2 novembre 2021 | Centre national pour la cybersécurité NCSC

Rapport semestriel 2021/I (de janvier à juin)

Sécurité de l'information

Situation en Suisse et sur le plan international

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF
Centre national pour la cybersécurité NCSC

1 Vue d’ensemble / Sommaire

Management Summary

Le deuxième rapport semestriel du Centre national pour la cybersécurité (NCSC) traite des principaux cyberincidents du premier semestre de 2021 en Suisse et sur le plan international. Il a pour thème principal les vulnérabilités des systèmes informatiques qui sont susceptibles d'être exploitées à des fins de cyberattaque.

Les vulnérabilités des logiciels et du matériel informatique font une cible de choix pour les escrocs lorsque les composants problématiques ne sont pas rapidement mis à jour au moyen de correctifs. Sonic Wall, PrintNightmare et QNAP NAS sont quelques-unes des failles de sécurité des serveurs MS Exchange qui sont examinées sous le thème principal du rapport.

Développement de la gestion des vulnérabilités

Le NCSC s'attache à développer la gestion des vulnérabilités afin que les failles de sécurité puissent être divulguées de manière coordonnée (*coordinated vulnerability disclosure*) sur une plateforme, et que celles et ceux qui en découvrent puissent le faire savoir anonymement à un service étatique. Il s'emploie aussi à informer le public des failles de sécurité critiques qui ont été décelées et à lui indiquer les mesures de sécurité qui s'imposent. Dans le cadre de la détection des failles de sécurité, au cours du premier semestre de 2021, le NCSC a suivi de près la phase de test de l'infrastructure du certificat COVID et le premier programme pilote de primes aux bogues mené dans l'administration fédérale.

Fréquence plus élevée de certaines escroqueries

La plupart des annonces reçues par le NCSC au cours du premier semestre de 2021 concernaient différents types d'escroquerie, principalement l'arnaque au président, l'arnaque au faux support technique et la fraude aux petites annonces. Actuellement, des escrocs font miroiter d'énormes retours sur investissement dans des cryptomonnaies. Durant la période sous revue, le guichet unique du NCSC a enregistré un total de 10 234 annonces de cyberincident, soit près du double des annonces reçues au premier semestre de 2020. Cette forte augmentation tient d'abord à l'introduction du nouveau formulaire d'annonce du NCSC, qui figure bien en évidence sur sa page d'accueil. Elle trouve cependant aussi son explication dans plusieurs grosses vagues de phishing et de messages de «fake sextorsion».

Hausse des annonces de rançongiciels et de sites de phishing

Le nombre d'incidents impliquant un cheval de Troie qui verrouille les données (rançongiciel) est tout à fait frappant. Il a triplé, passant de 32 cas au premier semestre de 2020 à 94 cas durant la période sous revue. Cette augmentation est avant tout due au rançongiciel «Qlocker», qui s'attaque en priorité aux utilisateurs privés de la solution de stockage en réseau de la marque QNAP.

Le NCSC a enregistré une forte recrudescence des cas de phishing. Alors que 497 incidents lui avaient été signalés au premier semestre de 2020 via le formulaire d'annonce, le nombre d'annonces avait pratiquement quintuplé au premier semestre de 2021 pour s'établir à 2439. La raison tient surtout à l'afflux, au cours des derniers mois, d'annonces concernant des courriels ou SMS frauduleux de notification de colis.

2 Éditorial

Sécurité participative – veillons ensemble à assurer la cybersécurité

Chère lectrice, cher lecteur,

La cybersécurité a évolué. Il y a quelques années encore, ce n'était qu'une discipline informatique parmi d'autres, spécialisée dans la protection des données et des systèmes. Les entreprises étaient bien contentes d'avoir des collaborateurs s'intéressant à ces questions. On n'y prêtait généralement attention que lorsqu'un pare-feu entravait le fonctionnement d'un système. Il arrivait qu'un tel pare-feu soit purement et simplement désactivé. Après tout il ne faisait que gêner, et aucun incident grave ne s'était jamais produit.

Fig. 1: Marcel Zumbühl, CISO de la Poste et coprésident de l'ISSS

Ces temps sont bien révolus! Dans toute entreprise ou institution, la cybersécurité est aujourd'hui non seulement du ressort de la direction mais aussi du conseil d'administration, tant les risques en jeu sont élevés. C'est aussi un facteur économique majeur, dans un monde numérique interconnecté. Les clients se méfient des services numériques et tiennent à savoir si l'entreprise a réellement pris le thème au sérieux. Or la cybersécurité n'est pas une discipline où seules les grandes entreprises se doivent d'exceller. Les PME helvétiques sont en effet devenues une cible de choix de cybercriminels pressés de gagner de l'argent et s'imaginant qu'ils ne rencontreront guère de résistance. Les maîtres chanteurs misent sur la crainte qu'ont les entreprises de subir un dégât d'image, en cas notamment de fuites d'informations confidentielles.

Par chance, le vent tourne là aussi. Nous réalisons que les attaques informatiques fructueuses sont en premier lieu des actes criminels. Il importe donc moins de savoir si l'on aurait dû mieux se protéger que d'identifier les coupables et de les mettre en accusation. Nous apprenons qu'il faut condamner non pas les victimes, mais leurs agresseurs. En outre, nous apprenons qu'en cas de cyberchantage, il ne faut pas essayer de payer la rançon demandée, par crainte d'une atteinte à la réputation. Notamment parce que selon une récente étude de la société Cybereason, les entreprises qui s'acquittent de la rançon demandée seront à nouveau appelées à passer à la caisse dans 80 % des cas.

Nous devons apprendre à nous organiser en réseau au profit de la cybersécurité. La «sécurité participative» est le mot d'ordre du jour. Les entreprises découvrent que loin d'être une activité de niche, la cybersécurité a sa place naturelle dans le développement des applications et des systèmes. Par exemple dans le modèle de travail agile DevSecOps, où les équipes de sécurité et les développeurs de logiciels collaborent étroitement. À La Poste Suisse, une équipe engagée de « Security Champions » analyse tous les projets décisifs sous l'angle de la cybersécurité.

À l'instar des communautés internes dédiées, des communautés externes aux entreprises aident à améliorer la cybersécurité. Les cercles de confiance et les plateformes d'échange entre experts en sécurité de diverses organisations existent depuis toujours et bien souvent, des experts entretiennent des contacts non pas dans un seul groupe d'échange, mais dans plusieurs. Des idées et de bonnes pratiques voient ainsi le jour, les spécialistes apprennent les uns des autres et ont ainsi une longueur d'avance sur les agresseurs.

La collaboration avec les pirates éthiques est un phénomène récent, qui confère davantage de poids encore à la sécurité participative. Des entreprises invitent toute personne intéressée à tester en détail leurs services en ligne, pour en découvrir les points faibles. Quiconque repère une faille de sécurité sera récompensé. La Poste utilise cette approche de la sécurité participative depuis 2019. Son programme est accessible depuis le monde entier. Les services en ligne, comme les timbres-poste numériques «Webstamp» ou l'application de la Poste, affichent ainsi un niveau de sécurité élevé. Les systèmes de santé numérique ou les services de vote électronique bénéficient également de cette nouvelle technique de détection et d'élimination des erreurs. Nous avons de la sorte la possibilité, grâce à la collaboration avec nos experts tant internes qu'externes, de découvrir et corriger à temps des erreurs. Aucun logiciel n'est parfait et nous faisons tout pour en détecter les failles au plus vite.

Le Centre national pour la cybersécurité (NCSC) de la Suisse rend des services d'une valeur inestimable au sein de ce réseau de sécurité participative. Les experts de la Confédération aident des entreprises comme la Poste à apprendre les unes des autres, ainsi qu'à reconnaître et à déjouer les menaces à temps. Les rapports semestriels du NCSC constituent une lecture obligatoire pour tout expert en sécurité, et je tiens à remercier ici le NCSC pour son infatigable engagement en faveur de la sécurité participative en Suisse.

Marcel Zumbühl, CISO de la Poste et coprésident de l'ISSS

3 Thème prioritaire: failles de sécurité

3.1 Principales vulnérabilités révélées au premier semestre 2021

3.1.1 Microsoft Exchange: ProxyLogon

La société de sécurité Volexity a découvert en début d'année des attaques tirant parti de plusieurs vulnérabilités du logiciel Exchange Server de Microsoft[1]. L'incident avait amené Microsoft à une publication extraordinaire de mises à jour de sécurité, le 2 mars 2021[2]. Le lendemain déjà, les autorités de sécurité américaines mettaient en garde contre des attaques émanant d'acteurs étatiques chinois et tirant parti de cette faille de sécurité[3].

La chaîne d'attaque exploite quatre failles de sécurité jusque-là inconnues. Tant la faille critique en amont que la chaîne dans son ensemble ont été baptisées ProxyLogon[4].

Cette chaîne d'attaque conçue pour les versions 2013, 2016 et 2019 des serveurs Microsoft Exchange s'efforçait d'établir une liaison avec le port 443 du serveur, responsable des connexions sécurisées HTTPS. Au départ, la chaîne exploite une faille de sécurité baptisée «Server-Side-Request-Forgery (SSRF)»: elle permet aux agresseurs d'envoyer n'importe quelle requête HTTP en s'authentifiant comme serveurs Exchange. La vulnérabilité a été qualifiée de critique, sachant qu'elle donne accès aux autres failles de sécurité[5]. Le degré de gravité des trois failles situées en aval a été qualifié d'élevé, car elles permettent d'exécuter du code sur l'infrastructure de la victime, ainsi que de lire et d'écrire des fichiers[6].

Les agresseurs parviennent à l'aide de cette chaîne d'attaque à contourner l'authentification et à s'annoncer comme administrateurs. Ils peuvent ainsi prendre le contrôle complet des serveurs Exchange et lire ou manipuler la correspondance électronique, les données du calendrier, les coordonnées et les tâches à effectuer. Bien souvent, les serveurs Exchange jouent aussi le rôle de contrôleurs de domaine, en vue de l'authentification des ordinateurs et des utilisateurs du réseau. Ils constituent dès lors une cible de choix pour les agresseurs.

Dès sa publication en mars, la chaîne d'attaque a fait des émules non seulement parmi les autres cyberacteurs étatiques, mais aussi parmi les cybercriminels, afin notamment de diffuser des rançongiciels[7]. À diverses reprises, des acteurs ont placé une *Web shell* et ainsi une porte dérobée dans des systèmes vulnérables, pour pouvoir y accéder même après une éventuelle mise à jour et exécuter plus tard des cyberattaques. C'est ainsi que les exploitants de

---

1 Voir Operation Exchange Marauder (volexity.com) et ProxyLogon (proxylogon.com)

2 On-Premises Exchange Server Vulnerabilities Resource Center (microsoft.com)

3 Mitigate Microsoft Exchange Server Vulnerabilities (cisa.gov); voir aussi ci-dessous, chap. 4.6.2.

4 ProxyLogon (proxylogon.com)

5 NVD - CVE-2021-26855 (nist.gov)

6 Des précisions sur les deux vulnérabilités d'écriture de fichier arbitraire post-authentification ainsi que sur la faille de désérialisation sont publiées sous NVD - CVE-2021-26857 (nist.gov), NVD - CVE-2021-26858 (nist.gov) et sous NVD - CVE-2021-27065 (nist.gov)

7 Par ex. les rançongiciels DearCry (fraunhofer.de), également connus sous le nom de DoejoCrypt, et BlackKingdom (fraunhofer.de)

systèmes ont dû procéder à la fois à des mises à jour, à l'analyse des fichiers journaux et à des enquêtes d'investigation, afin d'identifier et de neutraliser de tels codes encoquillés. Le Département américain de la justice a même autorisé les administrations publiques à intervenir auprès des victimes pour déjouer de telles attaques[8]. En Suisse, des centaines de serveurs non équipés de correctifs et donc vulnérables ont été découverts début mars 2021. Le NCSC a informé les entreprises concernées, en leur recommandant instamment d'actualiser leurs systèmes et de contrôler s'ils avaient été compromis[9].

Recommandations:

Pour une meilleure protection des serveurs Exchange, le NCSC recommande de manière générale les mesures de sécurité suivantes:

- Les serveurs Exchange ne doivent pas être directement accessibles depuis Internet. Installez un pare-feu pour applications (*Web Application Firewall*, WAF) ou placez un proxy de filtrage SMTP devant le serveur Exchange.
- Établissez une procédure pour l'application immédiate des mises à jour de sécurité et veillez à ce que celles-ci puissent être effectuées en l'espace de quelques heures. Cela vaut surtout pour tous les systèmes directement accessibles depuis Internet.
- Assurez-vous par une gestion du cycle de vie de n'utiliser que des versions pour lesquelles le fabricant (ici Microsoft) met à disposition des mises à jour de sécurité.
- Surveillez attentivement tous les fichiers journaux des serveurs Exchange, regroupez-les dans un SIEM (*Security Information and Event Management*) et vérifiez s'ils comportent des anomalies.
- Mettez en place un système d'authentification à deux facteurs sur tous les systèmes et pour tous les utilisateurs.
- Utilisez un cadre de gestion dédié pour l'accès à haut privilège aux serveurs Exchange.
- Enregistrez tous les fichiers journaux Active Directory de manière centralisée et analysez les régulièrement.
- Augmentez la visibilité de vos terminaux en utilisant un outil EDR (*Endpoint Detection and Response*).

Des compléments d'information et des recommandations sont publiés sur nos sites:

Exchange Vulnerability 2021 (govcert.admin.ch)

Failles de sécurité de Microsoft Exchange Server (ncsc.admin.ch)

Microsoft corrige d'autres vulnérabilités de son logiciel Exchange Server (ncsc.admin.ch)

---

8 Justice Department Announces Court-Authorized Effort to Disrupt Exploitation of Microsoft Exchange Server Vulnerabilities (justice.gov)

9 Exchange Vulnerability 2021 (govcert.admin.ch); Failles de sécurité de Microsoft Exchange Server (ncsc.admin.ch); Microsoft corrige d'autres vulnérabilités de son logiciel Exchange Server (ncsc.admin.ch).

3.1.2 PulseSecure et SonicWall

Le 20 avril 2021, des vulnérabilités critiques ont été signalées dans deux produits servant à établir des connexions à distance, fabriqués l'un par PulseSecure, l'autre par SonicWall. Le NCSC a rendu les menaces publiques et publié des recommandations pour y remédier[10].

PulseSecure: le prestataire de sécurité FireEye a fait état d'attaques avancées tirant parti d'une faille jusque-là inconnue d'un produit de PulseSecure, en soulignant que douze types de maliciels différents avaient été diffusés par ce canal[11]. Ladite faille permettait à une personne ne s'étant pas identifiée d'exécuter à distance n'importe quel code à l'aide du produit VPN SSL «PulseSecure Connect». Après avoir proposé une simple solution palliative, l'éditeur PulseSecure a publié le 3 mai le correctif de sécurité de la faille et de trois autres vulnérabilités[12]. Des chercheurs ont toutefois découvert que le correctif ne comblait pas entièrement les lacunes existantes[13]. PulseSecure a encore fourni le 16 juin un outil servant à vérifier l'intégrité des implémentations de son logiciel[14].

