Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Centre national pour la cybersécurité NCSC
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 2020/I (de janvier à juin)

29 OCTOBRE 2020

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

1 Aperçu / sommaire

2 Éditorial

La cyberdiplomatie helvétique dans la nouvelle géopolitique numérique

Envoyé spécial pour la politique étrangère et de sécurité relative au cyberespace, Jon Fanzun

Jon Fanzun, Envoyé spécial pour la politique étrangère et de sécurité relative au cyberespace

Il y a quelques années encore, la cybersécurité n'était qu'un créneau thématique suscitant, au niveau international, des débats généralement réservés aux experts techniques. Aujourd'hui, la cybersécurité est devenue un enjeu fondamental et un sujet brûlant en politique internationale – d'autant plus brûlant que les technologies numériques jouent un rôle central, à l'ère de la société de l'information. Les technologies clés se retrouvent ainsi au cœur des conflits mondiaux.

L'actuel bras de fer entre les États-Unis et la Chine à propos de la 5G montre de façon exemplaire comment des questions de politique de sécurité, de nature économique ou sociétale alimentent une nouvelle forme de géopolitique. On peut parler ici de «géopolitique numérique», où ce ne sont plus les technologies qui rivalisent, mais où un modèle libéral et un autre centré sur l'État s'affrontent, dans une véritable compétition idéologique.

Dans ce contexte, la Suisse se doit de défendre activement ses propres intérêts dans le cyberespace. Le Bureau DFAE Cyber remplit cette tâche, en collaboration avec ses divers partenaires de l'administration fédérale – dont le Centre national pour la cybersécurité (NCSC). L'actuelle stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC 2.0) ainsi que la stratégie de politique extérieure 2020-2023 fixent le cadre stratégique des activités déployées.

La Suisse s'engage pour un cyberespace libre, ouvert et sûr, qui soit utilisé à des fins pacifiques et qui repose à la fois sur des règles claires et sur la confiance réciproque. Elle considère que le droit international prévaut également dans le cyberespace. Nous prônons par ailleurs l'implication active des acteurs concernés, qu'il s'agisse de la société civile ou des milieux économiques. Nous défendons nos intérêts et nos valeurs dans les forums internationaux, à l'instar de l'ONU, de l'OSCE et de l'OCDE. Les cyberdialogues bilatéraux s'avèrent également importants. Durant les prochaines années, nous visons à intensifier et élargir de tels dialogues avec un certain nombre de pays, comme le prévoit la SNPC 2.0.

Alors que des blocs antagonistes tendent à se former, que la confiance interétatique est en chute libre et dès lors que le cyberespace se fragmente, les avancées sur le terrain de la cyberdiplomatie internationale s'annoncent ardues. Il sera déjà bien assez difficile de consolider le consensus international qui prévaut actuellement – tel qu'il figure notamment dans le rapport du «Groupe d'Experts Gouvernementaux des Nations Unies» (GGE) de 2015.

Or là où la confiance tend à disparaître et le ton des débats à se durcir, les bâtisseurs de ponts sont souvent les bienvenus. La Suisse a ici des atouts diplomatiques et une grande crédibilité à faire valoir. Elle peut transposer dans le monde en ligne sa vaste expérience acquise dans le monde hors ligne. La Genève internationale joue ici un rôle important. La Suisse y dispose

d'un cadre engageant pour les discussions sur la cybersécurité et les nouvelles technologies. Le «Geneva Dialogue on Responsible Behaviour in Cyberspace» est un bon exemple du pragmatisme dont la Suisse fait preuve en la matière, sachant que des entreprises mondiales comme Microsoft, Kaspersky ou Huawei participent aux discussions sur la cybersécurité.

La cyberdiplomatie est un sport d'équipe. Elle a besoin, pour défendre efficacement les intérêts de la Suisse sur la scène internationale, du savoir-faire d'un grand nombre d'acteurs. Le fait que le NCSC fédère et coordonne leurs forces est très précieux pour la cybersécurité internationale de la Suisse. Mes remerciements s'adressent à tous les acteurs des différents départements fédéraux œuvrant ensemble en faveur d'un cyberespace libre, sûr et ouvert.

Jon Fanzun

Au fait:

Le rapport semestriel MELANI paraît pour la dernière fois sous ce nom, et sera à l'avenir publié sous le label du Centre national pour la cybersécurité (NCSC). Car depuis le 1er juillet 2020, date d'entrée en vigueur de l'ordonnance sur la protection contre les cyberrisques dans l'administration fédérale (ordonnance sur les cyberrisques, OPCy), MELANI fait partie du NCSC.

Soucieux d'améliorer constamment nos produits et de répondre aux besoins de notre lectorat, nous vous invitons à nous donner **votre avis sur le présent rapport**:

https://www.melani.admin.ch/melani/fr/home/documentation/rapports/evaluation-halbjahresbericht1.html

3 Thème prioritaire: COVID-19

3.1 Une aubaine pour l'ingénierie sociale

Les cyberacteurs lancent régulièrement des attaques d'ingénierie sociale qui se réfèrent à l'actualité immédiate, comme une catastrophe naturelle ou un événement sportif. La pandémie actuelle ne fait pas exception à la règle. Un virus inédit, dont on ne sait pas grand-chose et qui peut infecter n'importe qui, est une aubaine pour de telles attaques, qui tirent parti du sentiment d'incertitude, des craintes ou de la curiosité. Les escrocs ont ainsi cherché à installer des maliciels sur les ordinateurs de la population, ou alors tenté d'amener des individus à leur communiquer des données personnelles, en prétendant détenir des informations exclusives concernant les vecteurs ou le nombre d'infections, ou encore la propagation du coronavirus. D'autres messages parlaient de mesures de protection ainsi que de méthodes de traitement. La pénurie initiale d'équipements de protection individuelle (masques faciaux, désinfectant) a conduit les agresseurs à diffuser des offres mensongères en la matière afin d'attirer l'attention.[1] Puis quand les gouvernements ont adopté des mesures de soutien à la population et aux entreprises, des courriels frauduleux ont fait miroiter de telles aides,[2] notamment là où des processus extraordinaires et donc inhabituels avaient été mis en place. De même, le suivi des contacts (*contact tracing*) a offert des occasions à l'ingénierie sociale. Enfin, les parcs de loisirs et d'attractions ayant lancé des offres spéciales à leur réouverture, les criminels ont diffusé leurs propres promotions fallacieuses.[3] De telles campagnes ont encore de beaux jours devant elles, quand des vaccins seront développés et mis sur le marché.

Un autre scénario a eu le vent en poupe suite aux fermetures de commerces et à l'envoi massif de commandes en ligne, avec de prétendus colis n'ayant pu être délivrés ou n'étant pas conformes aux prescriptions. De tels messages demandaient souvent au destinataire d'accomplir une action spécifique.[4] La victime était priée par courriel ou par SMS de payer l'affranchissement manquant ou de s'acquitter de frais de dédouanement. De tels courriels envoyés au nom de services de livraison comme DHL, FedEx et UPS, ou encore de la Poste ou des douanes, servent en général à diffuser des maliciels ou s'emploient à des fins de phishing et de fraude, ou encore pour tendre des pièges à l'abonnement (voir chap. 3.1.3 et aussi le chap. 4 pour l'aperçu des annonces reçues).

---

1 https://securityintelligence.com/posts/german-task-force-for-covid-19-medical-equipment-targeted-in-ongoing-phishing-campaign/

2 https://www.cisa.gov/sites/default/files/publications/Avoid_Scams_Related_to_Economic_Payments_COVID-19.pdf; https://www.proofpoint.com/us/blog/threat-insight/ready-made-covid-19-themed-phishing-templates-copy-government-websites-worldwide

3 https://www.cybercrimepolice.ch/de/fall/wieder-betrug-mit-themenpark-tickets-zoo-zuerich-nein-abofalle/; https://www.srf.ch/news/schweiz/abzocke-mit-abofalle-betrug-im-namen-des-zueri-zoo

4 https://www.cybercrimepolice.ch/de/fall/sms-angeblich-im-namen-der-post-betrueger-verteilen-spionage-app/; https://www.cybercrimepolice.ch/de/fall/angebliche-paketlieferung-mit-code-per-sms-freischalten/; https://www.kaspersky.com/blog/covid-fake-delivery-service-spam-phishing/35125/

3.1.1 Diffusion de maliciels

Presque toutes les familles usuelles de maliciels ont sévi à un moment ou l'autre en utilisant comme prétexte le coronavirus (COVID-19). Le facteur de diffusion le plus répandu était un courriel comportant une pièce jointe infectée ou un lien vers une page manipulée. Par ailleurs, des sites non officiels de téléchargement proposaient des applications censées indiquer sur une carte la propagation du virus et signaler la présence dans les parages de personnes infectées[5]. Des copies d'applications officielles de traçage enrichies par un maliciel ont également été découvertes[6]. Les escrocs ont encore tiré parti de l'engouement pour les solutions de vidéoconférences : des sites Web frauduleux, portant un nom de domaine pirate proche à s'y méprendre de celui d'une marque connue (*typo domain*), proposaient des fichiers d'installation de logiciels de conférence enrichis d'un maliciel[7].

Le 13 mars 2020, une vague de courriels renfermant un maliciel s'est abattue sur la Suisse[8]. Leur expéditeur était censé être l'Office fédéral de la santé publique (OFSP), indiqué avec son acronyme anglais FOPH (Federal Office of Public Health). Les courriels avaient été expédiés depuis l'ambassade du Kenya à Paris, dont l'infrastructure informatique avait été piratée. Un cheval de Troie appelé «AgentTesla», qui enregistre discrètement les frappes et parvient à faire des captures d'écran, se dissimulait dans un fichier Excel joint en annexe.

Fig. 1: Courriel expédié au nom de l'OFSP avec une pièce jointe infectée.

---

5 https://www.cybercrimepolice.ch/de/fall/vorsicht-vor-falscher-corona-virus-mapping-app/; https://symantec-blogs.broadcom.com/blogs/threat-intelligence/android-apps-coronavirus-covid19-malicious; https://research.checkpoint.com/2020/covid-19-goes-mobile-coronavirus-malicious-applications-discovered/

6 https://www.anomali.com/blog/anomali-threat-research-identifies-fake-covid-19-contact-tracing-apps-used-to-monitor-devices-steal-personal-data; https://www.bleepingcomputer.com/news/security/new-f-unicorn-ransomware-hits-italy-via-fake-covid-19-infection-map/; https://cert-agid.gov.it/news/campagna-ransomware-fuckunicorn-sfrutta-emergenza-covid-19/

7 https://blog.checkpoint.com/2020/03/30/covid-19-impact-cyber-criminals-target-zoom-domains/; https://blog.trendmicro.com/trendlabs-security-intelligence/zoomed-in-a-look-into-a-coinminer-bundled-with-zoom-installer/

8 https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/gefaelschte-emails-im-namen-des-bag.html

De tels leurres sur le thème du COVID-19 ont généralement servi à diffuser des maliciels capables de dérober des informations à la victime ou de recueillir des renseignements sur elle (*infostealer* ou *spyware*).[9] Ces logiciels espions renferment souvent aussi des modules capables de télécharger d'autres maliciels. Ce genre de courriel a parfois directement servi à diffuser des rançongiciels (ransomware), maliciels formulant une demande de rançon.

Recommandations :

Si vous avez cliqué sur des liens ou ouvert des annexes de courriels suspects, il se peut qu'un maliciel ait infecté votre appareil, auquel cas vous devriez l'analyser en détail, le nettoyer au besoin ou, mieux encore, le réinstaller complètement. Adressez-vous au besoin à un spécialiste. Il n'est jamais garanti qu'un antivirus parvienne à identifier et éradiquer toutes les infections. Après la réinstallation, n'oubliez pas de modifier tous les mots de passe utilisés sur l'appareil piraté.

3.1.2 Phishing

Dans leurs attaques d'ingénierie sociale, les cybercriminels n'ont aucun scrupule à profiter de l'actualité immédiate ou d'une situation exceptionnelle pour amener leurs victimes, en tirant parti de leur curiosité, de leurs craintes ou de leur ignorance, à exécuter des manipulations spécifiques. Ils se réfèrent volontiers à un événement précis pour donner à leur scénario la crédibilité nécessaire. Ainsi, des courriels expédiés au nom de Netflix promettaient, peu avant l'instauration du confinement, l'accès gratuit à ce service pendant la crise du coronavirus.[10] Pour accéder à cette offre, il fallait indiquer les données de sa carte de crédit. Le phishing à partir de prétendues plateformes de conférences est un autre exemple d'exploitation de situations exceptionnelles en vue du lancement de cyberattaques. Beaucoup d'utilisateurs découvraient pour la première fois les logiciels de conférences et de collaboration. Il n'allait donc pas de soi pour eux de savoir si un message venait bien de la plateforme ou s'il s'agissait d'une contrefaçon.[11] Les escrocs ont exploité ce sentiment d'insécurité pour rediriger les utilisateurs sur des masques de saisie manipulés et les amener à y indiquer leur mot de passe.

---

9 https://blog.checkpoint.com/2020/05/11/april-2020s-most-wanted-malware-agent-tesla-remote-access-trojan-spreading-widely-in-covid-19-related-spam-campaigns/; https://www.lastline.com/labsblog/infostealers-weaponizing-covid-19/; https://www.bleepingcomputer.com/news/security/microsoft-warns-of-covid-19-phishing-spreading-info-stealing-malware/;

10 https://www.cybercrimepolice.ch/de/fall/corona-phishing-mail-im-namen-von-netflix/

11 https://www.darkreading.com/cloud/fake-microsoft-teams-emails-phish-for-credentials/d/d-id/1337717; https://abnormalsecurity.com/blog/abnormal-attack-stories-microsoft-teams-impersonation/; https://abnormalsecurity.com/blog/abnormal-attack-stores-zoom-phishing-campaign/;

Recommandations :

Si vous recevez des messages inédits ou insolites, un certain scepticisme est de mise. Au lieu de suivre les liens de tels messages, vous devriez autant que possible vous connecter à votre compte d'utilisateur par la méthode habituelle. Vérifiez toujours que vous êtes bien sur la page souhaitée, avant d'y saisir des données personnelles, des mots de passe ou des informations concernant votre carte de crédit.

3.1.3 Abonnements abusifs

Pendant le semi-confinement de mars, des messages WhatsApp diffusés en Suisse annonçaient le tirage au sort de bons alimentaires. Ils étaient censés émaner de commerçants de détail désireux de «soutenir la nation pendant la pandémie du coronavirus». Les escrocs avaient contrefait des marques connues comme Migros, Coop et Denner.[12] La page Internet indiquée en hyperlien demandait les coordonnées de la carte de crédit – afin soi-disant de vérifier l'identité de la personne et de s'assurer qu'elle ne fasse valoir qu'un seul bon. En réalité, le visiteur souscrivait sans s'en douter un coûteux abonnement, mentionné en petits caractères sur la page, pour lequel une taxe mensuelle était perçue sur sa carte de crédit.

Recommandations :

Il importe de toujours contrôler en détail les décomptes de sa carte de crédit pour pouvoir le cas échéant la bloquer, en accord avec son émetteur, en cas d'irrégularités ou de prélèvements non autorisés. Les escrocs peuvent non seulement se servir des données dérobées pour effectuer des retraits, mais aussi les revendre à des tiers.

3.2 Cyberattaques contre des sites Web et des services en ligne

Dans plusieurs pays, les sites Internet d'hôpitaux ou d'autorités étatiques fournissant des renseignements sur la pandémie ou proposant des prestations ont subi des pannes de courte durée.[13] Certains responsables de sites ont attribué l'incident à des attaques DDoS. Il a beau s'agir d'une explication plausible et sans doute exacte la plupart du temps, il se pourrait ponctuellement que l'intérêt grandissant de la population pour les contenus publiés et les prestations proposées ait causé une surcharge des serveurs.

---

12 https://www.cybercrimepolice.ch/de/fall/whatsapp-fake-kettenbrief-im-umlauf-migros-verlost-kostenlose-lebensmittel-im-wert-von-250-euro-um-die-nation-waehrend-der-corona-pandemie-zu-unterstuetzen/; https://www.cybercrimepolice.ch/de/fall/weiterer-whatsapp-fake-kettenbrief-angeblich-von-denner-im-umlauf/; https://www.cybercrimepolice.ch/de/fall/wieder-whatsapp-fake-kettenbrief-diesmal-im-namen-von-coop/; https://www.cybercrimepolice.ch/de/fall/neuer-whatsapp-kettenbrief-migros-verlost-gutscheine-in-hoehe-von-chf-180-/

13 https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response; https://hungarytoday.hu/coronavirus-govt-website-attack-shutdown/; https://www.lesechos.fr/tech-medias/high-tech/laphp-victimes-dune-cyberattaque-1188022; https://news.trust.org/item/20200401133925-o6wx4/

Recommandations :

Toute entreprise tributaire de ses systèmes informatiques devrait s'assurer en priorité de la sécurité des canaux correspondants. Passez en revue les services importants au point qu'une panne affecterait gravement votre organisation. N'oubliez pas vos systèmes de base, sans lesquels vos applications professionnelles critiques ne fonctionneraient pas. Élaborez une stratégie contre les attaques DDoS. Il vous faut connaître les services internes ou externes compétents, ainsi que les autres personnes habilitées à agir en cas de cyberattaque. Idéalement, toute entreprise aura réfléchi à la problématique des attaques DDoS, dans la gestion générale des risques menée au niveau de sa direction, avant d'avoir subi une telle mésaventure et de façon à atteindre un niveau de préparation suffisant. Aucune organisation n'est à l'abri d'une attaque DDoS. Parlez à votre fournisseur Internet de vos besoins et des mesures préventives indiquées.

Liste de contrôle des mesures à prendre contre les attaques DDoS

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

3.3 Attaques lancées contre des hôpitaux

Les hôpitaux étaient déjà dans le collimateur des cybercriminels avant la pandémie, étant notamment victimes de rançongiciels (ransomware).[14] Avec la crainte de surcharge des institutions de santé, le moindre incident survenu dans la branche a rencontré un grand écho. Il y a ainsi eu un tollé international le 16 mars, lorsqu'un hôpital tchèque qui est aussi un important centre de dépistage du coronavirus a reconnu ne plus pouvoir fonctionner normalement à cause d'un rançongiciel. Divers gouvernements ont fermement condamné de telles attaques contre le secteur de la santé et appelé à une coopération internationale pour éradiquer ce fléau. Quelques opérateurs de rançongiciels ont promis là-dessus de ne plus s'en prendre aux hôpitaux. Par la suite, divers établissements ont néanmoins rencontré des incidents dus à des rançongiciels.[15] Plusieurs entreprises de sécurité se sont offertes pour aider gratuitement les institutions malchanceuses du secteur de la santé.[16]

3.4 Cyberespionnage

En temps normal, les espions récoltent des renseignements susceptibles de varier considérablement d'un continent et d'un pays à l'autre, selon les priorités des gouvernements qui les emploient. À l'heure de la pandémie, les États avaient tout intérêt à disposer des mêmes informations sur le virus et la maladie qu'il provoque. Or bien que ce problème mondial soit l'affaire de tous, les acteurs ne collaborent pas tous de manière inconditionnelle. Certains pays

---

14 Voir rapports semestriels MELANI 2016/1, chap. 5.4.3; 2017/1, chap. 3; 2019/1, chap. 3; 2019/2, chap. 4.6.1.

15 https://www.bleepingcomputer.com/news/security/ryuk-ransomware-keeps-targeting-hospitals-during-the-pandemic/; https://securityaffairs.co/wordpress/100548/malware/ryuk-ransomware-hospitals-covid19.html;

16 https://www.coveware.com/blog/free-ransomware-assistance-to-healthcare-coronavirus; https://cybersecurity.att.com/blogs/labs-research/a-surge-in-threat-activity-related-to-covid-19; https://coronahelp.isss.ch/

ne font pas confiance à d'autres, ni d'ailleurs à l'Organisation mondiale de la santé (OMS), et s'imaginent qu'on leur cache des informations. Ils chargent dès lors leurs propres espions d'enquêter sur place. Si les découvertes d'éventuelles manipulations statistiques commises dans un autre pays aident à mieux évaluer les risques ou peuvent être utilisées à des fins de propagande politique, les informations relatives à la pertinence des mesures de protection adoptées, de méthodes de traitement ou de médicaments spécifiques ont une utilité directe pour leurs propres solutions. Les choses se compliquent encore avec les vaccins potentiels : d'un côté, de nombreuses institutions académiques et d'autres organisations effectuent des recherches dans ce secteur et s'échangent des informations. De l'autre, des entreprises privées sont également impliquées, mues par l'espoir de réaliser de gros bénéfices en produisant leur propre vaccin ou en délivrant des brevets. Autrement dit, trouver un moyen efficace et ravitailler toute la population de son propre pays, voire du monde entier n'est pas qu'un défi scientifique et logistique, et comporte aussi une dimension économique et politique. Le chap. 4.6.1 reviendra sur l'espionnage en période de COVID-19.

Conclusion :

Quiconque mène des activités de recherche et de développement axées sur la pandémie actuelle doit s'attendre à subir des attaques d'espionnage d'origines diverses. Les données traitées, les résultats de la recherche et les secrets de fabrication présentent un intérêt bien réel pour les organisations tant étatiques que privées.

3.5 Télétravail – en toute sécurité!

La transformation numérique du quotidien professionnel a fait un bond en avant, en raison de la pandémie. Beaucoup d'entreprises ont introduit ou étendu le télétravail. Les téléconférences ou vidéoconférences ont pris le relais des séances présentielles. Prises de court, les organisations ont parfois adapté à la hâte leur infrastructure informatique au télétravail, sans avoir correctement pris les mesures de sécurité nécessaires, mettant ainsi leurs réseaux en danger.[17] Les agresseurs ont intensifié leurs activités de reconnaissance, afin d'identifier les solutions d'accès à distance vulnérables et de trouver les failles existantes ou les implémentations mal protégées de solutions *RDP (Remote Desktop Protocol)* et de serveurs *VPN (Virtual Private Network)* susceptibles de leur livrer accès aux réseaux des entreprises. Les attaques de phishing ont également tiré parti du chamboulement des habitudes de travail. Bien des utilisateurs utilisaient pour la première fois des logiciels de conférence ou collaboration et, faute d'avoir reçu jusque-là les messages émanant de telles plateformes, il leur était difficile de reconnaître les contrefaçons.[18] Voir aussi le chap. 6.1 consacré au télétravail.

