans le réseau d'une entreprise, les pirates en réalisent une image afin de rechercher les points stratégiques où ils pourront cacher leur maliciel. Cela leur permet d'agir en arrière-plan le plus longtemps possible en restant invisibles, et de collecter des informations sur la firme et ses produits dans l'espoir de découvrir des secrets d'entreprise. L'endurance est l'une des caractéristiques de Winnti. Les pirates installent aussi des portes dérobées afin de pouvoir accéder au réseau d'une entreprise à tout moment. En octobre 2019, l'entreprise de sécurité ESET a signalé avoir remarqué une porte dérobée ignorée jusque-là, ciblant Microsoft SQL et utilisée par Winnti[22].

Si Winnti a défrayé la chronique en Allemagne après son attaque contre ThyssenKrupp, le groupe est aussi actif dans d'autres pays d'Europe de l'Ouest, en Asie et aux États-Unis. Selon une enquête réalisée par ESET, il aurait infecté un gros producteur asiatique de matériel informatique mobile et de logiciels en passant par PortReuse, une porte dérobée découverte en mars 2019. On suppose que cette compromission est le signe qu'il préparait une attaque de grande ampleur contre la chaîne d'approvisionnement[23].

Le maliciel sert aussi à des fins d'espionnage politique. Selon les experts de Kaspersky Lab, au moins deux groupes utiliseraient actuellement cet outil. Il est du coup plus difficile de savoir si les responsables du cyberespionnage industriel sont les mêmes que ceux qui agissent plutôt dans le domaine politique (et qui s'attaquent, p. ex., au gouvernement de Hong Kong ou à l'opérateur de télécommunications indien de la région où se trouve le siège du gouvernement tibétain en exil[24]).

---

20 https://www.waz.de/wirtschaft/spionage-mehrere-dax-konzerne-von-hackern-angegriffen-id226573145.html; voir aussi MELANI, rapport semestriel 2016/2, chap. 5.1.3.

21 http://web.br.de/interaktiv/winnti/

22 https://www.zdnet.com/article/researchers-find-stealthy-mssql-server-backdoor-developed-by-chinese-cyberspies/; https://www.welivesecurity.com/2019/10/21/winnti-group-skip2-0-microsoft-sql-server-backdoor/

23 https://www.bleepingcomputer.com/news/security/winnti-group-uses-new-portreuse-malware-against-asian-manufacturer/

24 http://web.br.de/interaktiv/winnti/

Conclusion / recommandations:

Cela fait plusieurs années que les APT ne touchent plus uniquement les services gouvernementaux et militaires. Ces attaques hautement sophistiquées touchent de plus en plus souvent des organisations internationales et des entreprises privées dans de nombreux secteurs. On peut en partie expliquer cet état de fait par une certaine démocratisation des attaques les plus sophistiquées, du fait que les outils utilisés pour les lancer sont désormais largement disponibles (cf. rapport semestriel 2019/1, chapitre 5.1.1). Ainsi, un grand nombre d'attaquants poursuivant des buts variés sont désormais actifs. Cependant, un bon nombre d'entreprises ne disposent ni des ressources financières ni du savoir-faire nécessaires pour lutter contre une telle menace.

Pour y remédier, elles peuvent, par exemple, confier leur sécurité informatique à des experts externes tels que des prestataires de services en nuage. Cela ne les dispense pas de prendre en interne des mesures supplémentaires de sensibilisation et de formation du personnel. Il ne faut pas négliger le risque que des (anciens) collaborateurs donnent accès au système de l'entreprise à des tiers dans le but de s'enrichir facilement, par vengeance personnelle ou par désir de nuire à l'employeur.

Il est recommandé de rejoindre un ou plusieurs réseaux publics ou privés qui échangent des informations sur l'état des menaces et qui donnent des conseils sur les moyens d'identifier les risques et de se protéger.

Mesures techniques:

Si une analyse interne des risques révèle que votre organisation ou votre système sont menacés, vous avez intérêt à prendre quelques mesures techniques pour limiter le risque d'infection:

Au niveau du système:

- utilisation du programme Windows AppLocker (ou équivalent) pour éviter l'exécution de fichiers binaires inconnus, notamment à partir des dossiers des profils d'utilisateur;
- limitation des droits d'utilisateur non essentiels;
- utilisation d'une alerte pour l'exécution d'outils d'exécution du système.

Au niveau de l'Active Directory (AD):

- surveillance attentive de l'AD afin de détecter les requêtes inhabituelles ou de grande envergure;
- mise en place d'une authentification multiple pour l'AD, en particulier pour l'accès à distance;
- pour les clients Microsoft: utiliser régulièrement *RAP as a Service* (cf. https://services.premier.microsoft.com/assess/).

Au niveau du réseau:

- archivage des fichiers journaux pendant au moins 2 ans pour les systèmes de passerelle importants tels que les DNS de proxy;
- exécution de DNS passifs pour la vérification rapide de domaines suspects;
- mise en place du système de détection d'intrusion Snort fondé sur des signatures;
- mise en place d'une politique de segmentation interne (mieux vaut, de manière générale, éviter la communication de client à client);
- collecte des données de NetFlow à différents endroits du réseau interne;
- choix d'un point de contrôle central pour l'accès à Internet, et surveillance étroite de ce point;
- gestion hors bande des serveurs qui utilisent un LAN de gestion (pas de navigation ni de courriels à partir de la station de gestion);
- création d'une liste blanche des proxys pour les serveurs internationaux obligés de communiquer avec l'extérieur.

4.2 Systèmes de contrôle industriels

Dans son tout premier rapport semestriel, en 2005, MELANI écrivait dans un article consacré aux nouvelles directives sur la sécurité informatique des installations nucléaires aux États-Unis: «Les problèmes majeurs de sécurité que rencontrent les centrales avec leurs systèmes de télésurveillance et d'acquisition des données sont dus aux transmissions de données et de commandes, rarement chiffrées jusqu'ici, à leur raccordement aux réseaux publics et au manque de standardisation des technologies[25].»

Depuis lors, il y a eu une nette prise de conscience quant à la sécurité des systèmes de contrôle industriels (SCI). Les atteintes, révélées ces quinze dernières années, à l'intégrité de processus pilotés par ces systèmes y ont certainement contribué. Ces atteintes, outre les attaques dirigées contre les systèmes eux-mêmes, qui peuvent aussi nuire aux processus, attirent particulièrement l'attention des experts. Les exemples les plus frappants de cette catégorie sont Stuxnet[26] (2010), Industroyer/CRASHOVERRIDE[27] (fin 2016) et Triton/Trisis[28] découvert en 2017. À titre d'illustration, nous exposons au chap. 4.2.1 l'effet nuisible visé par CRASHOVERRIDE sur les processus liés à l'approvisionnement de l'Ukraine en électricité.

L'interconnexion poussée des systèmes de contrôle, mais aussi des acteurs et des capteurs, a contribué à compliquer considérablement la mise en sécurité d'infrastructures systèmes de ce genre. L'Internet industriel des objets (IIdO) permet des processus d'automatisation prometteurs tout en augmentant l'exposition de ces processus aux agressions. Garantir un niveau de sécurité approprié représente une difficulté qui n'a pas encore été entièrement réglée.

4.2.1 L'approvisionnement en électricité toujours en point de mire

Le fournisseur ukrainien d'électricité Ukrenergo a été victime en décembre 2016 d'une cyberattaque qui a généré une panne[29]. Cette fois, les techniciens de la sous-station Nord, située près de Kiev, ont réussi à rétablir le courant au bout d'une petite heure en procédant à des reconnexions manuelles. Un nouvel examen[30] de cette attaque perpétrée au moyen du maliciel CRASHOVERRIDE montre cependant que les agresseurs avaient l'intention (voir fig. 3) de provoquer la destruction physique d'éléments du réseau. Ils ont notamment ciblé les relais de protection du réseau de transmission. Mais ils ont manqué leur objectif, qui était de mettre hors service (*denial of service)* la fonction protectrice des relais. Sans cette protection, et sans visibilité dans les systèmes de contrôle attaqués, une séquence de mise en marche malencontreuse aurait pu endommager des parties du réseau, ce qui aurait causé, outre les dommages physiques, des pannes nettement plus longues.

---

25 MELANI, rapport semestriel 2005/1, chap. 7.1

26 MELANI, rapport semestriel 2010/2, chap. 4.1

27 MELANI, rapport semestriel 2017/1, chap. 5.3

28 MELANI, rapport semestriel 2017/2, chap. 5.3.2

29 MELANI, rapport semestriel 2016/2, chap. 5.3.1

30 https://dragos.com/resource/crashoverride-reassessing-the-2016-ukraine-electric-power-event-as-a-protection-focused-attack/

Fig. 3: Déroulement prévu de l'attaque (source: dragos.com)

Connaître les intentions des agresseurs révèle à quel point il est important de réduire les risques au minimum dans les secteurs essentiels. Un rapport de la Commission fédérale de l'électricité (ElCom)[31] a révélé en 2019 que la Suisse pouvait mieux faire s'agissant des mesures de sécurité relatives à son approvisionnement en électricité[32]. L'ElCom exige notamment que les systèmes de technologie opérationnelle (*operational technology* [OT]) soient testés régulièrement afin qu'on y détecte les éventuelles failles de sécurité. Pendant la période sous revue, par exemple, une multitude de faiblesses[33] ont été mises au jour dans le système d'exploitation en temps réel VxWorks, sur lequel sont fondés de nombreux systèmes de contrôle spécifiques à des applications. Cette intégration en profondeur nécessite l'implication de toute une chaîne de fabricants de systèmes et d'exploitants pour combler les failles dans les systèmes opérationnels de conduite des processus. Les lacunes de sécurité connues dans le domaine de la conduite des processus pourraient considérablement augmenter à l'avenir, étant donné que le concours de recherche sur les failles Pwn2Own[34] intégrera à l'avenir dans son champ d'étude les SCI en plus des systèmes informatiques traditionnels. Outre les systèmes utilisés, un nombre croissant d'éléments sont connectés au réseau[35], ce qui complique encore la mise en œuvre coordonnée des prescriptions de sécurité en tenant compte de tous les fournisseurs impliqués.

À cela s'ajoute le fait que chaque jour, de nouveaux pirates font leur point de mire du secteur de l'approvisionnement en électricité[36] et de sa chaîne de fournisseurs[37]. À la fin de l'été 2019, deux vagues de phishing ciblé ont tenté, aux États-Unis, d'introduire le maliciel LookBack dans des entreprises. Pour arriver à leurs fins, les agresseurs ont imité des organismes décernant des licences reconnues par le secteur dans l'espoir que les destinataires ouvriraient les pièces

---

31 https://www.elcom.admin.ch/dam/elcom/de/dokumente/2019/Cyber-Sicherheit%202019%20-%20Bericht%20der%20ElCom.pdf.download.pdf/Cyber-Sicherheit%202019%20-%20Bericht%20der%20ElCom.pdf

32 https://www.tagesanzeiger.ch/schweiz/standard/fuer-hacker-stehen-die-einfallstore-offen/story/20223699

33 https://www.armis.com/urgent11/

34 https://www.darkreading.com/vulnerabilities---threats/pwn2own-adds-industrial-control-systems-to-hacking-contest/d/d-id/1336191

35 https://www.zdnet.com/article/ameo-concerned-about-nation-state-attacks-on-power-grids/

36 https://www.proofpoint.com/us/threat-insight/post/lookback-malware-targets-united-states-utilities-sector-phishing-attacks

37 https://www.wired.com/story/iran-apt33-industrial-control-systems/

jointes à leur message. Le maliciel lui-même, une fois installé, agit comme un «cheval de Troie permettant un accès à distance» (*remote access trojan* [RAT]), qui met à la disposition de l'agresseur de nombreuses fonctionnalités sur le système infecté.