SonicWall: plusieurs vulnérabilités découvertes dans le produit «SonicWall Email Security» de SonicWall permettaient d'accéder en tant qu'administrateur au système pris pour cible et d'y exécuter à distance du code arbitraire[15]. FireEye a signalé que ces lacunes avaient été exploitées afin de compromettre des réseaux d'entreprise[16]. SonicWall a fourni des correctifs de sécurité le 20 avril 2021[17].

Conclusion / Recommandations:

Les vulnérabilités des solutions d'accès à distance sont très prisées des pirates à l'affût de moyens d'intrusion.

Il faudrait prévoir un second facteur d'authentification pour toute ouverture de session. Les accès à distance basés sur un seul facteur (combinaison d'un nom d'utilisateur et d'un mot de passe) n'offrent pas une protection suffisante et devraient donc être prohibés par des précautions techniques.

Les produits destinés à l'accès à distance doivent être configurés de façon à enregistrer toutes les tentatives d'accès, qu'elles aient été fructueuses ou non (journalisation). Les accès à distance feront en outre l'objet d'une surveillance visant à détecter les activités inhabituelles et à adopter en temps utile des mesures adéquates en cas d'abus.

---

10 Vulnérabilités critiques de type «zero day» dans les produits Pulse Secure et SonicWall (ncsc.admin.ch)
11 Check Your Pulse (mandiant.com) et Re-Checking Your Pulse (mandiant.com)
12 Pulse Security Advisory: SA44784 - 2021-04 (pulsesecure.net)
13 Technical Advisory: Pulse Connect Secure (nccgroup.com)
14 Pulse Secure Article: KB44755 - Pulse Connect Secure (PCS) Integrity Assurance (pulsesecure.net)
15 Vulnérabilités critiques de type «zero day» dans les produits Pulse Secure et SonicWall (ncsc.admin.ch)
16 Zero-Day Exploits in SonicWall Email Security Lead to Enterprise Compromise (mandiant.com)
17 Security Notice: SonicWall Email Security Zero-Day Vulnerabilities (sonicwall.com)

3.1.3 Accellion

Accellion File Transfer Appliance (FTA) est un logiciel de partage de fichiers qui arrivait en fin de vie en décembre 2020, quand il a été compromis. Des acteurs malveillants liés aux opérateurs du rançongiciel Clop[18] ont exploité différentes failles qui pourraient leur avoir livré accès aux données de 320 clients[19], menaçant leurs propriétaires de les publier sur le Darkweb en cas de non-versement de la rançon demandée. Les victimes, basées dans plusieurs pays, comptent des institutions majeures, comme la banque centrale néo-zélandaise ou le bureau de l'auditeur de l'État de Washington aux États-Unis. Six mois après l'exploitation de la faille, de nouveaux noms de victimes continuent d'émerger, triste fin de parcours pour un produit obsolète[20]. La communication du fournisseur concernant les failles de sécurité, ainsi que le correctif proposé ont manifestement atteint trop tard les clients concernés[21].

Conclusion / Recommandation:

Les logiciels utilisés font l'objet de mises à jour constantes. Ce constat vaut pour les prestataires comme pour les entreprises utilisatrices. Si tout indique qu'un fabricant va cesser l'actualisation d'un produit donné, il faudrait aussitôt lancer un processus de remplacement, afin que la solution subséquente n'arrive pas trop tard ou pour ne pas devoir l'organiser et la mettre en place dans la précipitation. L'utilisation d'un logiciel qui n'est plus pris en charge, et donc qui ne recevra aucune mise à jour, expose à des risques de sécurité considérables les entreprises comme les particuliers.

3.1.4 PrintNightmare

Le 8 juin 2021, Microsoft a publié une mise à jour de sécurité visant à combler la vulnérabilité «PrintNightmare» de la file d'attente d'impression (*print spooler*)[22]. Peu après, d'autres vulnérabilités affectant le spouleur d'impression ont été rendues publiques[23]. Les failles découvertes permettaient aux attaquants de se déplacer latéralement au sein des réseaux, ce qui a été exploité notamment par des opérateurs de rançongiciels[24]. En attendant que Microsoft ait publié des mises à jour exceptionnelles pour corriger cette vulnérabilité, il était recommandé de désactiver le service de spouleur des systèmes n'étant pas nécessaires pour l'impression. Il s'agissait de protéger en particulier les contrôleurs de domaines et les autres serveurs essentiels[25].

---

18 Cyber Criminals Exploit Accellion FTA for Data Theft and Extortion (mandiant.com)
19 Accellion FTA Attack Customer FAQs (accellion.com)
20 Accellion Announces End of Life (EOL) for its Legacy FTA Product (accellion.com)
21 Vulnérabilité Accellion FTA : les notifications en question (lemagit.fr)
22 CVE-2021-1675 – Vulnérabilité d'exécution de code à distance dans le spouleur d'impression Windows (microsoft.com)
23 CVE-2021-34527 – Vulnérabilité d'exécution de code à distance dans le spouleur d'impression Windows (microsoft.com)
24 Ransomware: Now attackers are exploiting Windows PrintNightmare vulnerabilities (zdnet.com)
25 CVE-2021-1675: Incomplete Patch and Leaked RCE Exploit (sans.edu)

Le NCSC a informé la population au sujet de cette menace et émis des recommandations[26].

Conclusion / Recommandation:

Pour donner moins de prise aux attaques, il faudrait en principe désactiver les services standard des systèmes qui n'en ont pas besoin. Une telle mesure devrait être prévue dans le cadre des processus visant à durcir les systèmes au moment de leur installation.

3.1.5 QNAP NAS

En avril 2021, des utilisateurs de la solution de stockage en réseau (NAS) de la société taïwanaise QNAP ont subi des attaques du rançongiciel Qlocker[27]. Les agresseurs ont exploité à cet effet une faille critique de ce produit permettant une injection SQL[28], pour laquelle QNAP avait fourni une mise à jour le 16 avril 2021 déjà. Or de nombreux utilisateurs avaient installé cette mise à jour trop tard, voire ne l'avaient pas appliquée. Plusieurs victimes suisses de ces attaques ont été signalées au NCSC, principalement des particuliers et des PME.

Le NCSC a informé la population au sujet de cette menace et émis des recommandations[29].

Conclusion / Recommandations:

Dans les réseaux domestiques, les serveurs de stockage (NAS) sont souvent directement reliés au routeur et donc exposés, selon la configuration adoptée[30].

Un NAS ne devrait jamais être directement accessible depuis Internet. Dans les entreprises comme dans le cadre familial, il convient d'éviter une telle situation et de définir à la place un accès à ces ressources par VPN, avec authentification à deux facteurs.

L'interface de gestion ne doit en aucun cas être exposée aux menaces venant d'Internet.

Les données et sauvegardes enregistrées sur un NAS doivent faire l'objet d'une copie supplémentaire (hors ligne).

3.1.6 Vulnérabilités de Dell-BIOSConnect

Le 24 juin 2021, des chercheurs de la société de sécurité Eclypsium ont publié plusieurs vulnérabilités du programme SupportAssist de Dell[31]. Ce logiciel préinstallé sur la plupart des ordinateurs Dell tournant sous Windows permet notamment de mettre à jour les micrologiciels

---

26 Faille de sécurité critique dans le spouleur d'impression des systèmes Microsoft (ncsc.admin.ch); Patches disponibles - Faille de sécurité critique dans le spouleur d'impression des systèmes Microsoft (ncsc.admin.ch).

27 Massive Qlocker ransomware attack uses 7zip to encrypt QNAP devices (bleepingcomputer.com); Qnap sichert NAS spät gegen Qlocker-Attacken ab (heise.de).

28 NVD – CVE-2020-36195 (nist.gov); SQL Injection Vulnerability – Security Advisory (qnap.com)

29 Rétrospective de la semaine 16 (ncsc.admin.ch); Rétrospective de la semaine 17 (ncsc.admin.ch)

30 The reason why you shouldn't connect QNAP NAS directly to the Internet without any protection (qnap.com)

31 Eclypsium Discovers Multiple Vulnerabilities in Dell BIOSConnect (eclypsium.com)

de la machine ou de restaurer d'importantes fonctions, en cas de défaillance du disque dur ou d'autres dommages. Le problème concernerait 129 modèles, et donc plus de 30 millions d'appareils. Les vulnérabilités permettraient aux agresseurs de contrôler le processus de démarrage de l'appareil et de contourner ainsi le système d'exploitation et les contrôles de sécurité de niveau supérieur. Les attaquants devraient toutefois avoir préalablement compromis le réseau dont fait partie l'ordinateur et obtenu par ailleurs un certificat de confiance. Enfin, ils auraient encore besoin qu'un utilisateur active manuellement la mise à jour ou la fonction de récupération[32].

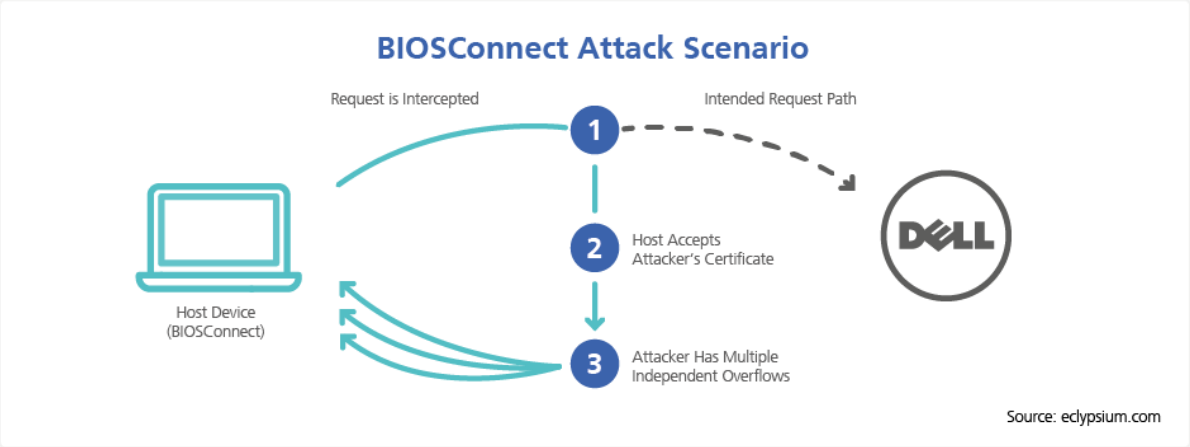


Fig. 2: La requête envoyée au serveur Dell est interceptée.

Conclusion:

Ces failles n'ont pas été exploitées à grande échelle, car de nombreuses conditions auraient dû être réunies pour qu'une attaque devienne possible. Il est à noter que les vulnérabilités situées à ce niveau permettent de contourner toutes les mesures de sécurité prises sur les terminaux, qui ne déploient leur effet qu'après le démarrage. Dans les réseaux d'entreprises compromis, de telles failles sont donc susceptibles d'infecter de nombreux terminaux.

3.1.7 Bad Alloc

Des chercheurs en sécurité de l'équipe Section 52 de Microsoft ont découvert plusieurs vulnérabilités liées à la gestion de la mémoire[33]. Comme il s'agit d'un problème d'allocation (*bad allocation*) de mémoire, cette série de vulnérabilités a été nommée «BadAlloc». En provoquant des débordements de mémoire tampon, des agresseurs parviendraient à exécuter du code malveillant sur l'appareil pris pour cible, ou à le faire tomber en panne. De tels incidents étaient dus à l'absence de validation des entrées.

---

32 DSA-2021-106 : mise à jour de sécurité de la plate-forme client Dell pour plusieurs vulnérabilités identifiées dans les fonctionnalités BIOSConnect et HTTPS Boot du BIOS du client Dell (dell.com)

33 "BadAlloc" – Memory allocation vulnerabilities could affect wide range of IoT and OT devices in industrial, medical, and enterprise networks (microsoft.com)

Microsoft et le Département américain de la Sécurité intérieure (DHS) ont conjointement informé les différents fabricants d'appareils vulnérables, afin qu'ils puissent corriger les failles et fournir des mises à jour[34]. Comme les systèmes en question comprennent notamment des systèmes d'exploitation en temps réel d'installations industrielles et des appareils médicaux (certifiés), leur sécurisation n'est pas anodine. Mais si selon la pratique recommandée de tels systèmes sont correctement séparés des systèmes environnants, il ne devrait pas être possible aux pirates de tirer parti de telles vulnérabilités.

Conclusion:

Il faut veiller à mettre en place des mesures de sécurité dès le stade de la programmation (*security by design*). Sinon d'énormes efforts seront nécessaires pour corriger les lacunes, à supposer même que ce soit possible.

3.2 Gestion des logiciels : processus d'inventaire et de mise à jour

Les cyberattaques ne reposent pas uniquement sur les vulnérabilités, mais aussi sur les chaînes d'approvisionnement logicielles (*software supply chain*). Lors de tels scénarios d'attaque, l'agresseur intervient dans le processus de fabrication ou de mise à jour du logiciel. Le logiciel compromis est ensuite distribué par les circuits ordinaires. À partir du moment où une telle attaque est connue, il est généralement facile de reconnaître le logiciel compromis, encore que ce ne soit pas toujours le cas. Pendant que la compromission de SolarWinds suscitait un tollé dans le monde entier[35], les entreprises devaient encore vérifier quelle version elles utilisaient et si elles étaient concernées. Or à diverses reprises, le logiciel avait été choisi par les fabricants de matériel informatique d'origine (OEM), et les clients finaux ne se rendaient pas compte que le logiciel faisait partie du produit utilisé par eux.

Le cas ci-après illustre bien cette complexité : le 15 avril 2021, la société Codecov, développeur d'outils d'audit logiciel, informait sa clientèle d'une vulnérabilité découverte dans son produit «Bash-Uploader»[36]. Mais comme des milliers de clients utilisent le script en question, qui fait d'ailleurs partie intégrante de différents programmes, il est très difficile de savoir sur qui cet incident fait réellement peser une menace.

Pour être à même de bien réagir en cas d'incident, les exploitants de systèmes ou réseaux doivent tenir un inventaire à jour. Au-delà du matériel informatique, il devra inclure tous les logiciels présents dans un tel environnement, en indiquant leurs liens de dépendance. La tenue d'un tel inventaire, qui doit être constamment à jour, exige d'importantes ressources.

Le matériel informatique et les logiciels devenant toujours plus complexes et la rapide transformation numérique de la société représentent un défi important pour la sécurité des entreprises. Ces dernières années, l'administration nationale des télécommunications et de

---

34 ICS Advisory (ICSA-21-119-04) – Multiple RTOS (cisa.gov)

35 Voir rapport semestriel NCSC 2020/2, chap. 4.7.2.

36 Bash Uploader Security Update (codecov.io)

l'information américaine (NTIA) a œuvré avec des partenaires au développement d'une nomenclature logicielle (software bill of materials, SBOM)[37]. À l'instar des denrées alimentaires, dont il faut déclarer les ingrédients du produit final, la SBOM imposerait d'indiquer pour les produits numériques tous les composants entrant dans la fabrication du produit final. Le 12 mai 2021, le gouvernement américain a publié un décret visant à renforcer la cybersécurité (Executive Order on Improving the Nation's Cybersecurity)[38], où la nomenclature logicielle détaillée (SBOM) est expressément mentionnée au chapitre sur l'amélioration de la sécurité de la chaîne d'approvisionnement logicielle.

