5 mai 2022 | Centre national pour la cybersécurité NCSC

Rapport semestriel 2021/II (juillet – décembre)

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

Dans ce rapport, le NCSC traite des principaux cyberincidents qui se sont produits au cours du deuxième semestre 2021 en Suisse et sur le plan international. Il analyse en particulier les attaques contre la chaîne d'approvisionnement en produits informatiques.

Différents fournisseurs et prestataires tiers participent aujourd'hui à la production de biens et de services. Lorsqu'ils subissent des attaques, des problèmes de grande ampleur peuvent toucher l'ensemble de la chaîne d'approvisionnement et entraîner notamment l'arrêt de la production. L'attaque lancée contre l'entreprise de logiciels Kaseya au milieu de l'année 2021 a ainsi fait la une des journaux dans de nombreux pays. En Suisse, les sites Internet de la ville et du canton de Saint-Gall ont été longtemps indisponibles à cause d'une attaque par déni de service distribué (DDoS) contre un fournisseur d'hébergement.

La plupart des signalements portent sur des cas de fraude

Au cours de la période sous revue, le NCSC a reçu 11 480 signalements de cyberincidents, dont la plupart concernaient des cas de fraude de différentes natures. En particulier, de nombreux cas de courriels prétendument envoyés par des autorités de poursuite pénale ont été rapportés. D'autres signalements concernaient des fraudes au paiement anticipé, des fraudes à l'investissement, des arnaques au président et des fraudes aux petites annonces. Certains cybercriminels tendent à utiliser des procédures plus complexes et individualisées. Avant de procéder à la tentative d'escroquerie proprement dite, ils manipulent les victimes sur une longue période afin de gagner leur confiance.

Rançongiciels et fuite de données

Le deuxième semestre 2021 a également été marqué par de nombreuses attaques aux chevaux de Troie. Également connues sous le nom de rançongiciels, ces techniques consistent à crypter les données, puis à demander une rançon. Les malfaiteurs recourent de plus en plus souvent à un double chantage. Avant de crypter les données, ils en font une copie et disposent ainsi d'un moyen de pression supplémentaire. En effet, si la victime refuse de payer la rançon, les malfaiteurs menacent de publier les données.

Vulnérabilités des composants logiciels

Des composants existants, comme des bibliothèques ou des codes *open source*, sont souvent utilisés lors du développement de logiciels. Or ils peuvent contenir des vulnérabilités. Lorsqu'une telle vulnérabilité est découverte, elle doit être corrigée dans tous les produits dans lesquels le composant a été intégré. Ce problème s'est posé en décembre 2021, lorsqu'une vulnérabilité qualifiée de critique a été identifiée dans la bibliothèque de programme Java «Log4j», qui est largement répandue.

Hameçonnage toujours d'actualité

Depuis le début de la pandémie, de nombreuses attaques de hameçonnage fondées sur de prétendus annonces de colis ou problèmes de livraison ont été signalées au NCSC. Outre des courriels, les malfaiteurs envoient fréquemment des SMS pour prendre contact avec leurs victimes. D'autres signalements concernaient des tentatives de hameçonnage en rapport avec Webmail et Office365. Les données d'accès ainsi dérobées sont souvent utilisées pour des fraudes à la facturation. Ont également été signalés de nombreux courriels d'hameçonnage concernant des factures de fournisseurs d'accès à Internet prétendument payées en double.

2 Éditorial

Aucun homme n’est une île

Dans ses Méditations en temps de crise parues en 1624, l’écrivain anglais John Donne a inventé l’expression «Aucun homme n’est une île», par laquelle il affirme que chacun de nous fait partie d’un grand tout et que nos destins sont tous liés entre eux.

Roger Wirth, Head of Cyber Security (CISO), Swissgrid SA

Notre environnement économique se caractérise par une spécialisation de plus en plus poussée, qui s’accompagne d’une réduction du degré d’intégration dans le but d’augmenter l’efficacité et de réduire les coûts grâce à des économies d’échelle. La chaîne de création de valeur des entreprises devient ainsi de plus en plus dépendante des fournisseurs, des prestataires de services et des partenaires, alors que la pandémie de COVID-19 nous a montré les limites et les risques de la mondialisation.

Une cyberattaque contre une entreprise affecte tous les participants à une chaîne d’approvisionnement: lancée contre un fournisseur, elle peut ainsi se répercuter sur les clients de ce participant, puis atteindre les destinataires des prestations de ces derniers. En février de cette année, par exemple, Toyota a dû fermer temporairement ses usines au Japon après la défaillance d’un fournisseur victime d’une cyberattaque. L’expression «Aucun homme n’est une île» s’applique donc aussi aux organisations.

Le problème s’est aggravé depuis que les cybercriminels se sont mis à cibler directement les chaînes d’approvisionnement: en créant des «portes dérobées» (backdoors) qui leur donnent par exemple accès aux produits de fournisseurs de périphériques réseau et leur permettent ensuite d’atteindre les clients (comme cela s’est passé récemment lors de l’attaque contre la société texane SolarWinds), ils multiplient l’effet de leur attaque.

Ne pas se protéger signifie donc aussi prendre le risque de mettre d’autres en danger.

Lors de mes entretiens, je constate régulièrement que la gestion des risques touchant la chaîne d’approvisionnement n’est abordée que timidement dans de nombreuses entreprises.

L’ampleur de nos rapports d’interconnexion et d’interdépendance montre que nous sommes peut-être en présence du plus grand cyberrisque systémique jamais connu par notre société moderne.

On peut dès lors se demander pourquoi cette problématique ne bénéficie pas d'une plus grande attention. L'une des réponses à cette question pourrait être que les dirigeants d'entreprises ne font pas qu'externaliser des services, mais s'emploient, par la même occasion, à transférer les responsabilités qui y sont liées. Cette situation crée un angle mort: même si je peux externaliser la fourniture de prestations, l'obligation de rendre des comptes à mes partenaires continue, dans tous les cas, de m'incomber. Comment puis-je donc rendre des comptes à mes partenaires si je ne maîtrise pas les risques que mes mesures d'externalisation font peser sur ma chaîne d'approvisionnement?

À mon avis, la gestion de ces risques doit faire partie intégrante de la conduite opérationnelle de chaque entreprise.