Le passage des carburants fossiles à l'électromobilité ne fait qu'accroître l'importance de l'approvisionnement en électricité. En même temps, les objectifs politiques en la matière déplacent la production de courant des grosses centrales vers de plus petites unités décentralisées produisant une énergie renouvelable. Ce mouvement s'accompagne de l'informatisation de l'approvisionnement en électricité (SmartGrid). MELANI s'efforce, avec les producteurs de courant et les exploitants de réseau, de protéger au mieux l'approvisionnement de la Suisse contre les risques liés à la sécurité de l'information. La fiabilité de l'approvisionnement est un élément clé pour le fonctionnement de l'économie et de la société et pour la préservation de notre prospérité.

Recommandation:

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

Formulaire d'annonce MELANI
https://www.melani.admin.ch/melani/fr/home/meldeformular.html

Mesures de protection des systèmes de contrôle industriels (SCI):
https://www.melani.admin.ch/melani/fr/home/dokumentation/checklisten-und-anleitungen/massnahmen-zum-schutz-von-industriellen-kontrollsysteme--ics-.html

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

4.3.1 Attaques DDoS pour exercer un chantage sur un service ou pour lui nuire

Au cours de la dernière semaine de l'année 2019, des attaques en déni de service distribué (*distributed denial of service* [DDoS]) ont pris pour cible des médias en ligne suisses[38], provoquant l'indisponibilité temporaire de certains sites. On ignore toujours les motivations de leurs auteurs.

Les attaques DDoS visent à perturber la disponibilité de systèmes informatiques. Au cours du dernier semestre, elles se sont multipliées en relation avec des tentatives de chantage[39]. Les

[38] https://www.20min.ch/digital/news/story/Technische-Probleme-auf-20minuten-ch-12858361; https://www.nzz.ch/wirtschaft/cyberattacke-gegen-schweizer-medien-ld.1530906

[39] À ce propos, voir notamment le rapport semestriel MELANI 2016/1, chap. 4.4.1, et les rapports semestriels MELANI 2018/1, chap. 4.3.1, 2017/2, chap. 4.3.1, 2016/2, chap. 4.4.1, 2015/2, chap. 4.3.4, et 2015/1, chap. 4.4.1.

agresseurs commencent souvent par une attaque-test pour prouver qu'ils ont les capacités nécessaires. Ils menacent ensuite la victime d'une attaque plus puissante si elle ne paye pas une rançon. Leurs motivations sont parfois politiques, comme l'a montré l'attaque DDOS contre le site web du parti travailliste britannique[40]. Selon certains chercheurs en sécurité, la tendance est plutôt aux attaques de faible intensité, suffisantes pour perturber la performance de sites ou de serveurs, mais pas pour déclencher les mesures de défense anti-DDoS[41].

Recommandation:

MELANI recommande toute une série de mesures préventives et réactives face aux attaques DDoS.

Liste de mesures à prendre contre les attaques DDoS

https://www.melani.admin.ch/melani/fr/home/dokumentation/checklisten-und-anleitungen/massnahmen-gegen-ddos-attacken.html

4.3.2 *Drive-by downloads*: la situation en Suisse

Il existe différents moyens d'infecter un appareil avec un maliciel. L'un des plus courants consiste à pirater un site web pour y placer un script. Ce script va alors rechercher des failles de sécurité dans le navigateur ou dans d'autres applications (FlashPlayer, p. ex.) en testant des exploits. La simple consultation de la page manipulée suffisant parfois pour provoquer l'infection, on parle de téléchargement furtif (*drive-by download*).

Au deuxième semestre 2019, MELANI a identifié quelque 500 sites infectés en Suisse et en a informé leurs exploitants afin qu'ils puissent les nettoyer.

Les utilisateurs qui découvrent des sites infectés sont priés de le signaler à MELANI afin de contribuer à la cybersécurité générale.

Recommandations:

1. Installez au moins deux navigateurs différents afin de pouvoir en changer rapidement si l'un des deux présentait soudain une grave faille de sécurité.
2. Installez systématiquement toutes les mises à jour de vos navigateurs, dans l'idéal en programmant les mises à jour de sécurité automatiques.
3. Utilisez si possible un bloqueur de publicités (*ad-blocker)* et restreignez l'utilisation de JavaScript au strict minimum.
4. Lorsqu'une page web vous invite de façon inopinée à télécharger un fichier, n'acceptez jamais.

40 https://www.theregister.co.uk/2019/11/12/labour_party_reports_cyber_attack/

41 https://www.zdnet.com/article/ddos-attacks-getting-smaller-sneakier-and-more-dangerous/#ftag=RSSbaffb68

4.3.3 Cyberattaque contre la plateforme d'échange de cryptomonnaies Upbit

Les plateformes d'échange de cryptomonnaies sont des cibles lucratives puisqu'en cas d'attaque réussie, les agresseurs peuvent voler beaucoup d'argent. La plateforme sud-coréenne Upbit s'est ainsi fait voler 342 000 ethereum dans son *Exchange Hot Wallet*. Au moment du vol, ces ethereum valaient 48,5 millions de dollars. Selon diverses hypothèses, il pourrait s'agir d'une escroquerie de sortie (*exit scam*), c'est-à-dire le fait, pour un initié, de transférer l'argent des utilisateurs de la plateforme vers son propre compte en prétendant qu'il y a eu une cyberattaque. Cela dit, il est difficile de convertir les ethereum volés en argent liquide, car une procédure complexe de «blanchiment»[42] serait nécessaire pour empêcher toute traçabilité[43].

4.4 Ingénierie sociale et phishing

4.4.1 Phishing

De très nombreuses attaques par phishing ont eu lieu au second semestre 2019, notamment au nom de différentes marques suisses. Le contenu du courriel en question est généralement assez semblable: certains demandent les coordonnées de votre carte de crédit à des fins de «vérifications», d'autres demandent votre identifiant et votre mot de passe pour accéder à des services internet. Ces courriels détournent régulièrement le logo d'une entreprise connue ou du service concerné, pour se donner une apparence de respectabilité. Ils ciblent souvent des services de messagerie car les identifiants de connexion à des comptes de courriel ouvrent la porte à de nombreuses autres possibilités d'attaque.

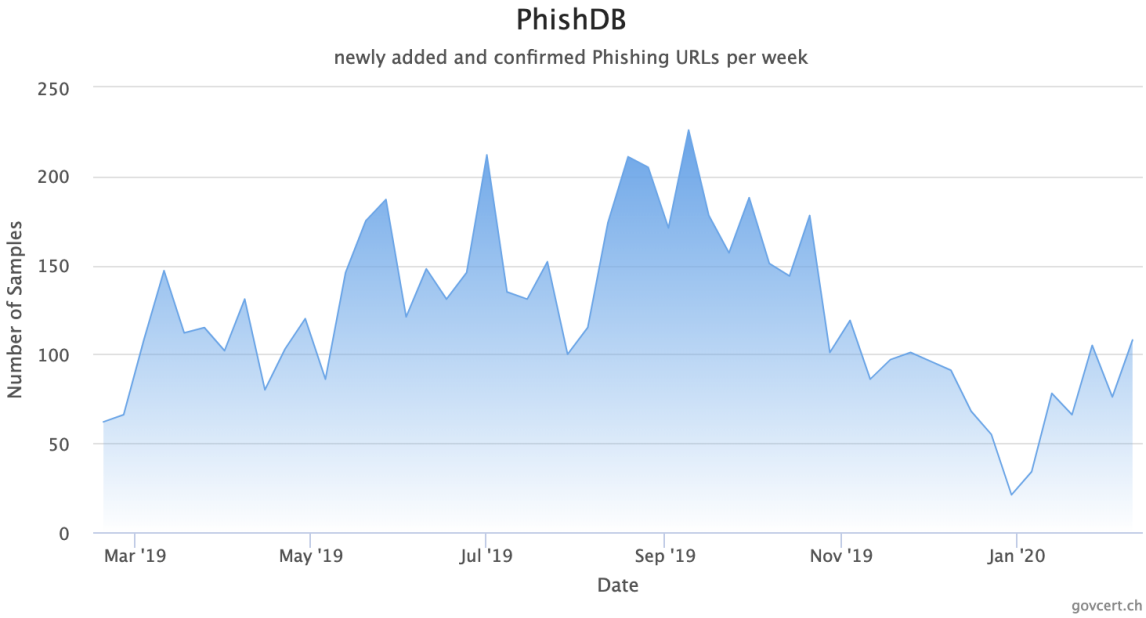

Fig. *4*: *Nombre de sites de phishing signalés et confirmés chaque semaine sur antiphishing.ch l'an dernier, état du 9 février 2020.*

42 Voir aussi le chap. 5.3.

43 https://www.zdnet.com/article/upbit-cryptocurrency-exchange-loses-48-5-million-to-hackers/

4.4.2 Sites de phishing avec page d'erreur 404

Une page d'erreur 404 informe le visiteur d'un site que la page qu'il souhaite consulter n'existe pas ou plus. La plupart des exploitants de site web créent à cet effet une page d'erreur 404 aux couleurs du site et l'utilisent comme message d'erreur standard. Cela leur permet, en cas d'erreur, d'afficher le contenu de leur choix et ainsi de fournir au visiteur des informations précises, voire de le rediriger vers une autre page. Comme toute page web, une page d'erreur 404 peut malheureusement contenir des éléments malveillants tels que phishing ou téléchargements furtifs. Microsoft a signalé en août dernier avoir détecté une campagne de phishing de ce genre dirigée contre ses utilisateurs. Une page de phishing imitant à la perfection le portail de connexion à un compte Microsoft avait été placée comme page d'erreur 404 sur le site d'un domaine enregistré par des cyberpirates. Chaque fois qu'un visiteur tentait de consulter une URL inexistante sur le site en question, il était renvoyé vers la page d'erreur 404 manipulée aux fins de phishing[44]. Cette méthode permet aux agresseurs de créer selon le principe du hasard un nombre illimité d'URL de phishing et ainsi de rendre plus difficile la détection et le blocage au moyen des liens figurant dans les courriels car les URL n'ont en commun que le nom de domaine.

Les créateurs de pages de phishing sont constamment à la recherche de nouveaux moyens d'inciter les utilisateurs à suivre des liens malveillants. Donc réfléchissez bien avant de cliquer sur un lien dans un courriel ou dans un message sur votre smartphone. Vous trouverez de nombreuses recommandations sur notre site:

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

Vous pouvez nous signaler des cas de phishing à l'adresse suivante:

https://www.antiphishing.ch/

Vos messages nous aident à prendre les mesures qui s'imposent afin de protéger d'autres utilisateurs.

4.4.3 Chantage assorti d'affirmations, nouvelles variantes

Des criminels continuent d'envoyer des courriels dans lesquels ils prétendent avoir accès à l'ordinateur et à la webcam du destinataire, menaçant celui-ci de publier des photos ou des vidéos compromettantes s'il ne paye pas, dans un délai donné, une rançon en cryptomonnaie (*fake sextorsion*). Ces courriels contiennent souvent des mots de passe et / ou des numéros de téléphone ayant un rapport réel avec la victime potentielle. MELANI a connaissance d'exemples récents de pirates relançant leurs victimes potentielles avant l'expiration du délai, pour leur rappeler les risques auxquels elles s'exposent en ne payant pas la rançon.

44 https://www.bleepingcomputer.com/news/security/microsoft-warns-of-phishing-attacks-using-custom-404-pages/

On lui a aussi signalé il y a peu des cas où l'expéditeur affirme être en possession de vidéos pédopornographiques compromettant le destinataire. Pour intimider la victime potentielle, le pirate donne comme titre aux fichiers qu'il lui envoie en pièce jointe le nom du destinataire ou son adresse de messagerie. Ce genre d'attaque cible aussi bien des femmes que des hommes.

Certains pirates exigent pour la rançon une cryptomonnaie différente du bitcoin, en misant sans doute sur le fait que les transactions seront plus difficiles à retracer avec une cryptomonnaie moins courante. Certains utilisent aussi, dans le texte en clair, des codes QR au lieu d'adresses de *wallet* car les logiciels de sécurité détectent fréquemment celles-ci dans les courriels qu'ils bloquent par conséquent par mesure de précaution. Ces ruses démontrent une fois de plus la nécessité d'associer mesures de sécurité techniques et campagnes de sensibilisation pour prévenir efficacement les cyberattaques.