Cette transparence accrue permettra de se faire une idée des produits numériques utilisés et de leurs liens de dépendance. La complexité croissante du domaine ainsi que la pléthore d'informations s'y rapportant requièrent toutefois un certain degré d'automatisation dans la maintenance de l'inventaire des logiciels et dans le traitement des avis de sécurité (*security advisories*) se rapportant aux éléments de l'inventaire.

À l'heure actuelle, les consignes de sécurité sont publiées de diverses manières et sous différents formats: certains fabricants les affichent sur leurs sites Web, alors que d'autres exigent qu'on s'annonce sur leur portail pour les consulter et que d'autres encore les envoient sous forme de fichiers pdf. De même, la structure des indications fournies dépend des préférences individuelles de chaque organisation.

OASIS Open, une organisation d'utilité publique responsable des normes *open source*, a lancé à des fins d'automatisation une discussion sur un nouveau format appelé «Common Security Advisory Framework (CSAF 2.0)». Ce format doit permettre d'établir les avis de sécurité nécessaires sous forme standardisée et lisible à la machine. Le but est d'établir une norme en vue du traitement automatisé des avertissements de sécurité[39].

Conclusion:

La tenue d'un inventaire régulièrement actualisé pour tous les composants matériels et logiciels s'avère primordiale, dans l'optique de la sécurité des infrastructures informatiques. Idéalement, on pourra ainsi se faire une vue d'ensemble des liens de dépendance entre logiciels. L'introduction de la nomenclature logicielle (SBOM) offrirait un tel aperçu, au prix d'une complexité accrue des bases de données à mettre à jour. On comprend donc bien l'importance de disposer d'un moyen de saisie et de traitement automatisé des avis de sécurité, pour tous les éléments disponibles dans Internet. «CSAF 2.0», mis au point par OASIS Open, pourrait couvrir ce besoin.

37 SOFTWARE BILL OF MATERIALS | National Telecommunications and Information Administration (ntia.gov)

38 Executive Order on Improving the Nation's Cybersecurity (whitehouse.gov)

39 Common Security Advisory Framework (CSAF) Website (csaf.io, oasis-open.github.io, oasis-open.org); BSI - Common Security Advisory Framework (CSAF) (bsi.bund.de).

3.3 Gestion des vulnérabilités dans l'optique du NCSC

Le grand public s'intéresse toujours plus aux failles de sécurité informatique. Les récentes attaques lancées contre les produits SolarWinds[40], les vulnérabilités de Microsoft Exchange[41] ainsi que celles du processus d'impression de Microsoft Windows[42] montrent comment les acteurs étatiques ou non étatiques exploitent de telles lacunes. Alors qu'il y a quelques années encore, les États étaient presque seuls à disposer des cybercapacités offensives nécessaires au lancement de telles attaques, les criminels d'aujourd'hui tirent toujours plus souvent parti des vulnérabilités existantes. Les failles de sécurité sont devenues en quelques années le cauchemar de tout responsable de la sécurité informatique, avec l'essor de kits de services criminels prêts à l'emploi et faciles à se procurer («*Crimeware-as-a-Service*») et la multiplication des logiciels en circulation. Pour contribuer à gérer cette menace, le NCSC a créé une division s'occupant des failles de sécurité. Ses objectifs sont multiples: informer, sensibiliser et soutenir le public (particuliers, entreprises, services étatiques) au sujet des failles de sécurité critiques et des précautions à prendre; offrir aux services étatiques une plateforme de primes aux bogues (*bug bounty*) afin d'identifier les éventuelles lacunes de sécurité des réseaux informatiques des collectivités publiques; créer une plateforme en vue de la divulgation coordonnée des vulnérabilités (*coordinated vulnerability disclosure*), pour permettre à quiconque ayant identifié une faille d'annoncer anonymement sa découverte à un service étatique[43]. Ce ne sont là que quelques-uns des objectifs que le NCSC poursuit avec sa nouvelle division, dont certains ont déjà été atteints. Et comme les problèmes de sécurité liés aux vulnérabilités logicielles ou matérielles vont s'exacerber dans un proche avenir, le travail du NCSC en matière de prévention, d'identification et de résolution des problèmes dans ce secteur revêtira une importance toujours plus grande.

3.4 Programme de primes aux bogues au sein de l'administration fédérale

Les programmes de primes aux bogues (*bug bounty*) sont un volet important de la gestion des vulnérabilités. Les pirates éthiques sont invités à découvrir les failles de sécurité des systèmes informatiques d'une organisation. Pour chaque bogue découvert, documenté et confirmé, le pirate reçoit une prime (*bounty*), dont le montant est fixé en fonction de la gravité de la faille détectée.

Du 10 au 21 mai 2021, le Centre national pour la cybersécurité (NCSC) a mené un projet pilote de primes aux bogues, en collaboration avec la société Bug Bounty Switzerland, le Département fédéral des affaires étrangères (DFAE) et les Services du Parlement. Quelque quinze pirates ont participé au projet, sur mandat de la Confédération. Au total, dix failles de sécurité ont été découvertes. Ce projet a donné de très bons résultats, et les enseignements

---

40 Voir rapport semestriel NCSC 2020/2, chap. 4.7.2 et ci-dessous chap. 4.6.1.

41 Voir ci-dessus chap. 3.1.1 et ci-dessous chap. 4.6.2.

42 Voir ci-dessus chap. 3.1.4.

43 Annonce d'une faille ou divulgation coordonnée d'une vulnérabilité (CVD) (ncsc.admin.ch)

qu'il a livrés serviront à la réalisation de futurs programmes du même genre au sein de l'administration fédérale[44].

Ces programmes de primes aux bogues sont efficaces pour détecter et corriger les failles présentes dans les systèmes et applications informatiques. Le retour sur investissement a été jugé élevé. Le programme de primes aux bogues que le NCSC met en œuvre au sein de l'administration fédérale contribue grandement à réduire les cyberrisques auxquels la Confédération est exposée.

4 Événements survenus / situation

4.1 Aperçu des annonces de cyberincidents reçues

Au premier semestre 2021, le guichet unique du NCSC a enregistré au total 10 234 annonces, soit près du double des annonces reçues au deuxième semestre 2020. Cette évolution tient d'une part à l'introduction d'un nouveau formulaire d'annonce[45], publié bien en évidence sur la page d'accueil du NCSC. D'autre part, il y a eu plusieurs vagues de *fake sextortion*[46] et de phishing, dont témoignent les pics d'annonces des 5e et 16e semaines.

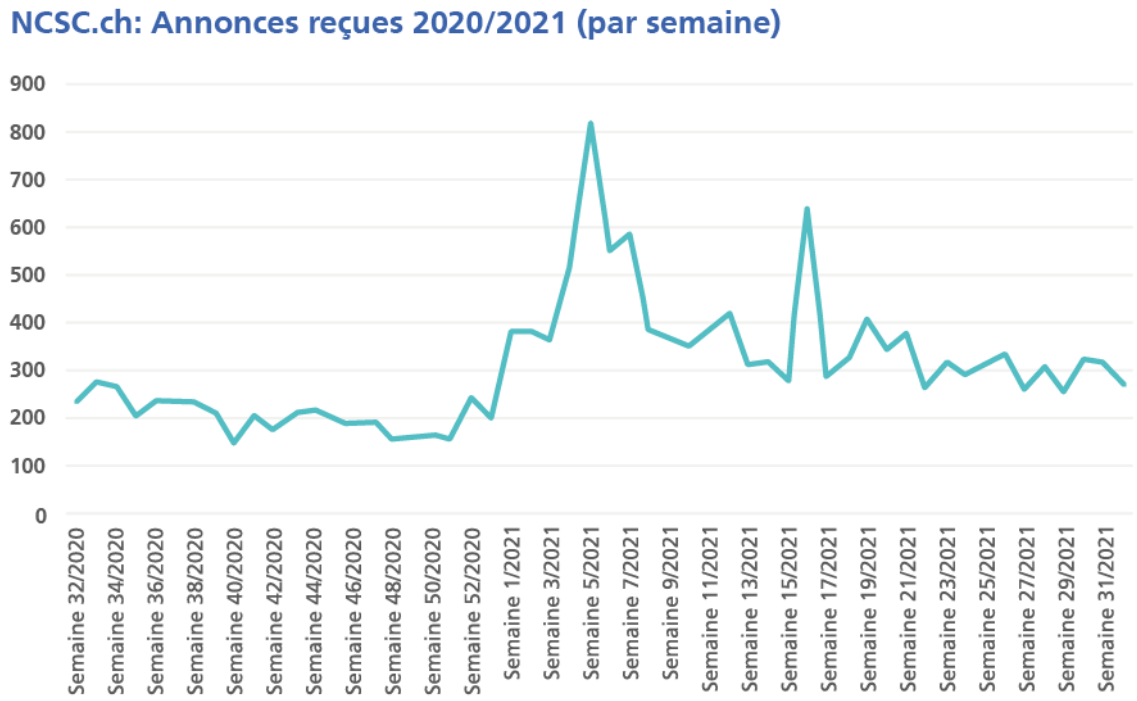


Fig. 3: Nombre d'annonces hebdomadaires parvenues au NCSC entre août 2020 et juillet 2021, voir aussi Chiffres actuels (ncsc.admin.ch).

---

44 Projet pilote de primes aux bogues mené avec succès au sein de l'administration fédérale (ncsc.admin.ch)

45 Formulaire d'annonce du NCSC (ncsc.admin.ch)

46 Informations sur la *fake sextortion* (ncsc.admin.ch); voir aussi Stop Sextortion (stop-sextortion.ch).

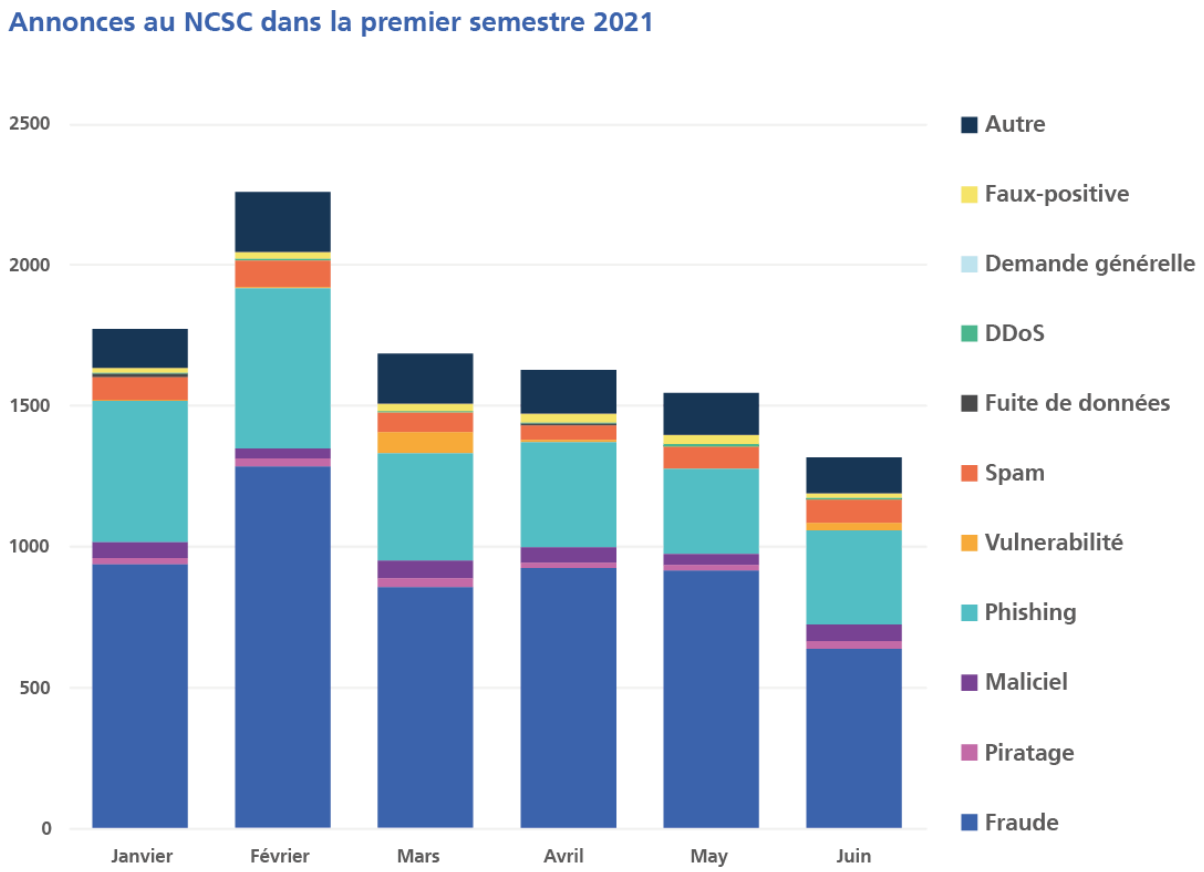


Fig. 4: Signalements effectués au NCSC au premier semestre 2021, par catégorie, voir aussi Chiffres actuels (ncsc.admin.ch).

4.1.1 Annonces de cas de fraude

Dans la catégorie des cas de fraude, qui représentent plus de la moitié des incidents avec 5526 signalements, les courriels de *fake sextortion* arrivent en tête au premier semestre 2021 avec 1351 signalements, reléguant en deuxième position la fraude au paiement anticipé, dénoncée à 1284 reprises. La fraude au paiement anticipé[47] était encore le phénomène le plus répandu aux deux semestres précédents.

Les autres types d'escroqueries fréquemment signalés comprennent l'arnaque au président[48] (239 annonces), les appels de *fake support*[49] (370 annonces) et la fraude aux petites annonces[50] (307 signalements). Outre les scénarios classiques consistant à vendre des marchandises inexistantes ou à ne pas livrer le produit payé, la fraude aux petites annonces comprend notamment la variante où sous un quelconque prétexte, alors même que vous avez

47 Informations sur la fraude au paiement anticipé (ncsc.admin.ch)
48 Informations sur l'arnaque au président (ncsc.admin.ch)
49 Informations sur le *fake support* (ncsc.admin.ch)
50 Informations sur la fraude aux petites annonces (ncsc.admin.ch);
Fraude aux petites annonces – Payer malgré la vente (ncsc.admin.ch).

réalisé une vente, vous devez encore verser de l'argent à l'acheteur ou à une autre entreprise qui se chargera par exemple du transport. Dans un autre scénario, le paiement doit être effectué par Paypal, et la victime reçoit ensuite un courriel falsifié semblant provenir de cette société lui indiquant qu'elle doit encore s'acquitter de frais pour que la transaction puisse être effectuée.

La fraude à l'investissement[51] fait partie des délits occasionnant typiquement des dommages élevés. Au total, 252 cas ont été signalés au NCSC, dont 38 ayant entraîné une perte financière. Des exemples de pratiques actuelles figurent ci-dessous au chap. 4.8.