Ceux-ci ne peuvent être gérés de manière conséquente que s'ils ont été décelés et s'ils sont compris. Dans ce cadre, une analyse des processus clés peut contribuer à l'identification des dépendances critiques par rapport à des tiers. De même, les méthodes de modélisation des menaces telles que STRIDE peuvent permettre de déterminer les menaces et les vulnérabilités se situant aux points de transition des systèmes.

La mise en place d'une organisation résiliente revêt également une grande importance. Si je parviens à maintenir le fonctionnement de mes processus centraux malgré la défaillance des outils informatiques de base (Business Continuity Management) ou si je prends des mesures pour limiter les effets d'une attaque et, qu'après une panne des technologies informatiques ou opérationnelles, je réussis à remettre celles-ci sur pied rapidement (Incident Response et Disaster Recovery), alors je contribue directement à assurer la résilience de l'ensemble de la chaîne d'approvisionnement à laquelle participe mon entreprise.

Si elles veulent que ces dispositifs soient efficaces en cas d'urgence, les entreprises doivent les tester périodiquement et sensibiliser régulièrement le personnel à leur maniement.

Des normes sectorielles ainsi que des certifications de produits et de services peuvent également être utiles. À cet effet, il est nécessaire que les entreprises d'un même secteur unissent leurs forces pour pouvoir imposer de telles normes et prescriptions à leurs fournisseurs.

Si nous voulons nous défendre efficacement contre les cybercriminels qui recourent à des méthodes toujours plus sophistiquées, il importe que toutes les entreprises prennent les mesures qui s'imposent pour juguler les cyberrisques pesant sur leurs chaînes d'approvisionnement.

Roger Wirth, Head of Cyber Security (CISO), Swissgrid SA

3 Thème prioritaire: Attaque contre la chaîne d'approvisionnement (supply chain)

3.1 Qu'entend-on par attaque contre la chaîne d'approvisionnement?

De nombreuses entreprises collaborent avec plusieurs partenaires (fournisseurs, prestataires tiers) qui fournissent des produits divers tels que des matières premières, des prestations de services ou des technologies pour fabriquer un produit final ou les intégrer dans des offres ou des prestations. Beaucoup de sociétés sont donc tributaires de prestations externes pour maintenir leur exploitation. Dans un contexte plus large, cette chaîne logistique ou chaîne d'approvisionnement (supply chain) englobe toute la chaîne de création de valeur. Chaque maillon fait partie d'un processus global et peut potentiellement servir de porte d'entrée aux attaquants (attaque *via* la chaîne d'approvisionnement). De même, des dysfonctionnements ponctuels peuvent interrompre cette chaîne (attaque *contre* la chaîne d'approvisionnement). Pour éviter les cyberattaques, toute la chaîne d'approvisionnement, y compris l'ensemble des fournisseurs et prestataires concernés, doit donc être protégée adéquatement, fonctionner de manière fiable et, si possible, des redondances doivent garantir sa continuité.

Une attaque via la chaîne d'approvisionnement combine en fait deux attaques: la première vise un seul fournisseur. L'accès à ses systèmes et sa relation privilégiée avec ses clients sont ensuite exploités pour atteindre le véritable objectif grâce à des accès à distance ou passerelles réseau mal protégés ou à des liaisons établies pour transférer des données. Dans le cadre d'opérations complexes, des attaquants ont déjà ciblé des fabricants de logiciels en ajoutant un code qui était ensuite transmis aux clients par l'intermédiaire de mises à jour régulières.[1] Des attaques visant des logiciels ou du matériel pendant le processus de fabrication sont également imaginables. Le produit est alors livré avec un point faible, une porte dérobée ou un maliciel préinstallé. Les attaques via la chaîne d'approvisionnement peuvent avoir un objectif précis de grande importance[2], cibler un groupe restreint de destinataires[3] ou déployer de vastes effets pour pouvoir ensuite sélectionner des cibles spécifiques.[4] De plus, la chaîne d'approvisionnement permet de mener des attaques contre un nombre de victimes potentielles aussi élevé que possible, par exemple en diffusant un rançongiciel par le biais d'un prestataire informatique compromis.[5]

Il est souvent difficile d'identifier clairement les attaques contre la chaîne d'approvisionnement qui visent à compromettre l'exploitation de clients finaux spécifiques.

---

1 Voir à ce sujet le rapport semestriel 2020/2 (ncsc.admin.ch), chap. 4.7.2 sur SolarWinds

2 Voir rapport semestriel 2010/2 (ncsc.admin.ch), chap. 4.1 sur Stuxnet, un ver qui a saboté de manière ciblée les capacités iraniennes d'enrichissement d'uranium.

3 Voir rapport semestriel 2017/1 (ncsc.admin.ch), chap. 3 sur le maliciel NotPetya qui s'est propagé via le logiciel ukrainien de déclaration de revenus.

4 Voir rapport semestriel 2020/2 (ncsc.admin.ch), chap. 4.7.2 sur le piratage de SolarWinds, et le rapport semestriel 2017/1 (ncsc.admin.ch), chap. 5.1.1 sur l'opération CloudHopper

5 Voir chap. 3.3 et 4.2.2 ci-après

En 2016, les attaques DDoS contre le fournisseur d'infrastructures Dyn ont rendu indisponibles pour de nombreux clients plusieurs plates-formes utilisant ses services (dont Twitter, Spotify et Soundcloud).[6] Les entreprises de la chaîne d'approvisionnement ont généralement conclu avec leurs clients des contrats concernant les prestations ou les livraisons. Des attaques par rançongiciel ont récemment ciblé des prestataires et des fournisseurs, qui ont dès lors subi une pression énorme pour pouvoir de nouveau proposer leurs prestations ou fabriquer leurs produits, car ils devaient honorer leurs engagements auprès de leurs clients. Les maîtres chanteurs espéraient ainsi que les victimes seraient disposées à payer la rançon.

3.2 Attaque au rançongiciel contre la chaîne d'approvisionnement du logiciel VSA de Kaseya

Kaseya Limited est un fournisseur de logiciels spécialisé dans les outils de surveillance et de gestion de systèmes à distance. Il propose en téléchargement à ses clients le logiciel VSA (Virtual System/Server Administrator), qui fonctionne également depuis ses propres serveurs en nuage. Les fournisseurs de services gérés (managed service providers, MSP) peuvent utiliser ce logiciel en local ou obtenir une licence pour les serveurs VSA en nuage de Kaseya. De leur côté, ils proposent différentes prestations informatiques à d'autres clients. En cas d'actualisation du logiciel, Kaseya envoie des mises à jour à distance à tous les serveurs VSA.