MELANI s'est aussi vu signaler des menaces d'attaque à l'acide ou d'engagement de tueurs à gages. Ce type de chantage est toutefois moins répandu que la *fake sextorsion*. Cela tient probablement au fait que les victimes hésitent moins à signaler aux autorités les menaces de violences physiques que les tentatives de *fake sextorsion*, qui se réfèrent à leur passé intime supposé.

Des chercheurs en sécurité informatique[45] ont découvert la raison pour laquelle on enregistre des vagues de campagnes de sextorsion d'une telle taille. Le maliciel Phorpiex a déjà infecté plus de 450 000 ordinateurs, qu'il réunit en un réseau de zombies grâce auquel les pirates peuvent envoyer leurs courriels de chantage en masse. Les adresses de messagerie des destinataires sont tirées, au hasard, d'une base de données. Le contenu des courriels est composé au moyen de modules de texte, ce qui accroît encore le degré d'automatisation. La fréquence d'expédition, qui avoisine les 30 000 courriels à l'heure, est relativement élevée. La campagne serait en mesure de toucher 27 millions de victimes potentielles.

INFO

Ne vous laissez pas intimider par les affirmations péremptoires, ne réagissez pas aux courriels de chantage, et en cas de doute, prenez contact avec les autorités. Pour en savoir plus sur la *fake sextorsion*, rendez-vous sur https://www.stop-sextortion.ch/. Vous pouvez aussi y signaler ce type de courriel. Si vous utilisez toujours le mot de passe indiqué dans le courriel, modifiez-le sur le champ. Il est de toute façon recommandé de changer régulièrement de mot de passe et de ne pas utiliser un même mot de passe pour des services différents. Pour prévenir efficacement les cyberattaques, associez les mesures de sécurité techniques et les campagnes de sensibilisation.

MELDEN

[45] https://m.pctipp.ch/news/artikel/user-pc-fuer-sextortion-spam-missbraucht-93135/

4.4.4 Attaques contre les messageries professionnelles: un procédé résistant, en évolution permanente

Depuis 2013, les rapports semestriels de MELANI ont traité à plusieurs reprises du phénomène de l'arnaque au président (*CEO fraud*)[46]. Le mode opératoire a connu de nombreuses transformations au fil du temps, le but étant de multiplier les cibles et les victimes.

Ces dernières années, les escrocs se sont mis à usurper l'identité de fournisseurs pour envoyer aux clients de ceux-ci des factures sur lesquelles l'IBAN a été modifié. Bien souvent, le piratage d'un compte de messagerie ou d'une plateforme de collaboration en ligne leur livre les informations nécessaires sur un plateau: ils n'ont plus qu'à falsifier les factures originales[47]. Les dernières statistiques du Financial Crimes Enforcement Network (FINCEN) aux États-Unis confirment cette tendance croissante à l'usurpation de l'identité de partenaires commerciaux externes de l'entreprise victime[48]. Les analyses du FINCEN fournissent aussi des chiffres intéressants sur les secteurs d'activité touchés. Aux États-Unis, le secteur manufacturier et le bâtiment sont en première ligne. Cela tient peut-être au fait qu'ils sont particulièrement dépendants de leurs fournisseurs externes et qu'ils travaillent avec de nombreux sous-traitants. Cela dit, tous les secteurs sont des cibles potentielles de cyberattaques en tout genre.

Les tentatives d'escroquerie consistant à se faire passer pour un collaborateur de l'entreprise cible restent fréquentes. Les criminels tentent d'exploiter les progrès technologiques pour perfectionner leur mode opératoire. Le *Wall Street Journal* a relaté en septembre 2019 une affaire dans laquelle les escrocs ne se sont pas contentés d'usurper l'identité d'un patron dans un courriel: associant logiciel vocal et intelligence artificielle, ils ont réussi à imiter sa voix et à ordonner par téléphone des transferts abusifs d'argent[49].

Dans une variante de cette méthode observée récemment en Suisse, les criminels se font passer pour les collaborateurs d'une entreprise. Ils écrivent aux personnes responsables du paiement des salaires (en général, le service du personnel) pour leur signaler que leur propre salaire doit désormais être versé sur un compte bancaire différent. Le spécialiste de la sécurité Trustave a documenté ce phénomène avec précision dès le début 2019[50], expliquant que les escrocs créent des adresses auprès d'un service de messagerie gratuit après avoir recueilli les informations nécessaires à l'attaque (identité des responsables de la gestion des salaires, p. ex.), lesquelles sont librement accessibles (site de l'entreprise, réseaux sociaux, etc.).

---

46 MELANI, rapports semestriels 2013/1, chap. 3.4; 2016/1, chap. 4.5.1; 2016/2, chap. 4.5.1; 2017/1, chap. 4.3.3; 2018/2, chap. 4.4.3; 2019/1, chap. 4.4.5

47 Voir MELANI, rapport semestriel 2018/2, chap. 4.4.3.

48 https://www.fincen.gov/sites/default/files/shared/FinCEN_Financial_Trend_Analysis_FINAL_508.pdf

49 https://www.zdnet.com/article/forget-email-scammers-use-ceo-voice-deepfakes-to-con-workers-into-wiring-cash/

50 https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/bec-payroll-scam-your-salary-is-mine/

Conclusion / recommandation:

Vu l'extrême inventivité des criminels et leur grande capacité d'adaptation, la prévention de ce genre d'attaques reste une gageure pour toutes les entreprises. Rappelez à vos collaborateurs que toutes les procédures et mesures de sécurité définies en interne doivent être respectées en permanence. Les transferts d'argent, en particulier, doivent obéir au principe du double contrôle avec signatures collectives. Les annonces de changement de compte doivent être examinées avec la plus grande précaution.

Informations et recommandations relatives à l'arnaque au président:
https://www.melani.admin.ch/melani/fr/home/themen/CEO-Fraud.html

4.4.5 Escroqueries au placement en ligne

Au cours du semestre sous revue, MELANI a reçu plusieurs signalements concernant de fausses plateformes de négoce en ligne et des sites en vantant les mérites, en promettant des gains rapides et importants en cryptomonnaies. Cette publicité mensongère se diffuse souvent sur les réseaux sociaux et usurpe l'identité de personnalités pour asseoir sa crédibilité. Dans des entretiens fictifs, des vedettes telles que Roger Federer ou DJ Bobo expliquent devoir une partie de leur fortune au bitcoin. Sur le Net, des alertes signalent que l'argent une fois investi est perdu[51]. Les *fake news* sont un phénomène actuellement très répandu dont on peut se protéger en gardant une distance critique par rapport aux informations étranges ou provenant d'une source douteuse.

Le négoce en bourse est une activité risquée en soi. Les messages non personnalisés provenant d'une plateforme de négoce (sur un réseau social, par courriel, par SMS ou par WhatsApp, p. ex.) doivent être interprétés comme des envois de masse sans fondement sérieux. L'Autorité fédérale de surveillance des marchés financiers (FINMA) explique, dans une vidéo, comment se prémunir contre les escroqueries au placement[52]. Elle publie en outre la liste des plateformes électroniques reconnues[53]. Attention: les publipostages (de masse) frauduleux peuvent aussi être expédiés sous une forme personnalisée (nom et autres données personnelles).

4.5 Fuites de données

4.5.1 Accès aux données de patients

Une étude[54] a révélé à l'été 2019 que les données de plusieurs millions de patients de différents pays figuraient sur le Net sans aucune protection. Ces données médicales ultrasensibles étaient archivées sur des serveurs non sécurisés qui sont restés accessibles à n'importe qui

51 https://www.20min.ch/schweiz/news/story/Wieso-stoppt-niemand-die-Bitcoin-Betrueger--13654244
52 https://finma.ch/fr/dokumentation/finma-videos/schutz-vor-anlagebetrug/
53 https://www.finma.ch/fr/finma-public/bewilligte-institute-personen-und-produkte/
54 https://www.br.de/nachrichten/deutschland-welt/millionenfach-patientendaten-ungeschuetzt-imnetz,RcF09BW

pendant des années. Il s'agit notamment de radiographies haute définition mentionnant les nom, prénom et date de naissance du patient, la date de l'examen, le médecin traitant voire le traitement. Les examens d'imagerie sont envoyés des appareils vers des serveurs spéciaux dits *picture archiving and communication system*s (PACS) pour y être archivés. Ce scandale porte sur 16 millions de lots de données dans une cinquantaine de pays, principalement aux États-Unis. En Allemagne, 13 000 lots de données seraient concernés. L'office fédéral allemand de la sécurité des technologies de l'information (*Bundesamt für Sicherheit in der Informationstechnik* [BSI]) a signalé l'affaire à 46 pays et entretient des contacts avec l'exploitant du PACS allemand. Il examine en outre les mesures relevant du droit de la surveillance, depuis les recommandations pour améliorer la sécurité informatique jusqu'à l'infliction d'une amende. Les analyses effectuées par MELANI n'ont pas révélé la présence de données de patients suisses bien que certains des PACS se trouvent en Suisse.

L'exemple qui suit illustre la large responsabilité des organes de direction des entreprises.

Certains fabricants de dispositifs médicaux assurent la maintenance de ces appareils en plus de leur distribution. En tant que prestataire de services, une entreprise est tenue de respecter des normes de sécurité courantes, spécifiques à un secteur, et parfois même fixées par contrat. Il est essentiel que la gestion des risques des entreprises médicales soit consciente de cette obligation: il appartient au destinataire de la prestation d'un tiers de s'informer des mesures de sécurité effectivement appliquées par ce tiers, documentation à l'appui. Cela permet de s'assurer que le prestataire externe traitera et archivera les données produites en interne avec les précautions requises. Dans l'idéal, ces programmes de sécurité doivent être vérifiés par un organisme externe indépendant.

Deux autres incidents survenus dans le secteur de la santé illustrent la portée des fuites de données et la charge de travail qu'implique leur gestion: deux entreprises ayant leur siège aux États-Unis (un centre médical et un fournisseur de matériel médical) ont signalé avoir subi des fuites de données concernant près de 220 000 personnes[55] après avoir été victimes l'une de phishing, l'autre d'un rançongiciel.

En procédant à une campagne de phishing ciblée, les pirates sont parvenus à accéder aux comptes Office 365 de collaborateurs, ce qui leur a permis de circuler pendant deux mois dans les comptes de messagerie correspondants sans se faire remarquer et, potentiellement, de s'emparer d'informations récentes ou anciennes concernant des patients et des collaborateurs: noms, adresses, dates de naissance, numéros de sécurité sociale, identifiants personnels, informations médicales, informations relatives à l'assurance-maladie, informations financières, moyens de paiement, informations sur des permis de conduire et sur des passeports, mots de passe, codes NIP, identifiants de connexion et données de facturation, notamment[56].

Le centre médical visé par le rançongiciel est un groupement de plusieurs prestataires de services médicaux. Les pirates ont entièrement chiffré la base de données d'un de ses membres. La victime a pu récupérer l'accès à ses données médicales grâce à des copies de sauvegarde (*backup*), mais les responsables n'ont pas réussi à rétablir l'accès à toutes les

---

55 https://www.inforisktoday.com/2-health-data-breaches-affect-total-220000-a-13440

56 Dans un cas semblable, les pirates avaient même réussi à accéder à des diagnostics et à des informations sur les traitements: https://www.bleepingcomputer.com/news/security/phishing-incident-exposes-medical-personal-info-of-60k-patients/

informations touchées. L'entreprise suppose que l'incident n'a pas entraîné la fuite de données de patients vers des tiers non autorisés.

Dans les deux cas, les personnes concernées ont été informées et se sont vu proposer, à cette occasion, un service de surveillance des crédits gratuit pendant une période donnée, pour parer à une éventuelle usurpation de leur identité.