4.1.2 Annonces de sites de phishing

Le guichet unique du NCSC a enregistré une forte recrudescence des cas de phishing[52]. Alors que 497 incidents lui avaient été signalés au premier semestre 2020 par le biais du formulaire d'annonce, leur nombre est passé à 2439 au premier semestre 2021[53]. Les annonces ont donc quasiment quintuplé. La raison tient surtout à l'afflux, au cours des derniers mois, de courriels ou SMS frauduleux de notification de colis[54]. En pareil cas, les escrocs invitent à s'acquitter d'une petite taxe pour recevoir un colis n'ayant pas pu être livré. À cet effet, la victime doit cliquer sur un lien puis saisir les coordonnées de sa carte de crédit. D'ordinaire, une forte somme sera directement débitée de sa carte. Dans un scénario similaire signalé 479 fois, la carte de crédit n'intervient pas et il est question de droits de douane à payer avec des cartes Paysafe. De tels courriels sont le plus souvent censés provenir de l'Administration fédérale des douanes (AFD). Les numéros des cartes Paysafe permettant aux criminels de retirer l'argent doivent être envoyés à l'adresse électronique indiquée. La manœuvre a ceci de perfide que l'adresse frauduleuse est dissimulée sous l'adresse officielle de l'administration des douanes et ne s'affiche que si l'on clique dessus. Les personnes ayant reçu de tels courriels ou SMS alors qu'elles venaient d'effectuer une commande en ligne seront tentées de croire qu'il y a eu une fuite de données. Or à ce jour, aucune fuite de données n'a été constatée à la Poste ou à l'administration des douanes. Le fait que ces courriels arrivent en même temps tient plutôt à des effets statistiques. Les commandes en ligne ont connu un formidable essor avec le COVID-19. Les criminels aussi l'ont remarqué et, depuis l'apparition de la pandémie, ils ont intensifié l'envoi de courriels et de SMS frauduleux de notification de colis réclamant des frais. Il n'y a donc rien d'improbable à ce qu'une commande réelle coïncide dans le temps avec un courriel frauduleux.

---

51 Informations sur la fraude à l'investissement (ncsc.admin.ch); voir aussi ci-dessous, chap. 4.8.

52 Informations sur le phishing (ncsc.admin.ch)

53 Ce chiffre se réfère aux courriels de phishing signalés au moyen du formulaire d'annonce du NCSC. Les annonces ont été analysées et les liens frauduleux transmis au portail antiphishing.ch, géré par le NCSC. Par conséquent, les chiffres d'antiphishing.ch (voir chap. 4.7.1) reprennent ceux du formulaire d'annonce.

54 Voir Rétrospective de la semaine 11 (ncsc.admin.ch), Rétrospective de la semaine 23 (ncsc.admin.ch) et chap. 4.7.2.

4.1.3 Annonces de maliciels

Les incidents impliquant un cheval de Troie verrouillant les données (rançongiciel) retiennent également l'attention au premier semestre 2021. Leur nombre a triplé, passant de 32 cas au premier semestre 2020 à 94 cas durant la période sous revue. Cette augmentation est avant tout due au rançongiciel «Qlocker», qui s'attaquait en priorité aux utilisateurs privés de la solution de stockage en réseau de la marque QNAP (voir ci-dessus, chap. 3.1.5). Avec 39 cas, «Qlocker» a été de loin le rançongiciel le plus souvent signalé. Beaucoup de personnes ont par ailleurs reconnu et signalé des courriels contenant une annexe infectée ou un lien suspect (voir chapitre suivant).

4.2 Maliciels

4.2.1 Diffusion des maliciels

Le courriel reste le moyen le plus utilisé pour la diffusion des maliciels. Le maliciel peut au choix figurer directement dans l'annexe d'un message et se télécharger puis s'installer lors de l'ouverture du fichier infecté, ou figurer sur une page Web dont le courriel renferme le lien. Dans le second cas, la victime est priée de télécharger le maliciel, ou son ordinateur subit d'emblée une infection par *drive-by download*[55]. Les destinataires de tels courriels sont typiquement encouragés par des méthodes relevant de l'ingénierie sociale[56] à effectuer des manipulations qui aboutiront à l'installation du maliciel.

L'infection d'un ordinateur ou d'un réseau se déroule typiquement en plusieurs phases. Tout commence par une manœuvre d'approche et une infection initiale. Des maliciels sont fréquemment déployés à large échelle lors de campagnes d'envoi de pourriels malveillants (*malspam*), comme «AgentTesla», «Lokibot» et «FormBook» qui ont sévi au semestre écoulé en Suisse. De tels maliciels servent typiquement de passe-partout et bien souvent, ils collectent des informations sur le système infecté et y installent, en cas de besoin, d'autres modules fonctionnels ou d'autres logiciels (malveillants). Les cybercriminels monnaient ensuite les accès aux appareils infectés sur des sites clandestins.

Le graphique ci-après indique les familles de maliciels que le NCSC a analysés et identifiés au semestre écoulé. Les fichiers et codes analysés proviennent de sources diverses, comme les capteurs ou les annonces faites par les responsables de la sécurité des infrastructures critiques, par des citoyens ou des PME. Le NCSC partage les indicateurs de compromission (*indicators of compromise*, IOC) découverts avec les exploitants d'infrastructures critiques, pour leur permettre de se protéger.

---

[55] Voir ci-dessous, chap. 4.3.2

[56] Voir ci-dessous, chap. 4.7

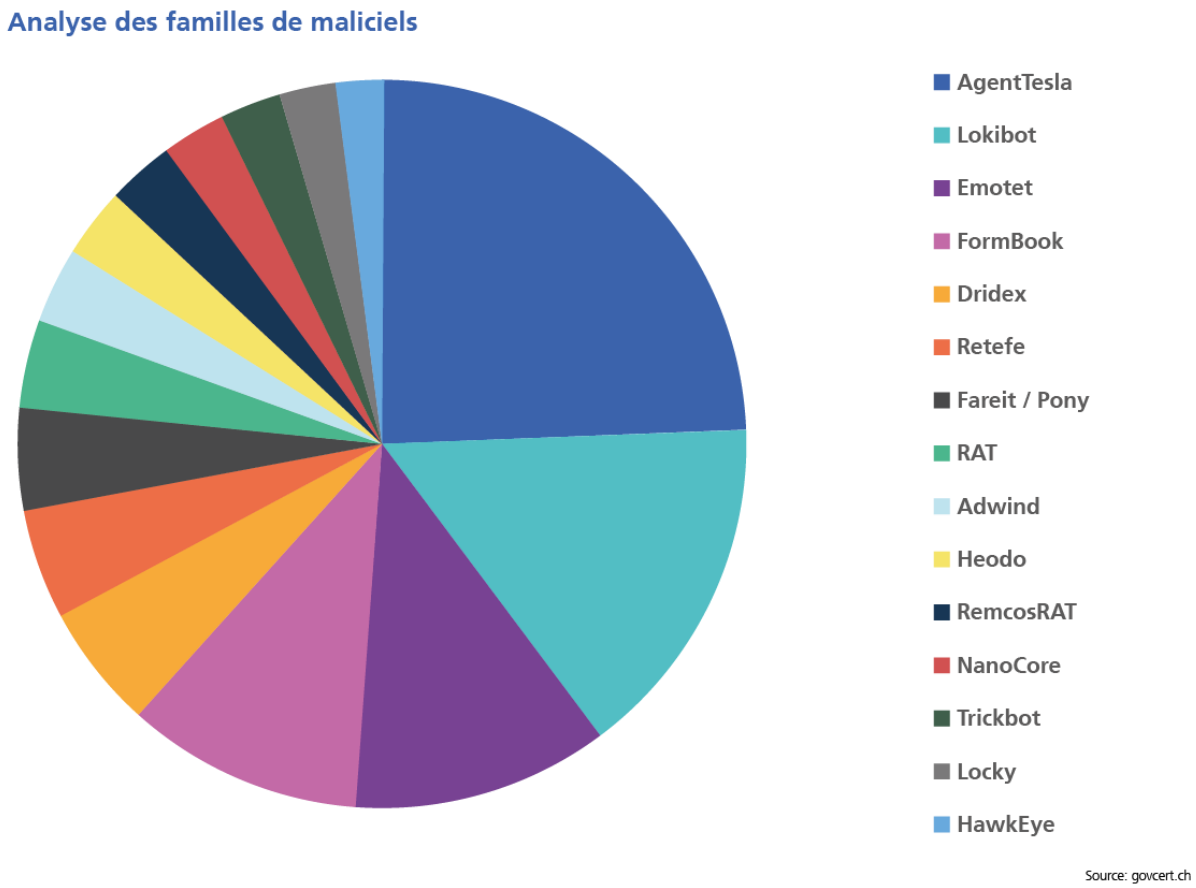


Fig. 5: Analyses du NCSC des familles de maliciels actifs en Suisse au premier semestre 2021.

Depuis qu'au début de 2021 les autorités de poursuite pénale ont démantelé et retiré du réseau l'infrastructure d'«Emotet»[57], d'autres familles de maliciels ont pris le relais. À côté de noms bien connus comme «TrickBot», «Retefe», «Dridex» ou «Qbot», des familles de maliciels plus discrètes jusque-là, comme «IcedID», sévissent en ce moment.

En février 2021, une vaste campagne de malspam a usurpé l'identité de la marque «DocuSign» afin de diffuser «TrickBot» dans des fichiers Excel infectés. Il s'agissait de la première vague de propagation massive de «TrickBot» depuis octobre 2020. Les courriels et documents utilisés étaient rédigés en termes très généraux en langue anglaise.

«SilentBuilder», une macro malveillante dissimulée dans des documents Excel, installe le maliciel «QBot» (alias «QakBot» et «QuakBot»). Le NCSC a connaissance de plusieurs cas où des documents Excel infectés ont franchi avec succès tous les dispositifs de sécurité, avant d'être ouverts par les utilisateurs finaux. Les escrocs avaient recouru à diverses techniques d'ingénierie sociale pour convaincre les destinataires d'ouvrir le fichier Excel annexé et d'en activer la macro. Une fois l'ordinateur infecté, une balise (*beacon*) «Cobalt Strike»[58] est

[57] Voir World's most dangerous malware EMOTET disrupted through global action (europol.europa.eu) et rapport semestriel NCSC 2020/2, chap. 4.3.2.

[58] Voir ci-dessous chap. 4.2.2.

installée et permet aux agresseurs d'interagir avec le système, soit d'y mener des opérations de reconnaissance, de s'y déplacer latéralement et d'étendre leurs droits.

Depuis le mois de mars, on constate une diffusion fortement accrue d'«IcedID» – y compris à partir de courriels rédigés en allemand[59]. Sa présence est notamment attestée dans les chaînes d'infection aboutissant au déploiement d'un rançongiciel. «IcedID» a été propagé par des liens ou sites Google, par le biais de formulaires de contact, et a servi à infecter des entreprises avec «Cobalt Strike»[60]. Les escrocs ont pu ainsi prendre le contrôle de réseaux afin d'en crypter les données avec leur rançongiciel.

«Retefe» se propage d'une autre manière: les pirates appellent d'ordinaire des numéros de téléphone publics (trouvés par ex. sur le site Web de l'entreprise) pour inviter leurs correspondants, sous un quelconque prétexte, à ouvrir un lien Google aboutissant à l'installation de «Retefe»[61].

Recommandations:

- Vérifiez comment vos produits de sécurité permettent d'identifier ou de bloquer les documents renfermant des macros. Veillez à ce que les fichiers d'archives soient également contrôlés.
- Bloquez autant que possible les types de données répertoriés dans la liste du NCSC.
- N'autorisez dans votre réseau que l'exécution des macros portant une signature numérique et contrôlez (par ex. avec «AppLocker») quelles applications peuvent être exécutées à partir de quel chemin d'accès.
- Assurez-vous que des corrections suffisantes ont bien été apportées à votre réseau interne. Veillez par exemple à ce que plus aucun contrôleur de domaine ne soit vulnérable à la faille «Zerologon» (CVE-2020-1472)[62].
- Accroissez la visibilité à tous les terminaux, en utilisant un logiciel EDR (*Endpoint Detection and Response*) ou un utilitaire de surveillance (*System Monitoring*, Sysmon).
- Sensibilisez vos collaborateurs afin qu'ils reconnaissent les messages ou appels suspects et sachent comment réagir le cas échéant.
- Établissez des processus internes pour la notification aux responsables de la sécurité.

Le graphique ci-dessous montre les données collectées par les gouffres DNS (*DNS sinkhole*). Un tel dispositif sert à rendre les maliciels inoffensifs, en empêchant les criminels d'accéder aux noms de domaine prévus et en réenregistrant ces derniers pour le compte d'une organisation de sécurité. Il devient ainsi possible d'identifier les appareils infectés qui, au lieu de se connecter avec les serveurs des exploitants du maliciel, s'adresseront aux serveurs de l'organisation de sécurité. Le NCSC collecte et analyse ces données dans tout l'espace

59 Aufstieg von IcedID (computerworld.ch)

60 Investigating a unique "form" of email delivery for IcedID malware (microsoft.com)

61 Voir Malware après un appel (ncsc.admin.ch); Aktuelle Ransomware-Angriffe mit Pakettrick (infoguard.ch)

62 CVE-2020-1472 (mitre.org); NVD - CVE-2020-1472 (nist.gov); Qu'est-ce que Zerologon? (trendmicro.com).

d’adressage suisse, et informe les propriétaires des appareils ayant subi une infection, par l’intermédiaire de leur fournisseur d’accès.

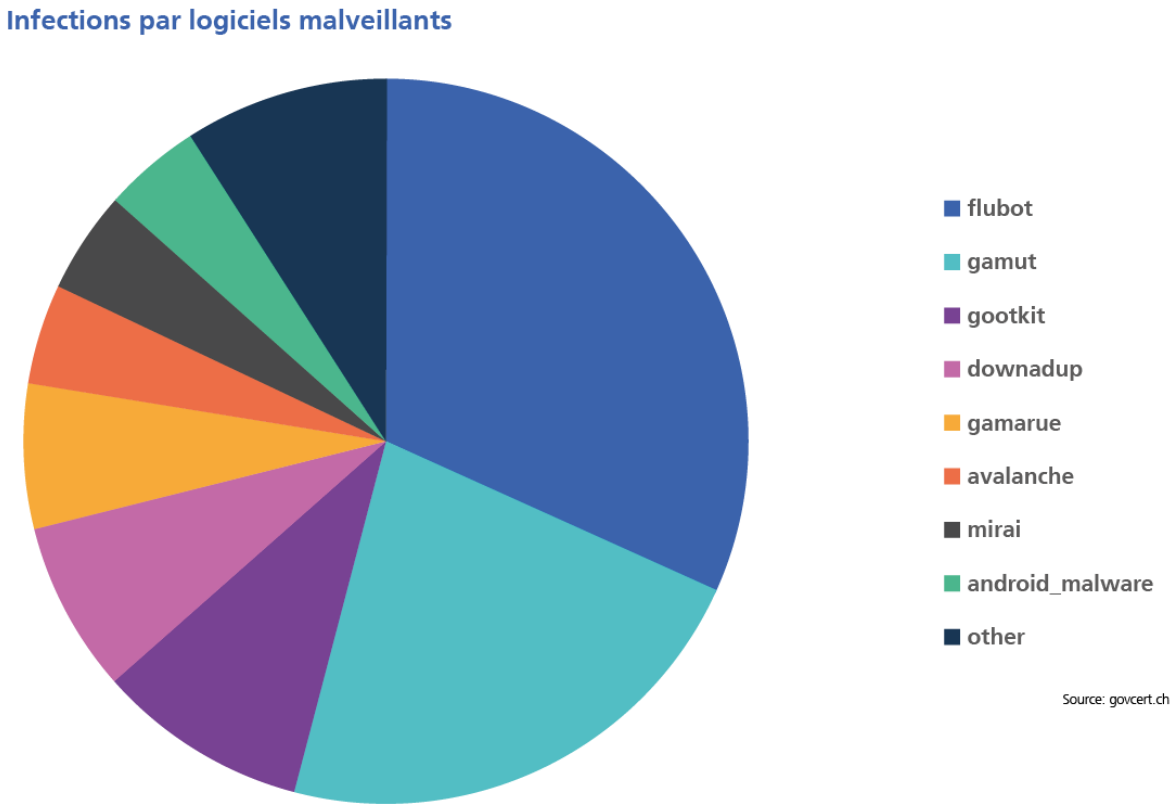


Fig. 6: Répartition d’infections par logiciels malveillants en Suisse détectés par le NCSC au premier semestre 2021.