Au milieu de l'année 2021, des attaquants ont utilisé une vulnérabilité de type zero day dans les propres systèmes de Kaseya (CVE-2021-30116)[7] pour exécuter à distance des commandes nuisibles sur les appareils VSA des clients de Kaseya. Le 2 juillet 2021, une mise à jour exécutant le code des attaquants a été adressée au logiciel VSA des clients de Kaseya. Ce code malveillant installait à son tour un rançongiciel chez les clients gérés avec VSA.[8]

Les autorités américaines ont ensuite publié un guide destiné aux MSP et à leurs clients qui avaient été affectés par les attaques au rançongiciel contre la chaîne d'approvisionnement VSA de Kaseya.[9]

3.3 Incidents en Suisse

Début septembre 2021, le rançongiciel BlackMatter a touché plusieurs petites et moyennes entreprises (PME) après que les attaquants ont réussi à compromettre un prestataire informatique autrichien et à cibler ses clients.[10] Des attaques DDoS visant une société d'hébergement,

---

6 Voir rapport semestriel 2016/2 (ncsc.admin.ch), chap. 3.2, 4.4.1 et 4.6

7 CVE - CVE-2021-30116 (mitre.org)

8 REvil ransomware hits 1,000+ companies in MSP supply-chain attack (bleepingcomputer.com); voir également le chap. 4.2.2

9 CISA-FBI Guidance for MSPs and their Customers Affected by the Kaseya VSA Supply-Chain Ransomware Attack (cisa.gov)

10 Hackerangriff auf 34 Firmen (orf.at)

qui abrite notamment le site Web du canton de Saint-Gall[11], ont temporairement entravé la disponibilité de plusieurs sites Internet (voir chap. 4.3.1 ci-après).

3.4 Interventions et mesures

Sur le plan politique, un rapport[12] du Conseil fédéral publié fin 2021 en réponse aux postulats Dobler 19.3135[13] et 19.3136[14] a examiné la gestion des risques de la chaîne d'approvisionnement et livré une interprétation des règles nationales et des normes internationales applicables. De plus, les bases légales concernant l'application de normes dans les infrastructures critiques ont été présentées.

Ce rapport porte également sur les demandes formulées par un groupe de travail de la Commission Cybersécurité d'ICTSwitzerland dans le livre blanc «Supply Chain Security»[15], qui prévoient notamment des centres de contrôle en Suisse pour les composants matériels et logiciels. La Confédération est disposée à soutenir des initiatives privées dans ce domaine en apportant ses connaissances spécialisées.[16]

Conclusion / Recommandations:

L'examen régulier des relations avec les fournisseurs et les prestataires à l'aune du profil de risque qui se dessine est un défi que les directions d'entreprises doivent relever urgemment en raison de la numérisation croissante de tous les secteurs d'activité.

Les petites entreprises qui n'ont pas leurs propres spécialistes n'ont guère qu'une possibilité: couvrir contractuellement les risques avec le soutien externe d'associations ou de conseillers-experts, y compris le droit à une vérification indépendante des prestataires. Cette charge supplémentaire, qui s'accompagne nécessairement de coûts plus élevés, est judicieuse uniquement lorsqu'il existe un risque accru pour l'entreprise.

Sur son site Internet, le NCSC du Royaume-Uni (NCSC UK) propose un guide[17] et un catalogue de questions[18] qui peuvent contribuer au processus de priorisation et à la sélection.

CISA, l'autorité américaine de cybersécurité, fournit elle aussi de nombreuses informations[19] sur les risques liés à la chaîne d'approvisionnement.

---

11 Communiqué «Website des Kantons wieder online» (sg.ch)
12 Sécurité des produits et gestion des risques de la chaîne d'approvisionnement dans les domaines de la cybersécurité et de la cyberdéfense (parlament.ch)
13 Acquisitions de l'armée. Avons-nous la maîtrise de la cybersécurité? (parlament.ch)
14 Infrastructures critiques. Avons-nous la maîtrise des composants matériels et logiciels? (parlament.ch)
15 White_Paper_Supply_Chain_Security_2019_09_25_FR.pdf (digitalswitzerland.com)
16 Voir également à ce sujet le rapport semestriel 2020/2 (ncsc.admin.ch), chap. 4.5.2
17 Supply chain security guidance (ncsc.gov.uk)
18 Supplier assurance questions (ncsc.gov.uk)
19 Supply Chain (cisa.gov)

Des recommandations sur la collaboration avec des prestataires externes de services informatiques (ncsc.admin.ch) figurent également sur le site Internet du NCSC.

3.5 Vulnérabilités des composants logiciels

La plupart des logiciels ne sont pas écrits à neuf et d'un seul tenant. Lors de leur développement, des codes open source ou provenant de bibliothèques existantes y sont souvent intégrés. Les vulnérabilités figurant dans ces éléments sont alors incorporées et diffusées de manière involontaire. Lorsque l'une d'elles est identifiée, elle doit être corrigée dans tous les produits comprenant les composants en question, comme l'a mis en évidence la faille Heartbleed au niveau mondial en 2014.[20]

En décembre 2021, une vulnérabilité classée critique sur le plan international a été identifiée dans la bibliothèque de programmes Java «Log4j»[21], qui est largement répandue. Cadre de programmation destiné à la journalisation des messages des applications, «Log4j» est un élément essentiel dans le développement actuel des logiciels. Elle est donc utilisée dans de nombreux produits logiciels commerciaux et open source.[22] Cette faille de sécurité permet d'exécuter à distance n'importe quel code (remote code execution, RCE), ce que des cybercriminels se sont empressés de faire à grande échelle sur le plan international dès l'annonce de la vulnérabilité (voir le chap. 4.5.3 à ce sujet).

4 Événements survenus / situation

4.1 Aperçu des annonces de cyberincidents reçues

En 2021, le NCSC a enregistré 21 714 annonces, un nombre impressionnant qui représente à peu près le double des annonces reçues au cours de l'exercice précédent (10 833). Cette forte augmentation pourrait notamment s'expliquer par l'introduction du nouveau formulaire d'annonce fin 2020. Remanié et simplifié, il est désormais placé plus en évidence sur la page d'accueil. La recrudescence notable de certains phénomènes a également contribué à cette hausse.