Recommandations:

Toute entreprise devrait pratiquer une gestion globale des risques. Les fuites de données importantes impliquent régulièrement des prestataires tiers. Les entreprises de tous les secteurs doivent formuler avec précision leurs exigences en matière de sécurité vis-à-vis de ces tiers et les intégrer dans les contrats. Elles doivent aussi discuter de la gestion des incidents, de la gestion de crise et de la gestion de la continuité des activités (*business continuity management* [BCM]). Autre précaution indispensable: s'assurer que la cyberassurance des tiers est suffisante pour couvrir les dommages financiers qui résulteraient de la perte des données de tous leurs clients.

4.5.2 Fuite de données chez Sytech, sous-traitant du FSB

Le 13 juillet 2019, un correspondant du FSB (le service de renseignements russe) chez Sytech aurait été hacké. Selon BBC Russie, les pirates auraient dérobé 7,5 téraoctets de données sur le réseau de l'entreprise, dont des informations sur une multitude de projets secrets développés par Sytech pour le compte du gouvernement russe et du FSB. Ils les ont ensuite transmises à un autre groupe de hackers, qui les a communiquées aux médias russes. Selon BBC Russie toujours, il s'agit de la plus importante fuite de données de l'histoire des services secrets russes[57].

Les données concernent de nombreux projets, dont:

1. Mentor, apparemment développé pour l'unité militaire russe n° 71330, qui ne serait autre que le service de renseignement radioélectronique du FSB; ce projet surveillerait à intervalles précis certains comptes de messagerie afin de recueillir des informations sur certains ensembles de mots;
2. Nadezhda (espoir), un projet qui analyse les liens entre la Russie et le reste d'Internet et qui s'inscrit dans le dessein russe de créer un «Internet souverain», isolé du reste du monde;
3. Nautilus, un projet développé en 2009 et 2010 pour récupérer des informations sur les utilisateurs des réseaux sociaux tels que Facebook, LinkedIn et MySpace;
4. Nautilus-S, projet consacré à la «désanonymisation» des utilisateurs du réseau Tor par la création de nœuds de sortie contrôlés par le gouvernement russe.

Le site de Sytech (www.sytech.ru) a été désactivé depuis lors, et l'entreprise a refusé de répondre aux questions de la BBC.

57 https://www.bleepingcomputer.com/news/security/russian-fsb-intel-agency-contractor-hacked-secret-projects-exposed/

4.6 Logiciels criminels (*crimeware*)

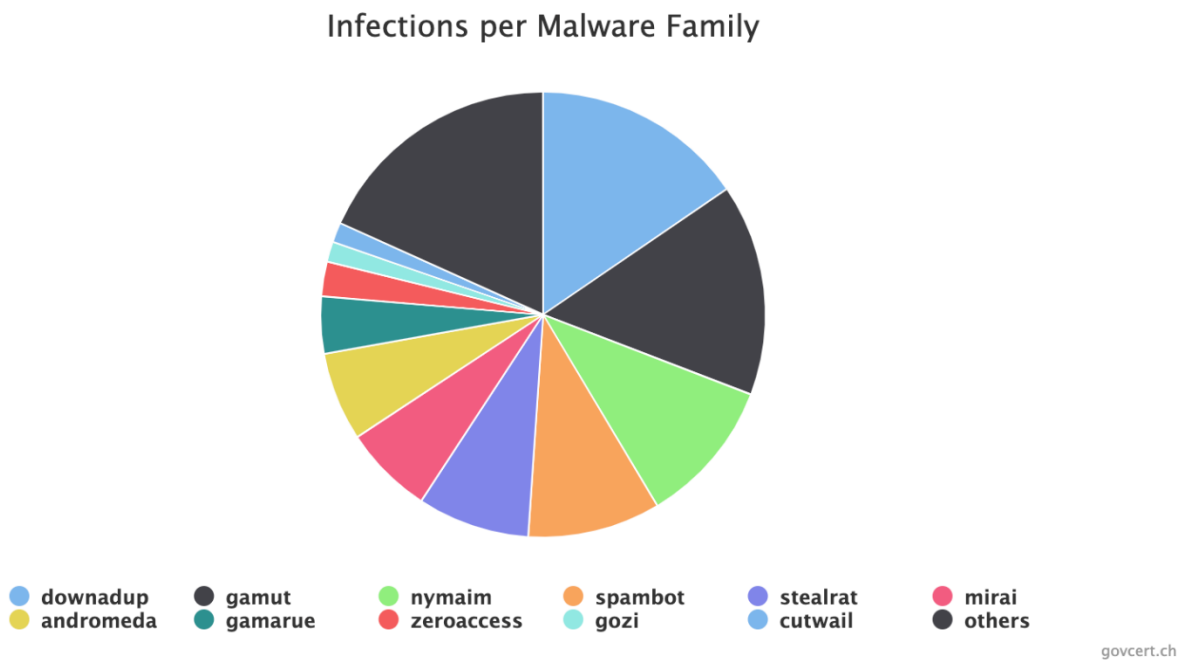

Fig. *5*: *Répartition des maliciels en Suisse, dont le CNCS a eu connaissance grâce à des gouffres de DNS (DNS sinkholes). État du 9 février 2020. Vous pouvez suivre la mise à jour des donnée sur: http://www.govcert.admin.ch/statistics/dronemap/*

4.6.1 Rançongiciels: derniers développements

Imaginez que vous voulez acheter des places pour un match de votre équipe préférée. La prévente en ligne n'est pas disponible pour le moment. Qu'à cela ne tienne, vous vous rendez à un point de vente physique. Malheureusement, vous n'avez pas d'argent liquide sur vous et le lecteur de cartes ne fonctionne pas. Le bancomat le plus proche est à plusieurs kilomètres, vous les parcourez à pied car aucun bus ne circule. Tout cela à cause d'un maliciel qui a mis hors service différents systèmes informatiques à des fins de chantage.

Ce scénario n'est qu'à demi inventé: pendant le semestre sous revue, un club de football suisse a bel et bien été victime d'une attaque par rançongiciel, avec les conséquences que nous venons de décrire sur le système de billetterie et de paiement[58], et une autre attaque de hackers a causé une perturbation légère des transports publics[59]. La seule part de fiction, c'est que ces deux incidents n'ont pas eu lieu en même temps ni dans la même ville.

La vague de rançongiciels aussi persistante que puissante dont MELANI a fait le thème prioritaire de son dernier rapport semestriel est loin de s'essouffler. De nombreuses attaques ont encore été enregistrées au cours des six derniers mois, sur le plan tant national qu'international. On a vu en outre apparaître de nouvelles tendances.

---

58 https://www.inside-it.ch/de/post/der-gehackte-fc-basel-und-die-konsequenzen-20191205

59 https://www.20min.ch/ro/news/romandie/story/Les-TPF-victimmes-d-une-attaque-informatique-23708264

Le secteur de la santé a encore été très touché partout dans le monde au deuxième semestre 2019. En novembre, les systèmes informatiques de l'hôpital universitaire de Rouen, en France, ont été paralysés par un rançongiciel qui a obligé le personnel à «repasser à la bonne vieille méthode du papier et du crayon»[60]. Quelques mois auparavant, en Allemagne, des hackers avaient chiffré les serveurs de 18 hôpitaux[61]. Outre-Atlantique, les chiffres sont encore plus impressionnants. Le rançongiciel Ryuk a attaqué l'entreprise informatique Virtual Care Provider Inc. (VCPI), qui héberge des données dans un nuage et qui protège et gère les accès d'une centaine d'établissements médico-sociaux aux États-Unis. Cette attaque a bloqué l'accès aux dossiers des patients[62]. Ryuk vise en priorité les entreprise et les organisations réalisant de gros chiffres d'affaires, afin d'exiger des rançons élevées. Les entreprises qui gèrent l'infrastructure informatique de nombreux clients sont une cible stratégique parce qu'elles permettent la propagation de l'infection et qu'elles sont susceptibles de payer de grosses sommes. En octobre, Ryuk a chiffré, toujours aux États-Unis, les données de 400 hôpitaux vétérinaires de la National Veterinary Associates. Il semble que l'*Active Directory* et un serveur *Exchange* aient été infectés dès l'été. Comme le virus n'avait pas été entièrement éradiqué, il a refrappé après avoir eu le temps de se repropager[63]. Ryuk est souvent transmis à l'occasion d'une première infection par les chevaux de Troie Emotet ou Trickbot, ce qui fut le cas pour au moins une des attaques évoquées (pour en savoir plus sur la structure d'agression en plusieurs étapes, voir le rapport semestriel MELANI 2019/1, chap. 3.4.1).

Mais Ryuk n'est pas le seul à procéder de la sorte. Cette méthode apparemment lucrative est de plus en plus fréquente ces derniers temps. Parmi les injecteurs (*droppers*) observés en Suisse et à l'échelle internationale figure Ostap, qui télécharge généralement le cheval de Troie TrickBot, lequel se propage à l'intérieur d'un réseau d'entreprises pour placer sur certains systèmes un rançongiciel (Ryuk, LockerGoga, MegaCortex, etc.).

Le secteur de la santé n'est pas une cible unique, tant s'en faut. Tous les secteurs sont des victimes potentielles. Les attaques par rançongiciel peuvent être aussi bien aléatoires que ciblées[64]. Elles affectent par exemple l'industrie, les transports, les administrations publiques, la communication et le sport. Il y a peu, Ryuk a visé au moins cinq organisations des industries gazière et pétrolière. Dans un cas au moins, les agresseurs seraient passés par le *Remote Desktop Protocol (RDP)* pour pénétrer dans le serveur AD de la victime[65]. Au deuxième semestre 2019, on a vu augmenter le nombre des attaques où les agresseurs scannent le web à la recherche de serveurs VPN et de ports RDP ouverts puis essayent d'obtenir un accès en recourant à des attaques par force brute. Ils utilisent ensuite cet accès comme vecteur initial pour infiltrer le réseau d'une entreprise. En Suisse, par exemple, on a pu observer comment

60 http://www.leparisien.fr/economie/plus-rien-ne-fonctionne-le-chu-de-rouen-victime-d-une-grosse-panne-informatique-16-11-2019-8194710.php

61 https://www.spiegel.de/netzwelt/web/rheinland-pfalz-und-saarland-hackerangriff-auf-krankenhaeuser-a-1277759.html

62 https://krebsonsecurity.com/2019/11/110-nursing-homes-cut-off-from-health-records-in-ransomware-attack/

63 https://krebsonsecurity.com/2019/11/ransomware-bites-400-veterinary-hospitals/

64 Voir thème prioritaire du rapport semestriel 2019/1 de MELANI, chap. 3.

65 https://www.darkreading.com/threat-intelligence/ryuk-ransomware-hit-multiple-oil-and-gas-facilities-ics-security-expert-says-/d/d-id/1336865

les maliciels Dharma, Phobos et Maze exploitent des accès RDP ouverts ou mal sécurisés visibles sur Internet.

Une fois que l'infection a eu lieu, les hackers utilisent les faiblesses du protocole RDP pour se déplacer latéralement dans le système. Dès le mois d'avril 2018, FireEye a identifié une campagne de distribution de fausses mises à jour pour différents navigateurs (Chrome, Internet Explorer, Opera et Firefox), qui ont propagé les maliciels Dridex, NetSupport Manager RAT, AZOrult ou Chthonic[66]. Une fois que le maliciel a examiné le réseau, volé les identifiants de connexion et acquis les droits nécessaires, il injecte les rançongiciels BitPaymer et DoppelPaymer. Les mises à jour ont surgi sur des pages infectées sur lesquelles les victimes potentielles avaient été redirigées par des redirections «http://», par exemple. Au deuxième semestre 2019, MELANI a observé des sites suisses compromis à cette fin.

Le modèle d'affaires du rançongiciel reposait jusqu'ici entièrement sur le principe du déchiffrement de données contre de l'argent. Depuis quelque temps, certains groupes d'agresseurs[67] exfiltrent des données avant de procéder au chiffrement, pour prouver, par une publication partielle, qu'ils sont les auteurs de l'attaque, pour exercer une pression supplémentaire sur la victime, ou bien pour faire chanter celle-ci en la menaçant de publier les informations volées, en guise de solution de secours si le chantage aux données chiffrées ratait parce que la victime parvient à récupérer ses données[68]. En novembre 2019, par exemple, le groupe Maze a divulgué près de 700 Mo de données qu'il avait volées à une entreprise de sécurité[69]. Il a ensuite fait de même avec les données d'autres victimes de son chantage: le laboratoire de diagnostic médical MDLab, le fabricant de câbles et de filins Southwire, et une petite ville de Floride[70]. Le groupe qui se cache derrière ce rançongiciel est aussi actif en Suisse.