Le maliciel «Flubot» s’est répandu au premier semestre dans toute l’Europe, à l’occasion de vastes campagnes basées sur des SMS. La menace a d’abord visé les utilisateurs de smartphones Android dans les pays nordiques et le Royaume-Uni, avant d’atteindre la Suisse et l’Autriche au mois de juin.

Le SMS contenant un lien infecté par Flubot est distribué à l’aide de différents scénarios. En Suisse, un SMS rédigé en allemand annonce un soi-disant nouveau message vocal. En cliquant sur le lien, la personne est guidée pour installer une application qui téléchargera le maliciel sur son téléphone[63].

Fig. 7: Exemple de SMS contenant le lien Flubot.

63 Das SMS "Neue Voicemail" ist die gefährliche Schadsoftware FluBot (cybercrimepolice.ch)

«Flubot» peut afficher une fausse page pour tromper l'utilisateur, lors d'attaques par recouvrement (*overlay attack*), et espionner ainsi les activités d'e-banking de la victime. Il a également pour propriété d'agir comme un ver, en dérobant la liste des contacts de la victime qui recevront à leur tour automatiquement le même SMS. Cette propriété explique la rapide propagation de la menace en Suisse.

Le NCSC a mis en garde la population ainsi que les infrastructures critiques face à Flubot[64].

Recommandations en cas de SMS ou autre message court suspect

- Ne pas cliquer sur un lien provenant d'un expéditeur inconnu.
- Effacer le SMS.
- En cas d'installation de l'application:
  - rétablir la configuration d'usine de son téléphone;
  - informer son fournisseur télécom;
  - bloquer ses cartes de crédit;
  - réinitialiser l'accès à tous ses comptes (bancaires, cryptomonnaies, messagerie).

4.2.2 Logiciel à double usage «Cobalt Strike»

«Cobalt Strike» est un outil commercial de sécurité, conçu afin de simuler dans le réseau un agresseur sophistiqué et endurant (*advanced persistent threat*, APT), de déployer les activités correspondantes et de tester les capacités de détection et de défense des administrateurs du réseau. Un tel logiciel peut bien sûr aussi être déployé lors de vraies agressions. Les escrocs comme les acteurs étatiques recourent volontiers à des copies pirates de «Cobalt Strike» pour se déplacer et se propager dans les systèmes qu'ils ont infectés. Les criminels s'en servent encore à des fins d'extraction de données, avant de déployer un rançongiciel. De même, les acteurs étatiques peuvent compliquer la découverte d'une attaque ciblée de cyberespionnage et son attribution grâce à «Cobalt Strike».

4.2.3 Rançongiciels (*ransomware*)

Les chevaux de Troie verrouillant les données, ou rançongiciels, perturbent les processus d'exploitation et freinent la capacité d'action des entreprises. Les préjudices causés peuvent aller d'un arrêt temporaire de production à la faillite, sans oublier la suspension de toutes les livraisons. Les clients tributaires des prestations de l'entreprise attaquée risquent également d'être sérieusement affectés.

Les maîtres chanteurs optent souvent pour une tactique à double voire triple détente[65]. Une fois qu'ils ont accès aux systèmes de leur victime, les escrocs commencent par en copier les données. Au cas où la victime refuserait de payer la rançon exigée pour le décryptage, ils la menacent de publier ses données. Si aucune des deux revendications n'aboutit, les

64 Rétrospective de la semaine 24 (ncsc.admin.ch)

65 Voir rapport semestriel NCSC 2020/2, chap. 4.3.1.

agresseurs contacteront le cas échéant des personnes ou organisations directement concernées par les données en leur possession, par exemple des partenaires contractuels ou des clients. En outre, durant la gestion de l'incident, les entreprises victimes sont parfois mises encore plus sous pression par des attaques DDoS[66].

Durant la période sous revue, toutes sortes de rançongiciels ont servi à lancer en Suisse des attaques contre des particuliers ou des PME actives dans tous les secteurs économiques[67].

Au niveau international, plusieurs incidents ont fait grand bruit. On retiendra par exemple les files d'attente aux stations-service du Sud-Est des États-Unis, où beaucoup de gens voulaient remplir encore une fois leur véhicule, par crainte d'une pénurie[68]. Le 7 mai 2021, Colonial Pipeline, un des principaux opérateurs de gazoducs du pays, a dû précipitamment fermer toutes les vannes en découvrant que le rançongiciel «Darkside[69]» s'était introduit dans son système informatique.[70] Les systèmes de pilotage intervenant dans le processus d'exploitation physique du pipeline avaient beau ne pas être directement concernés, eux aussi ont été mis à l'arrêt, par précaution. Le fonctionnement autarcique des systèmes de contrôle industriels est en effet devenu très délicat à assurer en raison de la connectivité accrue, à des fins d'optimisation des processus de gestion supérieurs, des environnements informatiques (IT) et des technologies opérationnelles (OT). À ce jour, les systèmes de contrôle industriels étaient considérés comme principalement vulnérables aux attaques de familles spécifiques de rançongiciels qui, comme «EKANS»[71] ou «Mega Cortex»[72], s'en prennent de façon ciblée aux processus industriels. Après avoir été sous le feu des médias et des autorités, le groupe «Darkside» a renoncé à une bonne partie de ses activités[73]. Par la suite, il est apparu que Colonial Pipeline avait versé une rançon, alors même que le groupe disposait de copies de sauvegarde[74]. Au cours de l'enquête, la justice américaine est parvenue à récupérer une partie de la rançon versée[75]. Cet incident, la cyberattaque lancée à la fin de mai contre le géant mondial de la viande JBS[76] et d'autres méfaits encore, où des cybercriminels avaient mis en

66 Extortion Payments Hit New Records as Ransomware Crisis Intensifies (paloaltonetworks.com)

67 Attaques au rançongiciel réussies contre des entreprises suisses (ncsc.admin.ch); Ransomware-Angreifer erpressen Schweizer Industriefirma Griesser (netzwoche.ch); Ransomware Angriffe in der Schweiz – was steckt dahinter? (entec.ch).

68 Colonial Pipeline systems resumes operations but Southeast still reeling from panic buying and gas price spikes (washingtonpost.com); Ransomware: Last Week Tonight with John Oliver (HBO) (youtube.com).

69 DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks (cisa.gov)

70 The Colonial Pipeline Hack Is a New Extreme for Ransomware (wired.com)

71 This is how EKANS ransomware is targeting industrial control systems (zdnet.com)

72 Voir rapport semestriel MELANI 2020/1, chap. 4.3.1.

73 DarkSide Ransomware Gang Quits After Servers, Bitcoin Stash Seized (krebsonsecurity.com)

74 Colonial Pipeline CEO: Paying DarkSide ransom was the 'right thing to do for the country' (zdnet.com)

75 DoJ Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside (justice.gov)

76 JBS: FBI says Russia-linked group hacked meat supplier (bbc.com); Ransomware: Meat firm JBS says it paid out $11m after attack (zdnet.com).

péril l'exploitation d'infrastructures critiques, ont convaincu le gouvernement américain qu'il fallait légiférer au plus vite et redoubler d'efforts au profit de la cybersécurité[77].

Le rançongiciel «Conti», qui a paralysé le système de santé irlandais a fait grand bruit[78]. Le 13 mai 2021, le National Cyber Security Centre (NCSC) d'Irlande était alerté concernant des activités suspectes menées dans le réseau du ministère de la santé publique. Il s'agissait d'une tentative d'accès à distance basée sur le logiciel «Cobalt Strike»[79]. Le lendemain, le Ministère parvenait à déjouer la tentative de verrouillage de ses systèmes. Or le service public de santé irlandais (HSE) était victime de «Conti» le 14 mai également. Des pans entiers du réseau du HSE ont dû être provisoirement déconnectés du réseau, pour des raisons de sécurité. Les prestations n'ont été disponibles que dans une mesure limitée, et il a fallu reporter divers traitements ou processus de diagnostic. Selon le HSE, les fonctions critiques liées aux soins intensifs et aux interventions d'urgence auraient néanmoins été garanties. Les agresseurs ont certes fourni gracieusement par la suite un programme de décryptage. Mais ils avaient dérobé du réseau du HSE des données de patients et ont menacé de les divulguer, en cas de non-paiement de la rançon. Des échantillons de données ont notamment été publiés comme moyen de preuve.

Des succès dans la lutte contre les rançongiciels méritent également d'être signalés: les autorités de poursuite pénale ukrainiennes sont ainsi parvenues à arrêter plusieurs membres de la bande organisée du rançongiciel «Clop» et à démanteler l'infrastructure utilisée par ce groupe pour lancer ses attaques. «Clop» a causé dans le monde un préjudice financier total d'environ 500 millions de dollars[80].

Conclusions / Recommandations:

Les chevaux de Troie verrouillant les données peuvent causer de graves dommages, en particulier si vos copies de sauvegarde sont affectées. Lors d'un tel incident, restez calme et agissez de façon réfléchie. Il est essentiel pour maîtriser un incident de découvrir le mode de propagation de l'infection et de prévenir toute récidive. Réinstallez les systèmes concernés et restaurez les données à partir de vos copies de sauvegarde.

Si personne dans votre entreprise ne dispose des connaissances requises, demandez l'assistance d'une entreprise spécialisée.

Le NCSC recommande aux victimes de ne jamais verser la rançon demandée. Tout paiement effectué conforte les criminels dans leur modèle d'affaires, renfloue leurs finances et les incite à poursuivre et développer encore leurs activités. Dans le pire des cas, on s'expose à perdre ses données et l'argent versé. Le NCSC conseille donc de porter plainte auprès des autorités de police compétentes.

Au fil des ans, l'attention s'est focalisée sur la couverture des cyberincidents par une cyberassurance. De tels produits ont leur légitimité: ils prennent notamment en charge les

77 Executive Order on Improving the Nation's Cybersecurity (whitehouse.gov)

78 Department of Health hit by cyberattack similar to that on HSE (irishtimes.com)

79 Voir ci-dessus chap. 4.2.2, à propos de «Cobalt Strike».

80 Ukraine arrests Clop ransomware gang members, seizes servers (bleepingcomputer.com)

risques liés à la cybercriminalité et aident à gérer les difficultés surgissant dans le cadre du commerce électronique, en cas d'atteinte à la réputation, d'attaque de virus, de vol de données ou encore d'usurpation d'identité. Or si les assurances couvrent le paiement de rançons, cela pourrait inciter les maîtres chanteurs à se concentrer sur les entreprises dûment assurées, afin d'augmenter leurs chances de se faire payer. La décision pour ou contre une cyberassurance relève de la seule compétence des entreprises. Une telle décision devrait être mûrement réfléchie. La conclusion d'une cyberassurance ne doit en aucun cas conduire à diminuer son budget informatique ou à négliger le fonctionnement correct de son parc informatique.

D'autres informations figurent sur le site du NCSC: Rançongiciels (ncsc.admin.ch).

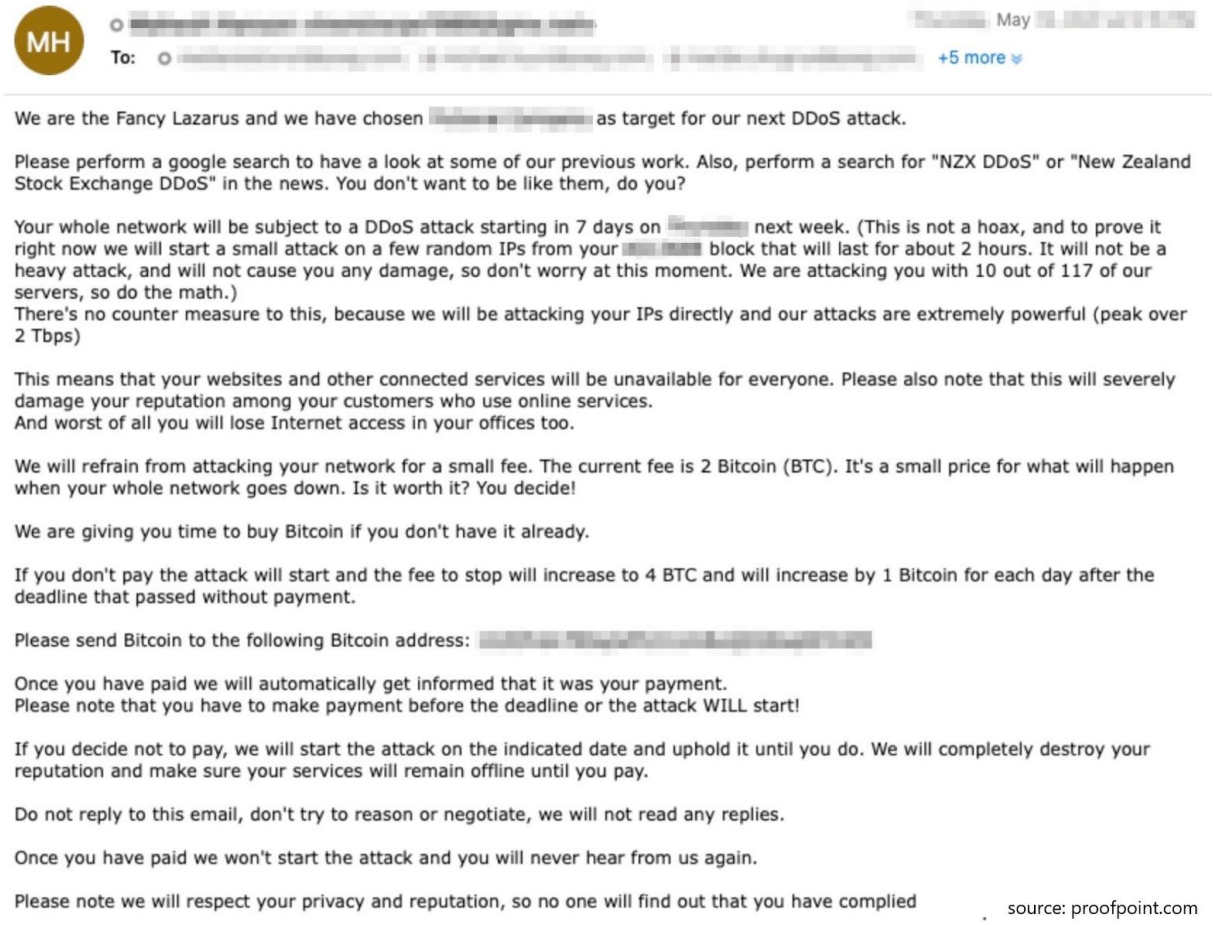
4.3 Attaques contre des sites ou services Web

4.3.1 Attaques DDoS

Comme en 2020, les attaques par déni de service distribué (DDoS) ont été nombreuses au premier semestre 2021, en Suisse et ailleurs dans le monde. Quelque 26 incidents de ce type ont été annoncés au NCSC. Le mode opératoire comprend d'ordinaire une attaque initiale conséquente mais maîtrisable (oscillant entre 40 et 120 gigabits par seconde), suivie ou précédée d'un courriel d'extorsion. La victime y est priée de verser une rançon, sous peine de subir une attaque massive, de plus de deux térabits par seconde. Ce n'était toutefois qu'un coup de bluff puisque dans aucun des cas observés, malgré le non-paiement de la rançon, les menaces n'ont été mises à exécution. Les organisations prises pour cibles se répartissent entre différents secteurs, dont la finance, la santé et l'aviation. Les fournisseurs Internet ont également subi ce genre d'attaques dont l'impact est resté limité, grâce aux mesures de défense adoptées. À l'exception notable de l'hébergeur des sites Web du canton, de la ville et de la police de Saint-Gall, qui sont restés indisponibles pendant plusieurs heures[81]. Dans le passé, les escrocs avaient usurpé le nom de deux groupes étatiques célèbres («Lazarus» et «Fancy Bear»)[82]. Dans les plus récentes vagues d'attaques, ils se font appeler «Fancy Lazarus».