La plupart des incidents déclarés concernent des tentatives d'attaques, et non des attaques ayant abouti. De plus, les chiffres réels devraient être sensiblement plus élevés, en particulier pour les tentatives infructueuses, car il n'existe en Suisse aucune obligation générale de déclaration.

---

20 Voir rapport semestriel 2014/1 (ncsc.admin.ch), chap. 4.1

21 Log4j – Apache Log4j Security Vulnerabilities (apache.org)

22 New zero-day exploit for Log4j Java library is an enterprise nightmare (bleepingcomputer.com)

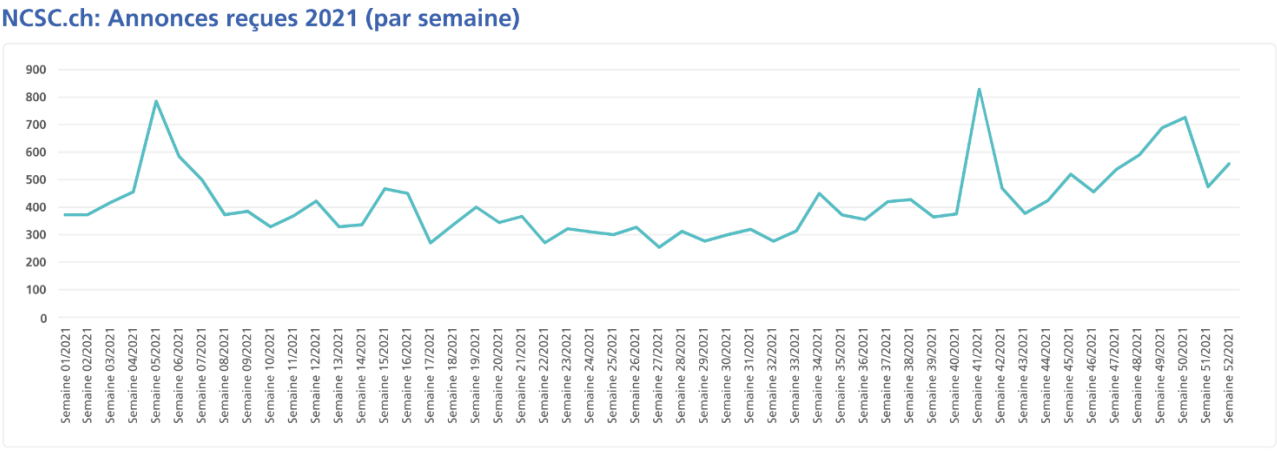

Fig. 1: Nombre d'annonces hebdomadaires parvenues au NCSC entre janvier et décembre 2021, voir aussi Chiffres actuels (ncsc.admin.ch).

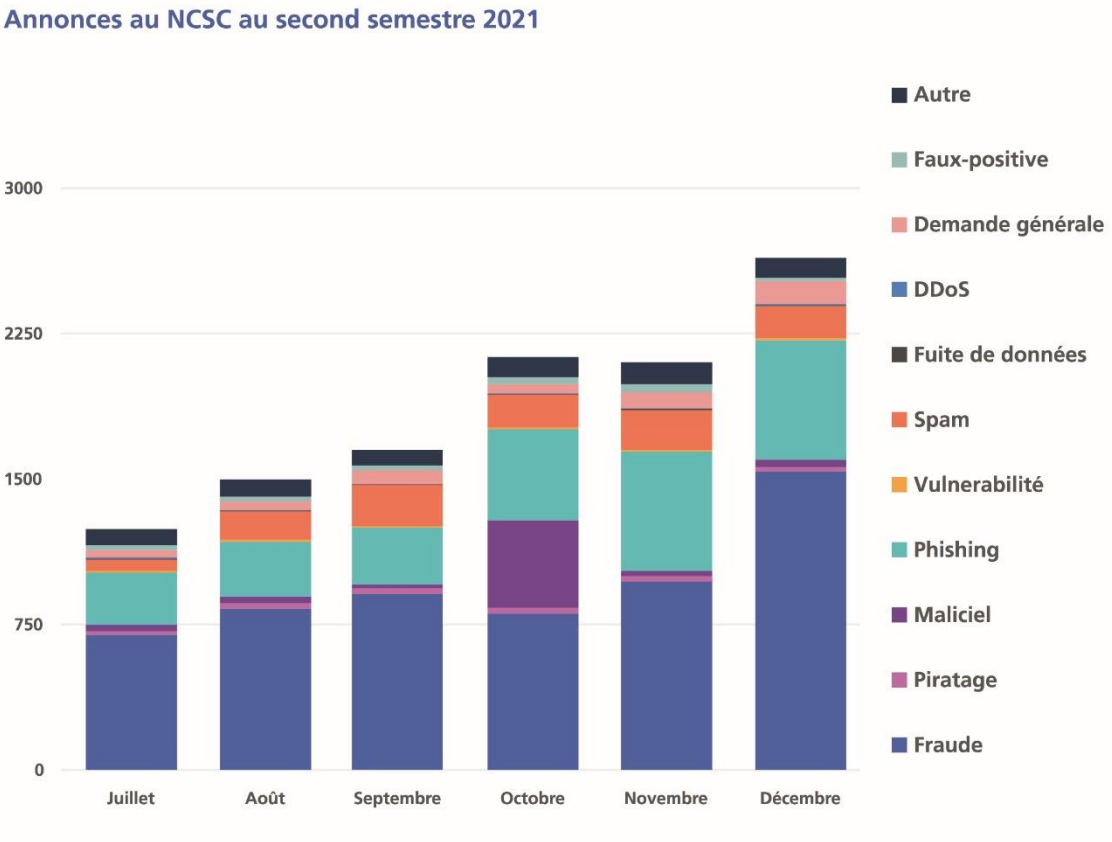

Fig. 2: Signalements effectués au NCSC au second semestre 2021, par catégorie, voir aussi Chiffres actuels (ncsc.admin.ch).