17 https://blog.shodan.io/trends-in-internet-exposure/

18 https://www.darkreading.com/cloud/fake-microsoft-teams-emails-phish-for-credentials/d/d-id/1337717; https://abnormalsecurity.com/blog/abnormal-attack-stories-microsoft-teams-impersonation/; https://abnormalsecurity.com/blog/abnormal-attack-stores-zoom-phishing-campaign/

Recommandations :

L'utilisation pour le télétravail de l'infrastructure informatique privée, à commencer par les ordinateurs, facilite les cyberattaques, dans la mesure où les appareils privés sont souvent moins bien protégés que les infrastructures d'entreprise administrées par des professionnels. En outre, les collaborateurs effectuant du télétravail sont souvent livrés à eux-mêmes face aux attaques d'*ingénierie sociale*, faute de pouvoir en parler tout de suite à des collègues. Les campagnes de sensibilisation consistant à établir et faire connaître les procédures de notification aux responsables de la sécurité informatique de l'entreprise peuvent être utiles dans ce contexte.

Listes de contrôle de MELANI sur le télétravail :

Entreprises : https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/fernzugriff.html

Utilisateurs : https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/fernzugriff-enduser.html

3.6 Applications de traçage de proximité

De nombreux pays ont introduit des applications mobiles (*Proximity* ou *Contact Tracing App*), afin de pouvoir retracer la progression du coronavirus et adopter de façon ciblée les mesures de protection utiles. Cette nouvelle technologie permet de comprendre les chaînes d'infection potentielles et d'informer les personnes concernées des risques encourus. De tels moyens techniques contribuent de manière significative à freiner la propagation du virus, en signalant quand quelqu'un s'est exposé au risque d'infection. La personne sait ainsi qu'elle devrait se soumettre à un test et prendre des précautions contre toute propagation involontaire du virus.

Malgré l'impatience d'en finir avec la pandémie, tout le monde n'est pas prêt à révéler des données personnelles, à accepter des restrictions ou à se voir imposer des obligations. À peine les applications de traçage lancées, les critiques ont fusé dans divers pays au sujet de la protection insuffisante des données ou d'éventuelles failles de sécurité d'ordre conceptuel. Il est très difficile de concilier les divers intérêts pour trouver une solution acceptée par la population. Il s'agit d'une nouvelle technologie qui est encore appelée à mûrir, sur la base des expériences réalisées.

Précisions :

Dans le cadre du projet suisse de traçage de proximité en lien avec le COVID-19, le NCSC a institué un groupe de travail chargé d'étudier les questions relatives à la cybersécurité et à la protection de la sphère privée. Un test dit de sécurité publique a permis à d'autres spécialistes ou personnes intéressées d'éprouver la sécurité de l'ensemble du système. Le test public de sécurité est en place depuis le 28 mai 2020.

https://www.melani.admin.ch/melani/fr/home/public-security-test/infos.html

4 Événements / Situation

Aperçu des annonces reçues

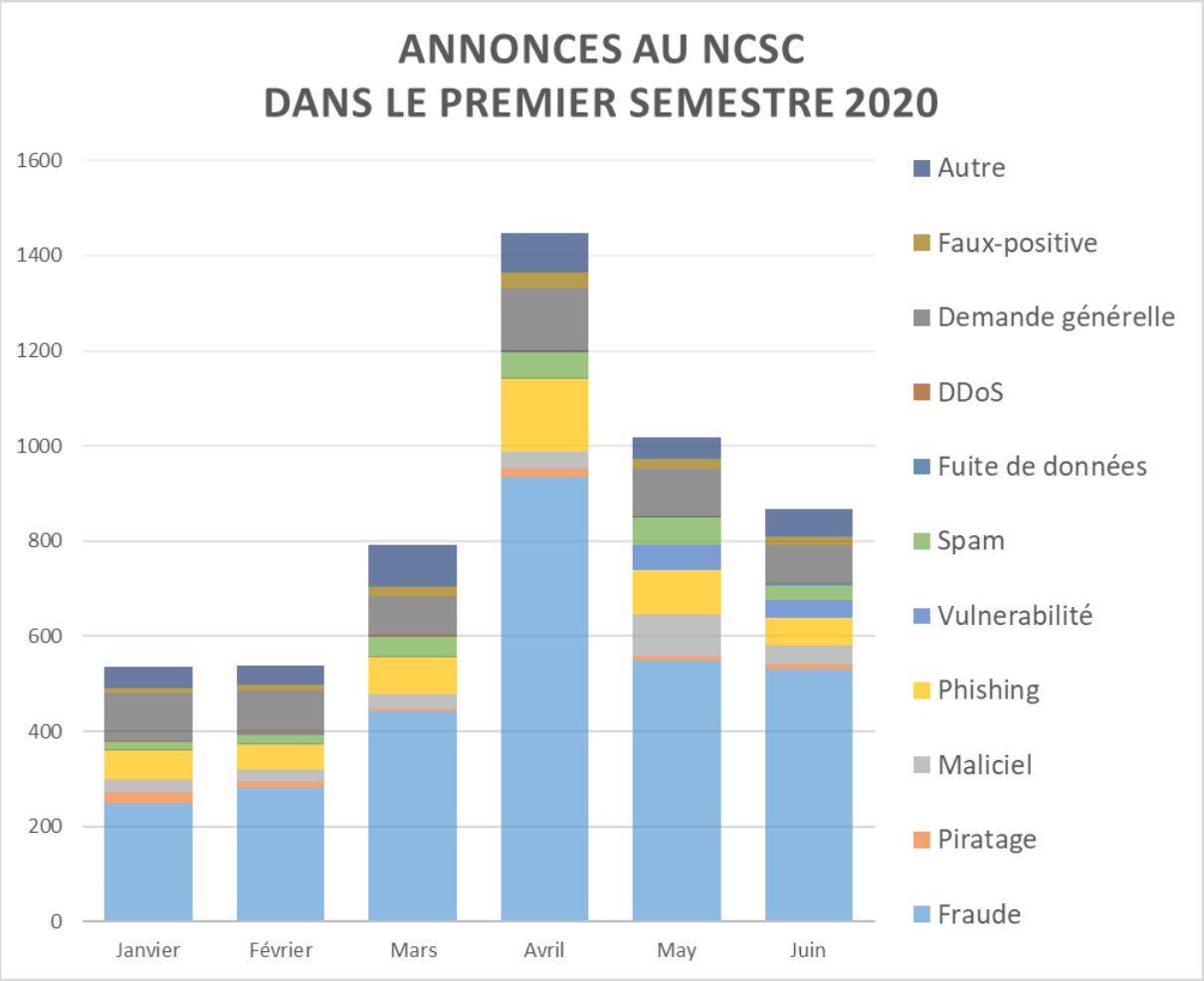

Fig. 2: Signalements effectués au NCSC au premier semestre 2020.

Au premier semestre 2020, le guichet unique suisse en matière de cyberrisques, qui fait partie du NCSC, a enregistré au total 5152 annonces. Les tentatives d'escroquerie représentaient, avec 2938 signalements, plus de la moitié des incidents. Quelque 825 cas de courriels de fraude à la commission figuraient dans cette catégorie.

Par ailleurs, 270 cas concernaient un abonnement abusif lié à un faux paquet. L'arnaque repose sur le piège à l'abonnement connu de longue date, où des offres prétendument gratuites se transforment, quelques jours plus tard, en abonnements payants. L'information figure à dessein en petits caractères. Les variantes mises en circulation durant l'été invitaient à s'acquitter d'une taxe modique afin de recevoir un prétendu paquet. Or là aussi, la victime contractait un abonnement à son insu. Il lui fallait indiquer les coordonnées de sa carte de crédit ou transmettre un code à un numéro court. Les escrocs se sont spécialisés dans cette nouvelle variante durant la crise du coronavirus, comme beaucoup de personnes avaient passé des commandes en ligne et attendaient un paquet (voir chap. 3.1).

De même, des courriels d'extorsion ont été envoyés à grande échelle. Il s'agissait principalement, dans 578 cas, de *fake sextortion*.[19] Le pirate prétend s'être introduit dans l'ordinateur de la victime et avoir eu accès à sa webcam, qui aurait réalisé des photos compromettantes. Ce n'est généralement que du bluff. Au premier semestre 2020, des tentatives de chantage ont également été observées contre des administrateurs Web. Les messages annonçaient le piratage de leurs sites et le pillage des bases des données leur étant associées. Les données volées allaient être publiées. Là encore, la menace était infondée (voir chap. 4.7.5). Les pirates n'ont pas craint d'échafauder des scénarios plus violents, comme le montrent dans deux cas les menaces d'attentat à la bombe envoyées par courriel à des entreprises, qui à nouveau se sont révélées être une imposture.

La bonne vieille arnaque au nom de domaine a connu un regain de popularité au premier semestre 2020, avec 63 annonces. Concrètement, un prétendu administrateur de noms de domaine communique au propriétaire d'un site Internet du domaine «.ch» qu'une autre société s'intéresse au même nom de domaine, mais avec l'extension générique «.com». Le propriétaire du site Internet aurait toutefois les moyens de l'en empêcher en achetant ledit nom de domaine «.com». De tels domaines sont proposés à un prix prohibitif, sans qu'on ait d'ailleurs la certitude qu'ils seront dûment enregistrés.

Des entreprises ont signalé dans 94 cas une arnaque au président (*CEO fraud*). Les escrocs commencent par collecter, en général sur le site de la société prise pour cible, les adresses électroniques et les fonctions de ses collaborateurs. Forts de ces informations, ils inventent une histoire sur mesure. Les filous prient la comptabilité ou le service financier, au nom du chef de l'entreprise, de procéder en son nom à un paiement urgent.

Des incidents liés à des maliciels ont été rapportés à 232 reprises. En particulier, 42 cas signalés impliquaient des rançongiciels (ransomware). Ce nombre a beau être faible par rapport aux autres tentatives d'escroquerie, les dommages potentiels n'en restent pas moins beaucoup plus élevés (voir chap. 4.1.1).

4.1 Maliciels : aperçu actuel

La statistique ci-après montre les principaux maliciels (malware) s'attaquant aux internautes suisses. Les statistiques, qui proviennent de sources diverses, ont été agrégées et filtrées pour tout l'espace IP suisse connu du NCSC. Les détails techniques sont mis à la disposition des fournisseurs de services Internet suisses, afin qu'ils puissent informer les clients ayant subi une infection et leur recommander les mesures utiles. Les différentes familles de maliciels sont parfois difficiles à distinguer, faute de tout schéma international de nommage. Il importe encore de se souvenir que ces chiffres ne représentent que la pointe de l'iceberg, dès lors que la base de données ne renferme que les données de quelques serveurs de commande et de contrôle.

[19] https://www.melani.admin.ch/melani/fr/home/meldeformular/formular0/meldeformularhaeufigefragen/Fake-Sextortion.html

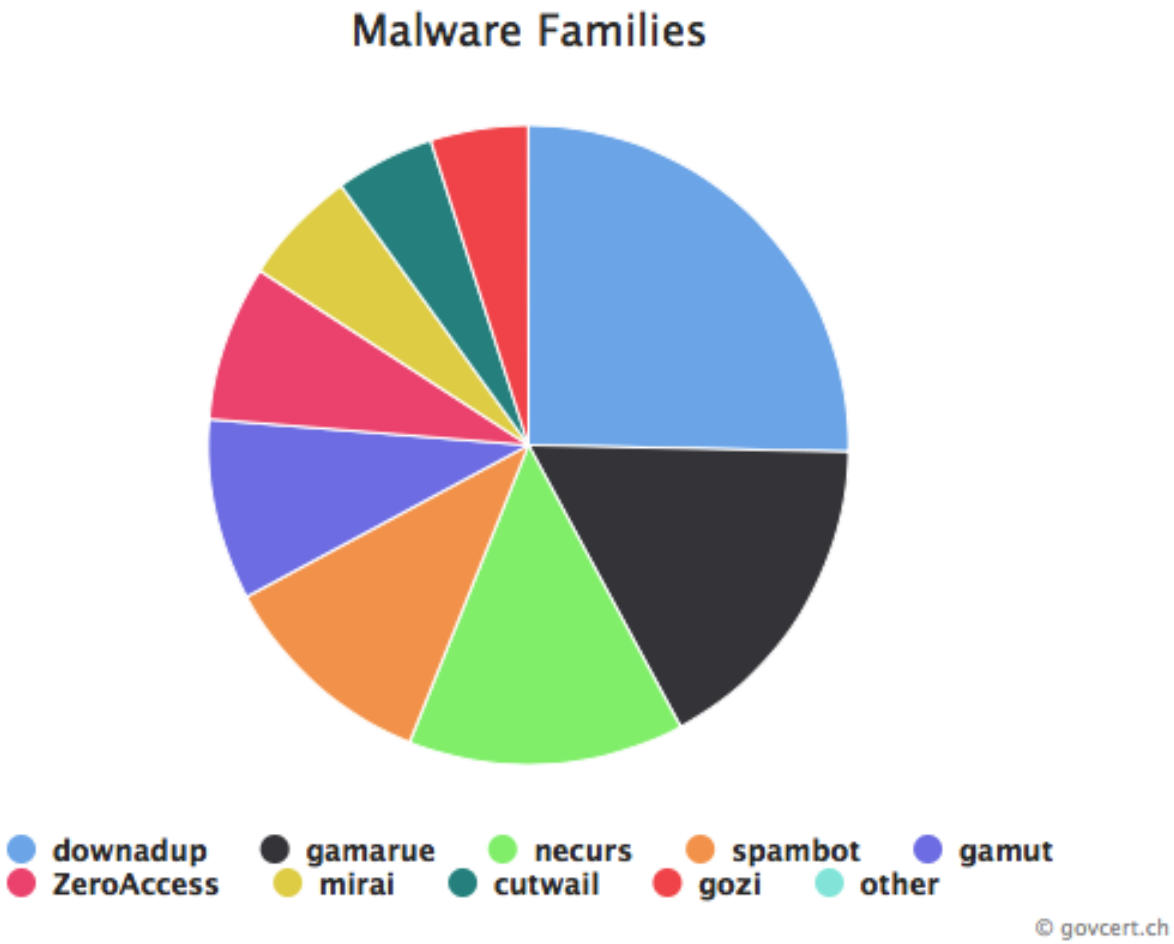

Fig. 3: Répartition des maliciels en Suisse selon les informations en possession du NCSC (état au 30 juin 2020). Des données actuelles sont publiées sous le lien: https://www.govcert.admin.ch/statistics/malware/.

4.1.1 Rançongiciels: derniers développements

MELANI s'intéresse depuis plusieurs années au phénomène des rançongiciels.[20] Cette menace toujours croissante a quadruplé en 2019, selon les statistiques de la société Trustwave,[21] pour se hisser au premier rang des incidents de cybersécurité les plus fréquents. Outre le nombre d'infections dues à un rançongiciel, les vecteurs d'attaque ainsi que les services vendus clés en main pour qu'un criminel puisse lancer une attaque et se faire verser la rançon demandée (*Ransomware as a Service*, *RaaS*) sont toujours plus nombreux. Selon un rapport de la société Coveware,[22] qui a pour mission d'endiguer les attaques dues aux rançongiciels, les demandes de rançon formulées au premier trimestre 2020 ont bondi de 33 % par rapport aux derniers mois de l'année passée.

---

20 Voir les rapports semestriels MELANI 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, 4.6.4 et 5.4.3; 2016/2, chap. 4.6.3 et 6.1; 2017/1, chap. 3; 2017/2, chap. 5.4.2; 2018/2, chap. 4.5.4 et 5.3.5; 2019/2, chap. 4.6.1.

21 https://www.zdnet.com/article/Ransomware-is-now-the-biggest-online-menace-you-need-to-worry-about/

22 https://www.coveware.com/blog/q1-2020-Ransomware-marketplace-report

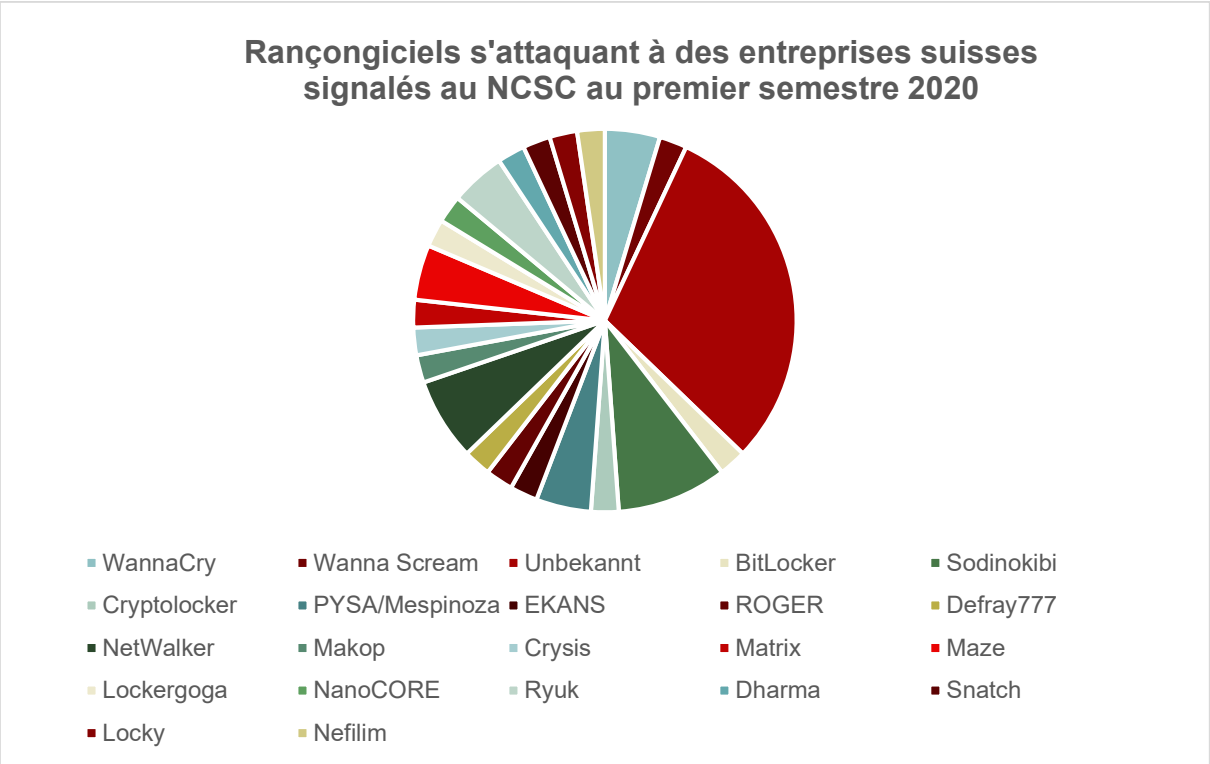

Fig. 4: Rançongiciels s'attaquant à des entreprises suisses annoncés au NCSC au premier semestre 2020.

Durant la période sous revue, des sociétés suisses ont également été victimes de rançongiciels. Au total, 42 cas d'attaques lancées contre des entreprises ont été signalés au NCSC. Les annonces ne précisaient hélas pas toujours le maliciel utilisé. Comme l'indique la figure 4, toutes sortes d'attaques par rançongiciel ont été annoncées durant la période sous revue. Bien que la majorité des cas signalés au NCSC concerne des PME, les grandes entreprises n'ont pas été épargnées. L'attaque lancée en janvier contre le géant français Bouygues Construction a fait grand bruit: la production a dû être interrompue dans toutes les filiales du groupe – en Suisse aussi – pour réparer les dégâts causés par le maliciel «Maze».[23] Au début du mois de mai, le constructeur de trains Stadler Rail subissait l'attaque d'un rançongiciel. L'agresseur menaçait de divulguer les données dérobées si la rançon de 5,8 millions de francs n'était pas payée.[24] Pour augmenter la probabilité d'un tel versement, les criminels fixent la somme réclamée en fonction des possibilités financières dont disposent selon eux leurs victimes. Les particuliers doivent ainsi s'acquitter de montants modiques – souvent inférieurs à 1000 francs. Les sommes réclamées varient aussi fortement d'une campagne à l'autre. «Ryuk», connu pour son âpreté au gain, a par exemple exigé d'une PME une rançon de 300 000 francs, tandis que «WannaCry» demandait à une entreprise comparable de s'acquitter de 1500 francs seulement – il est vrai qu'une partie seulement des données ont été dûment déchiffrées après le paiement de la rançon.