[81] Hackergruppe greift St. Galler Hoster nicht mehr an (netzwoche.ch)

[82] Voir rapport semestriel NCSC 2020/2, chap. 4.4.1.



MH

To: +5 more

May

We are the Fancy Lazarus and we have chosen as target for our next DDoS attack.

Please perform a google search to have a look at some of our previous work. Also, perform a search for "NZX DDoS" or "New Zealand Stock Exchange DDoS" in the news. You don't want to be like them, do you?

Your whole network will be subject to a DDoS attack starting in 7 days on next week. (This is not a hoax, and to prove it right now we will start a small attack on a few random IPs from your block that will last for about 2 hours. It will not be a heavy attack, and will not cause you any damage, so don't worry at this moment. We are attacking you with 10 out of 117 of our servers, so do the math.)
There's no counter measure to this, because we will be attacking your IPs directly and our attacks are extremely powerful (peak over 2 Tbps)

This means that your websites and other connected services will be unavailable for everyone. Please also note that this will severely damage your reputation among your customers who use online services.
And worst of all you will lose Internet access in your offices too.

We will refrain from attacking your network for a small fee. The current fee is 2 Bitcoin (BTC). It's a small price for what will happen when your whole network goes down. Is it worth it? You decide!

We are giving you time to buy Bitcoin if you don't have it already.

If you don't pay the attack will start and the fee to stop will increase to 4 BTC and will increase by 1 Bitcoin for each day after the deadline that passed without payment.

Please send Bitcoin to the following Bitcoin address:

Once you have paid we will automatically get informed that it was your payment.
Please note that you have to make payment before the deadline or the attack WILL start!

If you decide not to pay, we will start the attack on the indicated date and uphold it until you do. We will completely destroy your reputation and make sure your services will remain offline until you pay.

Do not reply to this email, don't try to reason or negotiate, we will not read any replies.

Once you have paid we won't start the attack and you will never hear from us again.

Please note we will respect your privacy and reputation, so no one will find out that you have complied

source: proofpoint.com

Fig. 8: Exemple de courriel d'extorsion de Fancy Lazarus.

La Belgique a été en mai le théâtre d'une vaste cyberattaque visant simultanément Belnet et d'autres opérateurs de télécommunications. Elle a provoqué une panne de plusieurs heures d'Internet et l'interruption, par effet domino, de nombreux services comme les débats du Parlement belge (tenus par visioconférence), les cours en ligne des universités ou encore les sites Web de divers services publics[83].

Conclusion / Recommandations:

Le chantage DDoS représente une activité de masse. Les pirates tentent leur chance auprès d'un maximum d'entreprises choisies un peu au hasard. Si la manœuvre échoue, ils poursuivent leur quête ailleurs. À supposer qu'une attaque DDoS (de démonstration) ait réussi à bloquer les systèmes d'une entreprise, cette dernière sera considérée comme une victime potentielle et les escrocs redoubleront d'efforts, dans l'espoir qu'une rançon leur soit versée. Il est par conséquent conseillé de bien se préparer à d'éventuelles attaques DDoS.

83 Belgium's government network goes down after massive DDoS attack (therecord.media)

Le NCSC recommande de conclure pour les systèmes critiques un abonnement à un service commercial de protection DDoS (*DDoS Mitigation Service*). Beaucoup de fournisseurs d'accès à Internet proposent une telle prestation, moyennant un forfait.

Le site Internet du NCSC indique diverses mesures utiles pour prévenir ou déjouer les attaques DDoS: Attaque affectant la disponibilité (attaque DDoS) (ncsc.admin.ch)

4.3.2 Sites Web compromis

Les agresseurs savent tirer parti des données dérobées ou de vulnérabilités non corrigées pour accéder à l'administration des sites Web et y placer du code malveillant. Les infections par *drive-by download* en sont un cas d'application typique, où les pirates tentent d'infecter l'appareil des visiteurs de pages manipulées par leurs soins. Dans d'autres cas, les internautes seront réacheminés vers des publicités douteuses, des sites frauduleux ou des offres louches. On peut encore citer les pratiques abusives de référencement (*Black Hat SEO*)[84], consistant à ajouter des mots-clés à un site pour influencer le résultat des moteurs de recherche.

Quand le NCSC constate que des sites Web ont été compromis, il en informe l'exploitant, l'administrateur ou l'hébergeur, afin qu'ils puissent prendre les mesures utiles. Au premier semestre 2021, le NSCS a envoyé 803 notifications et 445 courriels de rappel à propos de sites possédant un nom de domaine suisse (extension en «.ch» ou «.swiss»).

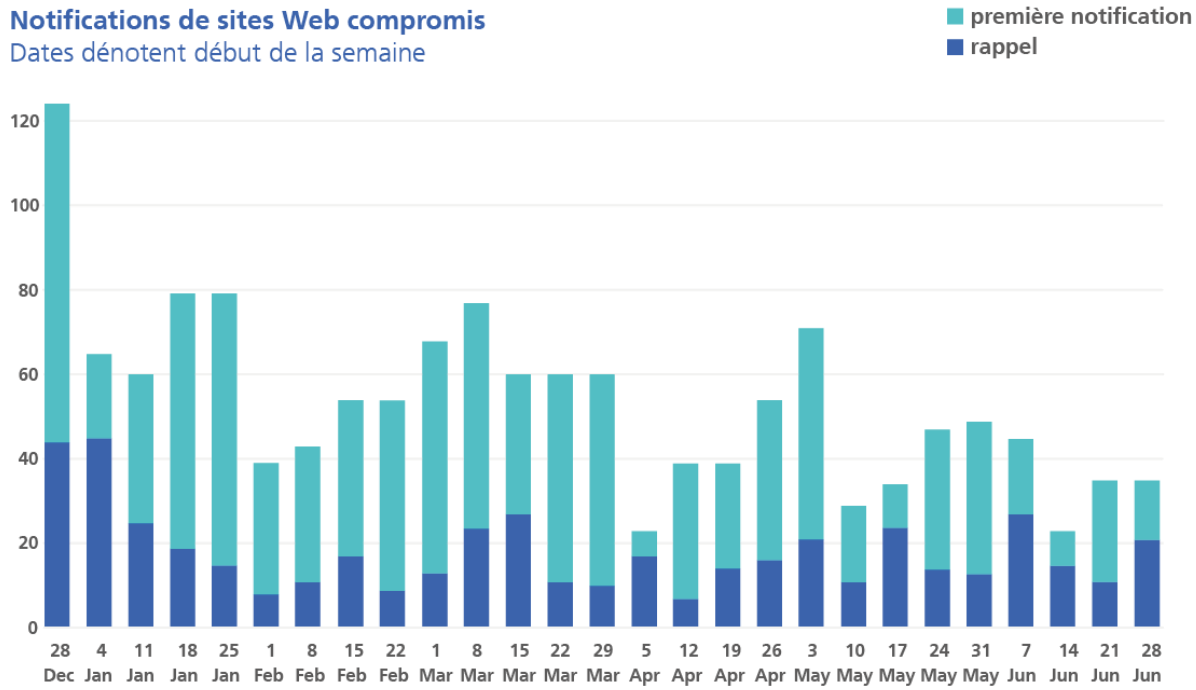


Fig. 9: Notifications envoyées par le NCSC aux exploitants, administrateurs ou hébergeurs de sites Web.

[84] Black hat SEO and You Won (ncsc.nl); L'optimisation pour les moteurs de recherche (*search engine optimization*, SEO) inclut l'ensemble des techniques visant à améliorer le positionnement d'un site Web dans les résultats d'un moteur de recherche. Voir: Optimisation pour les moteurs de recherche (wikipedia.org).

Recommandations:

Si un site Web a été piraté, il convient de procéder à son nettoyage systématique, en localisant et supprimant les maliciels ou les contenus étrangers qui y figurent. En outre, il faut veiller à disposer de la dernière version du système de gestion de contenu (*content management system*, CMS) et des modules d'extension (*plug-in*). Tous les ordinateurs servant à l'administration du site Web feront l'objet d'une analyse antivirus et d'un nettoyage, le cas échéant. Il reste enfin à modifier toutes les données d'accès. D'autres informations utiles figurent sur le site du NCSC: Site web piraté – que faire? (ncsc.admin.ch)

Après le nettoyage du site Web, il est recommandé d'adopter des mesures supplémentaires visant à prévenir toute nouvelle intrusion criminelle. Le site du NCSC indique encore des Mesures de protection pour les systèmes de gestion de contenu (ncsc.admin.ch).

4.4 Systèmes de contrôle industriels & OT

La pandémie et les conditions météorologiques extrêmes ont fait ressortir au cours des derniers mois l'importance des infrastructures critiques. La technologie opérationnelle (OT) soutient voire rend possible bien des processus, dont le pilotage est tributaire des systèmes de contrôle industriels (SCI). Or outre les facteurs environnementaux et les fausses manipulations, les attaques malveillantes lancées contre de tels systèmes ou visant les appareils leur étant raccordés représentent également une menace pour la disponibilité et l'intégrité des infrastructures critiques.

4.4.1 Infiltration du réseau électrique indien par «RedEcho»

À la fin février 2021, des chercheurs en sécurité de RecordedFuture ont publié un rapport sur des incidents survenus en Inde, où un acteur qu'ils ont baptisé «RedEcho»[85] était parvenu à s'introduire dans les systèmes de plusieurs exploitants d'infrastructures critiques. Le maliciel «Shadowpad»[86] a notamment servi à mener toute une série d'attaques prenant pour cibles, outre deux ports, des organisations d'approvisionnement électrique, dont leurs centres régionaux responsables de la stabilité du réseau (*dispatching*).

85 Chinese Group RedEcho Targets the Indian Power Sector (recordedfuture.com)

86 ShadowPad (Malware Family) (fraunhofer.de)

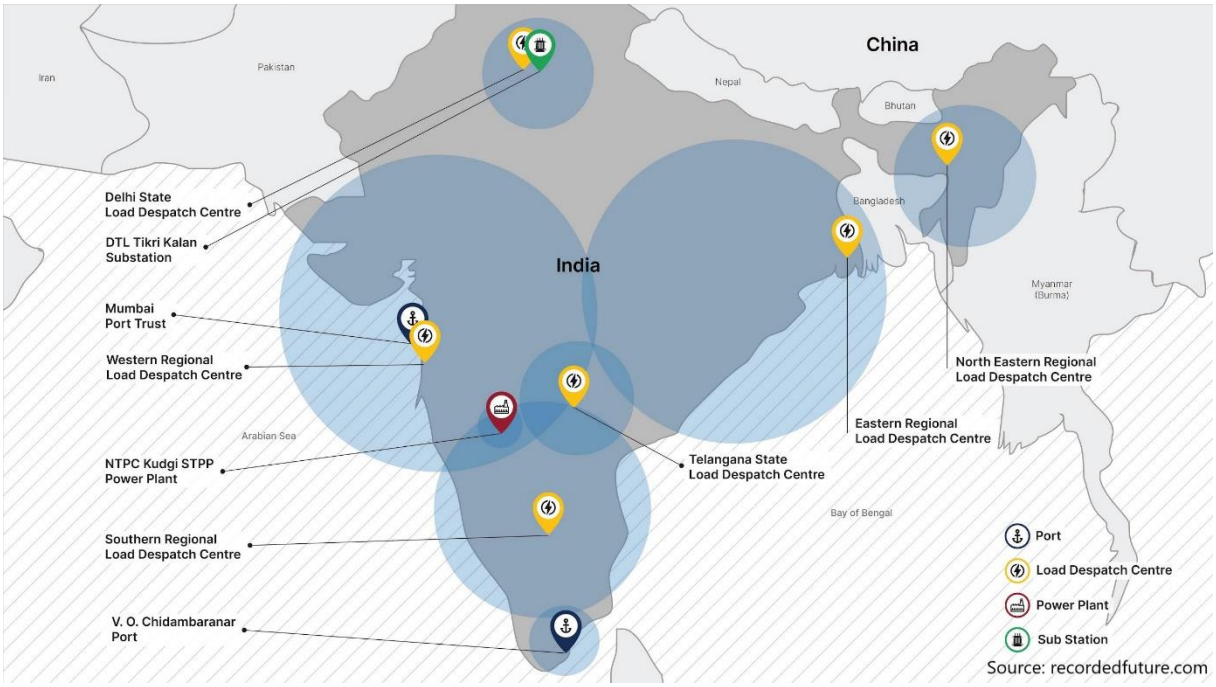


Fig. 10: Cibles de RedEcho.

RecordedFuture n'a découvert dans son analyse aucun indice de tentative de sabotage tout en signalant la corrélation temporelle de tensions à la frontière sino-indienne. Le rapport d'accompagnement publié par le New York Times[87] formule l'hypothèse selon laquelle les réseaux infiltrés serviraient à exercer des menaces en coulisse sur l'Inde. La panne électrique survenue en automne 2020 à Bombay[88] y est citée en exemple, bien qu'aucun lien avec les activités de «RedEcho» n'ait pu être prouvé selon RecordedFuture.