4.1.1 L’escroquerie, l’incident le plus courant

Comme l’an passé, les tentatives d’escroquerie ont été les incidents les plus fréquemment signalés au NCSC en 2021 (plus de 11 300 au total). La fake sextortion[23] dominait au premier semestre et plusieurs vagues ont été observées, tandis que les annonces correspondantes ont eu tendance à fléchir au second semestre. En revanche, les signalements de courriels de menace ont fortement augmenté dès le mois d’octobre. Ces courriels provenant prétendument des autorités de poursuite pénale exigent le paiement d’une amende ou d’une caution.[24] Connu depuis longtemps en France, ce phénomène apparenté à la fake sextortion représentait la majeure partie des annonces reçues en novembre et en décembre 2021, contribuant dès lors à une forte hausse générale de ces dernières. Les autres signalements fréquents en 2021 concernent la fraude au paiement anticipé (2704 annonces), la fraude à l’investissement (397 signalements), l’arnaque au président (394 annonces) et la fraude aux petites annonces (820 signalements). Dans ce dernier cas, une variante dans laquelle des émoluments de transport doivent être avancés au vendeur malgré la vente[25] semble s’imposer.

Pour ce qui est de la fraude à l’investissement, des opérations promotionnelles (give away) ont été signalées en plus des variantes habituelles.[26] Il suffirait de verser de l’argent sur un portefeuille de cryptomonnaie bien précis pour recevoir en retour le double du montant. Sur le site en question, le visiteur est mis sous pression par l’affichage d’un décompte indiquant le montant et le temps encore disponibles dans le cadre de cette opération publicitaire.

4.1.2 Annonces de sites de phishing

Les signalements de courriels de phishing sont demeurés à un niveau élevé en 2021 également. La plupart concernent des courriels frauduleux de notification de colis qui portent le nom de différents services de livraison ou de l’Administration fédérale des douanes et réclament de quelconques émoluments. Il existe plusieurs variantes de ces courriels. Dans certains cas, une carte Paysafe doit être achetée et le code, transmis aux escrocs; dans d’autres, un lien mène vers la souscription d’un abonnement. Le plus souvent, ces courriels redirigent toutefois vers un site d’hameçonnage sur lequel les données de carte de crédit doivent être indiquées.

Les factures de fournisseurs d’accès à Internet prétendument réglées en double restent d’actualité en matière de phishing, mais les informations fournies par les escrocs sont parfois laxistes. Dans certains cas, le délai de réponse mentionné, qui est censé mettre le destinataire sous pression, était échu depuis plus de six mois.

Des tentatives de phishing contre Webmail et Office365 ont également été observées. Ces données d’accès sont fréquemment utilisées pour pirater une messagerie professionnelle. Dans ce type d’escroquerie, les pirates font référence à un échange de courriels qui a eu lieu et qui comprenait un ordre de paiement ou une facture. Ils modifient alors l’IBAN sur lequel le montant doit être versé. Les pirates ayant accès au compte de messagerie de l’expéditeur ou

---

23 Informations sur la *fake sextortion* (ncsc.admin.ch)

24 Rétrospective de la semaine 37 (ncsc.admin.ch)

25 Voir également le ch. 5.2

26 Voir fraude à l'investissement (ncsc.admin.ch) et rapport semestriel 2021/1 (ncsc.admin.ch), chap. 4.8

d'un destinataire dans de tels cas, ils peuvent également consulter la communication interne correspondante de l'entreprise ou les échanges avec les clients, qui peuvent contenir des informations confidentielles. Cela ouvre la porte à d'autres escroqueries éventuelles et une victime peut en outre faire l'objet d'un chantage avec ces données.

4.1.3 Annonces de maliciels

Près de la moitié des signalements à propos de logiciels malveillants concernaient le maliciel «FluBot».[27] En effet, nous avons observé une vague d'attaques pendant les semaines 41 et 42. Les escrocs envoyaient des SMS pour inciter leurs cibles à télécharger une application Android malveillante, «FluBot», sur leur téléphone mobile. Cette vague a engendré pendant la semaine 41 le plus grand nombre de signalements de l'année.

Les annonces de rançongiciels ont elles aussi progressé davantage que la moyenne. Le NCSC a reçu 161 annonces à propos de rançongiciels en 2021, contre 67 l'année précédente. Elles ont fait état par exemple de nombreuses attaques de systèmes de stockage en réseau (NAS) par le rançongiciel «Qlocker» en début d'année, lesquelles ont principalement touché des particuliers. En tout, 44 cas signalés ont pu être attribués à «Qlocker».[28]

Les tentatives d'attaque avec le maliciel «Retefe» demeurent d'actualité et sont régulièrement signalées. Dans ce scénario, les courriels sont souvent suivis d'un appel téléphonique de l'entreprise Swiss Express Service (ou similaire) qui souhaite faire signer les documents relatifs à l'envoi. Au cours de la conversation téléphonique, l'auteur de l'appel explique que les documents en question ont été envoyés par courriel. Le lien figurant dans le courriel ou dans un document PDF joint mène vers un maliciel (en général, un cheval de Troie pour l'e-banking).

4.1.4 Annonces de failles de sécurité

Dans la catégorie des failles de sécurité, le NCSC a surtout reçu des annonces d'incidents en lien avec des serveurs Microsoft Exchange[29], sans compter les problèmes que pose la vulnérabilité «Log4j».[30] Ces failles sont exploitées, entre autres, afin d'infecter les systèmes cibles avec des maliciels. Plus concrètement, les pirates ajoutaient un lien vers le maliciel à un courriel volé avant de renvoyer ce dernier à son ou sa destinataire. En se servant d'une conversation connue de la cible, ils espéraient rendre cette dernière plus encline à ouvrir le fichier joint. Les documents Office contenaient une macro malveillante et un mode d'emploi précisant les paramètres à adapter afin que celle-ci puisse être exécutée sur l'ordinateur. La meilleure protection contre de telles attaques consiste donc à refuser l'activation de toutes les macros sans exception, même lorsqu'on est explicitement et fermement invité à le faire.