L'attaque par rançongiciel qui se transforme en fuite de données en cas de non-paiement de la rançon semble être un modèle d'affaires rentable. Les exploitants du rançongiciel REvil, également connu sous le nom Sodinokibi, ont annoncé adopter ce modèle[71].

Vu cette évolution, toute attaque par rançongiciel comporte désormais un risque de fuite de données, qui subsiste au-delà de la maîtrise de l'incident. Selon la valeur des données et des informations piratées, il faut s'attendre à ce que les criminels les exploitent tôt ou tard à leur profit. Les hackers devraient donc logiquement s'intéresser de plus en plus aux entreprises qui traitent des données personnelles importantes.

---

66 https://www.fireeye.com/blog/threat-research/2019/10/head-fake-tackling-disruptive-ransomware-attacks.html

67 Maze, Sodinokibi ou Doppel Paymer, p. ex.

68 https://www.bleepingcomputer.com/news/security/new-megacortex-ransomware-changes-windows-passwords-threatens-to-publish-data/; https://www.bleepingcomputer.com/news/security/maze-ransomware-not-getting-paid-leaks-data-left-and-right/

69 https://www.bleepingcomputer.com/news/security/allied-universal-breached-by-maze-ransomware-stolen-data-leaked/

70 https://www.bleepingcomputer.com/tag/maze/

71 https://www.bleepingcomputer.com/news/security/another-ransomware-will-now-publish-victims-data-if-not-paid/

Recommandations:

À l'intérieur de l'entreprise, les mesures ci-après ont fait leurs preuves: sauvegardez régulièrement l'intégralité de vos données afin d'augmenter vos chances de toutes les restaurer en cas d'attaque. Entraînez-vous aussi à lancer une procédure de restauration, pour être prêt le moment venu. Documentez votre infrastructure informatique, effectuez les mises à jour de logiciel dès qu'elles sont disponibles et actualisez vos directives en matière de sécurité. Élaborez des programmes de gestion des incidents, de communication et de gestion de la continuité des activités. Vérifiez l'efficacité de ces programmes en les testant régulièrement. La prévention efficace des cyberattaques associe les mesures techniques de sécurité à une sensibilisation régulière des collaborateurs. Les cadres doivent veiller à l'application de ces mesures. C'est une tâche qu'ils ne peuvent pas déléguer.

Aucune entreprise n'est en mesure de déjouer toutes les tentatives de cyberattaque. Il faut donc développer des capacités de réaction et de restauration pour atténuer les conséquences d'un incident inévitable.

INFO

Au deuxième semestre 2019, MELANI a publié une mise à jour des mesures de sécurité à prendre contre les nouvelles formes d'attaque par rançongiciel:

https://www.melani.admin.ch/melani/fr/home/dokumentation/newsletter/update-ransomware-neue-vorgehensweise.html

Attention: si vous êtes victime d'une infection en plusieurs étapes, la restauration des données à partir du backup ne suffira pas! Faites nettoyer le réseau et procédez à la réinstallation des systèmes infectés afin d'éliminer l'injecteur (dropper) à coup sûr.

4.6.2 Emotet, toujours la principale menace d'infection

Emotet est resté très actif en Suisse au second semestre 2019. Après une légère détente en juin, le groupe est revenu en force au mois d'août avec de nombreuses activités de propagation, faisant de nombreuses victimes.

Le mode opératoire est resté le même ce semestre: le cheval de Troie récupère le contenu d'échanges de courriels antérieurs et s'en sert pour générer de nouveaux messages qu'il envoie ensuite à tous les contacts figurant dans les listes de destinataires. Ces courriels sont accompagnés d'une pièce jointe, généralement un fichier Word contenant une macro malveillante. Dès qu'un destinataire ouvre ce fichier et active le mode édition, la macro s'exécute. Sans mesure de protection supplémentaire, Emotet télécharge des modules supplémentaires et instaure une persistance sur l'ordinateur de la victime[72].

Le groupe a perfectionné son mode opératoire et a revendu à d'autres acteurs des accès à des réseaux et à des systèmes. Il est ainsi devenu un acteur clé du cybercrime organisé. Le marché clandestin fourmille aussi de groupes proches de gouvernements, qui sont prêts, à des fins d'espionnage ou pour gagner de l'argent, à acheter des accès à des systèmes compromis.

[72] Cf. MELANI, rapport semestriel 2019/1, chap. 3.4.1 et 4.6 et annexe technique.

Recommandations:

Méfiez-vous des courriels entrants, qu'ils proviennent d'inconnus ou de relations à vous. Méfiez-vous également des courriels inattendus faisant référence à une ancienne conversation que vous avez eue. Les hackers usurpent volontiers l'identité de firmes particulièrement dignes de confiance pour envoyer des courriels à partir d'adresses falsifiées. En cas de doute, demandez à l'expéditeur supposé, en le joignant par un moyen éprouvé ou au moyen de coordonnées indiquées sur son site web, par exemple, de quoi il s'agit et si c'est bien lui qui a envoyé le message.

Soyez particulièrement prudent lorsque vous recevez un fichier Word. La plupart des entreprises et des organisations envoient à leur relations d'affaires des fichiers PDF (factures, devis, etc.) et non Word.

MELANI recommande aux entreprises de bloquer les pages Internet qui sont utilisées pour propager Emotet au niveau du périmètre du réseau, par exemple sur le proxy web ou le serveur DNS. Des sites tels que abuse.ch proposent une liste de ces pages.

4.7 Failles

Les erreurs de développement des logiciels fragilisent les systèmes, d'où l'importance cruciale de la gestion des cycles de vie et des correctifs (*patch management*). Chaque entreprise doit, quelle que soit sa taille, tenir un inventaire de tous ses systèmes et applications et fixer un planning des correctifs à installer et des logiciels à remplacer pour obsolescence. Ces précautions concernent aussi des composants comme les micrologiciels (*firmware*) ou les *management boards*. Lors du développement d'un logiciel, il faut aussi prendre en compte les vulnérabilités des cadres (frameworks) employés et de leurs interdépendances.

Les failles qui sont exploitables à distance, sans authentification, comme celles de *SMB* (EternalBlue[73]), de *RDP* (BlueKeep[74], BlueGate[75, 76]), de Citrix Netscaler[77] ou d'Oracle Weblogic[78], sont particulièrement vicieuses. Tant qu'une faille n'a pas été détectée (exploit *zero day*), sa valeur est élevée, et elle ne sert généralement qu'à des attaques ciblées. Dès qu'elle est découverte et que des correctifs sont créés, l'analyse des correctifs indique quelle faille est ouverte dans les systèmes non encore corrigés. Cette information permet de créer des *exploit codes*. Dès qu'un *exploit code* est disponible, la plupart des hackers et / ou des acteurs gouvernementaux l'intègrent dans leur boîte à outils et s'en servent abondamment. C'est à ce moment-là au plus tard que les systèmes accessibles de l'extérieur et présentant la faille doivent être considérés comme compromis. Les applications Internet et les systèmes de gestion

73 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0144
74 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-0708
75 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0610
76 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-0609
77 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-19781
78 https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-2546

de contenu (*content management systems* [CMS]) avec leurs différents modules complémentaires sont attaqués très fréquemment et nécessitent des mesures de sécurité spéciales (voir aussi «Mesures de prévention pour les systèmes de gestion de contenu (CMS)»[79]). Alors que le *patching* des systèmes et des applications informatiques courants est relativement facile, il en va autrement pour les systèmes de contrôle, les appareils de l'Internet des objets (IdO) ou les équipements médicaux. Une faille découverte en septembre 2019 dans VxWorks[80], un système d'exploitation en temps réel très souvent utilisé dans les systèmes de contrôle mais aussi dans les appareils médicaux, expose un grand nombre d'appareils dont certains sont très difficiles à mettre à jour.

L'exploitation des failles peut servir différents objectifs:

1. vol de données aux fins d'espionnage industriel ou de chantage;
2. propagation de maliciels;
3. prise du contrôle d'un système en vue de miner des cryptomonnaies;
4. envoi de maliciels ou de spams;
5. établissement d'un point d'ancrage pour pénétrer plus loin dans un réseau.

Recommandations:

Pour maintenir un niveau de sécurité constant, les entreprises doivent pratiquer une gestion rigoureuse des cycles de vie et des correctifs pour tous les composants utilisés. Cela concerne non seulement les systèmes de bureautique courants mais aussi les applications Internet, les appareils mobiles, les appareils IdO et les composants de contrôle. Elles doivent aussi tenir compte des bibliothèques de logiciels et des cadres employés.

En cas de vulnérabilité grave ne pouvant être résolue immédiatement, il faut des solutions de remplacement (second navigateur web, p. ex.) ou un moyen d'isoler temporairement la faille (pare-feu pour une application web, p. ex.).

Les solutions d'accès à distance tels que les portails VPN, les portails d'applications web, les accès aux messageries et les terminaux exposés font partie des cibles les plus intéressantes pour les agresseurs parce qu'elles livrent un accès direct aux ressources internes. Outre la gestion des cycles de vie et des correctifs, elles nécessitent impérativement des mesures de sécurité supplémentaires telles que l'authentification à deux facteurs, le renforcement (*hardening*) et l'évaluation centralisée des journaux.

Ceux qui développent des applications, des systèmes, des contrôles ou des appareils IdO doivent eux aussi mettre en place une gestion claire des cycles de vie et des correctifs et des canaux d'information appropriés entre eux-mêmes et leurs clients. Ils doivent aussi fournir un canal de communication facile à trouver sur lequel les chercheurs en sécurité peuvent signaler les failles qu'ils découvrent. Un programme de chasse aux bugs (*bug bounty*) peut se révéler un complément utile en favorisant le signalement précoce et l'élimination coordonnée des failles.

79 https://www.melani.admin.ch/melani/fr/home/dokumentation/checklisten-und-anleitungen/massnahmen-zum-schutz-von-content-management-systemen--cms-.html

80 https://go.armis.com/urgent11

4.8 Mesures de prévention

4.8.1 Une nouvelle norme minimale pour le secteur alimentaire

L'Office fédéral pour l'approvisionnement économique du pays (OFAE) a publié ces derniers mois plusieurs référentiels pour garantir la sécurité des systèmes d'information et de télécommunication (TIC) dans différents secteurs, compte tenu de la dépendance croissante des processus de production et de distribution à l'égard de ces systèmes. Si ceux-ci tombent en panne, cela risque de toucher les activités des entreprises et l'approvisionnement de la Suisse en biens et services critiques. Pour prévenir ce risque et pour garantir le ravitaillement de la population, l'OFAE a publié récemment la brochure «Norme minimale pour sécuriser la technologie de l'information et de la communication dans la filière alimentaire» dans le but d'aider les entreprises du secteur à éviter les pannes informatiques ou à les résoudre rapidement lorsqu'elles se produisent.

Cette recommandation fait suite à la norme minimale pour garantir la sécurité des TIC pour l'approvisionnement en eau, et au manuel *Grundschutz von «Operational Technology» in der Stromversorgung* (non traduit en français) pour l'approvisionnement en électricité. Ces normes sectorielles sont complétées par une norme minimale générale élaborée à partir des analyses de vulnérabilité quant aux cyberrisques de différents secteurs vitaux pour le fonctionnement de la Suisse. L'OFAE a effectué ces analyses dans le cadre de la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC)[81].

4.8.2 Blocage de magasins en ligne fictifs par la police suisse

Faire ses achats en ligne, c'est pratique mais non dépourvu de risques. Il peut arriver que l'acheteur ne reçoive jamais la marchandise commandée et payée, ou qu'il reçoive autre chose que ce qu'il a commandé. Au risque de vol s'ajoute celui de voir les données communiquées pour l'achat réutilisées pour commettre des infractions.