4.4.2 Tentatives de manipulation de l'approvisionnement en eau en Floride

En février 2021, le curseur de la souris d'un ordinateur servant à contrôler le système de traitement de l'eau potable de la petite ville d'Oldsmar, en Floride, s'est mis à bouger tout seul[89]. Le technicien de service est parvenu in extremis à empêcher l'intrus d'augmenter à distance la concentration de soude caustique (hydroxyde de sodium) à un niveau dangereux pour la santé. Les infrastructures municipales ont frôlé la catastrophe à cause d'un logiciel d'accès à distance mal protégé[90], grâce auquel le saboteur était parvenu jusqu'à l'appareil utilisé pour régler les paramètres de traitement de l'eau potable.

87 China Appears to Warn India: Push Too Hard and the Lights Could Go Out (nytimes.com)

88 Voir rapport semestriel NCSC 2020/2, chap. 4.5.1.

89 A Hacker Tried to Poison a Florida City's Water Supply, Officials Say (wired.com)

90 Compromise of U.S. Water Treatment Facility (cisa.gov)

Indication / Recommandations:

Afin de se préparer aux menaces qui pèsent sur les systèmes de contrôle industriel dans le domaine du pilotage des processus, les associations faîtières des secteurs de l'eau et de l'évacuation des eaux usées, du gaz et des denrées alimentaires ainsi que les entreprises de transports publics ont conçu avec l'Office fédéral de l'approvisionnement économique (OFAE) des normes utiles pour accroître la sécurité de l'information dans leurs champs d'activité respectifs:

Normes minimales par secteur (ofae.admin.ch)

4.5 Fuites de données

Le phénomène des fuites de données s'est aussi produit durant le semestre sous revue, dans divers contextes. De même que les groupes de rançongiciels ont intégré la publication de données dans leur mode opératoire (voir chap. 4.2.3), des fuites de données peuvent survenir lors de campagnes d'espionnage. En pareil cas, les données visées appartiennent souvent à des services étatiques ou relèvent de la propriété intellectuelle.

La valeur monétaire de certains types de données, à l'instar des données médicales, des données de clients ou d'identité ainsi que des données bancaires, en fait des cibles privilégiées. Il est vrai que les cybercriminels peuvent aussi utiliser à toutes sortes de fins des données supposées avoir une moindre valeur, par exemple pour échafauder des scénarios destinés à leurs futures fraudes dans les réseaux sociaux, ou simplement pour collecter des adresses électroniques auxquelles ils enverront de manière ciblée ou à grande échelle des courriels de phishing, des maliciels ou d'autres messages frauduleux.

4.5.1 SITA: vol de données de passagers

La Société internationale de télécommunications aéronautiques (SITA), fournisseur mondial de services informatiques dédiés à l'industrie du transport aérien, s'est fait dérober les données de passagers de diverses compagnies aériennes lors d'une cyberattaque[91].

L'incident est survenu dans le système de gestion des passagers (*passenger service system*, PSS), soit les serveurs où sont stockées les données des passagers de nombreuses compagnies aériennes. Les données de clients des programmes de fidélisation de Star Alliance et OneWorld ont notamment été compromises, à l'instar de celles de 1,35 million de participants au programme «Miles-and-More»[92]. Swiss compte parmi les clients de ce prestataire informatique. Bien que lorsque SITA a annoncé la cyberattaque en mars, il semblait qu'aucune donnée sensible n'ait été volée, la compagnie Air India par exemple a signalé cinq semaines plus tard que l'incident avait entraîné le vol des données de 4,5 millions de ses

91 SITA statement about security incident (sita.aero)

92 Hacker erbeuten 1,3 Millionen Datensätze von Swiss- und Star-Alliance-Kunden (inside-it.ch)

passagers. Les données dérobées incluaient les informations du passeport et de la carte de crédit[93].

4.5.2 Cyberattaques sur les réseaux sociaux et *data scraping*

Au début d'avril, les données de 533 millions de profils Facebook ont été publiées sur un forum de hackers. Les usagers concernés provenaient de plus de 100 pays. Les données, qui comprenaient le numéro de téléphone, l'adresse électronique, le nom complet, la date de naissance et la localisation des utilisateurs, étaient déjà connues depuis janvier et proposées à la vente au marché noir. La fuite serait toutefois antérieure. Facebook a fait savoir qu'elle était probablement due à une vulnérabilité corrigée en août 2019[94].

Vers la fin de juin, une base de données renfermant 700 millions de profils LinkedIn a été annoncée à la vente sur le Darkweb. Les informations, qui se rapportaient à plus de 90 % des utilisateurs de ce réseau social, ne contiennent visiblement là non plus ni données de cartes de crédit ni mots de passe. Bien que par précaution les utilisateurs aient été invités à changer de mot de passe, LinkedIn réfute toute intrusion dans ses serveurs et affirme qu'il s'agit d'un simple cas de récupération de données (*data scraping*)[95].

Il est en effet possible de recueillir d'énormes quantités de données par «*data scraping*»: toutes sortes de techniques permettent d'extraire systématiquement des sites Web publics des contenus tels que le numéro de téléphone ou l'adresse électronique. Ce genre d'activité est d'ailleurs pratiqué à des fins d'optimisation du marketing ou de *business intelligence,* etc. par des entreprises actives dans de multiples domaines. À l'instar de SocialArks, start-up chinoise aidant les multinationales à développer leur activité dans l'empire du Milieu, qui collecte les données de Facebook, Instagram et LinkedIn. C'est ce qu'a révélé un serveur mal configuré, sur lequel étaient stockés de manière non sécurisée plus de 400 Go de données publiques ou privées relatives aux profils de 214 millions d'utilisateurs de plateformes sociales, soit 318 millions d'entrées au total. La base de données renfermait aussi, pour des raisons inexpliquées, des données non accessibles au public[96].

Il est encore possible de regrouper les données provenant d'anciennes fuites pour créer une base de données agrégée. «Compilation of Many Breaches», la plus vaste compilation publiée à ce jour, présente par ordre alphabétique plus de 3,2 milliards d'adresses électroniques accompagnées de leur mot de passe, dont certains identifiants de connexion à Netflix et LinkedIn[97].

---

93 Data-Breach-Notification.pdf (airindia.in)

94 Bot Lets Hackers Easily Look Up Facebook Users' Phone Numbers (vice.com);
533 million Facebook users' personal data leaked online (cyberscoop.com).

95 LinkedIn denies exposure of 700 million user records is a data breach (computerweekly.com)

96 The SocialArk Data Breach Uncovered the Open Source Paradox (cybersecurity-magazine.com);
Millions of Social Profiles Leaked by Chinese Data-Scrapers (threatpost.com).

97 COMB: over 3.2 Billion Email/Password Combinations Leaked (cybernews.com)

Conclusion / Recommandations:

Une gestion attentive et responsable des données s'avère prioritaire pour les entreprises. En plus d'adopter des mesures de sécurité adéquates, toute entreprise devrait se préparer au scénario d'une fuite de données et élaborer à l'avance un plan de réponse aux incidents (*data breach response plan*), qui lui permette de déployer rapidement une action coordonnée en cas de besoin.

Les services Internet rendant accessibles au public leurs fichiers de données feraient bien de protéger leur plateforme par des dispositions appropriées contre les consultations (de masse) automatisées.

Pour se protéger à titre privé face au «*scraping*» des données, il est indiqué de restreindre l'accès public à ses profils sociaux et, de façon générale, de bien réfléchir aux contenus que l'on souhaite publier en ligne.

Il est également conseillé de vérifier les paramètres des applications et de ne leur accorder que les autorisations qui sont strictement nécessaires.

D'autres informations figurent sur le site du NCSC: Fuite des dates (ncsc.admin.ch)

4.6 Espionnage

4.6.1 Nobelium: nouvelles campagnes dans le sillage de SolarWinds

Le 27 mai, Microsoft a publié une mise en garde contre une nouvelle campagne de diffusion d'un maliciel, menée par un agresseur sophistiqué et persistant (*advanced persistent threat*, APT). «Nobelium» – nom donné aux pirates par Microsoft – avait déjà lancé en particulier l'attaque contre SolarWinds[98]. La campagne faisait suite à une phase d'essai, déployée du début de 2021 jusqu'à la fin de mai. Durant cette période, Microsoft a relevé toute une série de progrès techniques, dans la méthode de transmission des messages de phishing comme pour la définition des profils des destinataires. Cette capacité d'innovation permanente et d'utilisation d'outils ou infrastructures spécifiques pour chaque cible fait de «Nobelium» une menace extrêmement complexe et rend sa découverte d'autant plus difficile. Puis le 25 mai, la campagne s'est emparée du compte ouvert par une ONG américaine auprès de la plateforme de marketing «Constant Contact» pour lancer une attaque contre plus de 3000 comptes liés à 150 organisations, principalement basées aux États-Unis. Il s'agissait en particulier d'ONG, d'établissements de recherche, de services gouvernementaux et d'agences internationales. Les courriels envoyés parlaient notamment d'ingérences étrangères dans les élections présidentielles de 2020 et renfermaient une adresse URL aboutissant au service légitime «Constant Contact», avant d'être réacheminée vers l'infrastructure contrôlée par les pirates[99].

---

98 Voir rapport semestriel NCSC 2020/2, chap. 4.7.2.

99 New sophisticated email-based attack from NOBELIUM (microsoft.com)

4.6.2 «Hafnium» tire parti de MS Exchange

En mars 2021, Microsoft a signalé qu'un groupe baptisé «Hafnium» s'était engouffré dans une série de failles des serveurs Microsoft Exchange[100] inconnues jusque-là[101]. «Hafnium» était déjà soupçonné auparavant d'avoir obtenu accès à des serveurs Microsoft Exchange grâce à des mots de passe dérobés. Autrement dit, cet acteur avait eu tout loisir de se familiariser avec les réseaux des entreprises ou autorités concernées. Parmi ses cibles figuraient des établissements d'enseignement supérieur, des instituts de recherche spécialisés dans les maladies infectieuses, des cabinets d'avocats, des entreprises actives dans la défense, des groupes de réflexion et des ONG[102]. «Hafnium» exfiltre généralement les données vers des sites de partage de fichiers comme «MEGA»[103].

4.7 Phishing et ingénierie sociale

4.7.1 Phishing

Au premier semestre 2021, quelque 4682 sites de phishing signalés sur le portail antiphishing.ch géré par le NCSC ont été vérifiés. Soit un niveau à peine supérieur à celui du deuxième semestre 2020, où 4498 sites de phishing avaient été annoncés.

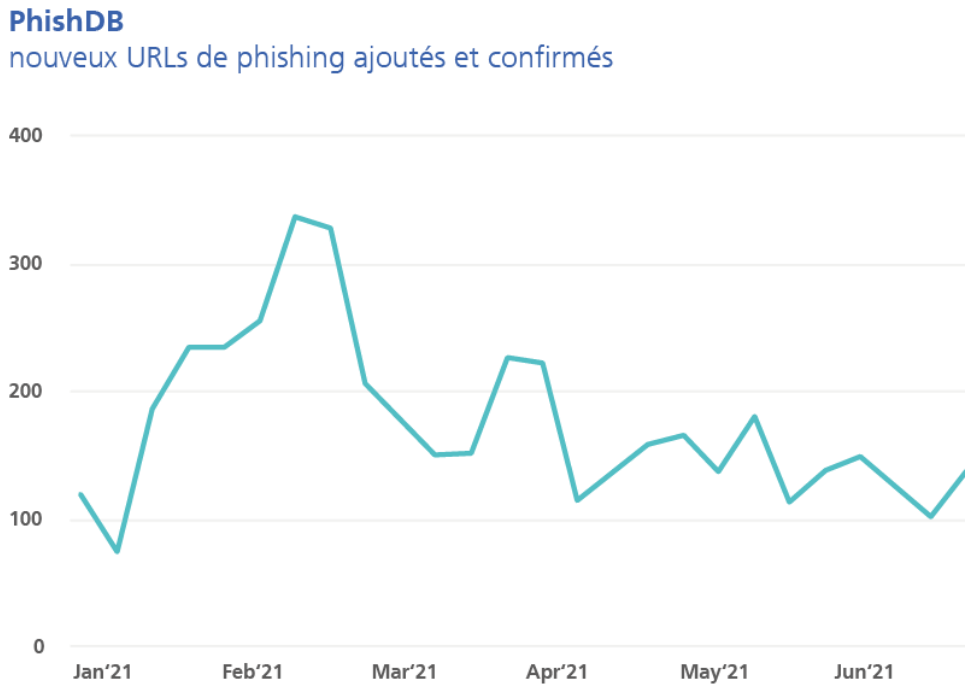


Fig. 11: Nombre d'adresses URL de phishing examinées et confirmées par le NCSC chaque semaine, au premier semestre 2021. Les données actuelles sont publiées sous: https://www.govcert.admin.ch/statistics/phishing/.

[100] Voir ci-dessus, chap. 3.1.1.
[101] HAFNIUM targeting Exchange Servers with 0-day exploits (microsoft.com)
[102] HAFNIUM, Operation Exchange Marauder, Group G0125 (mitre.org)
[103] HAFNIUM (Threat Actor) (fraunhofer.de)

Le NCSC observe ici une évolution des tentatives de phishing qui privilégient désormais, à la place des grandes marques internationales, des entreprises actives sur le marché suisse. Le secteur financier[104] figure toujours parmi les groupes cibles, au même titre que les sociétés de logistique[105], les fournisseurs d'accès à Internet[106], et d'autres encore.

Dans le cas des attaques de phishing ou d'autres attaques d'ingénierie sociale, les tactiques déployées varient beaucoup sur le fond. En règle générale, il est question d'un prétendu incident qui paraît ancré dans le quotidien et qu'on aura souvent tendance à prendre pour véridique. À première vue, les messages semblent émaner d'entreprises dignes de confiance et connues, dont le logo a été usurpé pour mieux tromper les destinataires.

4.7.2 Smishing (hameçonnage par SMS)

Les SMS et autres services de messages courts sont de plus en plus souvent détournés de leur but premier à des fins de phishing, en l'occurrence de «smishing»[107]. De tels messages abordent souvent un sujet du quotidien et comportent un lien s'affichant sur le téléphone mobile. Ce lien conduit à une page spécialement préparée par les escrocs, sur laquelle il faut indiquer ses données personnelles ou les détails de sa carte de crédit.