---

27 Voir rapport semestriel 2021/1 (ncsc.admin.ch), chap. 4.2.1, ainsi que le chap. 4.2.1 ci-après
28 Voir rapport semestriel 2021/1 (ncsc.admin.ch), chap. 4.1.3
29 Voir rapport semestriel 2021/1 (ncsc.admin.ch), chap. 3.1.1
30 Voir chap. 4.5.3

4.2 Maliciels

4.2.1 Situation générale

Au cours du second semestre 2021, les médias se sont particulièrement intéressés aux rançongiciels, bien que ceux-ci ne représentent qu'une infime part des attaques réalisées avec un maliciel. Cet intérêt reposait sur le fait que plusieurs de ces attaques avaient eu de graves conséquences pour les victimes en Suisse et à l'étranger (voir chap. 4.2.2). Pour déployer avec succès un rançongiciel, l'opérateur doit tout d'abord avoir accès au système cible. Cet accès passe principalement par d'autres maliciels, spécialisés pour se répandre et d'implanter dans les système. L'un d'eux est Qakbot, qui est traité plus en détail au chapitre 4.2.3. Emotet, le maliciel le plus répandu, avait subi un revers début 2021 lorsqu'une opération internationale de police avait réussi à mettre hors service son infrastructure.[31] Il a cependant fait son retour fin 2021[32] grâce à Trickbot, un maliciel qui était déjà en lien avec lui. Dans le passé, Emotet installait Trickbot; cette fois, Emotet a utilisé TrickBot pour reconstruire son infrastructure. Cette interaction découle notamment du développement du modèle «Malware as a Service»[33], dans lequel un opérateur de maliciel ou le gestionnaire d'un réseau de *bots* loue son infrastructure à d'autres criminels. Chaque acteur peut ainsi se concentrer sur certaines prestations partielles et les proposer au marché noir.

---

31 World's most dangerous malware EMOTET disrupted through global action (europa.eu); rapport semestriel 2020/2 (ncsc.admin.ch), chap. 4.3.2

32 Emotet malware is back and rebuilding its botnet via TrickBot (bleepingcomputer.com)

33 Malware-as-a-service is the growing threat every security team must confront today (securitymagazine.com); Malware-as-a-service (MaaS) (kaspersky.com); Malware Has Evolved: Defining Malware-as-a-Service (zerofox.com)

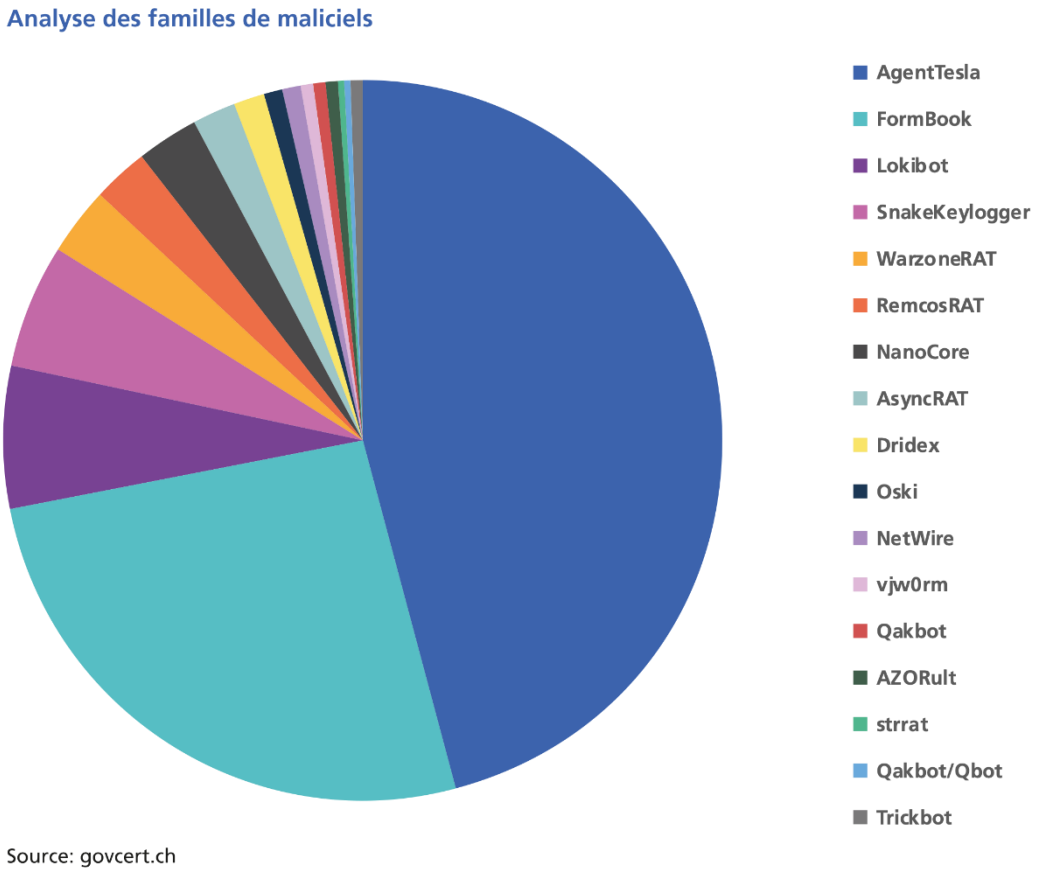

Fig. 3: Analyse des familles de maliciels actives en Suisse réalisée par le NCSC au deuxième semestre 2021.

Le graphique ci-dessous montre les familles de maliciels identifiées en Suisse pendant la période sous revue lors de l'analyse des données collectées par des gouffres DNS. Ceux-ci servent à repousser les maliciels en les empêchant d'accéder aux noms de domaine prévus et en réenregistrant ces derniers pour le compte d'une organisation de sécurité. On peut alors identifier les appareils infectés qui, au lieu de se connecter avec les serveurs des exploitants du maliciel, s'adresseront à ceux de l'organisation de sécurité. Le NCSC reçoit ces données de plusieurs partenaires internationaux pour tout l'espace d'adressage suisse et informe les propriétaires des appareils ayant subi une infection, par l'intermédiaire de leur fournisseur d'accès.