Le phénomène des magasins en ligne fictifs n'a pas épargné la Suisse: des cybercriminels enregistrent des pages frauduleuses sous un nom de domaine se terminant par «.ch». Cette activité connaît une croissance exponentielle à certaines saisons, par exemple avant Noël.

Le service *Cybercrime* de la police cantonale de Zurich traque avec SWITCH, le service suisse d'enregistrement des adresses internet en «.ch», les faux sites de vente en ligne utilisant ce genre d'adresse. En décembre 2019, cette collaboration a permis d'en bloquer 450 juste avant leur mise en ligne, portant à 6500 le nombre de ces sites identifiés et bloqués par la police cantonale de Zurich depuis le début 2018.

Ces opérations non seulement réduisent le nombre des faux magasins en ligne affichant un nom de domaine suisse, mais elles freinent fortement leur développement. La police cantonale de Zurich le confirme sur son site[82]. Elle y signale aussi les éléments qui doivent vous mettre la puce à l'oreille: noms de domaine sans rapport avec la marchandise proposée, absence du

81 https://www.admin.ch/gov/fr/start/dokumentation/medienmitteilungen.msg-id-75891.html

82 https://www.kapo.zh.ch/internet/sicherheitsdirektion/kapo/de/aktuell/medienmitteilungen/2019_12/1912161f.html

logo en forme de cadenas qui signale une connexion chiffrée, absence de l'impressum exigé par la loi[83].

4.8.3 Démantèlement d'un «RAT as a service» dans le cadre d'une opération internationale

MELANI a signalé à plusieurs reprises la pratique désormais largement répandue qui consiste à proposer des cyberattaques clé en main ou des outils permettant leur exécution[84]. La poursuite de ce genre de délits est particulièrement complexe. À la difficulté d'identifier les cybercriminels s'ajoute un obstacle supplémentaire: la frontière entre légalité et illégalité est mince, et parfois difficile à établir. Cela explique peut-être comment le développeur de logiciels Shockwave™ a pu, à partir de 2012, vendre en ligne le RAT Imminent Monitor sans être inquiété, jusqu'à ce qu'en novembre 2019 une opération internationale réunissant plusieurs autorités de poursuite pénale démantèle l'infrastructure.

Sur son site, le commerçant déclinait toute responsabilité quant à l'usage frauduleux que ses clients pourraient faire de ce produit. L'acheteur devait fournir une déclaration dans laquelle il s'engageait à ne pas utiliser ce service pour propager des maliciels. Mais le produit présentait de nombreuses fonctions atypiques et inutiles pour un RAT. Il permettait par exemple de désactiver l'antivirus, présentait des caractéristiques rendant plus difficile son identification, donnait accès au *remote desktop* qui restait caché à la vue de la victime et permettait même de rechercher des cryptomonnaies sur l'ordinateur infecté.

Le produit de base ne coûtait que 25 dollars, il était donc accessible à tous. Selon les autorités, il a été acheté par plus de 14 500 criminels, qui l'ont utilisé dans 124 pays contre des dizaines de milliers de victimes.

L'opération a été menée conjointement par la police fédérale australienne, Europol, Eurojust, le FBI et de nombreuses autres autorités policières et judiciaires, et a abouti à la saisie de 430 appareils et à l'interpellation de 13 utilisateurs mal intentionnés[85].

4.8.4 *Bug bounty*: chasse aux bugs sur Internet

Les programmes de chasse aux bugs sont des plateformes qui remettent des primes en échange du signalement de failles avérées. Ils se sont multipliés ces dernières années afin d'inciter les hackers à coopérer. Il en existe différentes sortes. Les plateformes commerciales jouent les intermédiaires entre le hacker et l'entreprise et fixent les règles à respecter par les deux parties. D'autres reposent sur un principe non commercial. Elles sont donc gratuites et fondées sur une communauté mais ne font pas l'intermédiaire entre les parties. Elles permettent aux experts en sécurité de signaler des failles constatées sur toutes sortes de sites. Du point de vue de l'entreprise, le *bug bounty* peut être soit ponctuel et accompagner le lancement

---

83 https://www.cybercrimepolice.ch/de/fall/betruegerische-internetshops-vorsicht-bei-der-online-schnaeppchenjagd/

84 MELANI, rapports semestriels 2009/2, chap. 4.7; 2016/2, chap. 6.1 et 2019/1, chap. 3.3

85 https://securityaffairs.co/wordpress/94525/cyber-crime/imminent-monitor-rat-shutdown.html
https://unit42.paloaltonetworks.com/imminent-monitor-a-rat-down-under/

d'un nouveau logiciel, soit permanent. Il peut être confié à un prestataire commercial ou conçu en interne. Certains États[86] ont défini leurs propres règles de gestion des failles.

La question de savoir comment les hackers doivent traiter les failles pour servir le grand public sans nuire aux entreprises fait débat depuis des années. Deux voies ont fini par s'établir: la «divulgation complète» et la «divulgation responsable». Dans le premier cas, le hacker informe simultanément l'entreprise et le grand public. L'entreprise subit ainsi une certaine pression puisque la faille étant connue, n'importe qui peut l'exploiter. C'est l'aspect critiquable de cette solution. Dans le second cas, le hacker informe dans un premier temps uniquement l'entreprise et lui laisse un délai (entre 60 et 120 jours) pour régler le problème. Il ne publie la faille qu'ensuite[87].

La plupart des programmes de chasse au bug fonctionnent selon la divulgation responsable, dont les grands principes sont les suivants:

1. L'entreprise dispose de suffisamment de temps (généralement de 60 à 120 jours) pour vérifier et supprimer la faille.
2. La faille n'est indiquée à aucun tiers.
3. Les tests concernant la faille ne doivent perturber ni les services, ni les produits ni le fonctionnement normal de l'entreprise.
4. Personne n'a le droit ni d'espionner ni de transmettre les données.
5. Les revendications (surtout financières) liées au signalement d'une faille ne sont pas prises en considération.

Il est probable que les entreprises vont être de plus en plus nombreuses à adopter cette pratique, ce qui offre de belles perspectives d'avenir aux chasseurs de bugs qualifiés et aux chercheurs en cybersécurité[88]. Les programmes existants, tel celui de Swisscom, produisent des chiffres impressionnants: l'entreprise a reçu et traité 844 signalements de failles, dont 427 ont abouti à une correction et au paiement d'une prime pour un montant total de 350 000 francs. Le type de failles signalé va du *low level cross-site scripting* (XSS) à de redoutables vulnérabilités *zero day* dans des produits connus et largement diffusés[89].

Tout récemment, des hacktivistes ont lancé une nouvelle forme de *bug bounty* visant à récompenser les hackers qui se font justice eux-mêmes et les hacktivistes qui organisent des piratages et des fuites de données au nom de l'intérêt public. Le nom de ces initiatives est leur seul point commun avec les programmes traditionnels, dont le but est d'apporter une contribution importante à la sécurité et d'identifier les failles dans les systèmes de sécurité afin de les corriger avant qu'elles ne puissent être exploitées.

---

86 Les Pays-Bas, p. ex.: https://www.government.nl/topics/cybercrime/fighting-cybercrime-in-the-netherlands/responsible-disclosure

87 https://www.zeit.de/digital/datenschutz/2013-09/bug-bounty-hack/seite-2

88 https://www.swisscyberstorm.com/2019/11/26/some-background-on-switzerlands-biggest-bug-bounty-program/

89 Chiffres à partir de 2018: https://www.swisscyberstorm.com/2019/11/26/some-background-on-switzerlands-biggest-bug-bounty-program/

Le CNCS (https://www.melani.admin.ch/melani/fr/home/ueber_ncsc/das_ncsc.html) est en train d'élaborer pour la Suisse une politique en matière de divulgation responsable.

Des informations concernant des failles peuvent être annoncées à :

incidents@ncsc.ch

5 Recherche et développement

5.1 Quand rien ne va plus: un rançongiciel et après?

Les rapports semestriels de MELANI évoquent régulièrement la pratique qui consiste, pour des groupes criminels, à chiffrer les données d'une victime pour lui extorquer de l'argent[90]. Son site propose des documents techniques expliquant comment se protéger au mieux contre les rançongiciels[91].

Mais aucune précaution technique n'offre une protection totale. On a assisté en 2019 à une professionnalisation des groupes de criminels, notamment de ceux qui recourent au modèle d'affaires «rançongiciel». Ils ne se contentent plus de chiffrer les données disponibles localement et par l'accès au réseau que leur a offert la victime en ouvrant sans se méfier une fausse facture ou un faux dossier de candidature. Après une première infection par un cheval de Troie, ils passent un temps assez long à se promener dans le réseau de la victime afin d'accéder si possible à tous les systèmes et les points névralgiques, y compris les copies de sauvegarde en ligne. Le but est de causer un maximum de dégâts lorsque le rançongiciel frappera.

Ce mode opératoire en plusieurs étapes peut permettre aux responsables de la sécurité informatique de détecter les agresseurs et de les neutraliser avant la catastrophe. Des entreprises de sécurité et des organisations partenaires signalent régulièrement des cas d'infection d'entreprises à MELANI, qui communique l'information aux exploitants de réseau concernés. Lorsque l'agresseur n'est pas détecté et qu'il déclenche son rançongiciel, neutralisant d'un seul coup non seulement les systèmes névralgiques de l'entreprise infectée, mais aussi des unités de production situées à l'étranger et reliées au réseau central, les dégâts peuvent être considérables.

5.1.1 Contre les rançongiciels, des remèdes non informatiques

Le modèle d'affaires des groupes pratiquant le rançongiciel consiste à exercer une pression maximale sur les entreprises et les organisations visées afin de donner plus de poids à leur demande de rançon. L'objectif est par conséquent de mettre à l'arrêt les processus fondés sur

---

90 MELANI, rapports semestriels 2011/2, chap. 3.5; 2013/2, chap. 3.1; 2014/2, chap. 3.6 et 5.3; 2015/1, chap. 4.6.1.5; 2015/2, chap. 4.5.1, 2016/1, chap. 4.6.3 et 5.4.3; 2016/2, chap. 6.1; 2017/1, chap. 3; 2017/2, chap. 5.4.2; 2018/2, chap. 4.5.4 et 5.3.5; 2019/1, chap. 3

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

l'informatique. Or l'informatique, qui devient de ce fait la source du problème, n'a aucun moyen de régler rapidement les difficultés concrètes: restauration des processus vitaux et activation du plan de continuité des activités, en espérant que le management a pensé à en élaborer un en amont.

Une fois qu'un rançongiciel a déployé ses effets, il faut identifier le plus vite possible les systèmes et les processus qui n'ont pas été touchés, c'est-à-dire ceux qui peuvent continuer de fonctionner même sans informatique.

Il faut aussi impliquer d'emblée des juristes, car dans tous les cas, les agresseurs ont eu accès à des données pendant quelques instants au moins. L'entreprise est soumise à la LPD et, si elle exerce une activité dans l'UE, au règlement général sur la protection des données (RGPD). Dans un deuxième temps très rapproché, il faut vérifier quels systèmes informatiques il est possible de restaurer à l'aide des backups et des instantanés de stockage (*snapshots*). L'idéal est de recourir aux services d'un spécialiste externe en sécurité informatique, à qui son expérience en matière de rançongiciels permettra de dresser un bilan relativement efficace des dégâts subis et des options envisageables.

Une fois que ces deux premières étapes ont fourni les informations recherchées, la direction va devoir, dans un troisième temps, se poser la question du paiement de la rançon en fonction de l'ampleur des dégâts et de leur coût potentiel. MELANI déconseille absolument le paiement de ces rançons, qui justifierait le modèle d'affaires des criminels en leur offrant en soutien financier. De plus, rien ne prouve que les criminels vont remplir leur part du contrat. Ce qui compte, c'est que l'entreprise concernée prenne immédiatement contact avec la police cantonale pour porter plainte et pour envisager avec elle la suite à donner à l'attaque.