23 https://www.itnews.com.au/news/bouygues-construction-it-taken-out-by-Ransomware-537516

24 https://www.srf.ch/news/cyberAngriff-auf-stadler-rail-solange-es-etwas-zu-holen-gibt-wird-schindluder-getrieben; https://www.swissinfo.ch/eng/cyberattack-_hackers-demand-millions-in-ransom-for-stolen-stadler-rail-documents/45794036

Évolution du mode opératoire

Dès novembre 2019, un groupe utilisant le rançongiciel «Maze» avait adapté son modèle d'affaires : avant de chiffrer les données de sa victime, il commençait par les télécharger pour pouvoir lui extorquer de l'argent en la menaçant de les publier sur un blog créé à cet effet, au cas où le chantage basé sur le chiffrement des données n'aurait pas l'effet escompté. Cette manière de procéder est prometteuse, car en plus de voir sa réputation écornée et ses secrets d'affaires publiés, la victime s'expose à des conséquences juridiques liées au traitement des données personnelles. En outre, les données publiées peuvent servir au lancement de nouvelles attaques. Au premier semestre 2020, le nombre de groupes utilisant cette stratégie a fortement augmenté. En dehors de «Maze», la société de cybersécurité Coveware a découvert que six autres familles de rançongiciels combinent leurs attaques à la publication de données : «Sodinokibi/REvil», «DoppelPaymer» (successeur de «BitPaymer»), «Mespinoza/PYSA», «NetWalker», «CLoP» et «Nephilim»[25] (et sa nouvelle version Nemty).[26, 27] Tous ces maliciels sévissent également en Suisse, même si les infections signalées à MELANI n'ont pas toujours entraîné de fuite de données. Une attaque par rançongiciel s'inscrivant dans une des campagnes précitées peut aller de pair avec un vol de données. Les opérateurs de «Maze» prétendent avoir sévi en Suisse non seulement contre Stadler Rail, en verrouillant ses systèmes et en lui dérobant des données, mais aussi contre l'assurance Chubb, qui n'a toutefois pas confirmé l'infection.[28]

Dans son dernier rapport semestriel,[29] MELANI prédisait que les cybercriminels allaient trouver d'autres moyens de tirer profit des données dérobées (en fonction de leur valeur), par exemple en ne se servant pas seulement des données pour faire pression. Tout récemment, les cybercriminels ayant diffusé le rançongiciel «Sodinokibi/REvil» ont vendu aux enchères les données subtilisées, comme les victimes avaient refusé de payer la rançon demandée pour leur déchiffrement.[30] D'autres groupes vont jusqu'à exiger le versement d'une double rançon, d'abord pour récupérer les documents chiffrés, puis pour obtenir la destruction définitive des données volées.[31] Les sommes réclamées varient selon la victime et la campagne, pour exploser littéralement dans quelques cas. Pour ne prendre qu'un exemple, «Sodinokibi/REvil» a réclamé en juillet à Grubman Shire Meiselas & Sacks, cabinet d'avocats des stars, une rançon de 42 millions de dollars pour éviter que les données dérobées ne soient publiées et pour obtenir le code nécessaire à leur déchiffrement. Comme la victime refusait de payer quoi que ce soit, les maîtres chanteurs ont commencé à écouler aux enchères quantité de documents se rapportant à des personnalités du secteur du divertissement, les prix de départ se situant entre

---

25 https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/investigation-into-a-nefilim-attack-shows-signs-of-lateral-movement-possible-data-exfiltration/

26 Autre confirmation de la popularité croissante de ce schéma parmi les cybercriminels, un rançongiciel a créé une plateforme hébergeant les données dérobées avant que la fuite de données n'ait été rendue publique. Il s'agit de «Sekhmet». Voir aussi: https://www.bleepingcomputer.com/news/security/three-more-Ransomware-families-create-sites-to-leak-stolen-data/.

27 Il faudrait encore citer le rançongiciel «RagnarLocker» (également appelé «Ragnarok»), qui n'a pas encore été repéré en Suisse: https://www.securityweek.com/ragnar-locker-Ransomware-uses-virtual-machines-evasion

28 https://www.bankinfosecurity.com/insurer-chubb-investigating-security-incident-a-14023

29 Voir MELANI, Rapport semestriel 2019/2, chap. 4.6.1.

30 https://www.bleepingcomputer.com/news/security/revil-Ransomware-creates-ebay-like-auction-site-for-stolen-data/

31 https://krebsonsecurity.com/2020/06/revil-Ransomware-gang-starts-auctioning-victim-data/

600 000 dollars et un million.[32] La revente sur les forums criminels de données dérobées a beau ne pas être un phénomène nouveau, leur publication et en général leur utilisation comme moyen de pression constituent une nouvelle variante pouvant inciter davantage de victimes à céder aux demandes de rançon. Voir aussi le chap. 4.5 sur les fuites de données.

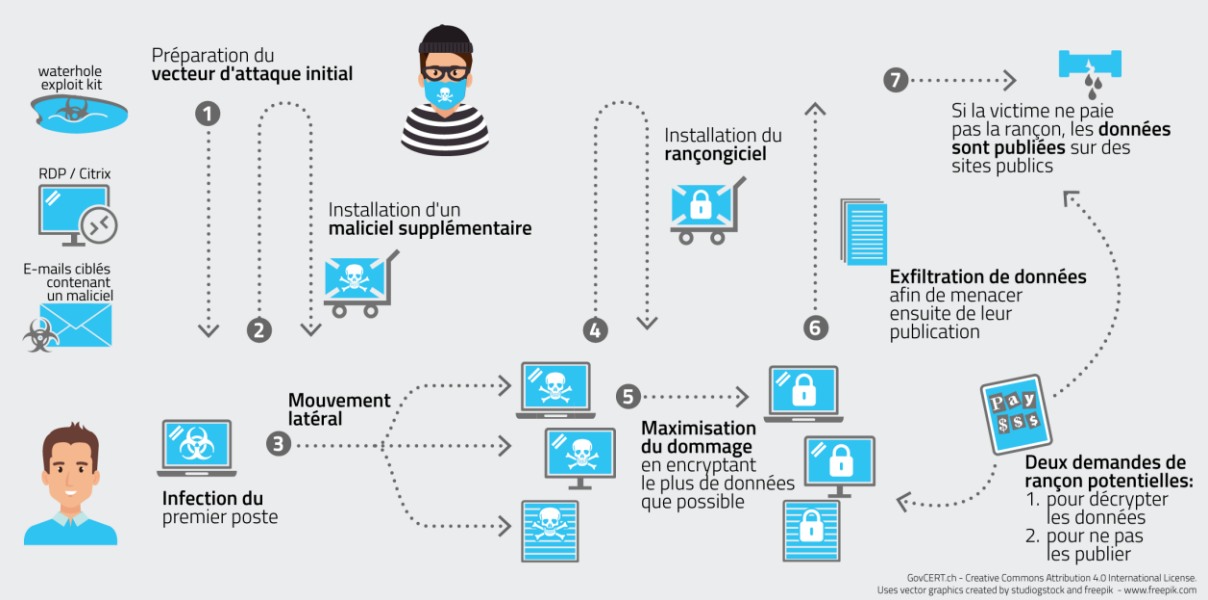

Fig. 5: Mode opératoire actuel des rançongiciels.

La possibilité de réaliser des bénéfices colossaux ainsi que la complexité des attaques en plusieurs étapes ont favorisé l'essor des modèles de collaboration entre différents groupes, ainsi qu'entre les membres d'un groupe et des indépendants. Selon FireEye par exemple, le rançongiciel «Maze» n'est pas utilisé par un seul groupe, mais plutôt par différents acteurs organisés en réseau de partenariat (*affiliate network*). Autrement dit, les développeurs de rançongiciels collaborent avec d'autres acteurs qui procèdent à la diffusion de leurs maliciels, établissent l'accès aux réseaux, prospectent les réseaux infectés ou se chargent d'autres aspects spécifiques. Ces acteurs sont engagés en tant qu'employés, ou alors ils reçoivent une commission dès que la victime a payé la rançon.[33]

Au départ, «Maze» était surtout diffusé à l'aide de courriels infectés; au premier semestre 2020, ce rançongiciel a toujours plus sévi dans le cadre d'attaques structurées, tirant parti d'une infection préalable due à un autre maliciel pour dérober des données en s'infiltrant dans l'ensemble du réseau de la victime, avant de verrouiller ses données. Le spécialiste de la sécurité FireEye a constaté des différences frappantes dans le déroulement des attaques, au niveau par exemple du laps de temps écoulé entre l'infection initiale et l'emploi du rançongiciel, ou du vecteur d'intrusion utilisé (ports RDP ouverts, services accessibles par Internet ou mal configurés, services possédant un mot de passe faible ou dont les données d'accès ont été dérobées et revendues sur le Darkweb, etc.). D'autres différences concernent encore

32 https://www.scmagazine.com/home/security-news/cybercrime/lebron-james-among-the-1st-stars-to-have-their-stolen-law-firm-files-put-up-for-auction/

33 https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-Ransomware-incidents.html

les stratégies déployées pour assurer la persistance du maliciel dans le réseau, ou pour favoriser les interactions avec les systèmes de la victime aux diverses phases de l'exploration et de la propagation dans le réseau (*lateral movement*). Cette diversité est un indice supplémentaire de la participation de plusieurs acteurs. Les opérateurs de «Maze» ont d'ailleurs publié sur leur site Web des données dérobées à un bureau d'architecture par les exploitants de «LockBit». Et un membre du groupe «Maze» a indiqué que des relations professionnelles seraient nouées sous peu avec un troisième groupe.[34]

«Maze» n'est pas le seul rançongiciel dont les opérateurs ont pour stratégie d'unir leurs efforts. Les opérateurs de «NetWalker» tissent aussi, depuis mars 2020, des réseaux de partenariat destinés à propager leur rançongiciel, lors de réunions organisées dans le cadre d'un blog clandestin. Pour recruter des partenaires, ils leur promettent des indemnités colossales, à hauteur de 70 % de la rançon versée; soit des revenus en perspective de 487 000 dollars, voire d'un million. «NetWalker» dispose également de sa propre plateforme pour la publication des données dérobées. Ses partenaires sont libres d'y publier, pour optimiser les bénéfices de leurs attaques, des informations sur les victimes infectées.[35]

Développements techniques

Le dernier rapport semestriel[36] signalait déjà que dans bien des cas, une infection par rançongiciel n'exige aucune interaction des utilisateurs. Outre d'autres avantages, comme la possibilité de se servir du même maliciel auprès de nombreuses victimes, ce facteur aide à comprendre l'essor des rançongiciels. Les ports *RDP* mal protégés,[37] dont les droits d'accès s'achètent à vil prix sur le marché noir, ont été l'un des vecteurs d'attaque préférés des campagnes déployées entre janvier et juin 2020 contre les réseaux d'entreprise. Les serveurs mal sécurisés servent également de porte d'accès à l'infrastructure informatique. «Sodinokibi/REvil», qui s'était déjà engouffré dans les failles de sécurité des serveurs *VPN* de Pulse Secure, a été au premier semestre 2020 le premier rançongiciel à s'installer dans un réseau d'entreprise en exploitant la vulnérabilité Citrix «CVE-2019-19781» (voir chap. 4.4). Deux autres rançongiciels, «Maze» et «RagnarLocker», ont tiré parti de la même faille durant la période sous revue.[38] Il n'est pas exclu qu'en Suisse aussi, des serveurs VPN de Pulse Secure ou des serveurs Citrix vulnérables soient à l'origine d'infections informatiques.

Le NCSC a constaté ces derniers mois une recrudescence des attaques contre les ports *RDP* (*Remote Desktop Protocol*), prélude à d'autres attaques ciblées menées avec des rançongiciels. Les ports *RDP* font l'objet de nombreuses analyses où les escrocs testent les mots de passe faibles (attaques par dictionnaire ou par force brute). Une autre tactique d'intrusion repose sur les serveurs non mis à jour et donc vulnérables. Le NCSC a encore relevé que d'autres protocoles d'accès à distance étaient exposés aux cyberattaques, à l'instar du VPN de Pulse Secure, ou que les vulnérabilités du système Citrix NetScaler étaient recherchées et

---

34 https://www.scmagazine.com/home/security-news/Ransomware/new-Ransomware-trends-spotted-auctioning-stolen-files-cybergangs-joining-forces/

35 https://www.bleepingcomputer.com/news/security/Ransomware-recruits-affiliates-with-huge-payouts-automated-leaks/

36 Voir MELANI, rapport semestriel 2019/2, chap. 4.6.1.

37 Le FBI a lui aussi incriminé, à la conférence RSA de février 2020 sur la cybersécurité, les ports RDP ayant servi de vecteur d'attaque dans 70 à 80 % des incidents dus à un rançongiciel: https://www.bleepingcomputer.com/news/security/Ransomwares-big-jump-ransoms-grew-14-times-in-one-year/

38 https://www.zdnet.com/article/hackers-target-unpatched-citrix-servers-to-deploy-Ransomware/

utilisées comme vecteur initial d'attaque, par exemple par REvil. Selon le NCSC, de telles données d'accès s'échangent au sein de forums spécialisés, qui permettent à divers groupes de cyberpirates d'accéder aux réseaux de leurs victimes.

Recommandations :

Les mesures suivantes devraient être mises en place :

- Protéger tous les accès à distance (RDP, Citrix, VPN) par une procédure d'authentification à deux facteurs.
- Il est en outre possible d'utiliser un autre port que celui activé par défaut, plus difficile à identifier (important : cela n'est pas en soi une mesure de sécurité suffisante).
- Adoption et mise en œuvre d'une directive excluant l'emploi de mots de passe simples
- Dans la mesure du possible, seules les adresses IP uniques ou des adresses IP spécifiques devraient être admises, ou alors les adresses IP situées en Suisse.
- Analyse des tentatives d'accès fructueuses ou non dans les fichiers de logs .

Quelques attaques par des rançongiciels observées durant le semestre sous revue ont tiré parti de techniques novatrices, afin de contourner les mesures de sécurité et d'explorer d'autant plus longtemps le réseau de leur victime. «RagnarLocker» par exemple a installé sa propre machine virtuelle (*virtual machine*, VM) Windows XP de 280 Mo, afin de ne pas être dérangé par les programmes de surveillance de l'ordinateur hôte durant ses investigations. Tous les lecteurs de l'ordinateur attaqué ont été partagés et rendus accessibles à l'intérieur de la VM, qui a pu ensuite les chiffrer à l'aide de son rançongiciel.[39] «NetWalker» par contre a repris une technique déjà utilisée par d'autres types de maliciels, l'injection DLL (*reflective DLL injection*). Elle consiste à charger une bibliothèque de liens dynamiques (*dynamic-link library*, fichier avec l'extension .dll) dont le code d'exécution destiné au maliciel ne se trouve que dans la mémoire de travail. Autrement dit, les instruments de surveillance qui n'analysent que le disque dur ne détectent pas le code binaire du rançongiciel.[40] «NetWalker» bloque par ailleurs les processus des programmes de sécurité.

Développements au niveau des cibles

Les attaques de rançongiciels lancées contre les systèmes de contrôle industriels sont devenues un sujet d'inquiétude au niveau mondial. Ce phénomène fait l'objet d'un chapitre spécial du présent rapport semestriel de MELANI (voir chap. 4.3.1).

Un autre développement observable depuis peu est lié à l'infection par «Maze» révélée le 18 avril par Cognizant, un des leaders mondiaux de l'infogérance (*managed service provider MSP*).[41] Cet incident est le dernier d'une longue série d'attaques menées au deuxième semestre 2019 contre des fournisseurs de services en technologies de l'information.[42] On a ainsi

39 https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/
40 https://blog.trendmicro.com/trendlabs-security-intelligence/netwalker-fileless-Ransomware-injected-via-reflective-loading/
41 https://www.bleepingcomputer.com/news/security/it-services-giant-cognizant-suffers-maze-Ransomware-cyber-attack/
42 https://www.zdnet.com/article/at-least-13-managed-service-providers-were-used-to-push-Ransomware-this-year/

affaire à une tendance de fond, comme le montre le rapport d'analyse des menaces de CrowdStrike paru en mars.[43] «Ryuk», qui compte notamment parmi ses victimes Data Resolution (décembre 2018), CloudJumper (mai 2019), CorVel (juillet 2019) et TSM Consulting (août 2019), se distingue parmi les rançongiciels spécialisés dans l'attaque des fournisseurs de service. En mars 2020, «Ryuk» a en outre infecté la société de technologie financière londonienne Finastra, qui fournit des logiciels et des services à plus de 8500 clients, dont 90 des 1000 plus grandes banques au monde. Pour stopper la propagation de l'infection, Finastra a rapidement désactivé une partie de ses serveurs, ce qui a provoqué une panne passagère pour les nombreux clients du service.[44] L'infection d'un MSP ou d'un fournisseur de services basés sur le cloud a le potentiel de causer d'énormes dégâts, en donnant accès aux pirates à toutes les entreprises dont ledit prestataire exploite l'infrastructure informatique. Par exemple, ils pourront se servir du logiciel de télésurveillance et de télégestion (*remote monitoring and management*, RMM). Cognizant s'est donc empressé d'informer sa clientèle et de lui fournir des indicateurs de compromission (*indicators of compromise*, IoC) pour qu'elle puisse le cas échéant détecter une infection dans son réseau interne.

Afin de ne pas attirer l'attention, certains agresseurs par rançongiciel ont pour principe d'utiliser comme porte d'entrée les programmes utilisés par les MSP, à l'instar des outils de partage de bureau et des logiciels de prise en main à distance. C'est ainsi qu'en avril, «RagnarLocker» s'en est pris au groupe Energias de Portugal (EDP), un des plus gros producteurs d'énergie d'Europe. Certains groupes de rançongiciels, comme «Sodinokibi/REvil», font l'inverse : après avoir attaqué divers petits MSP, dont PerCSoft (août 2019), Complete Technology Solutions (décembre 2019) et Synoptek (janvier 2020), le groupe s'intéresserait toujours plus depuis le début de 2020, selon Coveware, aux grandes entreprises dont le réseau VPN est vulnérable.

Recommandations :

Les mesures suivantes ont fait leurs preuves dans la protection des entreprises contre les attaques de rançongiciels : assurez-vous de l'exhaustivité de vos pratiques de sauvegarde informatique (backup). Vous aurez ainsi la certitude de pouvoir restaurer toutes vos données, en cas d'attaque par un rançongiciel. Testez au passage vos processus de sauvegarde. Documentez votre infrastructure informatique, installez les mises à jour logicielles dès leur parution et actualisez vos directives en matière de sécurité. Établissez des plans d'action pour la gestion des incidents, pour la communication ainsi que pour la gestion de la continuité des activités. Assurez-vous, au moyen d'exercices réguliers, de l'efficacité de ces plans d'action. Toute prévention efficace des cyberattaques comporte, à côté des mesures techniques, des activités régulières de sensibilisation du personnel. Il incombe aux organes dirigeants de chaque entreprise de surveiller la bonne mise en œuvre des mesures correspondantes, et cette tâche ne saurait être déléguée.

43 https://www.channelfutures.com/mssp-insider/msps-under-heavy-Ransomware-attack ; https://www.crowdstrike.com/press-releases/crowdstrike-global-threat-report-reveals-big-game-hunting-telecommunication-targeting-top-adversary-trends/

44 https://www.bloomberg.com/news/articles/2020-04-08/how-finastra-survived-a-Ransomware-attack-without-paying-ransom

Aucune entreprise ne peut avoir la certitude de déjouer à coup sûr toutes les cyberattaques. Il vous faut par conséquent prévoir des capacités de réaction et de restauration de vos systèmes, afin de limiter les dégâts d'un éventuel incident.

INFO

Au deuxième semestre 2019, MELANI a publié des mesures de protection actualisées contre le nouveau mode opératoire d'attaque par rançongiciel:

https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/update-ransomware-neue-vorgehensweise.html

4.1.2 Regain d'activité de «Gozi»

Le cheval de Troie bancaire «Gozi»,[45] qui sévit depuis plus de dix ans en Suisse, s'était fait plus discret ces dernières années.

En mars 2020, il est apparu que «Gozi» était distribué au moyen de courriels se référant à la correspondance électronique antérieure de la victime (*thread hijacking*). D'autres chevaux de Troie bancaires, dont «Emotet», avaient déjà utilisé cette méthode. Le courriel renfermait un mot de passe servant à ouvrir un fichier .zip qui n'était toutefois pas enregistré en annexe, mais dans Google Drive. Une prétendue présentation s'y trouvait. En réalité, il s'agissait d'un fichier Javascript, qui téléchargeait et exécutait «Gozi». Au mois d'avril, «Gozi» a été envoyé en annexe d'un fichier .xls infecté. Les courriels, rédigés en italien, se référaient à une facture.

Le maliciel «Gozi» et ses variantes sont proposés sur des plateformes illégales de vente en ligne, et donc à la portée de tous les cybercriminels. Leur diffusion s'est faite de multiples manières au fil des ans, notamment sur les sites compromis de quotidiens en ligne ou par le biais de logiciels manipulés, vantés dans de petites annonces accrocheuses. Outre les systèmes de e-banking, «Gozi» prend pour cibles les logiciels de paiements électroniques et les portefeuilles de cryptomonnaies.[46]

4.1.3 Module d'«Emotet» jusque-là dissimulé

Au début de 2020, des experts en sécurité de Binary Defense ont découvert un module pour réseau local sans fil (Wi-Fi ou *Wireless Local Area Network*, WLAN) dans le maliciel «Emotet»[47]. Cette fonction peu étudiée lui sert à s'enquérir des divers réseaux Wi-Fi auxquels la victime est connectée. «Emotet» tente alors d'accéder à tous ces réseaux, à l'aide d'une liste de mots de passe préétablie. Si un réseau Wi-Fi n'est pas protégé ou alors par un mot de passe figurant dans la liste prédéfinie, «Emotet» pourra s'y glisser. À partir de la première victime, le maliciel tentera d'infecter les autres ordinateurs du réseau où il vient de pénétrer, afin de s'y déployer partout.

---

45 Billets du GovCERT concernant Gozi: https://www.govcert.admin.ch/blog/18/gozi-isfb-when-a-bug-really-is-a-feature; https://www.govcert.ch/blog/when-gozi-lost-its-head/ (tous deux en anglais).

46 Voir MELANI, rapport semestriel 2018/1, chap. 4.7.3.

47 https://www.binarydefense.com/emotet-evolves-with-new-wi-fi-spreader/

Selon les premiers résultats, le module existerait depuis 2018. Mais comme les analyses de maliciels s'effectuent en général sur des machines virtuelles sans Wi-Fi, les chercheurs ne se sont doutés de rien pendant longtemps. Cette découverte montre que les pirates sont constamment à l'affût de nouveaux moyens de diffuser leurs maliciels, et qu'ils ne manquent pas d'imagination pour arriver à leurs fins.

«Emotet» sert souvent de porte d'entrée à des attaques menées par d'autres maliciels, à l'instar des chevaux de Troie chiffrant les données (rançongiciels)[48].

Conclusion :

La diffusion des maliciels s'apparente à un jeu du chat et de la souris entre les agresseurs et les défenseurs. Quand une méthode s'essouffle, les concepteurs de maliciels développent de nouvelles variantes d'infection ou en reviennent à une ancienne méthode à laquelle les experts font moins attention. Première composante permettant de relier des appareils informatiques à Internet, le Wi-Fi est un vecteur d'attaque de portée locale, qui n'est donc pas extensible comme les attaques par courriel ou dans le Web. On aurait toutefois tort de sous-estimer le réseau Wi-Fi comme vecteur d'attaque.