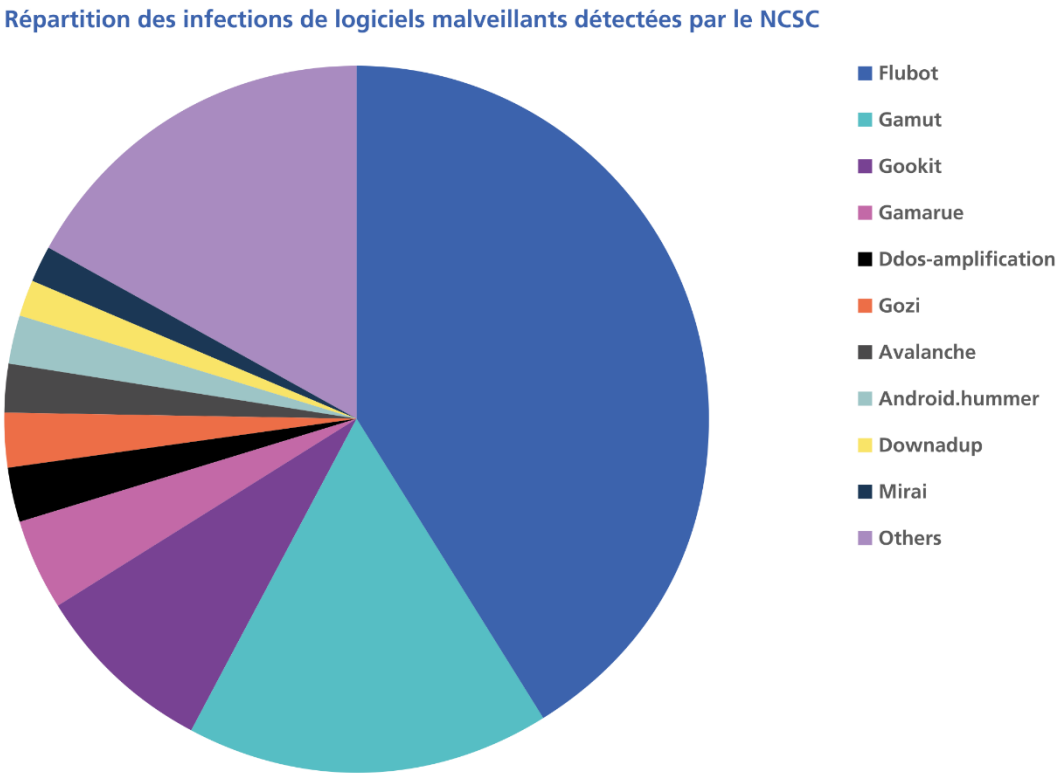

Fig. 4: Répartition des infections par maliciel identifiées par le NCSC en Suisse au second semestre 2021

Comme au premier semestre 2021, la famille de maliciels Flubot était la plus répandue au second semestre. Pour propager ce maliciel sur les appareils Android, les criminels envoient un SMS comprenant un lien vers un prétendu message vocal. Ce lien dirige vers une supposée application qui doit être installée pour écouter le message. En fait, la victime installe Flubot sur son appareil. Les malfaiteurs peuvent alors voler les données enregistrées sur celui-ci et accéder notamment aux applications protégées par une authentification à deux facteurs lorsque le second facteur est envoyé par SMS. Ils peuvent également espionner les activités d'e-banking de la victime.[34]

Conclusion / Recommandations:

- N'installez sur votre téléphone mobile que des applications proposées dans la boutique en ligne officielle de votre système d'exploitation.
- N'installez surtout pas d'applications à partir d'un lien reçu par SMS ou par message sur une autre application de messagerie (WhatsApp, Telegram, etc.).

[34] FluBot (Malware Family) (fraunhofer.de); rétrospective de la semaine 41 (ncsc.admin.ch)

- Si vous avez déjà téléchargé une telle application, faites contrôler l'appareil par un spécialiste et n'effectuez aucune opération bancaire ou achat en ligne avant ce contrôle. Ne saisissez par ailleurs aucun mot de passe.
- Dans la plupart des cas, la seule solution pour se débarrasser du logiciel malveillant est de rétablir la configuration d'usine de l'appareil touché.

Le spambot Gamut occupe la deuxième place. Les appareils qu'il infecte sont intégrés à un réseau de bots et utilisés pour envoyer des courriels indésirables concernant majoritairement des rencontres intimes, des produits pharmaceutiques ou des opportunités professionnelles.[35]

Le maliciel Gootkit, qui est spécialisé dans le vol des données bancaires de la victime, se place sur la troisième marche du podium. Il utilise des campagnes de spams ainsi que des sites Internet compromis qui incitent les visiteurs à télécharger le programme.[36]

4.2.2 Rançongiciels (*ransomware*)

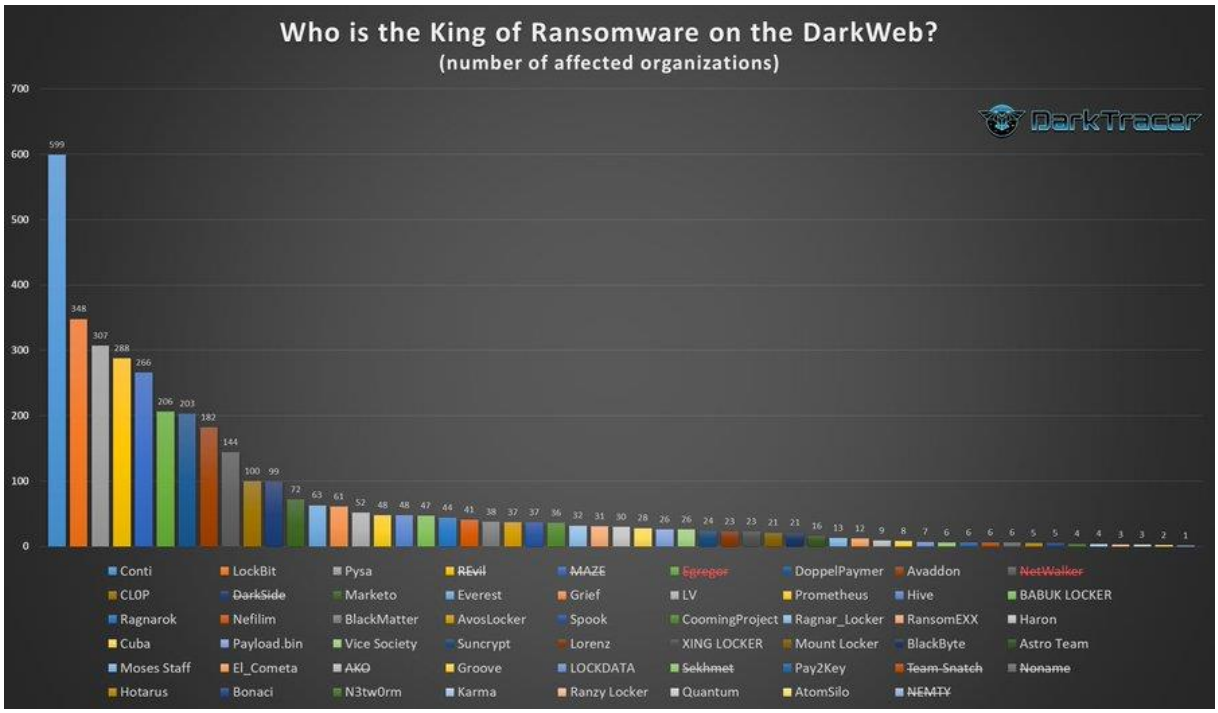

Fig. 5: Victimes de rançongiciels dans le monde, par malfaiteurs, selon les sites recensant les fuites de données. Les groupes barrés n'étaient plus actifs au moment de la création du graphique. (source: darktracer.com).