5.1.2 Action pénale: une démarche utile

La gestion de l'incident mène, après les mesures immédiates, à une quatrième étape souvent sous-estimée mais pourtant indispensable, que la victime paye ou non la rançon: l'action pénale.

La plupart des entreprises frappées par un rançongiciel s'abstiennent d'engager des poursuites pénales. Beaucoup de gens pensent en effet que la police est impuissante face aux groupes cybercriminels étrangers. Or les autorités de poursuite pénale ont une vraie expérience de ce genre d'affaires et enquêtent sur les groupes de rançongiciel à l'échelle internationale. Lorsqu'une entreprise décide de payer quand même la rançon, la police dispose de collaborateurs spécialement formés pour entrer en contact avec les criminels.

L'engagement de poursuites en vaut donc la peine à plus d'un titre. Il permet à la police de recueillir des preuves qui lui permettront non seulement de traiter l'affaire en question mais aussi de soutenir d'autres enquêtes en cours en procédant à des recoupements. Il la transforme de facto en son propre centre de compétence pour le traitement des affaires de rançongiciel. Il lui permet de prodiguer des conseils, car selon le groupe de malfaiteurs, elle dispose de connaissances qui pourront être utiles aux collaborateurs et aux prestataires externes chargés de restaurer les systèmes.

5.1.3 Plan B comme BCM

En 2019, les entreprises suisses ont été la cible de nombreuses attaques par rançongiciel selon une logique simple: une entreprise empêchée de produire est prête à payer une forte rançon pour éviter d'être mise à l'arrêt pendant des journées entières. Cela se comprend. Un entrepreneur touché a qualifié d'«expérience de mort imminente» l'effet initial de l'arrêt général provoqué par une telle attaque.

Le rançongiciel interrompt les processus, ce qui le rapproche, de ce point de vue, des attaques en déni de service lancées contre les magasins en ligne. Ce que les pirates espèrent, c'est que l'entreprise ainsi bloquée sera prête à payer pour retrouver sa liberté de mouvement. Plus une entreprise est dépendante de l'informatique, plus elle souffre. C'est la raison pour laquelle les agresseurs cherchent en priorité à déconnecter les réseaux.

Il appartient à la direction de toute entreprise, de toute organisation, de veiller à ce que les procédures vitales puissent, au besoin, continuer de fonctionner indépendamment du service informatique. La gestion de la continuité des activités (BCM) ne peut être efficace que si elle a été mise au point avant toute cyberattaque.

5.2 L'escalade des conflits au Proche-Orient, une menace pour des partenaires commerciaux en Suisse

Les organisations qui entretiennent des relations commerciales avec le Proche-Orient risquent de servir de tremplin à des attaques contre des cibles liées aux conflits locaux.

Outre les guerres qui font rage en Syrie et au Yémen, le Proche-Orient est depuis longtemps une région à risque du point de vue de la sécurité de l'information. Les gouvernements de la région appliquent d'ailleurs un régime de surveillance nettement plus strict que celui de la plupart des États européens. L'an dernier, l'agence de presse Reuters[92] a consacré un article au projet Raven dans le cadre duquel des vétérans des services de renseignement américains ont aidé les Émirats arabes unis à développer leurs cybercapacités offensives. Elle explique que le projet a ensuite été transféré dans l'entreprise DarkMatter. Le Royaume d'Arabie saoudite a fait la une des médias en employant GovWare préalablement à l'assassinat du journaliste Jamal Khashoggi[93] et aussi, probablement, contre Jeff Bezos, fondateur d'Amazon et propriétaire du *Washington Post*[94]. Par ailleurs, les forces israéliennes ont dirigé une attaque aérienne contre un bâtiment d'où, selon un communiqué israélien, le Hamas palestinien lançait contre elles des cyberattaques[95].

Dans ce contexte tendu, les gouvernements concernés et les entreprises privées, en particulier les exploitants d'infrastructures critiques, n'ont cessé ces dernières années d'investir dans leur dispositif de sécurité de l'information. Ces organisations endurcies devenant des cibles de plus en plus difficiles à atteindre, les agresseurs ont commencé à s'intéresser à leur chaîne

92 https://www.reuters.com/investigates/special-report/usa-spying-raven/

93 https://citizenlab.ca/2019/04/dubious-denials-scripted-spin-spyware-company-nso-group-goes-on-60-minutes/

94 https://techcrunch.com/2020/01/22/bezos-nso-group-hack/

95 https://www.zdnet.com/article/in-a-first-israel-responds-to-hamas-hackers-with-an-air-strike/

d'approvisionnement en Europe[96, 97] et en Amérique du Nord[98]. Outre les fournisseurs du secteur industriel[99], les prestataires de services informatiques[100], notamment, constituent une cible intermédiaire de choix d'où lancer l'attaque contre l'institution visée en réalité.

Comme il est peu probable que le Proche-Orient s'apaise à court terme, les organisations suisses qui y entretiennent des relations doivent prévoir le risque d'une cyberattaque orchestrée de là-bas. Il suffit d'être un fournisseur, un prestataire de services ou un simple partenaire commercial d'une organisation accessoirement liée aux régions en conflit pour entrer dans le collimateur des agresseurs. Les groupes tels que APT33[101], Oilrig[102], Muddywater[103], Leafminer[104], APT39/Chafer[105], etc. ne lésinent pas sur les moyens lorsqu'il s'agit de trouver une porte d'entrée pour leurs opérations.

Les descriptifs référencés des groupes dans le catalogue «MITRE ATT&CK»[106] indiquent aussi bien les méthodes et les techniques employées par les agresseurs que des mesures d'évitement. La mise en place rigoureuse d'une authentification à plusieurs facteurs empêche de nombreuses attaques de ce type, ou en tout cas les complique considérablement.

5.3 De nouveaux modèles d'affaires pour «laver encore plus blanc»

Les cybercriminels sont des as de la division du travail. Chaque type de cyberattaque peut se voir comme une suite de tâches clairement définies dans lesquelles certains acteurs se sont souvent spécialisés. Ces acteurs recherchent constamment l'efficience maximale, contribuant ainsi à la rentabilité du phénomène. Parmi ces tâches spécifiques, le blanchiment de l'argent acquis illégalement occupe une place à part. En effet, toute la chaîne criminelle ne servirait à rien s'il n'était pas possible, en fin de compte, de recycler l'argent pour l'utiliser sur le marché légal. Cette activité est en plein boom: selon une étude publiée en 2018 par Bromium, les cybercriminels blanchissent chaque année de 80 à 200 milliards de dollars[107].

Le développement des monnaies virtuelles a révolutionné les transactions issues d'activités cybercriminelles. Aujourd'hui, bon nombre de pirates du Net financent leurs opérations au moyen de ces monnaies, notamment le bitcoin. Cela leur permet, même si les transactions sont documentées, de brouiller les pistes à l'aide de la *blockchain*, en utilisant par exemple

---

96 MELANI, rapport semestriel 2018/2, chap. 5.2.2

97 https://securingtomorrow.mcafee.com/other-blogs/mcafee-labs/shamoon-attackers-employ-new-tool-kit-to-wipe-infected-systems/

98 https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage

99 https://www.wired.com/story/iran-apt33-industrial-control-systems/

100 https://www.symantec.com/blogs/threat-intelligence/tortoiseshell-apt-supply-chain

101 https://attack.mitre.org/groups/G0064/

102 https://attack.mitre.org/groups/G0049/

103 https://attack.mitre.org/groups/G0021/

104 https://attack.mitre.org/groups/G0077/

105 https://attack.mitre.org/groups/G0087/

106 https://attack.mitre.org/

107 https://www.bromium.com/press-release/up-to-200-billion-in-illegal-cybercrime-profits-is-laundered-each-year-comprehensive-research-study-reveals/

des «mixeurs» (*tumblers*)[108]. Certaines activités cybercriminelles continuent cependant de rapporter de la monnaie sonnante et trébuchante. Par exemple, le recours aux chevaux de Troie bancaires, ou les paiements effectués avec une carte de crédit volée. Ces activités nécessitent un service de blanchiment plus traditionnel. On sait depuis longtemps que des particuliers se font enrôler pour mettre à disposition leur compte bancaire, réceptionner des fonds puis virer ceux-ci vers un compte différent moyennant une commission. On appelle ces personnes *money mules* ou agents financiers. Résolument opportunistes, les criminels tentent aussi de profiter de plateformes existantes. Certaines méthodes de blanchiment bien connues reposent sur des micropaiements PayPal ou des achats majorés sur eBay.

Actuellement, les criminels s'intéressent beaucoup aux plateformes telles qu'AirBnB ou Uber, qui permettent à un fournisseur de services d'entrer directement en contact avec ses clients grâce aux nouvelles technologies. La panoplie des méthodes de blanchiment d'argent compte désormais les «courses fantômes» en Uber. Le criminel commence par rechercher des chauffeurs Uber pas trop regardants et désireux d'arrondir leurs fins de mois. Pour ce faire, il publie des annonces sur des forums clandestins. Il commande ensuite une course qu'il règle au chauffeur selon la forme prescrite. Mais la course est purement fictive: le chauffeur ne quitte pas son domicile et reverse l'argent au criminel en conservant un pourcentage en guise de rémunération. La plateforme de location immobilière AirBnB a donné lieu à des opérations du même genre: le criminel loue un appartement dans lequel il ne mettra jamais les pieds. Là aussi, le propriétaire lui rembourse la location en conservant une commission.

La lutte contre la cybercriminalité vise à casser une chaîne d'activités hautement lucrative en attaquant un de ses maillons. C'est la raison pour laquelle la police cible régulièrement ces méthodes de blanchiment d'argent. Europol a par exemple annoncé en décembre 2019 avoir mené une opération réunissant 31 pays, qui a abouti à l'arrestation de 228 «agents financiers»[109]. En mai, elle avait déjà annoncé avoir fermé avec le concours des autorités luxembourgeoises et néerlandaises le site Bestmixer.io, qui permettait de blanchir près de 200 millions de dollars par an[110]. Comme le montrent les exemples de détournement d'Uber et d'AirBnB, les criminels ne manquent pas d'imagination ni de connaissances pour diversifier leurs méthodes de blanchiment. Outre le travail de la police et les mesures de sensibilisation à destination des *money mules* potentielles, une partie de la solution réside sans aucun doute dans les mesures mises en place par les services en ligne piratés et dans leur capacité à identifier le détournement de leurs activités à des fins de blanchiment.

---

[108] Service permettant de mélanger des crypto-transactions dans le but de cacher la véritable provenance des fonds.