Vous trouverez sur notre site Web des recommandations sur la sécurité du réseau sans fil (Wi-Fi / WLAN) :

https://www.melani.admin.ch/melani/fr/home/schuetzen/sekundaere-grundschutz.html

4.2 Attaques de sites ou de services Web

4.2.1 Supercalculateurs (HPC)

À la mi-mai 2020, l'EGI-CSIRT, soit l'équipe de sécurité de l'European Grid Infrastructure (consortium d'universités dotées de centres de calcul de haute performance) a rendu publique une attaque ayant affecté plusieurs de ses membres.[49] Les centres de calcul de haute performance (*High-performance Computing*, HPC) sont un instrument très précieux pour la résolution de calculs complexes, à l'instar de la modélisation aérodynamique ou actuellement des modèles de propagation du COVID-19. Or cette même puissance de calcul peut aussi servir à miner des cryptomonnaies (*crypto mining*) ou à déchiffrer des données. Les centres offrent par ailleurs une bande passante conséquente. Les HPC sont dès lors des cibles très convoitées. Le rapport publié par l'EGI-CSIRT a permis à de nombreux centres de calcul à travers le monde, dont plusieurs en Suisse,[50] de déceler des accès indus à leurs systèmes et d'expulser leurs visiteurs indésirables. L'objectif des agresseurs n'est pas connu à ce jour.

---

48 Voir rapports semestriels MELANI 2019/1, chap. 3.4.1 et 2019/2, chap. 4.6.1.

49 https://csirt.egi.eu/academic-data-centers-abused-for-crypto-currency-mining/

50 https://www.rts.ch/info/suisse/11329094-soupcons-de-hacking-du-plus-gros-superordinateur-de-suisse-.html; https://www.tagesanzeiger.ch/eth-supercomputer-gehackt-370887112689

4.2.2 Attaques DDoS: mise à jour

Les attaques par déni de service distribué (*Distributed Denial of Service*, DDoS), qui réussissent à paralyser un système informatique afin de rançonner l'organisation ciblée ou de la léser gravement en rendant ses services web indisponibles, ont globalement diminué en nombre au cours des dernières années. Cette évolution est due à l'engagement des acteurs de la lutte contre les attaques DDoS. Le prestataire de sécurité Link11 est ainsi parvenu à déjouer au premier trimestre 2020 une attaque de 406 Gbit/s, tandis que Cloudflare subissait, lors d'une attaque DDoS, des pics de plus de 550 Gbit/s.[51]

Comme l'ont constaté ces deux services, de telles attaques ont gagné en complexité et en volume par rapport à l'année dernière. Au premier trimestre 2020, Link11 a recensé 51 attaques d'un volume supérieur à 50 Gbit/s, alors que la largeur de bande moyenne avoisinait 5,0 Gbit/s (soit 0,7 Gbit/s de plus qu'au même trimestre de l'année précédente).[52] Cloudflare signale une recrudescence des petites attaques de courte durée, dont 92 % n'atteignent même pas 10 Gbit/s. En outre, 79 % des attaques ont duré 30 à 60 minutes. Concrètement, les brèves attaques ont bondi de 19 % depuis le deuxième semestre 2019.[53]

Les attaques DDoS recensées par Cloudflare ont visiblement redoublé depuis mars surtout, en parallèle à la pandémie de COVID-19. D'autres entreprises de sécurité informatique l'ont confirmé, telle Netscout qui signale ne jamais avoir enregistré autant d'attaques DDoS en 31 jours qu'entre le 11 mars et le 11 avril 2020 (plus de 864 000).[54] Les cybercriminels devaient s'imaginer que leurs attaques seraient plus fructueuses, en raison du transfert d'activités quotidiennes telles que le travail et l'école vers des solutions en ligne (télétravail, enseignement à distance), avec à la clé une dépendance accrue de la connectivité et de l'accès aux ressources. Dans divers États, la politique de distanciation sociale a renforcé le degré de dépendance de l'économie à l'égard des réseaux, tandis que l'audience de certains canaux d'information en ligne explosait. Ce constat vaut par exemple pour les sites Internet des services gouvernementaux responsables de la santé publique. De nombreux citoyens désireux d'en savoir plus sur le coronavirus les ont consultés au quotidien. À ce propos, le site Internet du ministère américain de la santé a subi à la mi-mars une attaque DDoS, qui n'a toutefois pas ralenti significativement les systèmes de cette autorité gouvernementale.[55] Ce genre d'attaque peut être déclenché très vite et à un faible coût, grâce aux fournisseurs de *DDoS-as-a-Service*. Le NCSC n'a cependant pas constaté d'augmentation significative des attaques DDoS en Suisse pendant la situation extraordinaire. De façon générale, quelques vagues d'attaques non spécifiques ont été observées en Suisse au premier semestre 2020, le plus souvent sans demande de rançon. Cela signifie que les acteurs ont seulement voulu tester l'infrastructure concernée ou trouver des vulnérabilités.

Deux des plus puissantes attaques du genre jamais enregistrées se sont intercalées entre les multiples attaques de faible ampleur et de courte durée. La première, survenue à la mi-février et atténuée par le service de protection d'Amazon (AWS Shield), a duré trois jours et atteint

---

51 https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/

52 https://www.helpnetsecurity.com/2020/04/20/ddos-attacks-increasing/

53 https://blog.cloudflare.com/network-layer-ddos-attack-trends-for-q1-2020/

54 https://www.netscout.com/blog/asert/measuring-cruellest-month

55 https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response

un pic de trafic de 2,3 Tbit/s. L'opération visait un client spécifique, qu'Amazon n'a pas voulu nommer.[56] La seconde, lancée fin juin contre une banque européenne, s'est distinguée moins par sa bande passante (tout juste 418 Gbit/s) que par son flux de paquets de données à la seconde, le plus intense jamais enregistré : 809 millions p/s.[57] Avant cette cyberattaque atténuée par le fournisseur de solutions d'infrastructure Akamai, la plus redoutable attaque DDoS du genre jamais lancée s'élevait à 580 millions de paquets par seconde.[58] Les deux attaques survenues au premier semestre 2020 constituent de fait les plus graves incidents DDoS jamais enregistrés. Il est difficile de dire laquelle fut la plus massive, les agresseurs ayant utilisé des méthodes différentes pour atteindre leur objectif: bits par seconde (bit/s) dans le premier cas, paquets par seconde (p/s) dans le second. Les attaques présentant un débit élevé en bits/s visent à assécher le pipeline Internet, alors que celles affichant un nombre élevé de p/s cherchent à atteindre les dispositifs du réseau ou des applications situées dans des centres de données ou dans le cloud.[59] L'attaque de février affichait un volume de paquets de 293 millions p/s, soit bien moins que celle de juin. Une troisième attaque, enregistrée entre le 18 et le 21 juin, a atteint 754 millions de paquets par seconde. Menée durant quatre jours, elle provenait de plus de 316 000 adresses IP, qui toutes cherchaient à contacter la même adresse Cloudflare.[60]

Recommandations :

Toute entreprise tributaire de ses systèmes informatiques devrait s'assurer en priorité de la sécurité des canaux correspondants. Passez en revue les services importants au point qu'une panne affecterait gravement votre organisation. N'oubliez pas vos systèmes de base, sans lesquels vos applications professionnelles critiques ne fonctionneraient pas. Élaborez une stratégie contre les attaques DDoS. Il vous faut connaître les services internes ou externes compétents, ainsi que les autres personnes habilitées à agir en cas de cyberattaque. Idéalement, toute entreprise aura réfléchi à la problématique des attaques DDoS, dans la gestion générale des risques menée au niveau de sa direction, avant d'avoir subi une telle mésaventure et de façon à atteindre un niveau de préparation suffisant. Aucune organisation n'est à l'abri d'une attaque DDoS. Parlez à votre fournisseur Internet de vos besoins et des mesures préventives indiquées.

DOCU

Liste de contrôle des mesures à prendre contre les attaques DDoS :

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

4.3 Systèmes de contrôle industriels (ICS)

La numérisation et la mise en réseau croissantes dans le domaine de l'approvisionnement de base conduisent certes à une gestion plus rationnelle des prestations, comme la fourniture du courant ou de l'eau, mais comportent aussi des risques de vulnérabilité et donc de fiabilité.

56 https://www.zdnet.com/article/aws-said-it-mitigated-a-2-3-tbps-ddos-attack-the-largest-ever/
57 https://blogs.akamai.com/2020/06/largest-ever-recorded-packet-per-secondbased-ddos-attack-mitigated-by-akamai.html
58 https://www.imperva.com/blog/this-ddos-attack-unleashed-the-most-packets-per-second-ever-heres-why-thats-important/
59 https://www.bleepingcomputer.com/news/security/european-bank-suffers-biggest-pps-ddos-attack-new-botnet-suspected/
60 https://blog.cloudflare.com/mitigating-a-754-million-pps-ddos-attack-automatically/

Alors que de tels systèmes avaient traditionnellement un ancrage local ou régional et possédaient leurs propres réseaux physiques, leur pilotage s'effectue toujours plus souvent à distance, par Internet. Idéalement, leurs éléments de commande ne devraient pas être directement accessibles par Internet, et une série de mesures de protection devraient les mettre à l'abri des accès non autorisés.

4.3.1 Intérêt des rançongiciels pour les systèmes de contrôle industriels

Comme l'explique le chapitre 4.1.1, le nombre d'attaques avec des rançongiciels a continué d'augmenter sur le plan mondial durant le premier semestre 2020. Jusque-là, les attaques lancées par des rançongiciels visaient l'infrastructure informatique des victimes et les systèmes de contrôle ne subissaient, le cas échéant, que des dommages collatéraux. Un rançongiciel observé au premier semestre a toutefois été spécialement conçu pour s'attaquer au pilotage des processus. Il s'agit d'«EKANS», qui sévit depuis décembre 2019 mais ne s'est fait connaître qu'en début d'année.[61] Il dispose de fonctions spécifiques pour attaquer les processus liés aux SCI. «EKANS» lance des attaques ciblées et vérifie, une fois dans le réseau, si les domaines internes et les adresses IP correspondent à ses critères. Avant de chiffrer les fichiers, le rançongiciel dérobe des données et ordonne à toute une série de processus de s'arrêter, sans toutefois les manipuler ni envoyer de commandes. Outre les SCI, ces processus se rapportent aux logiciels de sécurité ou de gestion, aux bases de données et aux solutions de sauvegarde des données. Le fournisseur de services de sécurité Dragos, qui a publié un rapport détaillé sur cette menace, cite parmi les produits SCI attaqués le logiciel «Proficy Historian» de General Electric et les serveurs de «GE Fanuc ma» qui délivrent les licences, mais aussi l'application «HMIWeb» de Honeywell et les administrateurs de licences «FLEXNet», «Sentinel HASP» et «ThingWorx Industrial Connectivity Suite».[62] Une fois les fichiers chiffrés, «EKANS» affiche sa demande de rançon.

«EKANS» a d'abord passé pour un pionnier de ce genre d'attaques. En analysant ce maliciel, Dragos a toutefois découvert des analogies frappantes avec «MegaCortex», rançongiciel qui s'en prenait depuis l'été 2019 aux SCI. La découverte de ces similitudes a conduit à relativiser l'importance d'«EKANS». En particulier, la liste des processus auxquels s'intéresse «MegaCortex» (plus de 1000) est bien plus longue que celle d'«EKANS» (64). De même, si les deux rançongiciels s'attaquent aux mêmes processus de contrôle industriels, «MegaCortex» bloque encore toute une série de processus de sécurité. L'unique développement significatif d'«EKANS» serait l'obfuscation du code de programme, afin de le rendre plus difficile à détecter.

Ces deux rançongiciels constituent une menace pour le secteur industriel et pour de nombreuses infrastructures critiques. Un rançongiciel qui s'en prend à l'infrastructure informatique n'infectera en général que les systèmes de contrôle basés sur Windows, qui en outre devront être atteignables par Internet, et il doit par conséquent posséder un certain potentiel de diffusion. Par contre, «EKANS» et «MegaCortex» ont été développés pour s'attaquer expressément aux systèmes d'automatisation industrielle. Il est vrai qu'à ce jour, aucune des victimes d'«EKANS» dont les noms ont été rendus publics n'a confirmé que ses SCI aient souffert d'une

---

61 https://www.bloomberg.com/news/articles/2020-01-28/-snake-Ransomware-linked-to-iran-targets-industrial-controls; https://www.otorio.com/blog/snake-industrial-focused-Ransomware-with-ties-to-iran/

62 https://www.dragos.com/blog/industry-news/ekans-Ransomware-and-ics-operations/

cyberattaque. Le constructeur automobile Honda[63] par exemple a admis avoir subi une infection de son réseau informatique, mais elle n'a eu aucun impact sur la production ou les ventes, et par conséquent la clientèle est restée épargnée. La multinationale du secteur de l'énergie Enel[64] a bien constaté le 7 juin une intrusion dans son système informatique, mais son antivirus a été en mesure d'arrêter le rançongiciel avant qu'il n'entre en action. Par précaution, Enel a brièvement isolé son réseau d'exploitation. Là non plus, les systèmes de contrôle n'ont subi aucun dommage et aucune fuite de données n'a été découverte. Parmi les victimes d'«EKANS» dont les noms sont connus figure Fresenius Medical Care, important fournisseur privé européen du secteur hospitalier. Des données aussi sensibles que les résultats d'analyses médicales, les notes concernant les traitements et les allergies, ou encore le nom, la profession, le numéro de téléphone et l'adresse de patients ont été publiés après l'attaque du rançongiciel.[65] Selon le spécialiste de la protection informatique Kaspersky, les constructeurs automobiles figurent également parmi les victimes d'«EKANS»; en outre, dans un cas au moins l'infection n'en serait pas restée au réseau bureautique, sachant que le maliciel a été découvert et bloqué dans le système de vidéosurveillance d'une organisation basée en Chine.[66]

Indépendamment des rançongiciels qui avaient dans leur ligne de mire les systèmes de contrôle industriels, un nombre élevé d'attaques contre les infrastructures critiques du secteur de l'énergie ont été observées au premier semestre 2020. De telles attaques représentent aussi une menace pour la productivité d'une entreprise. Le 18 février par exemple, l'agence américaine de cybersécurité (CISA) a découvert une attaque contre le réseau de technologies opérationnelles (OT) d'une station de compression de gaz naturel. L'agresseur, dont le nom n'a pas été révélé, s'est introduit grâce à un courriel ciblé dans le réseau informatique de l'entreprise. Il est ensuite parvenu à se propager en interne (*lateral movement*) et à pénétrer dans le réseau OT. L'acteur a alors initié le chiffrement des deux réseaux. Les processus OT infectés incluent les interfaces Homme-machine (*Human Machine Interface*, HMI), la chronologie des données et les serveurs à scrutation (*polling*). La victime a été bien obligée de stopper son activité d'exploitation pour effacer toute trace du maliciel, ce qui lui a causé une perte de productivité et de bénéfice.[67]

Le tableau qui suit passe en revue les attaques de rançongiciels fructueuses et rendues publiques durant le semestre sous revue contre des organisations du secteur de l'énergie.

63 https://www.bleepingcomputer.com/news/security/honda-investigates-possible-Ransomware-attack-networks-impacted/
64 https://www.bleepingcomputer.com/news/security/power-company-enel-group-suffers-snake-Ransomware-attack/
65 https://www.bleepingcomputer.com/news/security/snake-Ransomware-leaks-patient-data-from-fresenius-medical-care/
66 https://ics-cert.kaspersky.com/media/Kaspersky_ics_cert_alert_Snake_EN.pdf
67 https://us-cert.cisa.gov/ncas/alerts/aa20-049a

Date	Rançongiciel	Victime	Conséquences
1er avril	Maze	Groupement Berkine, réunissant Sonatrach, société publique algérienne des hydrocarbures, et son partenaire commercial américain Anadarko	Publication de plus de 500 Mo de documents renfermant des informations confidentielles (par ex. liste de salaires et coordonnées des employés, quantités produites, budget et objectifs fixés).[68]
14 avril	Ragnar Locker	Energias de Portugal (EDP), multinationale portugaise du secteur de l'énergie (courant et gaz)	Après avoir verrouillé les données de l'entreprise, les opérateurs du rançongiciel ont exigé une rançon de 11 millions de dollars. Les escrocs auraient encore dérobé 10 TB de documents sensibles, menaçant de les divulguer avant d'en publier une partie comme mise en garde. L'attaque n'aurait pas perturbé la production de courant électrique.[69]
30 avril	NetWalker	Northwest Territories Power Corporation NTPC, compagnie électrique canadienne	Les systèmes électriques auraient fonctionné sans interruption, selon la compagnie. Son site Internet a subi une défiguration, et les cybercriminels y ont publié leur message.[70]
4 mai	Inconnu; les autorités taïwanaises soupçonnent toutefois la Chine.[71]	Raffinerie étatique de Taïwan CPC Corp	Le site Web de CPC a été touché et diverses stations-service ont dû fermer temporairement, faute de pouvoir traiter les paiements effectués avec la carte de CPC Corp.[72] L'attaque n'a eu aucun impact sur la production d'énergie de CPC.
14 mai	REvil / Sodinokibi	Elexon, intermédiaire majeur du réseau électrique britannique	L'incident a perturbé le réseau informatique interne et mis hors service le serveur de messagerie. Les systèmes de transport du courant n'ont subi aucun dégât.[73] Début juin, les pirates ont publié sur le Darkweb un dossier renfermant 1280 fichiers dérobés à Elexon.[74]

68 https://www.inter-lignes.com/des-documents-hyper-confidentiels-de-sonatrach-derobes-par-des-hackers/
69 https://www.bleepingcomputer.com/news/security/ragnarlocker-Ransomware-hits-edp-energy-giant-asks-for-10m/
70 https://www.cbc.ca/news/canada/north/ntpc-apparent-Ransomware-attack-1.5551603
71 https://www.cyberscoop.com/cpc-Ransomware-winnti-taiwan-china/
72 https://www.taiwannews.com.tw/en/news/3927869
73 https://www.elexonportal.co.uk/news/view/27108?cachebust=ebf1vtjsp0
74 https://www.theregister.com/2020/06/01/elexon_Ransomware_was_revil_sodinokibi/

Mesures de sécurité :

Les exploitants de systèmes de contrôle industriels (SCI) devraient séparer autant que possible hermétiquement leurs systèmes d'exploitation courants, d'une part, et le réseau OT, d'autre part. Il convient d'introduire pour le réseau OT une structure multiniveaux, où les processus moins critiques sont séparés des processus réellement critiques. Il faut encore s'assurer que seul le personnel autorisé ait accès aux SCI, de façon à limiter les accès tant virtuels que physiques aux systèmes critiques.

Le NCSC a publié sur son site Web la liste de contrôle «Mesures de protection des systèmes de contrôle industriels (SCI)» :
https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/mesures-de-protection-des-systemes-de-controle-industriels--sci-.html

L'Agence américaine de cybersécurité et de sécurité des infrastructures (CISA) a récemment mis en ligne des recommandations en la matière :
https://www.cisa.gov/sites/default/files/publications/Cybersecurity_Best_Practices_for_Industrial_Control_Systems.pdf

4.3.2 Actes de sabotage dans le cadre des conflits au Proche-Orient

Le 3 janvier 2020, un tir de drone américain causait la mort du général iranien Qassem Soleimani, commandant de la Force Al-Qods du corps des Gardiens de la révolution islamique ainsi que de Jamal Jafaar Ibrahimi, chef des Brigades du Hezbollah et commandant adjoint des Forces de mobilisation populaire, à la sortie de l'aéroport de Bagdad.[75] Cette opération cinétique trouvait place dans le conflit au Proche-Orient, où les confrontations ne sont pas seulement de nature physique. Depuis des années en effet, les adversaires s'affrontent régulièrement dans le cyberespace et n'ont pas peur des retombées physiques de leurs cyberattaques, quand elles ne sont pas délibérément voulues.[76]

La compagnie pétrolière nationale de Bahreïn, Bapco, a subi en fin d'année 2019 une cyberattaque destructrice.[77] Le maliciel a rendu inutilisables plusieurs appareils de son environnement système. Bien que Bapco ne l'ait jamais confirmé, tout indique un lien avec la mise en garde[78] lancée peu avant par l'autorité de cybersécurité saoudienne contre le virus effaceur (*wiper*) «Dustman».[79] Les pirates auraient initialement compromis un système d'accès à distance. La société de cyberintelligence ClearSky a expliqué, dans un rapport consacré à la campagne de piratage «Fox Kitten»,[80] comment des accès *RDP* mal protégés ou des serveurs VPN non actualisés et donc vulnérables de Pulse Secure, Fortinet ou Palo Alto ont permis aux

75 https://www.defense.gov/Newsroom/Releases/Release/Article/2049534/statement-by-the-department-of-defense/
76 Voir MELANI, rapport semestriel 2019/2, chap. 5.2.
77 https://www.zdnet.com/article/new-iranian-data-wiper-malware-hits-bapco-bahrains-national-oil-company/
78 https://www.scribd.com/document/442225568/Saudi-Arabia-CNA-report
79 https://malpedia.caad.fkie.fraunhofer.de/details/win.dustman
80 https://www.clearskysec.com/fox-kitten/

escrocs de s'introduire dans des réseaux d'entreprises. L'arsenal des agresseurs sévissant au Proche-Orient inclut encore le script «PowDesk»,[81] pour compromettre les systèmes utilisant la suite logicielle «LANDesk Management Agent». Microsoft a par exemple découvert des attaques lancées par le groupe «HOLMIUM» via le cloud.[82] D'autres outils spécifiques ont été utilisés, comme «POWERTON».[83] Le cyberacteur «APT34/Oilrig» a attaqué, selon le fournisseur de services de sécurité Yoroi, un serveur de messagerie du gouvernement libanais avec l'aide de «Karkoff Implant».[84] Lorsque de telles tentatives aboutissent et livrent accès au réseau, les systèmes de pilotage en font les frais. Le gouvernement israélien a ainsi mis en garde, en avril, contre des attaques visant les systèmes *SCADA* pour l'approvisionnement en eau.[85] Par la suite, d'autres tentatives d'intrusion dans les systèmes d'irrigation de l'agriculture israélienne ont été rendues publiques, [86] et on peut supposer que les cyberattaques subies par le principal port iranien du détroit d'Ormuz[87] ont eu lieu en représailles à de telles opérations.