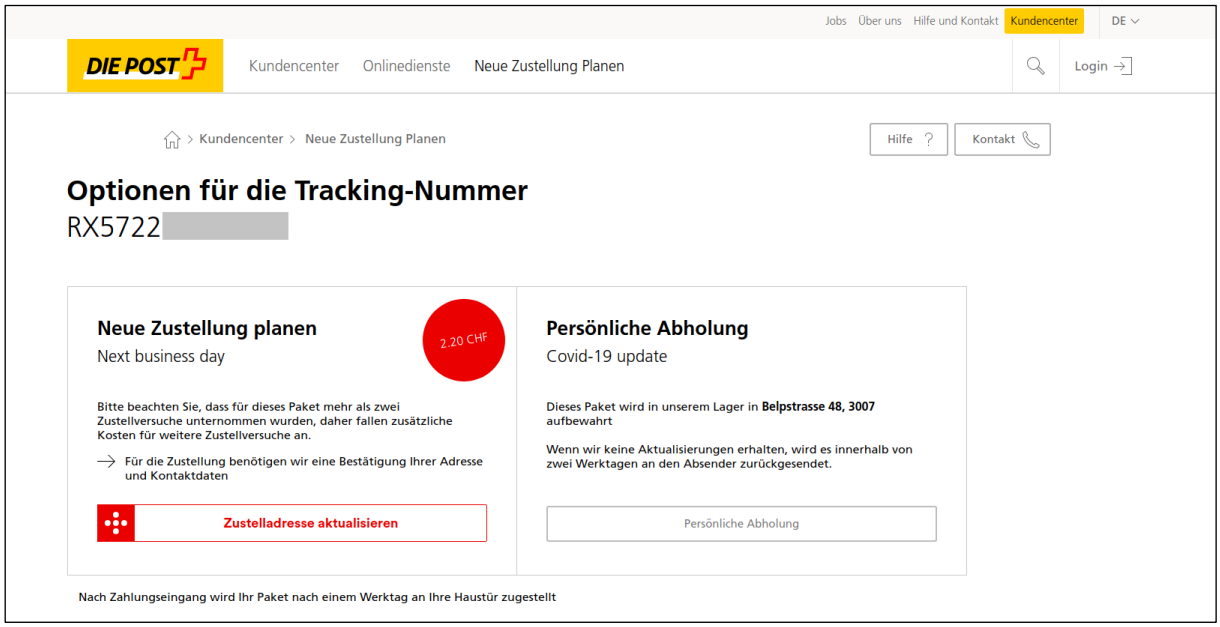


Fig. 12: Exemple de contrefaçon de site Web destinée à dérober les données d'accès.

104 Viseca Phishing Mails - nicht autorisierte Transaktion - Zugriff eingeschränkt (cybercrimepolice.ch)

105 Phishing Mail im Namen der Post - Paket konnte nicht geliefert werden, da kein Zoll bezahlt wurde (cybercrimepolice.ch)

106 E-Mail angeblich von der Swisscom (Schweiz) AG betr. Rückerstattung (cybercrimepolice.ch); les attaques visant les propriétaires de sites Web restent aussi d'actualité: Phishing Attackers Targeting Webmasters (govcert.admin.ch).

107 SMS - Sie haben eine DIE POST-Sendung (cybercrimepolice.ch)

4.7.3 Ingénierie sociale

Il existe différentes familles de maliciels qui épient notamment les conversations électroniques sur les systèmes infectés. Les échanges de courriels parviendront naturellement aussi aux escrocs, s'ils se sont procuré par phishing les données d'accès de leur victime. Il s'ensuit que toujours plus de messages sont adressés aux personnes ayant participé à de telles conversations. Bien souvent, l'expéditeur semble être un autre protagoniste de l'échange. Soit son adresse a été falsifiée, soit le courriel émane d'un compte compromis et aura par conséquent été expédié à partir de l'adresse indiquée, mais pas par le propriétaire du compte. Le courriel donne l'impression d'avoir été envoyé une seconde fois (avec une annexe spécialement préparée), ou alors il semble prolonger la conversation en cours. Au cas où il renfermerait du texte, celui-ci sera (à ce jour) généralement rédigé en anglais et reste très général (par ex. «Bonjour. Veuillez examiner les documents annexés» ou «Hello, le document annexé renferme une information intéressante») et les éventuelles annexes porteront un nom vide de sens (par ex. «Documentation (60243).xls», «docs_(20210412).xls» ou «Application (756.466).xls»), ou alors elles auront une appellation piquant la curiosité (par ex. «CompensationClaim.xls» ou «fiches de salaire.xls»). Un clic sur une telle annexe provoquera une infection de l'appareil.

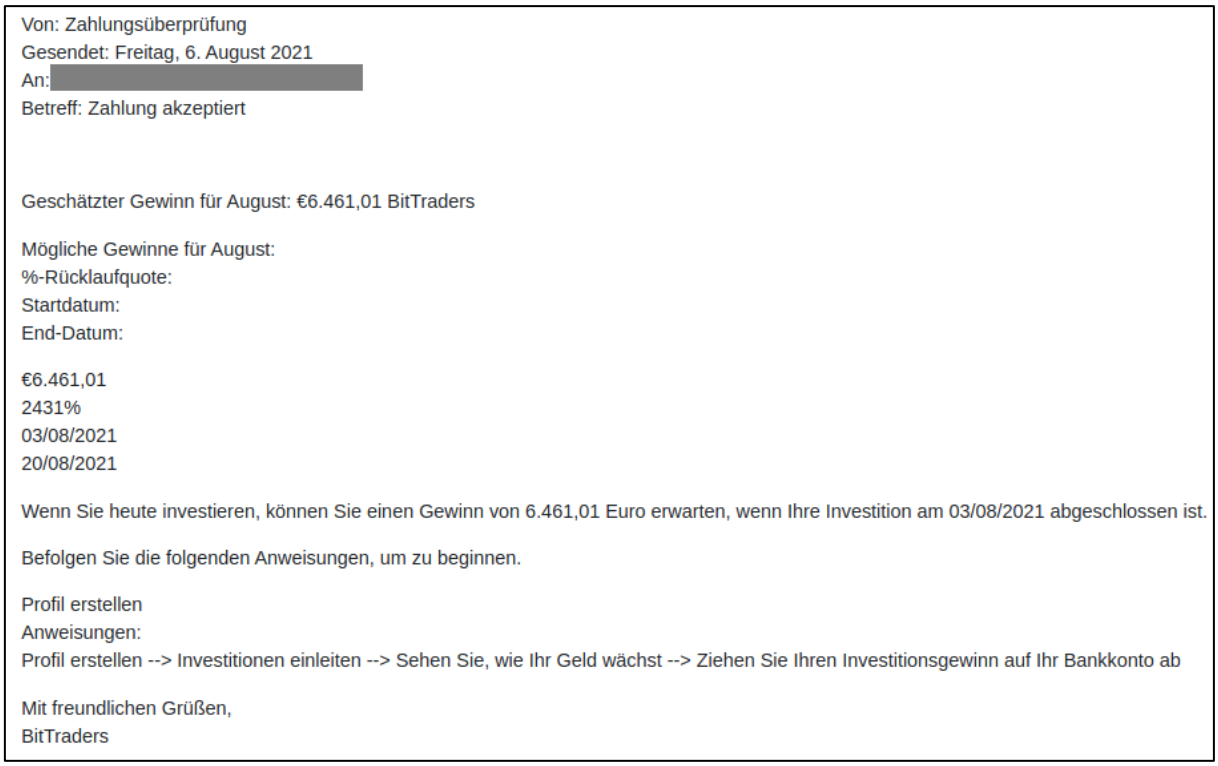
Recommandations:

- Méfiez-vous des courriels et des SMS non sollicités: faites preuve de prudence non seulement avec les expéditeurs qui vous sont inconnus, mais aussi avec ceux qui vous sont (apparemment) familiers.
- Méfiez-vous des documents qui vous parviennent à l'improviste sans commentaire, ou alors dont le texte d'accompagnement reste très vague.
- Si lorsque vous ouvrez un fichier, il vous est demandé d'activer une macro, informez-en votre responsable de la sécurité.
- Soyez sceptique, si vous recevez des courriels ou des SMS cherchant à piquer votre curiosité ou exigeant de votre part une action spécifique (clic sur un lien, ouverture d'un document). Un délai vous est souvent imparti, afin de vous mettre sous pression.
- Ne cliquez pas sur les annexes et ne suivez jamais les liens de messages suspects, même par curiosité – vous risquez sinon d'infecter votre appareil ou d'aboutir à des sites Web douteux. En cas d'hésitation, interrogez le prétendu expéditeur en utilisant un moyen de contact que vous connaissiez auparavant ou qui est indiqué sur son site Web par exemple, pour savoir de quoi il s'agit et si le courriel émane réellement de lui.

4.8 Escroquerie: variantes actuelles de la fraude à l'investissement

La majeure partie des annonces parvenant au NCSC ont trait à des tentatives de fraude, qui peuvent être de différents types. La fraude à l'investissement en fait partie. Il est très facile de diffuser de telles offres alléchantes par courriel, sur des pages Web ou dans les médias sociaux. À l'heure actuelle, les escrocs surfent sur la vague des cryptomonnaies et font miroiter un bénéfice élevé à court terme, moyennant un petit investissement dans de telles devises.

Dans bien des cas, ils font même un (modeste) versement à la victime. L'idée étant de gagner sa confiance pour la convaincre d'effectuer de plus gros investissements[108].



Von: Zahlungsüberprüfung
Gesendet: Freitag, 6. August 2021
An: [redacted]
Betreff: Zahlung akzeptiert

Geschätzter Gewinn für August: €6.461,01 BitTraders

Mögliche Gewinne für August:
%-Rücklaufquote:
Startdatum:
End-Datum:

€6.461,01
2431%
03/08/2021
20/08/2021

Wenn Sie heute investieren, können Sie einen Gewinn von 6.461,01 Euro erwarten, wenn Ihre Investition am 03/08/2021 abgeschlossen ist.

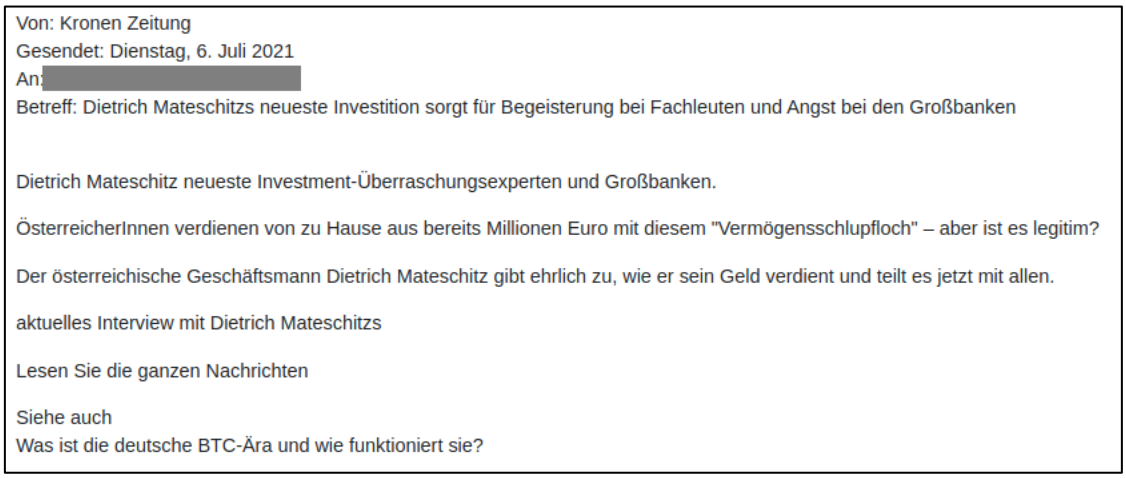
Befolgen Sie die folgenden Anweisungen, um zu beginnen.

Profil erstellen
Anweisungen:
Profil erstellen --> Investitionen einleiten --> Sehen Sie, wie Ihr Geld wächst --> Ziehen Sie Ihren Investitionsgewinn auf Ihr Bankkonto ab

Mit freundlichen Grüßen,
BitTraders

Fig. 13: Exemple de courriel promettant un très gros profit.

Au cours des dernières années déjà, le NCSC a reçu des annonces concernant des contrefaçons de plateformes de commerce en ligne ou des portails publicitaires portant le nom de personnalités comme Roger Federer et DJ Bobo. Des interviews fictives expliquaient que ces personnes devaient leur richesse aux cryptomonnaies[109].



Von: Kronen Zeitung
Gesendet: Dienstag, 6. Juli 2021
An: [redacted]
Betreff: Dietrich Mateschitzs neueste Investition sorgt für Begeisterung bei Fachleuten und Angst bei den Großbanken

Dietrich Mateschitz neueste Investment-Überraschungsexperten und Großbanken.

ÖsterreicherInnen verdienen von zu Hause aus bereits Millionen Euro mit diesem "Vermögensschlupfloch" – aber ist es legitim?

Der österreichische Geschäftsmann Dietrich Mateschitz gibt ehrlich zu, wie er sein Geld verdient und teilt es jetzt mit allen.

aktuelles Interview mit Dietrich Mateschitzs

Lesen Sie die ganzen Nachrichten

Siehe auch
Was ist die deutsche BTC-Ära und wie funktioniert sie?

Fig. 14: Exemple de courriel frauduleux envoyé au nom de l'Autrichien le plus riche.

[108] Krypto Anlagebetrüger ködern Nutzer mit SMS (cybercrimepolice.ch)

[109] Voir rapport semestriel MELANI 2019/2, chap. 4.4.5.

La rétrospective de la semaine établie par le NCSC présente à chaque fois les scénarios actuels de fraude à l'investissement[110]. Afin de se démarquer dans le flot de publicités, les escrocs semblent vouloir surenchérir en proposant des profits irréalistes. Dans un cas, ils annonçaient même un bénéfice de 12 000 euros en 72 heures, moyennant une mise de 250 euros[111]. Les criminels cherchent encore à tromper leurs victimes une seconde fois: de faux avocats, notaires ou même des autorités de poursuite pénale ou des régulateurs prennent contact avec elles et leur promettent de les aider à récupérer l'argent perdu. La première étape consiste à établir une relation de confiance. La victime doit fournir des données sensibles, comme une copie de carte d'identité ou un numéro IBAN. Dans un second temps, des émoluments lui sont demandés pour la prétendue aide apportée. Les organisations fictives censées lutter contre la fraude à l'investissement publient même parfois des sites improvisés pour gagner la confiance de leurs victimes[112].

Le risque de perdre beaucoup d'argent est bien réel. Un cas en particulier a entraîné la perte de plus d'un million de francs suisses[113].

Conclusion / Recommandation:

Il faut se méfier des promesses de rendements mirifiques à court terme (et sans travail).

Si vous avez subi un préjudice financier, annoncez-vous personnellement au poste de police local pour déposer plainte.

Méfiez-vous des tiers qui vous proposent soudainement leur aide après une fraude. Surtout, n'effectuez pas d'autres paiements, y compris de prétendus émoluments, pour récupérer l'argent perdu.

D'autres informations figurent sur le site du NCSC: Fraude à l'investissement (ncsc.admin.ch)

Le site Internet de l'Autorité fédérale de surveillance des marchés financiers FINMA publie des informations concernant les prestataires de services financiers autorisés en Suisse (finma.ch). Si un prestataire est absent de la liste publiée, une prudence particulière s'impose. Renseignez-vous à son sujet en lisant des avis publiés sur Internet. La FINMA tient également une liste noire (non exhaustive) concernant les entreprises qui sont susceptibles d'exercer sans autorisation une activité soumise à autorisation et assujettie à sa surveillance (finma.ch).

110 Actuel (ncsc.admin.ch)
111 Rétrospective de la semaine 14 (ncsc.admin.ch)
112 Rétrospective de la semaine 21 (ncsc.admin.ch)
113 Rétrospective de la semaine 11 (ncsc.admin.ch)