[109] https://www.europol.europa.eu/newsroom/news/228-arrests-and-over-3800-money-mules-identified-in-global-action-against-money-laundering

[110] https://www.europol.europa.eu/newsroom/news/multi-million-euro-cryptocurrency-laundering-service-best-mixerio-taken-down

6 Produits publiés par MELANI

6.1 Blog GovCERT.ch

6.1.1 Trickbot - An analysis of data collected from the botnet

We are monitoring various threats and in that context we have collected quite some data about the Trickbot botnet in the past few years. This paper is based on an analysis of selected aspects of our Trickbot data collection. Our analysis consists of two main parts. In the first part we consider the PE timestamps of Trickbot droppers (i.e., the binaries being distributed by the Trickbot operators) and of the respective payloads (i.e., the PE binaries which are unpacked and then executed once a dropper is executed). The analysis is based on a collection of approximately 2100 droppers and corresponding payloads which were collected between July 2016 and February 2019.

https://www.govcert.admin.ch/blog/37/trickbot-an-analysis-of-data-collected-from-the-botnet (en)

6.2 Lettres d'information de MELANI

6.2.1 Mise à jour rançongiciels: nouvelle façon de procéder

30.07.2019 – Ces dernières semaines, des entreprises suisses ont été la cible d'un nouveau type d'attaque, ayant permis à des criminels d'infiltrer des réseaux et y déployer un rançongiciel permettant de chiffrer énormément de données. Différentes entreprises suisses renommées ont été touchées par ces attaques.

https://www.melani.admin.ch/melani/fr/home/dokumentation/newsletter/update-ransomware-neue-vorgehensweise.html

6.2.2 Fin du service d'assistance pour les produits plus anciens de Microsoft: attention, danger!

16.12.2019 – L'entreprise Microsoft a signalé qu'à partir du 14 janvier 2020, elle ne fournirait plus de service d'assistance ni de mises à jour pour ses produits les plus anciens, tels les systèmes d'exploitation Windows 7, Windows Server 2008 et Windows Server 2008 R2.

https://www.melani.admin.ch/melani/fr/home/dokumentation/newsletter/microsoft-end-of-life.html

7 Glossaire

Dénomination	Description
Advanced Persistent Threat (APT)	Menace pouvant infliger de sérieux dommages à une organisation ou à un pays. L'agresseur est disposé à investir beaucoup de temps, d'argent et de savoir-faire dans ce genre d'attaque ciblée et furtive, et dispose d'importantes ressources.
Agent financier	Un agent financier est un intermédiaire légal effectuant des opérations de courtage en devises. Depuis peu, cette notion s'utilise aussi à propos de transactions financières illégales.
Attaque DDoS	Attaque par déni de service distribué (*Distributed Denial-of-Service attack*) Attaque DoS où la victime est inondée de messages envoyés simultanément par de nombreux systèmes.
Attaque de la chaîne d'approvisionnement (supply chain)	Méthode consistant à s'en prendre à un maillon de la chaîne logistique de la victime afin de l'infecter.
Authentification à deux facteurs	Au moins deux des trois facteurs d'authentification sont exigés : un élément que l'on connaît (p. ex. mot de passe, code PIN, etc.) un élément que l'on détient (p. ex. certificat, jeton, liste à biffer, etc.) un élément qui nous est propre (p. ex. empreinte digitale, scanner rétinien, reconnaissance vocale, etc.).
BGP Border Gateway Protocol	Protocole de routage externe utilisé pour l'échange d'informations entre différents réseaux.
Bitcoin	«Bitcoin» désigne à la fois un système de paiement à travers le réseau Internet et l'unité de compte utilisée par ce système de paiement.
Bot	Du terme slave «robota», signifiant travail. Programme conçu pour exécuter, sur commande, certaines actions de manière indépendante. Les programmes malveillants (*malicious bots*) peuvent diriger à distance les systèmes compromis et leur faire exécuter toutes sortes d'actions.
C2 Command & Control	Infrastructure de commande et de contrôle de réseaux de zombies. La plupart des machines zombies peuvent être surveillées et recevoir des instructions par un canal de communication.

Dénomination	Description
CaaS Cybercrime as a service	Le développement d'outils malveillants vendus «clés en main» permet à des criminels de mener des cyberattaques même sans compétences techniques.
CEO fraud	On parle de l'arnaque au président (*CEO fraud*) quand l'identité d'un dirigeant d'entreprise est usurpée et le service compétent (service financier, comptabilité) est prié en son nom de procéder à un versement sur un compte (typiquement) à l'étranger.
CPU / Processeur	Le CPU (*Central Processing Unit*) désigne un processeur ou un microprocesseur, c'est-à-dire l'organe central d'un ordinateur, qui contient les circuits logiques exécutant les instructions des programmes.
Defacement	Défiguration de sites Web.
DNS	Système de noms de domaine (*Domain Name System*). Le DNS rend les services Internet plus conviviaux, puisqu'au lieu de l'adresse IP les utilisateurs composent un nom (p. ex. www.melani.admin.ch).
drive-by download	Infection d'un ordinateur par un maliciel, lors de la simple visite d'un site Web. Différents exploits, tirant parti des lacunes de sécurité non comblées par le visiteur, sont souvent testés à cet effet.
Dropper / Downloader	Injecteur; programme conçu pour charger et activer un ou plusieurs programmes malveillants.
Failles de sécurité	Erreur inhérente au matériel ou aux logiciels, permettant à un pirate d'accéder au système.
Force Brute	La recherche par force brute (*brute force*) ou recherche exhaustive consiste, en informatique, en cryptanalyse ou dans la théorie des jeux, à tester toutes les combinaisons possibles pour résoudre les problèmes.
Global Positioning System (GPS)	*Global Positioning System* (GPS), dont le nom officiel est NAVSTAR GPS, est un système mondial de navigation par satellite, permettant de déterminer à un moment précis une position géographique.
Internet des objets	Ensemble des objets branchés à Internet capables de communiquer pour collecter, transmettre et traiter des données, avec ou sans intervention humaine.

Dénomination	Description
ISP Internet Service Provider	Fournisseur d'accès à Internet, entreprise ou société fournissant aux utilisateurs finaux une connexion Internet et d'autres services réseau (boîte aux lettres, hébergement de contenu, etc.).
JavaScript	Langage de script basé objet pour le développement d'applications. Les Javascripts sont des éléments de programmes intégrés au code HTML qui permettent d'implémenter certaines fonctions dans le navigateur Internet. Un exemple est le contrôle des indications saisies par l'utilisateur dans un formulaire Web. Il permet de vérifier que tous les caractères introduits dans un champ demandant un numéro de téléphone sont effectivement des chiffres. Comme les composants ActiveX, les Javascripts s'exécutent sur l'ordinateur de l'internaute. Outre les fonctions utiles, il est malheureusement possible aussi d'en programmer de nuisibles. Au contraire d'ActiveX, le langage JavaScript est compatible avec tous les navigateurs.
Kit d'exploits	Outil permettant de générer des scripts, programmes ou codes, visant à exploiter des failles de sécurité.
Malspam	Courriel indésirable (spam) envoyé à grande échelle pour diffuser des maliciels.
Malware / Malicious code	Maliciel / 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.
Métadonnées	Les métadonnées ou métainformations sont des données renseignant sur la nature de certaines au-tres données.
Minage	Utilisation de la puissance de calcul d'un ordinateur pour valider et sécuriser, par blocs, les transactions d'un réseau de cryptomonnaie. Cette activité est rémunérée à cause de sa forte consommation d'énergie.
MSP Managed Services Provider	Fournisseur de services d'infogérance, prestataire externe s'occupant de la totalité ou d'une partie de l'infrastructure informatique de ses clients.

Dénomination	Description
NAS Network Attached Storage	Serveur de stockage en réseau; serveur de fichiers autonome, relié à un réseau pour permettre à ses utilisateurs de stocker et de mettre en commun leurs données.
Patch	Rustine. Programme qui remplace une partie de programme comportant des erreurs par une partie exempte d'erreurs et remédie ainsi p.ex. à une lacune de sécurité.
Peer to Peer (P2P)	Architecture de réseau où tous les postes de travail ont les mêmes possibilités de communication (à l'inverse des réseaux client/serveur). P2P sert fréquemment aux échanges de données.
Phishing	Hameçonnage. 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.
Porte dérobée	Une porte dérobée (*backdoor*) désigne une fonctionnalité inconnue de l'utilisateur légitime, qui permet à un pirate d'accéder secrètement à un programme ou à un système d'exploitation, en contournant les mécanismes de sécurité en place.
Pourriel (spam)	Désigne le courrier électronique non sollicité, constitué surtout de publicité, envoyé automatiquement. L'auteur de tels messages est qualifié de polluposteur (*spammer*) et ses envois de pollupostage (*spamming*).
PowerShell (script)	PowerShell est une suite logicielle Microsoft qui intègre une interface en ligne de commande et un langage de script, permettant d'automatiser des tâches ou de configurer et d'administrer des systèmes.
Protocole SMB	Server Message Block (SMB) est un protocole permettant le partage de ressources (fichiers, imprimantes, etc.) sur des réseaux locaux.
Proxy	Programme servant d'intermédiaire pour accéder à un autre réseau, en collectant les requêtes et en les transmettant vers l'extérieur à partir d'une même adresse.

Dénomination	Description
RaaS Ransomware as a service	Service vendu clés en main pour qu'un criminel puisse rançonner les utilisateurs informatiques même sans compétences techniques.
Ransomware	Maliciel utilisé comme moyen de chantage contre le propriétaire de l'ordinateur infecté. Typiquement, le pirate chiffre ou efface des données et ne fournit la clé nécessaire pour les sauver qu'après le versement d'une rançon.
Remote Administration Tool (RAT)	Un RAT (*Remote Administration Tool*, outil de télémaintenance) est un programme permettant la prise de contrôle totale, à distance, d'un ordinateur depuis un autre ordinateur.
Remote Desktop Protocol (RDP)	Protocole propriétaire, servant à la prise de contrôle à distance des postes Microsoft Windows.
Réseau de zombies	Plusieurs ordinateurs infectés peuvent former ensemble un réseau, dirigé par une infrastructure de commande et de contrôle (C&C).
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.
Smartphone	Un smartphone est un téléphone mobile doté des fonctions d'un assistant numérique personnel (agenda, calendrier, navigation Web, consultation du courrier électronique, messagerie instantanée, GPS, etc.).
SMS	Short Message Service, Service de messages courts. Service permettant d'envoyer des messages courts (max. 160 caractères) à un (utilisateur de) téléphone mobile.
Social Engineering	Les attaques de social engineering (subversion psychologique) utilisent la serviabilité, la bonne foi ou l'insécurité des personnes pour accéder par exemple à des données confidentielles ou conduire la victime à exécuter certaines actions spécifiques. Une forme commune d'attaque de social engineering est le phishing.

Dénomination	Description
Spear Phishing	Pêche au harpon. La victime aura p. ex. l'illusion de communiquer par courriel avec une personne connue d'elle.
Spoofing	Action malveillante consistant à utiliser délibérément l'adresse d'un autre système au lieu de la sienne.
Systèmes de contrôle industriels (SCI)	Les systèmes de contrôle-commande sont formés d'un ou plusieurs appareils qui pilotent, règlent et/ou surveillent le fonctionnement d'autres appareils ou systèmes. Dans le domaine industriel, l'expression «systèmes de contrôle industriels» (*Industrial Control Systems*, ICS) est entrée dans le langage courant.
Take-Down	Retrait de contenu frauduleux, désactivation d'adresse Web par un hébergeur ou un registraire.
TCP / Adresse IP	*Transmission Control Protocol* / *Internet Protocol*. Adresse identifiant l'ordinateur sur Internet (ou dans un réseau TCP/IP) (exemple : 172.16.54.87).
Top-Level-Domain (TLD)	Chaque nom de domaine est formé d'une suite de signes, séparés par des points. Le domaine de premier niveau (TLD) est toujours situé à l'extrême droite du nom Internet. Par exemple, dans l'adresse http://www.melani.admin.ch, le TLD est «ch». Quand il correspond à un code de pays, représenté par des abréviations à deux caractères, on parle de domaine national (ccTLD).
UDP	*User Datagram Protocol*. Protocole sans connexion, utilisé pour expédier de petits messages (datagrammes) d'une application Internet à l'autre.
USB	*Universal Serial Bus*. Bus série permettant (avec les interfaces physiques) de raccorder des périphériques tels qu'un clavier, une souris, un support de données externe, une imprimante, etc. Il n'est pas nécessaire d'arrêter l'ordinateur pour brancher ou débrancher un appareil USB. Les nouveaux appareils sont généralement (selon le système d'exploitation) reconnus et configurés automatiquement.
Ver	À la différence des virus, les vers n'ont pas besoin de programme hôte pour se reproduire. Ils utilisent les lacunes de sécurité ou des erreurs de configuration des systèmes d'exploitation ou des applications, pour se propager d'ordinateur en ordinateur.

Dénomination	Description
Watering Hole Attack	Attaque dite du point d'eau, attaque ciblée par un maliciel, diffusé à travers des sites supposés être visités par un groupe spécifique d'utilisateurs.
WLAN	Un WLAN (*Wireless Local Area Network*) est un réseau local sans fil.
Zero day	Vulnérabilité, pour laquelle aucun correctif de sécurité n'est pour l'instant disponible.
Zip	Zip est un algorithme et un format de compression des données destiné à réduire l'espace mémoire occupé par les fichiers lors de l'archivage ou du transfert.