À supposer qu'aucune des variantes essayées ne les mène directement à leur cible, les pirates remontent la chaîne d'approvisionnement, en quête d'un point d'entrée plus éloigné de leur cible. Le FBI a ainsi publié en février une mise en garde[88] pour les fournisseurs de logiciels contre des attaques lancées par le cheval de Troie d'accès à distance «Kwampirs».[89] Ce maliciel recherchait activement des sociétés qui travaillent dans le champ des systèmes de contrôle industriels liés à la production, au transport et à la distribution d'énergie.

Précision :

Les organisations opérant en marge de tels conflits devraient savoir qu'elles s'exposent à subir ce genre d'attaques, directement ou comme victimes collatérales.

4.3.3 Intrusions répétées dans les réseaux d'approvisionnement électrique

Les gestionnaires de réseaux de transport d'électricité de toute l'Europe collaborent au sein de l'association ENTSO-E, afin de coordonner l'approvisionnement électrique du continent. Au printemps 2020, cette organisation a admis avoir dû gérer l'année dernière un cyberincident, dû à une intrusion dans son réseau. «Le réseau bureautique d'ENTSO-E n'est pas relié aux systèmes opérationnels des gestionnaires du réseau de transport», a tenu à préciser ENTSO-E dans un bref communiqué de presse paru en mars 2020.[90] Beaucoup des 42 membres actifs

81 https://www.clearskysec.com/powdesk/

82 https://www.microsoft.com/security/blog/2020/06/18/inside-microsoft-threat-protection-mapping-attack-chains-from-cloud-to-endpoint/

83 https://attack.mitre.org/software/S0371/

84 https://securityaffairs.co/wordpress/98802/apt/karkoff-malware-lebanon.html

85 https://www.gov.il/he/departments/publications/reports/scadaalert

86 https://www.zdnet.com/article/two-more-cyber-attacks-hit-israels-water-system/

87 https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html

88 https://www.zdnet.com/article/fbi-warns-about-ongoing-attacks-against-software-supply-chain-companies/

89 https://malpedia.caad.fkie.fraunhofer.de/details/win.kwampirs

90 https://www.entsoe.eu/news/2020/03/09/entso-e-has-recently-found-evidence-of-a-successful-cyber-intrusion-into-its-office-network/

dans 35 pays européens (voir fig. 6), dont la société suisse Swissgrid, ont confirmé l'analyse de l'association faîtière au sujet de la portée de l'incident.[91] Une telle attaque n'aurait pas pu affecter directement l'approvisionnement électrique de l'Europe.

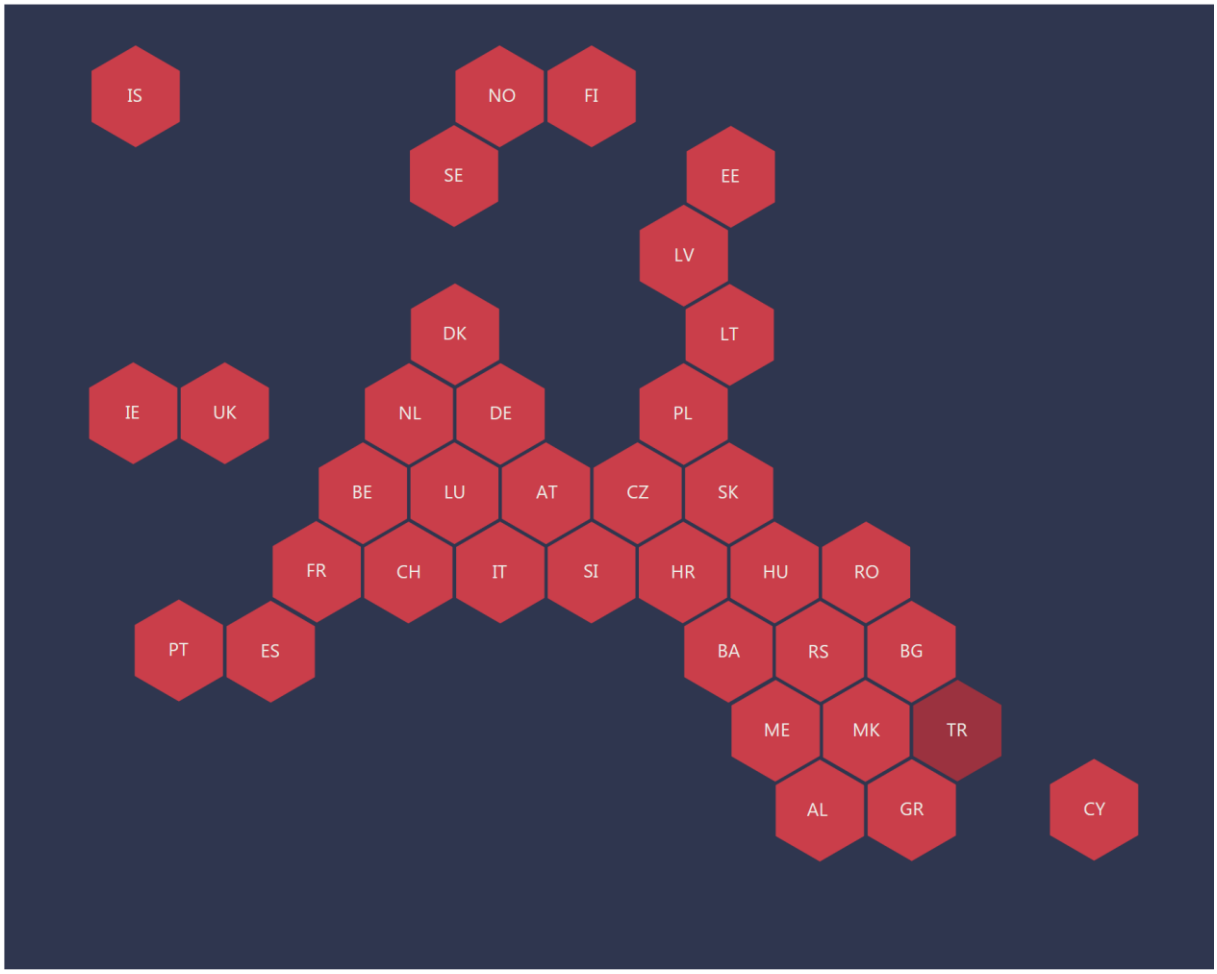

Fig. 6: Membres d'ENTSO-E[92]

Cet incident montre que des acteurs cherchent à comprendre le mode d'organisation du secteur électrique dans différentes parties du monde. Le précédent rapport semestriel fournit d'autres références à ce sujet[93]. Or il ressort de l'exemple actuel que l'Europe n'est pas épargnée. Les journalistes de Cyberscoop[94] ont établi un rapprochement entre une analyse publiée par RecordedFuture[95] et l'incident subi par ENTSO-E. Dans le passé, le même maliciel «Pupy RAT» a notamment servi à des groupes qui n'ont pas hésité à lancer des attaques destructives avec un virus effaceur (*wiper*). Or jusqu'ici, de telles opérations destructrices n'étaient enre-

91 https://www.swissgrid.ch/en/home/about-us/newsroom/newsfeed/20200309-01.html
92 https://www.entsoe.eu/about/inside-entsoe/members/
93 Voir MELANI, rapport semestriel 2019/2, chap. 4.2.1.
94 https://www.cyberscoop.com/europe-grid-pupy-rat/
95 https://www.recordedfuture.com/pupyrat-malware-analysis/

gistrées que dans le contexte de conflits ouverts, à l'instar des tensions au Proche-Orient décrites au chap. 4.3.2. Au vu des développements géopolitiques possibles, chaque pays et toutes les compagnies de distribution d'électricité doivent être dûment prêts à affronter de telles attaques, en fonction des risques encourus. À côté de l'opération de reconnaissance observée en Europe, des fournisseurs de courant américains ont aussi été confrontés à des tentatives d'intrusion[96] dans lesquelles le maliciel «Flowcloud» a été utilisé.[97]

Un récent incident dû à un rançongiciel qui, lui non plus, n'a pas eu d'impact sur les systèmes de pilotage opérationnel a touché Elexon, l'administrateur du marché britannique de l'électricité. Comme Elexon refusait d'entrer en matière sur les revendications des maîtres chanteurs de «Sodinokibi/REvil», ces derniers ont publié les fichiers dérobés.[98] Elexon semble jusqu'ici s'en être tiré à bon compte. Mais tout indique que des acteurs n'ayant pas des mobiles purement financiers pourraient tirer parti des informations publiées pour mettre au point de futures attaques. D'autres exemples similaires sont d'ailleurs survenus, comme les incidents liés à «RagnarLocker» au Portugal ou au rançongiciel utilisé contre la raffinerie de CPC Corp à Taïwan (voir chap. 4.3.1). De telles attaques par rançongiciel constituent en ce moment la menace la plus aiguë, à commencer par les variantes cherchant à perturber les systèmes de pilotage opérationnel pour prendre le contrôle des processus physiques.

Précision :

Le NCSC est régulièrement en contact avec des représentants du secteur de l'approvisionnement en électricité de la Suisse, dans le cadre du cercle fermé de clients de MELANI. Des efforts conjoints sont entrepris pour prévenir de telles attaques en Suisse, pour les détecter au plus vite et en limiter l'impact.

4.4 Vulnérabilités

Les incidents liés à l'exploitation des failles de sécurité publiées au premier semestre 2020 ont augmenté de manière exponentielle pendant le confinement. Beaucoup d'entreprises sont en effet passées au télétravail. Or un tel mode de fonctionnement requiert une infrastructure complexe qu'il n'est déjà pas simple d'aménager de manière sûre en temps normal, sans le stress d'une situation d'urgence.

Bien des entreprises suisses, dont des infrastructures critiques, auraient eu de quoi s'inquiéter le 17 décembre 2019, quand était publiée la vulnérabilité «CVE-2019-19781» des solutions de mise à disposition d'applications (*Application Delivery Controller*, ADC) ainsi que des produits *Gateway* (passerelles) de Citrix. Car cette faille de sécurité permet à des tiers non autorisés d'exécuter du code sur toutes sortes d'appareils. Et comme les produits Citrix vulnérables sont souvent déployés à la périphérie des réseaux d'entreprises, un attaquant pouvait s'y glisser en exploitant ladite faille. Bien que Citrix ait publié un avertissement de sécurité et vivement recommandé à ses clients de sécuriser leurs produits, tout le monde ne l'a pas fait. Le 10 janvier 2020, plusieurs *exploits* permettant de tirer profit de ces failles paraissaient. Dans les

96 https://www.proofpoint.com/us/blog/threat-insight/ta410-group-behind-lookback-attacks-against-us-utilities-sector-returns-new

97 https://www.proofpoint.com/us/blog/threat-insight/flowcloud-version-413-malware-analysis

98 https://www.theregister.com/2020/06/01/elexon_ransomware_was_revil_sodinokibi/

heures qui ont suivi, l'activité de reconnaissance pour identifier les produits Citrix vulnérables connectés à Internet a explosé, puis les criminels ont utilisé les exploits fournis pour compromettre des réseaux d'entreprises et les faire chanter lors d'une attaque par rançongiciel. Dès la publication des exploits, le NCSC avait expressément signalé à plus de 50 exploitants d'infrastructures critiques le danger potentiel et les mesures de protection à mettre en place.

Les criminels ciblent notamment les routeurs ou les serveurs VPN utilisant des versions logicielles dont les failles n'ont pas été corrigées par des mesures spécifiques. Leur stratégie consiste à repérer une porte d'accès au réseau de l'entreprise, puis à déployer par exemple un rançongiciel. Ces dernières années, un nombre croissant d'organisations ont subi de lourdes pertes imputables à une application ou à un produit connectés à Internet qui contenaient une faille récemment publiée.[99]

Recommandations :

Les entreprises devraient tenir à jour un inventaire de leur infrastructure informatique, en donnant la priorité absolue aux produits connectés à Internet. Dans un deuxième temps, elles devraient se tenir informées des vulnérabilités et des mises à jour, dans le cadre d'une gestion en temps réel des risques, qui consiste à souscrire aux consignes des fabricants, à les analyser et à les classer par degré de priorité. Il s'agit encore de prévoir des plages et des procédures pour les mises à jour urgentes d'éléments clés (à la périphérie du réseau notamment).

La base de données *Common Vulnerabilities and Exposures* CVE, qui recense toutes les failles publiées, figure sous le lien: https://nvd.nist.gov.

4.5 Fuites de données

Le phénomène des fuites de données a beau ne pas être nouveau, le nombre d'incidents a augmenté durant la période sous revue. Et tout indique que la tendance se poursuivra à l'avenir. Certains cybercriminels se sont fait une spécialité de la divulgation et de la revente des données d'entreprises. Selon une étude, une société sur quatre subira d'ici deux ans une fuite de données.[100]

EasyJet a dû expliquer au mois de mai avoir été victime d'une cyberattaque sophistiquée qui portait sur les données de près de neuf millions de clients, dont les adresses électroniques et les dates de voyage, sans oublier les données des cartes de crédit. Aux dires d'EasyJet, il avait fallu du temps pour mesurer l'ampleur des dégâts et savoir qui était concerné. L'entreprise n'a pas voulu préciser les modalités ou les motifs de l'attaque, mais a souligné que selon ses propres recherches, les pirates s'intéressaient aux enjeux de propriété intellectuelle et non aux informations réutilisables pour un vol d'identité. Elle a néanmoins mis en garde sa clientèle contre de possibles attaques de phishing, en lui recommandant une vigilance accrue. Selon le règlement européen sur la protection des données (RGPD), EasyJet s'expose à une peine pécuniaire pouvant atteindre 4 % de son chiffre d'affaires annuel mondial, s'il s'avère que des

99 Voir rapports semestriels MELANI 2019/2, chap. 4.6.1 et 2020/1, chap. 4.1.1.

100 https://www.itgovernance.co.uk/blog/do-you-have-a-data-breach-response-plan

données de clients ont été utilisées à mauvais escient. Et s'il devait y avoir eu négligence de sa part, les clients pourront lui intenter des actions en dommages-intérêts, ce qui alourdirait encore les coûts de la compagnie aérienne.

En février 2020, le groupe hôtelier Marriott International a annoncé une fuite de données personnelles concernant jusqu'à 5,2 millions d'hôtes. La cyberattaque aurait débuté à la mi-janvier. L'incident n'avait été découvert qu'à la mi-février, où les données d'un nombre anormalement élevé de clients avaient fuité à partir des comptes de deux employés d'une des franchises du groupe. Marriott avait alors ouvert une enquête, durci sa surveillance et prévu les ressources utiles pour informer et assister ses hôtes, lançant par exemple un portail Web que les clients potentiellement touchés pouvaient interroger afin de savoir ce qu'il en était. C'est déjà le deuxième incident en deux ans. En novembre 2018, le groupe Marriott avait signalé que des pirates avaient eu accès au système de réservation des hôtels Starwood.

Selon une enquête récente, quasiment 80 % des entreprises avaient subi, au cours des 18 derniers mois, au moins une violation de leurs données stockées dans le cloud, et 43 % faisaient état d'au moins une dizaine d'incidents.[101] Les 300 responsables de la sécurité de l'information (*CISO*) ayant participé à l'enquête redoutaient principalement, pour leurs données hébergées dans le cloud, une mauvaise configuration de la sécurité (67 %), un manque de transparence quant aux paramètres et aux activités d'accès (64 %), ainsi qu'une pratique laxiste dans la gestion des identités et des accès (61 %).[102] Les autorisations délivrées en surnombre sont un piège risquant de passer longtemps inaperçu, car bien souvent, elles sont accordées par défaut quand une ressource supplémentaire ou un nouveau service viennent s'ajouter aux environnements cloud. Il s'agit donc d'une cible privilégiée des agresseurs, qui peuvent ainsi se livrer à des activités malveillantes comme le vol de données sensibles ou l'infiltration de maliciels. Les priorités essentielles pour la sécurité, lors de l'accès au cloud, sont dès lors le maintien de la confidentialité des données sensibles, le respect des prescriptions légales et la garantie d'un niveau d'accès adéquat.

Les fuites de données ne s'expliquent pas uniquement par des calculs financiers et peuvent aussi avoir des mobiles idéologiques. Le 19 juin 2020, un groupe appelé «Distributed Denial of Secrets (DDoSecrets)» a mis en circulation 269 Go de données constituées par plus de 200 postes de police américains durant plus de 24 ans.[103] Son but déclaré était de mettre en libre accès des données d'intérêt public, dans une optique de transparence collective. Or il s'agit plus probablement d'un acte de vengeance suite aux protestations antiracistes contre la police aux États-Unis. Les forces de l'ordre n'avaient jamais subi jusque-là de fuite de données d'une telle ampleur. Dans cette masse de documents qui, à l'instar des rapports et bulletins du FBI, renferment des données personnelles, on découvre des coordonnées bancaires détaillées, des photos de suspects, ou le numéro de téléphone et l'adresse électronique tant des victimes que des agresseurs. Il va de soi qu'à l'avenir, des hacktivistes et des cybercriminels sont susceptibles de puiser dans cette mine de données. Dans le cas d'espèce, les autorités craignent surtout une mise en danger des victimes. L'authenticité des données a été entretemps confirmée. La fuite aurait été rendue possible par une faille de sécurité de Netsential, société spécialisée dans le développement web et basée à Houston, Texas. Il est trop tôt pour dire dans quelle mesure les autres clients de Netsential sont également concernés.

---

101 https://www.helpnetsecurity.com/2020/06/03/cloud-data-breach/

102 https://www.itgovernance.co.uk/blog/do-you-have-a-data-breach-response-plan; https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/

103 https://krebsonsecurity.com/2020/06/blueleaks-exposes-files-from-hundreds-of-police-departments/

Comme indiqué au chap. 4.1.1, les récents incidents liés à un rançongiciel comportaient presque toujours une fuite de données. Cette évolution est due au groupe «Maze», qui a créé un site spécial baptisé «Maze News», sur lequel sont publiées les données dérobées aux victimes ayant refusé de verser la rançon demandée. D'autres groupes, dont «Nefilim», «Sekhmet» et «Sodinokibi/REvil», ont rapidement recouru à la même tactique. Certains groupes excellent déjà à faire chanter par leurs propres moyens les entreprises, encaissant des rançons d'un montant moyen supérieur à 100 000 dollars, voire de plusieurs millions à leurs dires pour quelques gros poissons. Or ces derniers temps, il y a eu des comptes rendus d'une collaboration entre les groupes «Maze» et «Lockbit», ainsi qu'avec les opérateurs de «Sodinokibi/REvil», qui ne se contentent plus de publier les données dérobées si les victimes ne paient pas, mais qui à la place les revendent au plus offrant. En pratiquant la division du travail, en échangeant des conseils, en opérant de manière tactique et en se dotant d'une plateforme centralisée pour les fuites de données, les bandes peuvent toujours plus se concentrer sur le développement d'attaques raffinées ou de méthodes de chantage fructueuses. Une telle division du travail a déjà été observée dans quelques cas. C'est ainsi que sont apparues des fuites d'informations qui ne provenaient pas d'une attaque par rançongiciel de «Maze», mais d'un autre incident imputable à «LockBit».

Les rançongiciels et les fuites de données tendent clairement à devenir des «services». Le chiffrement de données par rançongiciel ainsi que les fuites de données constituent deux services à part entière, pouvant s'acheter sur le Darkweb. Autre nouveauté importante : les données ne sont plus seulement publiées, mais commercialisées, voire vendues aux enchères.

Conclusion / Recommandations :

L'utilisation minutieuse et responsable des données constitue un défi à ne pas sous-estimer. D'un côté, l'entreprise risque sa réputation et s'expose à subir des coûts énormes. De l'autre, les gens ou les clients sont en droit d'attendre que les entreprises et les organisations traitent leurs données personnelles de manière sûre et responsable. Une mesure importante ici consiste à élaborer un plan de réponse aux violations de données (*data breach response plan*). Sa simple élaboration révélera déjà où se situent les risques spécifiques et de quelle manière il serait possible de les réduire.

La description qui précède montre que les pirates déploient toutes sortes de moyens pour faire main basse sur les données. Chaque entreprise devrait donc se préparer au scénario d'une fuite de données. Cela implique notamment d'adopter les mesures suivantes : inventaire du système, analyse des menaces et des vulnérabilités, évaluation et réduction des risques, développement constant des mécanismes de contrôle ainsi que de la surveillance.

Au cas où l'entreprise subirait malgré tout une fuite de données, un plan de réponse spécifique lui permettra une action rapide et coordonnée. Outre les mesures classiques de gestion des incidents, il devrait inclure des processus servant à préciser l'ampleur du dommage (nature exacte et volume des données dérobées), la manière d'informer les victimes et les rapports à publier. Si des prestations externes (conseil, soutien opérationnel, etc.) s'imposent, il est important de connaître au préalable les partenaires et d'avoir fixé par contrat leurs services. La communication (personnes concernées, médias) est un autre point central. Il s'agit de régler non seulement les contenus communiqués, mais aussi les ressources pouvant lui être consacrées (par ex. soutien pour gérer les multiples appels et courriels). À côté de l'analyse technique et de l'évaluation des incidents, il faut par ailleurs procéder à une analyse immédiate de la situation et de ses conséquences juridiques ou financières possibles. Enfin, il faudrait encore veiller à préserver la réputation de l'entreprise.

4.6 Espionnage

L'espionnage demeure une menace bien réelle, comme l'ont montré une fois de plus les événements des derniers mois. Les groupes étatiques ou soutenus par leur gouvernement conservent un rôle de premier plan. Mais il est d'ores et déjà possible de faire appel à des entreprises privées, à des fins d'espionnage ciblé (voir chap. 4.6.3).

4.6.1 Espionnage à l'ère du COVID-19

Selon Kaspersky, les attaques *APT* comme «Kimsuky», «APT27», «Lazarus» ou «Vicious-Panda» ainsi que d'autres cyberacteurs ont su mettre à profit la crise du coronavirus.[104] Même si la pandémie n'a pas influencé les tactiques, techniques ou processus (*Tactics, Techniques and Procedures*, TTP) déployés par ces groupes, elle réapparaît comme leitmotiv dans leurs scénarios d'attaque (voir chap. 3.1 sur l'ingénierie sociale).

Pendant une pandémie, le besoin d'informations concernant le domaine de la santé au sens large est logiquement plus grand. Cela explique par exemple que l'OMS, un des acteurs clés de la crise au niveau international, ait subi des cyberattaques bien plus fréquentes qu'en temps normal. Comme le CISO de l'OMS l'a signalé à Reuters, les tentatives d'espionnage émanaient généralement de pirates d'élite.[105] Outre l'OMS, des activités d'espionnage ont été déployées contre plusieurs établissements actifs dans la recherche d'un vaccin contre le COVID-19 – car la course à la découverte du vaccin se poursuit. Les États-Unis, le Canada et la Grande-Bretagne ont accusé un service secret russe d'espionner des laboratoires situés sur leur territoire.[106] Les États-Unis ont en outre porté plainte contre deux citoyens chinois, accusés d'avoir mené des opérations d'espionnage pour le compte du ministère chinois de la sécurité publique.[107] Ces tentatives d'espionnage visaient des compagnies biotech américaines à la recherche d'un vaccin contre le COVID-19.[108] Il semblerait que les cyberpirates accusés fassent partie d'un groupe criminel qui organise, depuis 2009 au moins, des campagnes d'espionnage dans de nombreux secteurs, et qui ont réalisé de juteux profits financiers liés notamment au vol de la propriété intellectuelle.

4.6.2 L'espionnage économique est une réalité, en Suisse aussi

L'espionnage économique désigne l'acquisition d'informations ou de données économiques, scientifiques ou technologiques volontairement tenues secrètes (secrets d'affaires). Il est très difficile d'en chiffrer l'ampleur en Suisse, car il s'agit d'une question très sensible, sur laquelle quasiment rien n'a été publié. Afin de mieux cerner le problème, le Service de renseignement

---

104 https://securelist.com/apt-trends-report-q1-2020/96826/

105 https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive/exclusive-elite-hackers-target-who-as-coronavirus-cyberattacks-spike-idUSKBN21A3BN

106 Grande-Bretagne: https://www.ncsc.gov.uk/news/advisory-apt29-targets-covid-19-vaccine-development; États-Unis: https://us-cert.cisa.gov/ncas/current-activity/2020/07/16/malicious-activity-targeting-covid-19-research-vaccine-development; Canada: https://cse-cst.gc.ca/en/media/2020-07-16

107 https://www.courtlistener.com/recap/gov.uscourts.waed.91446/gov.uscourts.waed.91446.15.0.pdf

108 https://www.cisa.gov/publication/fbi-cisa-psa-prc-targeting-covid-19-research-organizations; https://www.nytimes.com/2020/07/21/us/politics/china-hacking-coronavirus-vaccine.html

de la Confédération (SRC) a lancé un appel d'offres portant sur une étude consacrée à l'espionnage économique en Suisse. En janvier 2020 est parue l'étude qualitative et quantitative menée par l'Institut de droit pénal et de criminologie de l'Université de Berne et consacrée aux actes d'espionnage économique commis aux dépens d'entreprises suisses de taille variable, actives dans des domaines divers[109].

Les résultats de cette étude montrent que l'espionnage économique touche 15 à 33 % des entreprises helvétiques, toutes tailles confondues. Les secteurs les plus exposés sont l'informatique, les télécommunications, les sciences de la vie, la construction mécanique, l'industrie et la pharma. Des collaborateurs (anciens ou actuels) étaient impliqués dans 40 % des cas. Les entreprises les plus menacées dans les autres branches sont celles qui fabriquent des produits de niche ou des produits liés à la sécurité. Les sociétés qui ont participé à l'étude soulignent la difficulté de distinguer entre les attaques visant directement à générer un profit économique et la collecte de données effectuée à des fins d'espionnage. L'attribution des cas semble également délicate (absence de tout indice sur l'auteur dans 38 % des cas). Quant aux dommages subis, les plus souvent cités sont la perte d'avantages compétitifs (18 %), les pannes informatiques (14 %), ainsi que la perte de clients ou de mandats (11 %). Enfin, 11 % des cas d'espionnage ont mis en péril l'existence de l'entreprise touchée.

4.6.3 Espionnage à la demande

En juin 2020, le laboratoire de recherche canadien Citizen Lab a publié un rapport sur les activités massives d'espionnage à la demande (*hack for hire*) commises par un groupe du nom de «Dark Basin».[110] Depuis 2017, «Dark Basin» s'en est pris à des journalistes et à des activistes, mais aussi à des banques, à des fonds spéculatifs et à des entreprises actives dans d'autres secteurs. Citizen Lab a démontré l'existence de nombreux liens avec une société indienne du nom de BellTroXInfoTech Services. Le groupe aurait agi pour différents mandataires non identifiés.

Une vaste action de phishing a ainsi été menée contre diverses organisations à but non lucratif ayant participé à la campagne «#exxonknew». Cette campagne reprochait à la compagnie pétrolière américaine Exxon d'avoir volontairement minimisé pendant des dizaines d'années les conséquences du changement climatique. De même, Dark Basin a espionné des employés de la société allemande de paiements en ligne Wirecard ainsi que des journalistes ayant couvert les suspicions de fraude au sein de cette entreprise.[111]

4.6.4 Nouveautés concernant «Winnti»

Le fournisseur de solutions de sécurité FireEye a rendu publique une vaste action d'espionnage du groupe «APT41».[112] Entre le 20 janvier et le 11 mars 2020, «APT41» a tenté d'exploiter chez 75 clients de FireEye les vulnérabilités des applications Citrix NetScaler/ADC, des routeurs Cisco ou de Zoho ManageEngine Desktop Central. L'attaque a été menée dans de

---

109 https://boris.unibe.ch/139072/

110 https://citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation/

111 https://www.ft.com/content/19c6be2a-ee67-11e9-bfa4-b25f11f42901

112 https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html

nombreux pays, dont la Suisse. De multiples domaines ont été touchés, dans les secteurs gouvernemental et financier notamment. «APT41» est un acteur très sophistiqué, qui diversifie régulièrement ses activités. Ce groupe est également connu sous le nom de «Winnti», dont il a déjà été question dans le dernier rapport semestriel.[113]

4.6.5 Un serveur de messagerie Linux populaire victime de «Sandworm»

L'agence nationale de sécurité américaine (NSA) a émis le 28 mai 2020 des recommandations visant à déjouer les tentatives d'intrusion dans le serveur de messagerie électronique Exim.[114]. Dans son communiqué, la NSA attribuait ces attaques à un groupe baptisé «Sandworm», rattaché selon elle au Centre principal des technologies spéciales (GTsST) du service de renseignement militaire russe (GRU). «Sandworm» serait aussi impliqué dans le piratage des centrales électriques ukrainiennes survenu en décembre 2015[115] et en décembre 2016[116].

La faille (CVE-2019-10149) était déjà connue depuis un an et cela faisait longtemps que des mises à jour étaient disponibles.[117] Le moteur de recherche Shodan a néanmoins signalé la présence de 2,5 millions de systèmes vulnérables, lors de la mise en garde de la NSA.[118] Exim est d'autant plus souvent utilisé que ce logiciel propose par défaut la fonction de messagerie dans de nombreuses distributions Linux. Les systèmes vulnérables permettent aux agresseurs d'introduire et d'exécuter à distance les codes malveillants de leur choix.

4.6.6 Menace permanente due à «Berserk Bear»

Depuis le printemps 2018 où les États-Unis avaient lancé l'alerte contre les intrusions de ce groupe,[119] qui à l'époque étaient principalement dirigées contre les fournisseurs d'énergie américains, les agresseurs ont régulièrement fait les gros titres.[120] Ils ont ainsi récemment compromis le site Web de l'aéroport de San Francisco[121] pour s'emparer des données d'accès des visiteurs non méfiants.[122]

Un jour après les journalistes de Cyberscoop,[123] qui relayaient une mise en garde des autorités allemandes, le journal télévisé allemand annonçait lapidairement le 27 mai 2020: «Le cyber-ours russe a encore frappé».[124] Dans un document n'ayant pas été rendu public, le Service fédéral de renseignement (BND), l'Office fédéral de protection de la constitution (BfV) et l'Office fédéral de la sécurité des technologies de l'information (BSI) signalaient les incessantes

---

113 Voir MELANI, rapport semestriel 2019/2, chap. 4.1.2.

114 https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/2196511/exim-mail-transfer-agent-actively-exploited-by-russian-gru-cyber-actors/

115 Voir MELANI, rapport semestriel 2015/2, chap. 5.3.1.

116 Voir MELANI, rapport semestriel 2016/2, chap. 5.3.1.

117 https://www.qualys.com/2019/06/05/cve-2019-10149/return-wizard-rce-exim.txt

118 https://www.bleepingcomputer.com/news/security/nsa-russian-govt-hackers-exploiting-critical-exim-flaw-since-2019/

119 https://us-cert.cisa.gov/ncas/alerts/TA18-074A

120 https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112

121 https://www.bleepingcomputer.com/news/security/russian-hackers-tried-to-steal-san-francisco-airport-windows-accounts/

122 https://attack.mitre.org/techniques/T1187/

123 https://www.cyberscoop.com/german-intelligence-memo-berserk-bear-critical-infrastructure/

124 https://www.tagesschau.de/investigativ/br-recherche/hacker-angriff-infrastruktur-101.html

tentatives d'intrusion dues à un groupe connu sous le pseudonyme de «Berserk Bear».[125] Les entreprises actives dans les secteurs de l'énergie, de l'approvisionnement en eau et des télécommunications étaient surtout menacées.

L'Office fédéral de protection de la constitution (BfV) avait mis en garde dès l'été 2018 contre de telles attaques,[126] qui visaient aussi des entreprises allemandes. Selon les recherches de la radio-télévision bavaroise (Bayerischer Rundfunk), les autorités allemandes se sont crues obligées de rappeler avec force ce danger, à cause des tentatives de compromission incessantes et parfois fructueuses intervenues entre-temps.

Précision:

«Berserk Bear» est un acteur qui, dans le passé, s'est déjà introduit à plusieurs reprises dans des réseaux jusqu'aux systèmes utilisés pour le pilotage des processus, par exemple dans l'approvisionnement électrique. Il ne reste donc qu'un pas à franchir jusqu'au cybersabotage ayant des retombées dans le monde physique.

4.6.7 Australie – cible de cyberattaques

L'Australie a subi ces derniers mois, aux dires de son propre gouvernement, une vague nourrie d'attaques raffinées visant un grand nombre d'institutions gouvernementales, le monde politique, la santé et l'éducation, l'industrie et les exploitants d'infrastructures critiques. Même si les cyberpirates s'en étaient déjà souvent pris à l'Australie, cette vague se démarquait des précédentes par la fréquence et l'ampleur des agressions, par la technique raffinée à l'œuvre et par ses retombées potentielles.

Selon un rapport de l'Australian Cyber Security Centre,[127] les agresseurs ont utilisé pour pénétrer dans les systèmes de leurs victimes la tactique du copier/coller (*copy-paste-compromises*). Autrement dit, ils ont tiré parti d'*exploits* et d'autres outils repris à l'identique, à partir du code source libre. Pour accéder aux réseaux cibles, ils ont par exemple exploité les failles de versions non actualisées de Telerik UI, Microsoft Internet Information Services (IIS), SharePoint ou encore Citrix (cf. chap. 4.4). Quand cela n'était pas possible, ils ont tenté des attaques de phishing ciblé (*spear phishing*). Les agresseurs se sont procuré des accès à distance légitimes à l'aide d'identités dérobées. Tirant parti de scripts *Web shells* et du trafic *HTTP/HTTPS*, ils ont utilisé des sites compromis comme *serveurs de commande et de contrôle*. Une fois dans le réseau cible, ils y ont déployé des outils libres et d'autres sur mesure, afin de s'assurer une présence durable (*persistence*) et des interactions régulières avec le réseau.

Le gouvernement australien considère que ces attaques étaient d'origine étatique, même si le Premier ministre Scott Morrison n'a pas indiqué de nom. Par la suite, des sources gouvernementales ont évoqué la Chine comme agresseur présumé.[128] Le gouvernement chinois a

125 https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2018GlobalThreatReport.pdf
126 https://www.wirtschaftsschutz.info/SharedDocs/Kurzmeldungen/DE/ITSicherheit/Cyberbrief_1_18_dow.html
127 https://www.cyber.gov.au/sites/default/files/2020-06/ACSC-Advisory-2020-008-Copy-Paste-Compromises.pdf
128 https://www.theguardian.com/australia-news/2020/jun/19/australia-cyber-attack-attacks-hack-state-based-actor-says-australian-prime-minister-scott-morrison

aussitôt démenti et accusé l'Institut australien de stratégie politique (Australian Strategic Policy Institute, ASPI) d'avoir délibérément lancé des accusations mensongères.[129]

Moins d'un mois après la divulgation de ces attaques, un comité d'experts formé par le gouvernement australien publiait un rapport renfermant des recommandations pour la stratégie nationale de cybersécurité 2020.[130] Ces recommandations couvrent cinq domaines:

- Dissuasion : empêcher les acteurs malveillants de s'en prendre à des cibles australiennes.
- Prévention : éviter que des personnes ou des secteurs ne soient piratés en ligne.
- Détection : identifier les cybermenaces et réagir rapidement.
- Résilience : réduire l'impact des cyberincidents.
- Investissements : investir dans la cybersécurité.

L'Australie entend investir durant les dix années à venir un montant record de 1,35 milliard de dollars australiens (900 millions de francs) pour mettre en œuvre sa nouvelle stratégie. Le tiers de cette somme permettra au gouvernement australien d'embaucher 500 spécialistes de la cybersécurité.[131]

4.6.8 L'Autriche prise pour cible

Deux attaques d'espionnage visant l'Autriche ont été rendues publiques ces derniers mois. L'une remontant au début de 2020, qui émanerait d'un acteur étatique, a touché le Ministère autrichien des affaires étrangères. Les détails n'ont pas été divulgués.[132]

A1 Telekom Austria, premier opérateur de téléphonie du pays, a confirmé en juin 2020 avoir subi une cyberattaque, alors qu'un lanceur d'alerte proche de l'entreprise avait prévenu un expert en sécurité.[133] L'opération semble remonter à novembre 2019 déjà et avoir été découverte en décembre. Il aura fallu six mois pour qu'A1 Telekom parvienne à éradiquer définitivement l'infection.[134] Selon A1, les acteurs malveillants n'ont compromis qu'une petite partie de son réseau, la complexité des systèmes ayant permis d'éviter le pire. Les agresseurs étaient manifestement parvenus à pénétrer en profondeur dans les systèmes, en se procurant les droits d'un administrateur local puis ceux d'un administrateur de domaine pour accéder au réseau Windows.[135] A1 affirme que les intrus n'ont pas dérobé de données. Le lanceur d'alerte prétend au contraire que les pirates auraient eu accès à des données sensibles des clients. Enfin, si A1 n'est pas parvenu à déterminer la provenance des agresseurs, le témoin anonyme attribue l'attaque à un acteur étatique chinois, le groupe «Gallium» spécialisé dans l'espionnage d'opérateurs télécom.

---

129 https://www.abc.net.au/news/2020-06-19/china-responds-to-accusation-of-australia-cyber-attack/12375324
130 https://www.homeaffairs.gov.au/cyber-security-subsite/files/2020-cyber-security-strategy-iap-report.pdf
131 https://www.itnews.com.au/news/govt-reveals-135bn-investment-into-cybersecurity-over-next-decade-549856
132 https://www.bbc.com/news/world-europe-50997773
133 https://blog.haschek.at/2020/the-a1-telekom-hack.html
134 https://www.zdnet.com/article/hackers-breached-a1-telekom-austrias-largest-isp/
135 https://www.heise.de/hintergrund/Massiver-Angriff-auf-A1-Telekom-Austria-4775451.html

4.7 Ingénierie sociale et phishing

4.7.1 Phishing

Des systèmes comme Google reCAPTCHA Version 3 ont révolutionné le fonctionnement des CAPTCHA. Un CAPTCHA est un système qui permet à un site Web – avec l'aide de puzzles à compléter ou de lettres distordues à interpréter – d'exclure qu'un robot ne se dissimule derrière le prétendu visiteur. Cette mesure permet par exemple d'éviter qu'un formulaire ne soit rempli automatiquement à de multiples reprises. Les reCAPTCHA facilitent le processus, en invitant simplement les visiteurs à confirmer d'un clic dans la bonne case qu'ils ne sont pas des robots.

Les chercheurs de la société de sécurité Barracuda ont constaté que des cybercriminels utilisaient le système reCAPTCHA de Google pour éviter que leurs attaques ne soient découvertes.[136] Une telle précaution empêche les systèmes automatiques de sécurité vérifiant les liens figurant dans les courriels d'accéder aux pages de phishing et donc de les identifier comme telles. Avantage supplémentaire pour les agresseurs, la présence d'un reCAPTCHA sur leurs sites de phishing est perçue comme une mesure de sécurité par les internautes, qu'elle conforte dans l'illusion de se trouver sur un site légitime. Dans l'attaque observée par Barracuda, les cybercriminels avaient envoyé un courriel comportant en annexe un prétendu message vocal perdu. En cas de clic sur l'annexe, le destinataire était redirigé vers un site Internet ne contenant que le reCAPTCHA. S'il confirmait ne pas être un robot, il aboutissait à une fausse page de connexion à Microsoft.[137]

Des attaques pourvues de CAPTCHA ont également été repérées en Suisse. Elles ne visaient toutefois pas des entreprises locales, mais des systèmes de paiement internationaux utilisés par des citoyens suisses (par ex. PayPal).

Phishing as a Service

Le *cybercrime as a Service* (CaaS) est un concept répandu depuis des années dans tous les domaines de la cybercriminalité. Le Darkweb propose un vaste assortiment d'instruments servant à lancer des cyberattaques. Selon le géant singapourien de la cybersécurité Group-IB, la demande de kits de phishing est en hausse et l'offre aurait doublé par rapport à l'année dernière. Il apparaît encore que de tels produits ont connu une hausse de leur prix. Un kit de phishing inclut tous les composants nécessaires à l'exploitation d'une page malveillante. Amazon, Google, Instagram, Office 365 et PayPal ont été en 2019 les cibles favorites des opérations de phishing. Autrement dit, les kits de phishing les plus recherchés sont ceux s'en prenant à des marques réputées et possédant une vaste clientèle. De tels outils prêts à l'emploi sont vendus à des cybercriminels aux connaissances techniques limitées, à qui ils permettent de multiplier à l'infini les sites de phishing.[138]

---

136 https://blog.barracuda.com/2020/04/30/threat-spotlight-malicious-recaptcha/

137 https://hotforsecurity.bitdefender.com/blog/cybercriminal-are-using-google-recaptcha-to-hide-their-phishing-attacks-23156.html

138 https://securityaffairs.co/wordpress/101616/cyber-crime/underground-market-phishing-kits.html

Situation en Suisse

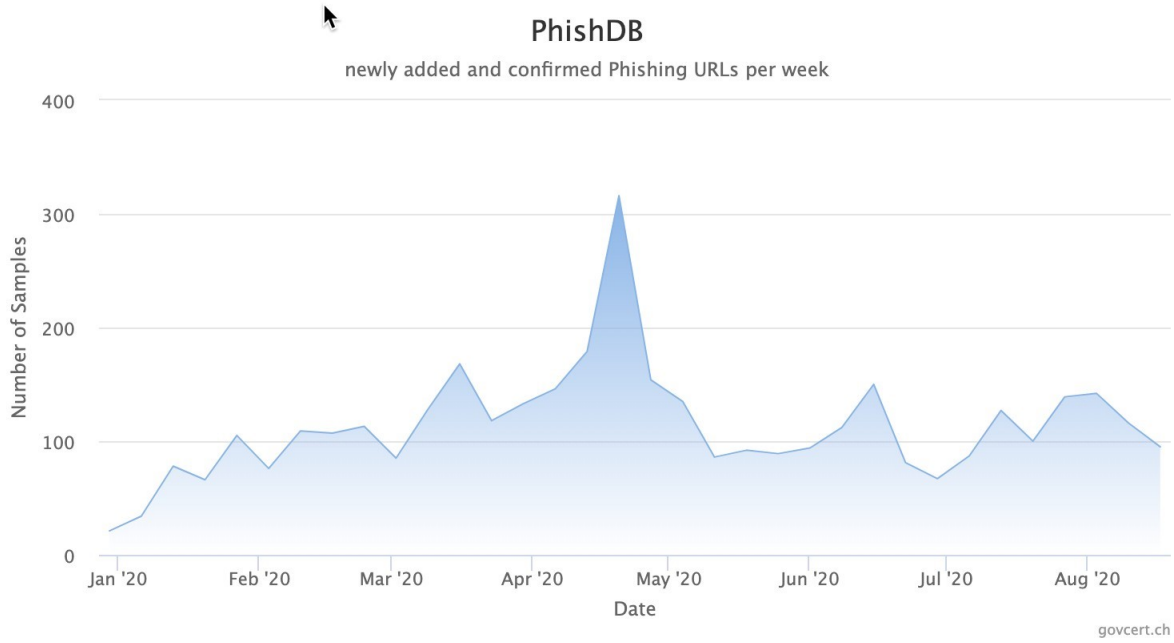

Fig. 7: Nombre de sites de phishing signalés et confirmés chaque semaine sur antiphishing.ch au premier semestre 2020.

Au premier semestre 2020, quelque 3029 cas avérés de pages de phishing ont été signalés sur le portail antiphishing.ch, géré par le NCSC. La figure 7 indique le nombre de sites signalés par semaine au premier semestre 2020.

À partir d'avril 2020, le NCSC a enregistré une forte hausse des attaques de phishing visant les exploitants de sites Web et les propriétaires de domaines. Des cybercriminels leur expédiaient des courriels censés émaner du fournisseur d'hébergement, afin de se procurer les données d'accès servant à l'administration de leurs sites. La plupart des courriels renfermaient un lien personnel qui aboutissait, par le biais d'une page infectée, à la page finale de phishing. Le nom de domaine et/ou le nom du fournisseur d'hébergement y étaient préenregistrés, et la victime était priée d'indiquer ses données d'accès.

Recommandations :

INFO

Le GovCERT a publié sur son blog un article (en anglais) décrivant en détail les attaques lancées contre les administrateurs de sites, avec des recommandations générales aux utilisateurs et des conseils spécifiques aux fournisseurs d'hébergement.

4.7.2 Usurpation d'identité (spoofing)

Le spoofing (de l'anglais *to spoof* = tromper ou falsifier) est une technique de piratage informatique qui consiste à usurper une identité, notamment en modifiant des éléments d'adressage, à l'instar de l'adresse électronique de l'expéditeur ou de son numéro de téléphone;

l'adresse Internet, l'adresse IP, l'adresse MAC (*medium access control*) ou les messages ARP (*address resolution protocol*) peuvent également être truqués.[139] L'usurpation d'identité sert à inspirer confiance au destinataire pour l'amener à un comportement spécifique. Il s'agit en ce sens d'une technique d'ingénierie sociale.

Les méthodes d'usurpation d'identité sont continuellement peaufinées, au gré des nouvelles possibilités numériques. De telles pratiques sont par conséquent très répandues, malgré les mesures de protection existantes. Les acteurs criminels ou étatiques déploient avec succès toutes sortes de méthodes d'usurpation d'identité, dans des contextes différents. À cet effet, ils falsifient l'adresse électronique, le numéro de téléphone, l'expéditeur des SMS, le logo et la raison sociale des entreprises, en misant sur la confiance humaine et le besoin d'information des destinataires. Pendant la pandémie de COVID-19, des maliciels ont ainsi été envoyés à la population suisse dans des courriels censés émaner de l'Office fédéral de la santé publique (OFSP), cf. chap. 3.1.1.

Usurpation d'adresse électronique : il est aisé d'usurper une adresse électronique, car le protocole SMTP (*Simple Mail Transfer Protocol*) ne vérifie pas l'adresse de l'expéditeur. Si un serveur de messagerie dépourvu de toute protection est pleinement accessible par Internet, n'importe quel utilisateur pourra s'y connecter afin d'expédier des messages. Le nom d'expéditeur à afficher peut être librement choisi. Au cas où aucune restriction n'aurait été configurée sur le serveur de messagerie, l'adresse de l'expéditeur pourra être définie librement et contenir un nom de domaine dépourvu de tout lien avec le serveur, par exemple comptabilite@ncsc.ch.

Des mesures techniques de protection sont toutefois possibles :

- Le protocole d'authentification de l'expéditeur SPF (*sender policy framework*) permet de préciser quels serveurs sont autorisés à envoyer des courriels en utilisant un domaine spécifique. Les serveurs d'envoi, de relais ou de réception peuvent vérifier les courriels au moyen de SPF, et les filtrer le cas échéant.

- Le protocole d'authentification du nom de domaine DKIM (*DomainKeys Identified Mail*) ajoute à un courriel une signature numérique permettant au système qui le reçoit de vérifier l'authenticité du domaine expéditeur et d'avoir, le cas échéant, la certitude de l'intégrité du message. Si la vérification n'est pas concluante, le courriel ne sera pas accepté.

- Le protocole DMARC (*Domain-based Message Authentication, Reporting and Conformance*), reposant à la fois sur l'authentification de l'expéditeur (SPF) et sur la vérification de l'intégrité (DKIM), requiert un contrôle de signature.

Usurpation de numéro de téléphone ou d'expéditeur de SMS : à l'ère de la téléphonie par Internet (*Voice over IP*, VoIP), il est aisé de falsifier ou de dissimuler son numéro de téléphone. Il existe même un marché de services proposant de truquer le numéro d'appel (*caller ID spoofing*). Il est également possible d'envoyer des SMS par Internet. Comme l'opération ne s'effectue pas à partir d'un téléphone mobile, certains services permettent de choisir librement le numéro s'affichant sur l'écran du destinataire. Des initiatives internationales cherchent bien à

[139] Voir par ex. https://www.cybersecurityintelligence.com/blog/beware-spoofing-attacks-4890.html

interdire l'usurpation des numéros d'appel.[140] Or à l'heure actuelle, aucune mesure technique couvrant l'ensemble des fournisseurs n'est à même d'empêcher ce fléau. L'introduction d'une norme en la matière prendra encore du temps. Dans de nombreux pays, dont la Suisse, l'usurpation de numéros d'appel ne fait pas l'objet d'une interdiction pénale et seul la personne dont l'identité a été usurpé peut agir en justice (droit privé) contre l'envoi de ces messages. Le projet de révision de la loi sur la protection des données prévoit toutefois l'introduction dans le code pénal d'une disposition réprimant le vol d'identité, et donc aussi certaines formes d'usurpation de numéros d'appel.

Usurpation de sites Web: il est possible de copier des sites Internet afin de les publier sous une autre adresse. Les contrefaçons de sites vont jusqu'à reprendre des logos originaux pour mieux faire illusion. Si les visiteurs ne contrôlent pas le nom de domaine indiqué à la ligne d'adresse et ne remarquent pas l'absence de certificat ou l'usage d'un faux certificat, ils risquent de se faire piéger par de tels sites. Les escrocs enregistrent souvent des noms de domaine proches à s'y méprendre de l'adresse originale (*typo domain*), comme «svvisscom.ch» au lieu de «swisscom.ch». Des noms de domaine trompeurs apparaissent également dans des courriels, où ils serviront par exemple à du phishing, à des escroqueries ou à la diffusion de maliciels.

Divers agresseurs combinent avec succès plusieurs méthodes d'usurpation d'identité. Ainsi, le groupe «Retefe» appelle ses victimes à partir de faux numéros, afin de les persuader sous un quelconque prétexte d'ouvrir un fichier PDF qui leur est envoyé par courriel pendant la conversation téléphonique ou après (cf. chap. 4.7.4). Si la victime clique sur l'hyperlien, le cheval de Troie bancaire «Retefe» infectera son ordinateur. Afin de protéger les entreprises suisses et la population, le NCSC met à la disposition des fournisseurs d'accès à Internet les informations nécessaires afin qu'ils puissent bloquer les tentatives de leurs clients d'accéder aux sites sur lesquels «Retefe» est diffusé. Pour dissimuler leurs liens malveillants, les escrocs utilisent souvent des raccourcisseurs d'URL (*shortener services*), par exemple les outils bit.ly ou goo.gl.

Précision / Recommandation :

Il est possible de falsifier l'adresse de l'expéditeur de n'importe quel message.

Si vous recevez des messages inédits ou insolites, un certain scepticisme est de mise. Au lieu de suivre les liens de tels messages, vous devriez autant que possible vous connecter à votre compte d'utilisateur par la méthode habituelle. Vérifiez toujours que vous êtes bien sur la page souhaitée, avant d'y saisir des données personnelles, des mots de passe ou des informations concernant votre carte de crédit.

Ne cliquez jamais sur les liens de courriels suspects – même par curiosité. Vous risquez sinon d'infecter votre appareil avec un maliciel, ou d'aboutir à des sites louches. En cas de doute sur l'authenticité du message, adressez-vous à l'entreprise concernée, par un des canaux indiqués sur son site ou par l'intermédiaire des contacts connus de vous, pour savoir de quoi il s'agit et si le message vient véritablement d'elle.

[140] Par ex. "STIR/SHAKEN", voir https://www.metaswitch.com/knowledge-center/reference/what-is-stir/shaken.

4.7.3 Phishing par SMS (smishing)

Le terme smishing est issu de la contraction des termes SMS et phishing. Le smishing désigne de façon générale l'utilisation de messages courts, mais aussi toujours plus celui d'applications de messagerie instantanée comme WhatsApp, comme vecteur d'attaque pour dérober des informations sensibles à l'instar des données d'accès, des mots de passe ou des informations concernant une carte de crédit ou un compte bancaire. Bien souvent, le numéro et le nom de l'appelant sont falsifiés (voir chap. 4.7.2 sur l'usurpation d'identité ou spoofing). Les escrocs recourent notamment au smishing dans le contexte des services de paiement mobile, afin de s'emparer du code *mTAN* ou de contourner l'authentification à deux facteurs, par exemple avec un cheval de Troie spécial (*SMS Stealer*). Une combinaison de techniques d'ingénierie sociale a été observée en Suisse comme à l'étranger : un message court priait les victimes de transférer un code d'authentification qu'elles venaient de recevoir par SMS, sous prétexte qu'il s'agissait d'un envoi par erreur ou que la situation était vraiment urgente. Une telle méthode permet en théorie de compromettre tous les services protégés par l'authentification à deux facteurs, si un agresseur a déjà connaissance de l'identifiant, du mot de passe et du numéro de téléphone de la victime. Dans le cas de WhatsApp, les réglages par défaut font qu'un escroc disposant d'un tel code d'authentification peut prendre le contrôle de n'importe quel compte d'utilisateur.[141]

Au premier semestre 2020, les escrocs s'en sont pris aux services de paiement de la téléphonie mobile. De tels services permettent de payer les factures par téléphone. Le prestataire de services envoie à cet effet au téléphone mobile un code SMS, qui doit être inscrit pour confirmation sur son site Web. Dans un cas d'espèce, les escrocs faisaient croire à la victime qu'un paquet n'avait pas pu lui être remis. Pour que la livraison puisse se faire, elle devait indiquer son numéro de téléphone, puis télécharger une application. Or il s'agissait d'un cheval de Troie spécial (*SMS Stealer*). Les pirates effectuaient ensuite des paiements à partir du numéro de téléphone mobile de la victime, et l'application leur transmettait directement le code de confirmation nécessaire.

On observe par ailleurs, dans un nombre croissant de cas, la diffusion par SMS de liens vers des maliciels comme «Emotet» ou «EventBot» afin de dérober des données d'accès aux applications e-banking ou financières.[142] Dans le contexte du smishing, le nom de l'expéditeur est falsifié et toutes les techniques de l'ingénierie sociale sont déployées, afin d'amener les personnes visées à adopter un comportement donné. Les pirates se réfèrent notamment aux événements actuels et à leurs retombées, à l'instar de la pandémie de COVID-19 : en mars 2020, les autorités sud-coréennes ont par exemple mis en garde contre les attaques de smishing. Quelque 10 000 messages censés provenir d'entreprises et portant sur la remise gratuite de masques de protection avaient été expédiés à la mi-février.[143]

---

[141] Voir aussi https://www.20min.ch/story/mit-diesem-code-bist-du-dein-whatsapp-8203-8203-konto-los-252382069481 et https://www.mimikama.at/allgemein/vorsicht-wenn-ein-whatsapp-kontakt-einen-verifizierungscode-verlangt/

[142] Voir à propos d'«EventBot» https://www.zdnet.de/88379272/cybereason-warnt-vor-neuem-mobilen-banking-trojaner/; pour «Emotet», voir https://threatpost.com/sms-attack-spreads-emotet-bank-credentials/153015/.

[143] https://www.zdnet.com/article/south-korea-sees-rise-in-smishing-with-coronavirus-misinformation/

Les attaques de smishing constituent une menace croissante, pour les particuliers comme pour les entreprises: aux États-Unis, le phishing par le canal de la téléphonie mobile a bondi de 37 % au premier trimestre 2020.[144] Les cas rendus publics en Suisse restent peu nombreux : seuls 16 cas de smishing avaient été signalés au NCSC jusqu'en juillet 2020. Il est vrai que presque la moitié se sont produits en juin, et que le NCSC s'attend à une hausse de ce phénomène au deuxième semestre.

Des arnaques sévissent déjà en Suisse par le canal des SMS ou services de messagerie : des messages censés émaner d'entreprises suisses connues comme Coop, Migros ou la Poste faisaient s'abonner à de coûteux services à valeur ajoutée les victimes qui croyaient participer à un tirage au sort ou compléter un bon d'achat gracieusement offert (cf. chap 3.1.3).

Précision / Recommandations :

Il est possible de falsifier l'adresse de l'expéditeur de n'importe quel message.

Des méthodes de filtrage très efficaces ont été conçues au fil des ans pour permettre aux infrastructures de messagerie de trier les pourriels. Or cette technologie ne convient pas aux SMS. Il n'est pas possible d'introduire un tel mécanisme pour les services de messagerie comme WhatsApp ou Threema, sachant que les messages sont acheminés sous forme chiffrée de l'expéditeur au destinataire et qu'aucun intermédiaire ne peut en vérifier le contenu.

Ne cliquez jamais sur les liens de courriels suspects – même par curiosité. Vous risquez sinon d'infecter votre appareil avec un maliciel, ou d'aboutir à des sites louches. En cas de doute sur l'authenticité du message, adressez-vous à l'entreprise concernée, par un des canaux indiqués sur son site ou par l'intermédiaire des contacts connus de vous, pour savoir de quoi il s'agit et si le message vient véritablement d'elle.

Vérifiez toujours, avant d'inscrire vos données personnelles, votre mot de passe ou les informations de votre carte de crédit, que vous êtes bel et bien sur le site recherché.

4.7.4 Envoi de maliciels après un appel téléphonique

Les escrocs ne ménagent pas leur peine pour installer des maliciels chez une victime, comme le montrent les cas signalés à 64 reprises et dans différentes variantes au NCSC au premier semestre 2020. Dans toutes les variantes, la victime avait reçu en plus du courriel un appel téléphonique. Tantôt les pirates commençaient par un téléphone annonçant un courriel renfermant un document PDF, tantôt ils prenaient contact après coup avec la victime pour attirer son attention sur le courriel envoyé, afin qu'elle ouvre l'annexe et clique sur le lien renfermé. Le maliciel s'installait lors du clic sur l'hyperlien.

La raison sociale indiquée au téléphone était souvent CH-Express, Delivery Experts ou Delivery Suisse, et l'entreprise s'annonçait comme service de distribution. Les destinataires étaient fréquemment des PME, comme des bureaux d'architecture, des entreprises horticoles ou des menuiseries. Il était question de leur remettre une demande de devis. Dans d'autres cas, les pirates se faisaient passer pour une haute école et utilisaient pour l'envoi de leurs courriels un nom de domaine ressemblant à s'y méprendre à celui de la haute école (*typo domain*). Par la suite, ils se sont également adressés à des particuliers.

144 https://blog.lookout.com/global-mobile-phishing-encounters-surged-by-37-percent-amid-wfh-shift

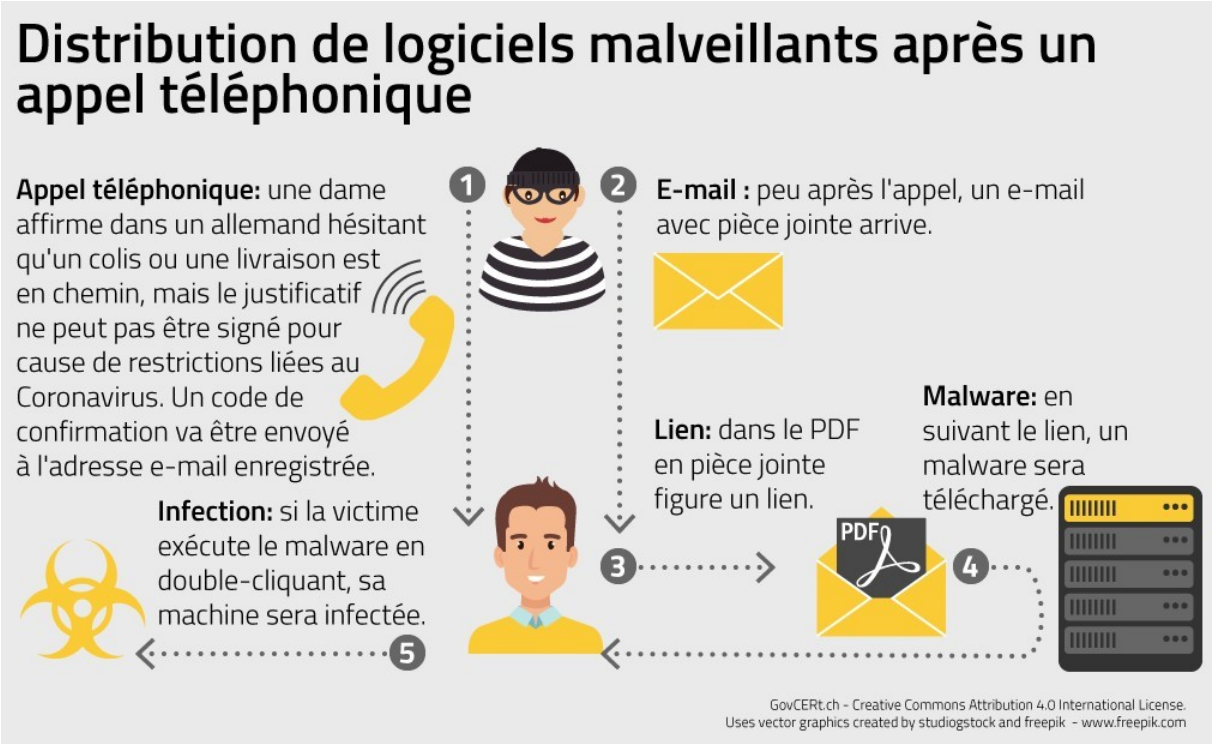

Fig. 8: Étapes d'une infection par le cheval de Troie «Retefe». Le scénario utilisé pour l'appel peut varier à l'infini.

La pandémie actuelle a aussi été invoquée pour convaincre les victimes d'installer un maliciel. Les escrocs expliquaient qu'en raison du risque d'infection, il n'était pas possible de confirmer par signature la livraison d'un paquet. À la place, le destinataire allait recevoir par courriel le code de confirmation à communiquer au service de transport. Là encore, l'auteur de l'appel téléphonique faisait croire que le code figurait dans le fichier PDF annexé au courriel, sur lequel il suffisait de cliquer (cf. chap. 4.7.2 sur le spoofing).

Des informations détaillées sont publiées sur le site cybercrimepolice.ch.[145]

Conclusion / Recommandations :

Il est étonnant que les pirates prennent la peine de téléphoner personnellement à leurs victimes. Ils n'arrivent apparemment plus aussi facilement à installer un maliciel sur un appareil, ce qui les a conduits à déployer ce surcroît d'efforts. Autre sujet d'étonnement, le lien malveillant ne se trouve pas directement dans le courriel, mais dans le fichier PDF annexé. Il paraît douteux que cela soit une bonne idée, et cette solution risque d'être contre-productive. Outre que l'attaque devient plus compliquée, la victime a le temps de s'interroger sur la plausibilité du scénario échafaudé. Bien des victimes se sont méfiées après avoir ouvert le fichier PDF et en sont restées là. La prudence est plus que jamais requise lors de l'ouverture de liens et d'annexes, et il ne faudrait jamais se laisser dicter sa conduite par des inconnus.

145 https://www.cybercrimepolice.ch/de/fall/online-betrueger-aufforderung-packetsendung-freischalten-nicht-nur-per-mail-sondern-neu-auch-per-telefon/

4.7.5 Chantage contre les exploitants de sites Web

Durant la période sous revue, de nombreux exploitants de sites Web ont reçu des courriels leur annonçant que leur site avait été piraté grâce à une faille de sécurité et que toute leur base de données avait été pillée.[146] Les maîtres chanteurs menaçaient d'en informer leur clientèle, de publier ou de vendre les données dérobées, et ainsi de ternir la réputation de la victime, à moins qu'elle ne s'acquitte d'une rançon en bitcoins. Les courriels étaient rédigés en anglais ou en allemand. Dans un cas d'espèce, le cybercriminel affirmait que sa prétendue attaque avait été commanditée par une entreprise concurrente, à des fins de sabotage. En voulant marchander sur le prix initialement convenu, le mandant avait toutefois indisposé l'expéditeur, qui avait alors choisi de prendre contact avec la victime pour lui proposer de lui restituer les données dérobées, moyennant un dédommagement conséquent. Cette variante signalait, comme moyen de pression supplémentaire, les problèmes juridiques auxquels la victime s'exposait pour avoir enfreint le règlement européen sur la protection des données (RGPD). Voir aussi le chap. 4.5 consacré aux fuites de données).

Dans cette escroquerie, les cybercriminels jouent sur la peur des conséquences d'une éventuelle fuite de données, en espérant amener ainsi les exploitants de sites Web à leur verser la rançon demandée. En réalité, les sites Web n'ont pas été compromis, du moins pas dans les cas portés à la connaissance du NCSC. Ces courriels rappellent à bien des égards les vagues de faux messages de sextortion, dont plusieurs autres rapports semestriels ont déjà parlé. Les escrocs y affirment avoir piraté la caméra de l'ordinateur de la victime et l'avoir surprise en train de consommer de la pornographie.[147] Dans de tels cas non plus, les ordinateurs n'avaient pas subi d'attaque et les cybercriminels ne possédaient pas de matériel susceptible de causer du tort à la personne rackettée. Les escrocs avaient toutefois tiré parti des méthodes d'ingénierie sociale afin d'amener malgré tout la victime à s'acquitter d'un montant donné en bitcoins.

Recommandations :

Gardez votre calme si vous recevez une lettre de chantage. Ne cédez pas aux pressions. Les menaces sont souvent infondées et envoyées à un grand nombre de personnes, dans l'espoir que quelques-uns des destinataires se laissent intimider et paient à la légère. Les tentatives de chantage sont punissables et peuvent être dénoncées à la police.

Si vous avez des indices montrant que les allégations pourraient être vraies, annoncez-vous immédiatement au poste de police le plus proche (voir https://polizei.ch/fr), afin que des poursuites puissent être ouvertes à l'égard de leurs auteurs.

146 https://www.watchlist-internet.at/news/website-betreiberinnen-aufgepasst-erpressungsmails-im-umlauf/

147 Voir MELANI, rapports semestriels 2018/2, chap. 4.4.2 et 2019/2, chap. 4.4.3; Site web MELANI: https://www.melani.admin.ch/melani/fr/home/meldeformular/formular0/meldeformularhaeufigefragen/FakeSextortion.html.

4.8 Mesures préventives et poursuites pénales

4.8.1 Mise en accusation d'un hébergeur allemand «à l'épreuve des balles»

Les hébergeurs «à l'épreuve des balles» (*bulletproof hosting*) sont des centres de données situés hors d'atteinte des autorités – et donc à l'abri des enquêtes de police. Ils sont souvent implantés dans des pays dont la justice ne fonctionne pas comme elle devrait ou, au moment de leur raccordement administratif et technique à Internet, des indications mensongères et la présence d'hommes de paille auront servi à dissimuler leur emplacement exact. L'hébergement «à l'épreuve des balles» est utilisé par de multiples formes de criminalité.

Les autorités allemandes ont réussi l'automne dernier, après quatre ans de travail d'enquête, un coup de filet contre un hébergeur qui, des années durant, avait sévi en Allemagne à partir d'un ancien bunker de l'OTAN, mettant sa plateforme à la disposition de nombreux cybercriminels. Les serveurs de ce cyberbunker hébergeaient notamment la place du marché de la drogue «Wall Street Market» ou le marché clandestin «Flugsvamp», où se concentraient 90 % des activités suédoises de trafic en ligne de stupéfiants, et ont servi au pilotage du réseau de zombies «Mirai». En automne 2019, plus de 700 agents de police ont perquisitionné le périmètre du bunker installé près de Traben-Trarbach, et ont retiré du réseau plus de 800 serveurs. Le ministère public régional a dressé l'acte d'accusation contre huit personnes pour aide à la commission de multiples infractions (recel de données, attaques par réseau de zombies, trafic de drogue, etc.). Des liens à la pornographie infantile et à des meurtres commandités ont également été établis. Il a fallu traiter dans cette procédure complexe un volume total de données de deux pétaoctets, qui a poussé les enquêteurs aux limites de leurs capacités.

Pour qu'il y ait complicité en droit allemand, il faut toujours une infraction principale. Autrement dit, les enquêteurs ont d'abord dû élucider les délits commis à l'aide des sites Web hébergés dans le cyberbunker. Il leur a en particulier fallu accéder au système de messagerie interne où s'effectuait la communication entre l'hébergeur et ses clients. C'est sur cette base qu'ils ont pu prouver que loin d'être de simples prestataires techniques dont la responsabilité n'aurait pas été engagée, les accusés avaient délibérément participé aux infractions commises et partant, qu'ils s'étaient rendus coupables de complicité.[148]

4.8.2 Arrestation de cybercriminels par les autorités suisses

Les autorités de poursuite pénale suisses et polonaises ont démantelé en avril 2020, avec l'aide d'Europol, un groupe dénommé «InfinityBlack». Ce groupe de cybercriminels était actif dans la diffusion de données d'utilisateurs dérobées, dans la création et la propagation de maliciels ou d'outils de piratage, ainsi que dans des fraudes diverses.

La police a confisqué du matériel électronique, des disques durs externes et des portefeuilles de cryptomonnaies , pour une valeur de 100 000 euros. La police a également saisi et fermé deux plateformes, dont les bases de données renfermaient plus de 170 millions d'entrées.

Le modèle d'affaires du groupe de pirates consistait à créer des plateformes en ligne pour la revente de listes de milliers de «combos» (binôme identifiant/mot de passe). Le groupe était

[148] https://www.heise.de/newsticker/meldung/Cyberbunker-Staatsanwaltschaft-erhebt-Anklage-gegen-Betreiber-4698785.html

organisé de manière rationnelle en trois équipes bien définies. Les développeurs créaient des outils servant à tester la qualité des bases de données dérobées, tandis que les testeurs analysaient la validité des données d'accès. Enfin, les responsables de projet revendaient les données volées, en se faisant payer en cryptomonnaie. Les pirates ont ainsi eu accès à un grand nombre de comptes de clients suisses. Bien que le préjudice ait été estimé à un peu plus de 50 000 francs seulement, les escrocs auraient pu dérober un montant potentiel de 650 000 francs. Leur principale source de revenus consistait à subtiliser les données d'accès au programme de fidélisation d'un grand distributeur suisse pour les revendre à d'autres groupes criminels moins avancés techniquement. Ces derniers échangeaient les bons de fidélités contre de coûteux appareils électroniques. Les escrocs et les cyberpirates, dont des mineurs et de jeunes adultes, ont été démasqués en cherchant à échanger dans des commerces helvétiques les points volés contre de la marchandise. Après avoir arrêté les malfrats, la police a découvert des liens avec un groupe de cyberpirates basé en Pologne. Les données des ordinateurs analysés ont donc été transmises aux autorités polonaises et ont permis au bout du compte l'arrestation sur sol polonais de membres présumés du groupe «InfinityBlack».[149]

5 Recherche et développement

5.1 SCION: une architecture Internet plus rapide et sûre

Ilona Wettstein, Adrian Perrig, ETH Zürich, Network Security Group

Un Internet plus sûr s'avère indispensable, en réponse à la transformation numérique croissante de tous les secteurs du quotidien et de l'activité économique. Chaque jour, des milliards de personnes veulent pouvoir expédier des données sans qu'elles se perdent, soient détournées ou analysées en route. La performance ne doit pas pour autant en pâtir, et donc les mécanismes de sécurité ne doivent ni réduire la capacité du réseau ni occasionner de retard supplémentaire dans la transmission des données.

149 https://www.europol.europa.eu/newsroom/news/hacker-group-selling-databases-millions-of-user-credentials-busted-in-poland-and-switzerland ; https://www.blick.ch/news/cyberkriminalitaet-treuepunkte-hacker-nach-polizeioperation-in-waadt-in-polen-gefasst-id15877097.html; https://www.watson.ch/!158091108

Internet repose sur un protocole de passerelle frontière (*Border Gateway Protocol*, BGP) qui achemine les paquets de données d'une manière quasiment inchangée depuis 30 ans. Ce protocole décide à chaque nœud de réseau du chemin qu'un paquet de données va emprunter. Or la forte expansion d'Internet a mis en lumière ses nombreux points faibles, et Internet vacille toujours plus sur ses fondations : le trafic de données est détourné par des acteurs étatiques ou criminels, qui sont à même de l'espionner ou de l'interrompre.

SCION est une architecture Internet résolument nouvelle.[150] Son nom signifie «**S**calability, **C**ontrol and **I**solation **O**n **N**ext-Generation Networks». Mise au point par l'ETH Zürich, elle remplace BGP par un protocole plus sûr et plus efficace, et résout beaucoup d'autres problèmes liés à l'Internet actuel, comme les faux certificats de sécurité ou les attaques DDoS (*distributed denial of service attack*). À la différence de l'Internet en place, où toutes les décisions de routage sont du ressort des nœuds du réseau, SCION rend le routage transparent et permet aux utilisateurs de contrôler les chemins réseau. Comme l'itinéraire d'acheminement est fixé dès le stade de l'envoi, les paquets de données ne risquent pas de faire fausse route. En outre, cette approche reposant sur un choix intelligent de l'itinéraire permet d'optimiser la vitesse de transmission. Il suffit de quelques millisecondes à SCION pour changer de route, au cas où la communication serait entravée.

Les hautes écoles suisses et plusieurs banques tirent déjà parti de la nouvelle architecture. Une liaison établie par SCION offre plusieurs avantages de poids:

- Communication garantie et souveraineté dans Internet : ni les attaques lancées depuis l'étranger ni un quelconque acteur ne peuvent empêcher la communication (pas de coupure de connexion de type *kill switch*);
- Possibilité de restreindre le trafic des données sur le plan organisationnel ou géographique. Cela évite que des informations confidentielles ne transitent par des réseaux non approuvés;
- Établissement de plusieurs liaisons simultanées pour optimiser la communication et accroître la fiabilité du réseau même en cas de panne locale (continuité des activités);
- Capacités accrues, grâce à l'utilisation de plusieurs chemins réseau.

L'Internet de la prochaine génération sera non seulement plus sûr, mais plus performant aussi. Plusieurs opérateurs formant un consortium seront à la fois intégrateurs et fournisseurs de connexions, en Suisse comme à l'étranger. La commercialisation et la mise en place de SCION incombent à Anapaya Systems, spin-off de l'ETH Zürich.[151]

6 Perspectives et tendances actuelles

6.1 Travailler partout – et plus seulement au bureau

Comme l'explique le thème prioritaire de ce rapport (chap. 3.5), le monde du travail a radicalement changé, pour les employés de bureau notamment. Bien des gens ont eu la possibilité ou l'obligation de travailler de chez eux (*home office*). Beaucoup d'entreprises et de salariés

150 https://www.scion-architecture.net/

151 https://www.anapaya.net/

se sont ainsi familiarisés avec le télétravail ou d'autres modèles dans lesquels le travail s'effectue non plus au bureau, mais depuis n'importe où. Par conséquent, le travail mobile tend à être toujours mieux accepté – quand son introduction n'est pas réclamée. Il est trop tôt pour dire quand la pandémie actuelle prendra fin et la vie reprendra son cours normal. Mais il ne faut pas oublier qu'un retour à la situation d'avant la pandémie n'est peut-être ni possible ni souhaitable. Si quelques entreprises se sont dotées depuis longtemps d'une infrastructure stable et sécurisée propice au nomadisme numérique, d'autres ne disposent que de solutions installées à la hâte et plutôt improvisées. Il vaut donc la peine de profiter dès à présent des expériences réalisées et de contrôler les solutions utilisées, afin de les améliorer ou de lancer un projet de refonte complète pour intégrer dès la phase de conception, outre les capacités des infrastructures, la sécurité des appareils, des réseaux ainsi que des données (*security by design*).

Les infrastructures d'accès à distance constituent un vecteur d'attaque pour quiconque cherche à compromettre le réseau des entreprises. D'où la nécessité d'une configuration sûre et d'une protection adéquate des connexions VPN ou RDP. Depuis quelque temps déjà, des acteurs passent Internet au crible pour identifier des solutions d'accès à distance mal configurées. Ces activités de reconnaissance se sont intensifiées au moment précis où en raison de la pandémie, les solutions d'accès à distance gagnaient en popularité (voir chap. 3.5). Le moindre système vulnérable finira tôt ou tard par être détecté et attaqué. En particulier, les pirates peuvent déployer par l'accès à distance un rançongiciel dans le réseau d'une entreprise (voir chap. 4.1.1 sur les rançongiciels et chap. 4.4 sur les vulnérabilités).

Les plateformes collaboratives dans le cloud et les logiciels de conférence sont d'importants outils de travail indépendants du lieu. Là encore, il faut opter pour des configurations sûres et apprendre aux collaborateurs à utiliser correctement de tels instruments.

Le travail effectué sur du matériel électronique privé (*bring your own device*, BYOD) dont le service informatique interne n'assure pas la maintenance limite les possibilités de contrôle de l'employeur sur la sécurité de ses données et confère davantage de responsabilités aux collaborateurs. Pour s'acquitter de manière appropriée de leurs obligations, ils doivent connaître les directives de l'entreprise, qui veillera à les sensibiliser régulièrement aux risques et menaces.

Recommandations :

Étant donné que le travail indépendant du lieu présente de nombreux risques, il faudrait adopter une stratégie claire en la matière, avec un plan complet de mise en œuvre. Outre les mesures techniques de sécurité, il faut également prendre en compte la dimension des utilisateurs, dont le comportement peut contribuer dans une large mesure à la réduction des risques.

DOCU

Inspirez-vous des listes de contrôle de MELANI sur le télétravail:

Entreprises: https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/fernzugriff.html

Utilisateurs: https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/fernzugriff-enduser.html

6.2 Géopolitisation d'Internet

Un coup d'œil aux débuts d'Internet fait découvrir un monde de chercheurs s'intéressant à des questions purement techniques, de bureaux de normalisation et de premiers utilisateurs experts en informatique. Tous ces gens avaient beaucoup de choses en tête, mais la politique internationale de sécurité, la géopolitique et en particulier la politique du pouvoir, les Nations Unies ou la diplomatie n'étaient pas leur souci majeur. L'agence américaine pour les projet de recherche avancée (Advanced Research Projects Agency, ARPA), l'Union internationale des télécommunications (UIT), l'Internet Assigned Numbers Authority (IANA), la Société pour l'attribution des noms de domaine et des numéros sur Internet (ICANN) ou le Conseil européen pour la recherche nucléaire (CERN) basé à Genève ont joué un rôle clé dans la création de l'Internet d'aujourd'hui, dont ils sont encore les gardiens : une infrastructure planétaire qu'en 2020, la plupart des gens considèrent comme acquise et, comme le suggèrent les noms des organisations impliquées, qui se voulait essentiellement un progrès technique en matière de communication et de technologie – et donc qui gagnait à demeurer entre les mains d'experts apolitiques.

Entre-temps, Internet est au cœur de la plupart des avancées économiques ou de politique sociale, à commencer par la transformation numérique. On lui doit par exemple le pilotage à distance des centrales électriques, l'Internet des objets (IoT, Internet of Things) dont il est tant question, l'industrialisation 4.0 et – a fortiori en cette période de coronavirus – le maintien de la productivité grâce au télétravail. Conçu jadis comme une technologie redondante, permettant de partager facilement des informations et d'assurer la continuité des activités même en cas de panne d'un sous-système, Internet est devenu dans le monde entier un passage obligé des processus critiques, dans tous les domaines. Il n'a évidemment pas fallu attendre l'année 2020 pour s'en apercevoir, et la politique internationale de sécurité s'est très tôt intéressée à ce défi. La crise du COVID-19 nous rappelle toutefois à quel point des infrastructures critiques comme les hôpitaux sont vulnérables face aux cyberattaques, en raison du développement de l'interconnexion et de la numérisation.

En 1998, la résolution proposée par la Russie aux Nations Unies sous le titre «Les progrès de la téléinformatique dans le contexte de la sécurité internationale» a fait de la mise en réseau et de la numérisation un enjeu multilatéral de premier plan. Les États membres devaient par la suite s'entretenir régulièrement sur la manière d'empêcher au niveau international tout risque d'abus et d'exploitation des technologies de l'information et de la communication. Les Nations Unies ont ainsi créé en 2004 un premier groupe d'experts gouvernementaux (*Group of Government Experts*, GGE), formé de quinze États membres. Il devait notamment déterminer si ses activités liées aux technologies de l'information et de la communication porteraient aussi sur les contenus ou alors se limiteraient à l'infrastructure sous-jacente aux échanges de contenus. Sans surprise, avec une question aussi controversée à examiner, le mandat du premier GGE ne s'est pas achevé en 2005 sur un rapport de consensus.

Que doit recouvrir la définition des technologies de l'information et de la communication? Qu'entend-on au juste par infrastructure critique? Dans quelle mesure le droit international s'applique-t-il au cyberespace? Toutes ces questions ont servi de fil rouge aux discussions des GGE ultérieurs. Celui de 2015 est notamment parvenu, dans son rapport, à établir pour les États membres des Nations Unies des normes certes juridiquement non contraignantes, mais d'application générale, sur la bonne conduite dans l'usage des technologies de l'information et de la communication. À titre d'exemple, il est interdit de lancer des cyberattaques contre les infrastructures critiques. Le GGE a également confirmé que le droit international s'appliquait au cyberespace. Des efforts similaires sont déployés et des discussions comparables

menées au niveau régional, par exemple au sein de l'Organisation pour la sécurité et la collaboration en Europe (OSCE).

Conçu au départ comme un projet purement technique, destiné à créer des réseaux informatiques résistants et redondants, Internet est devenu du fait de son omniprésence le centre d'intérêts nationaux de politique de sécurité parfois contradictoires. Les avancées au niveau international se font rares, dans le climat international d'aujourd'hui. Il n'y a quasiment plus eu de progrès concret depuis le rapport du GGE de 2015. Celui de 2017 n'a abouti à aucun consensus. Un nouveau GGE a été lancé en 2019. La même année, un groupe de travail à composition non limitée (*Open Ended Working Group*, OEWG) présidé par la Suisse entamait ses délibérations et consultations. Cet engagement essentiellement diplomatique est dans l'intérêt de tout le monde, afin de maintenir sur la bonne voie les divers processus et dialogues. La Suisse a reconnu de longue date la nécessité d'aborder le thème du cyberespace dans son contexte international et de politique de sécurité. Dotée d'une petite économie ouverte et fortement interconnectée, elle a besoin de prévisibilité et d'ordre, dans le contexte international et sur le plan de la politique de sécurité. Aussi la Suisse a-t-elle fait partie des GGE de 2017 et 2019, de l'OEWG et joue-t-elle encore un rôle actif dans l'élaboration, au sein de l'OSCE, de normes et mesures destinées à renforcer la confiance. Avec la Genève internationale, la Suisse était d'ailleurs prédestinée à mener les débats sur la transformation numérique, le cyberespace et sa gouvernance. Elle a déjà des réalisations concrètes à son actif, à l'instar du «Geneva Dialogue on Responsible Behavior in Cyberspace», lancé en 2018 par la Suisse et qui s'est poursuivi fructueusement en 2020, avec de nombreux représentants internationaux de l'économie. Une douzaine de rencontres virtuelles ont servi à développer, dans le domaine de la cybersécurité, de bonnes pratiques qui reflètent un consensus mondial entre les géants mondiaux de l'informatique et les secteurs d'activité fortement dépendants de l'informatique. Autrement dit, la Suisse contribue largement à la concrétisation des normes et principes internationaux en vigueur dans le cyberespace, à l'instar des normes et principes des GGE ou des principes du «Paris Call for Trust and Security in Cyberspace».[152] Genève parvient ici à affirmer son rôle central dans la mise en place d'une gouvernance mondiale du numérique et des nouvelles technologies.

7 Produits publiés par MELANI

7.1 GovCERT.ch Blog (en anglais)

7.1.1 Analysis of an Unusual HawkEye Sample

20.02.2020 - Currently, we are observing HawkEye samples being distributed by large malspam waves. HawkEye is a keylogger which has been around quite a long time (since 2013) and has evolved since then and gained more functionality. There are several good blog posts about HawkEye in general. Recently we observed an interesting obfuscation method in a HawkEye binary, which we are going to describe in this blog post.

https://www.govcert.admin.ch/blog/analysis-of-an-unusual-hawkeye-sample/

[152] https://pariscall.international/fr/

7.1.2 Phishing Attackers Targeting Webmasters

22.04.2020 - Since the beginning of April 2020, we are seeing an increase in phishing attacks against webmasters and domain owners in Switzerland. Unknown threat actors are phishing for credentials for accounts on web admin panels of at least three major hosting providers in Switzerland.

➔ https://www.govcert.admin.ch/blog/phishing-attackers-targeting-webmasters/

7.2 MELANI Newsletter

7.2.1 Prudence: un nombre croissant de PME victimes de rançongiciels

19.02.2020 - Ces dernières semaines, MELANI / GovCERT a traité plus d'une douzaine de cas d'attaques impliquant des rançongiciels: des escrocs non identifiés verrouillent les systèmes de PME et de grandes entreprises suisses, les rendant inutilisables, puis exigent une rançon de plusieurs dizaines de milliers de francs, voire parfois de plusieurs millions.

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

7.2.2 Mise en garde contre des courriels envoyés frauduleusement au nom de l'OFSP

14.03.2020 - Depuis le vendredi 13 mars 2020 à midi, des cybercriminels essaient de tirer parti de l'incertitude dans laquelle vit la population en raison de la situation concernant le coronavirus. Ils usurpent le nom de l'Office fédéral de la santé publique (OFSP) pour tenter de propager un maliciel par courriel. La Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) met la population en garde contre de tels courriels, qu'il faut effacer immédiatement.

➔ https://www.melani.admin.ch/melani/fr/home/documentation/lettre-d-information/gefaelschte-emails-im-namen-des-bag.html

7.2.3 Vulnérabilité critique dans Microsoft Windows Server (SIGRed)

15.07.2020 - Mardi soir dernier (14 juillet 2020), Microsoft a publié une mise à jour de sécurité concernant une vulnérabilité critique dans le système de noms de domaine Windows (winDNS). Microsoft évalue la vulnérabilité à 10.0 points CVSS (Common Vulnerability Scoring System), qui est le maximum sur l'échelle disponible.

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

7.2.4 Le cheval de Troie Emotet est de nouveau actif

23.07.2020 - La Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI a observé de nouveau différentes vagues d'e-mails malveillants avec des documents Word en pièce jointe. Ces vagues contiennent le maliciel Emotet, connu depuis longtemps et se faisant aussi appeler Heodo. Ce maliciel était originellement un cheval de Troie ciblant le "e-banking".

Actuellement, Emotet est utilisé pour envoyer du spam mais aussi pour télécharger des maliciels supplémentaires.

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

7.3 Listes de contrôle et instructions

7.3.1 Télétravail: Sécuriser son accès à distance

24.03.2020 - Étant donné l'utilisation accrue des solutions d'accès à distance pour le télétravail, il est opportun de rappeler les bonnes pratiques afin de minimiser le risque lié à ces technologies. Nous sommes convaincus que ce dernier augmente avec l'accroissement des différentes connexions à distance. Des attaquants sont informés de cette situation et tentent, par différents moyens, de gagner accès au réseau des organisations.

➔ https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/fernzugriff.html

7.3.2 Télétravail: Recommandations pour l'utilisateur

02.04.2020 - En tant que complément au document "Télétravail: Sécuriser son accès à distance", nous souhaitons mettre à disposition une information brève à destination des utilisateurs finaux. Celle-ci leur permettra de mieux protéger leur infrastructure, et ainsi également réduire le risque pour leur employeur.

➔ https://www.melani.admin.ch/melani/fr/home/documentation/listes-de-controle-et-instructions/fernzugriff-enduser.html

8 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 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.

Dénomination	Description
Authentification à deux facteurs (2FA)	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.
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.
crypto mining (minage)	Utilisation de la puissance de calcul d'un ordinateur pour trouver et valider les nouvelles unités d'une cryptomonnaie, p.ex. Bitcoin.
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.
Defacement	Défiguration de sites Web.

Dénomination	Description
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.
Exploit	Programme, script ou ligne de code utilisant les failles de systèmes informatiques.
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.
Infostealer	Maliciel qui peut récolter des frappes de clavier, des captures d'écran, des activités de réseau et d'autres informations sur les systèmes où il est présent.
Internet des objets	Ensemble des objets branchés à Internet capables de communiquer pour collecter, transmettre et traiter des données, avec ou sans intervention humaine.
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

Dénomination	Description
	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 (crypto mining)	Utilisation de la puissance de calcul d'un ordinateur pour trouver et valider les nouvelles unités d'une cryptomonnaie.
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.
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.

Dénomination	Description
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.
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.

Dénomination	Description
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.
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.
Spyware	Spyware collecte des informations, à l'insu de l'utilisateur, sur ses habitudes en matière de navigation (surf) ou sur les paramètres du système utilisé pour les transmettre à une adresse courriel prédéfinie.

Dénomination	Description
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.
VPN	Virtual Private Network. Réseau privé virtuel. Permet, par le chiffrement du trafic de données, d'établir une communication sécurisée entre ordinateurs à travers un réseau public (p.ex. Internet).

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.