35 ENISA Threat Landscape 2020 - Spam (enisa.europa.eu)

36 GootKit (Malware Family) (fraunhofer.de); «Gootloader» expands its payload delivery options (sophos.com); Gootkit: the cautious Trojan (securelist.com)

Au second semestre 2021, les infections par rançongiciel restent les incidents qui présentent les conséquences potentielles les plus graves pour les entreprises suisses.

Pendant la période sous revue, le NCSC a enregistré des signalements concernant plus de 20 variantes de rançongiciels en Suisse. REvil (alias Sodinokibi), qui est déjà connu, LockBit 2.0, Conti et ech0raix sont particulièrement actifs. Parmi les nouveaux arrivants, on distingue notamment Blackmatter et Grief, le successeur de Doppelpaymer.

Même si les annonces d'attaques par rançongiciel auprès du NCSC ont un peu reculé depuis le semestre précédent, passant de 91 à 70, de nombreuses attaques ont visé des particuliers et des PME de différents secteurs économiques en Suisse au second semestre 2021. Elles ont également ciblé des infrastructures critiques, dont plusieurs communes[37], ainsi qu'une banque[38] et une clinique privée.[39] La Cinémathèque suisse[40], la Foire Suisse[41], le célèbre site de comparaison Comparis.ch[42] et Matisa, le géant de la construction de machines destinées à l'entretien des voies de chemin de fer[43], ont eux aussi fait l'objet d'incidents notables. En outre, des attaques visant à verrouiller les systèmes ont touché des filiales suisses d'entreprises domiciliées à l'étranger, comme les succursales helvétiques de MediaMarktSaturn à la suite de l'attaque de leur société-mère Ceconomy[44] avec le rançongiciel Hive.

Comme indiqué dans les précédentes éditions du rapport, certains opérateurs de rançongiciels appliquent désormais une tactique de chantage à plusieurs échelons.[45] Lorsque les criminels ont pu accéder aux systèmes de leurs victimes, ils copient autant de données que possible avant l'encryptage. Les pirates menacent leur victime de publier ses données si elle refuse de payer la rançon exigée pour les récupérer. Au second semestre également, des informations sensibles dérobées à des entreprises ou à des citoyens suisses lors d'attaques au rançongiciel ont été vendues ou publiées sur le Dark Web, notamment des données fiscales subtilisées à des fiduciaires grâce au rançongiciel Lockbit 2.0[46] ou des informations sur les habitants de la commune de Rolle que le groupe Vice Society avait exfiltrées lors d'une attaque de ce type.[47] Les pirates ont également mis en ligne les passeports de voyageurs suisses qu'ils avaient volés au tour-opérateur allemand FTI avec le rançongiciel Conti.[48]

Les prestataires informatiques constituent des cibles intéressantes, car les cybercriminels dotés de compétences techniques suffisantes peuvent s'infiltrer dans leur réseau pour s'immiscer ensuite dans les systèmes de leurs clients, comme l'illustrent clairement les attaques contre

---

37 Montreux a été victime d'une cyber-attaque (watson.ch)
38 Hacker-Angriff hält Aquila in Bann (finews.ch)
39 20210823_MM_Pallas_Kliniken_Cyberattacke.pdf (pallas-kliniken.ch)
40 Cinémathèque suisse: Cyberattaque à la Cinémathèque suisse (cinematheque.ch)
41 Cyber-attaque: Informations et recommandations à nos clients et partenaires (mch-group.com)
42 Ransomware attackers demand $400,000 from Swiss website (swissinfo.ch)
43 Matisa: les hackers Grief ayant piraté Comparis volent le géant du rail (watson.ch)
44 Cyberangriff auf Media-Markt-Mutter Ceconomy (inside-it.ch)
45 Voir rapport semestriel 2020/2 (ncsc.admin.ch), chap. 4.3.1; rapport semestriel 2021/1 (ncsc.admin.ch), chap. 4.3.2
46 48 heures pour payer la rançon de 200'000 francs en bitcoins (24heures.ch)
47 Cyberattaque contre Rolle: la commune appelle ses résidents à la vigilance (ictjournal.ch)
48 Hacker stehlen Daten eines Touristikriesen, darunter Reisepässe von Schweizern (inside-it.ch)

Kaseya et un fournisseur informatique autrichien, qui ont été réalisées respectivement avec REvil et BlackMatter et sont présentées aux chapitres 3.2 et 3.3.

Après l'attaque contre Colonial Pipeline[49], les autorités et les poursuites pénales subséquentes ont accentué la pression sur les opérateurs de rançongiciels. À l'automne, les autorités de poursuite pénale européennes et américaines en ont arrêté certains lors de plusieurs opérations.[50]

Conclusion / Recommandations:

Les rançongiciels peuvent causer de graves dommages, en particulier si vos copies de sauvegarde sont affectées. Des aspects importants de la résolution des incidents sont présentés sur le site Internet du NCSC: rançongiciels - que faire? (ncsc.admin.ch)

Le NCSC recommande aux victimes de ne pas 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.

Des réflexions concernant la possibilité d'assurer les cyberincidents figurent au chapitre 4.2.3 de l'édition précédente du rapport semestriel.

Par ailleurs, l'autorité américaine de cybersécurité CISA a publié un document destiné aux entreprises. Celui-ci vise à prévenir les fuites de données lors d'attaques par rançongiciel et conseille sur la manière de réagir.[51] Le CERT néozélandais a quant à lui établi un diagramme sur le cycle de vie des rançongiciels, y compris les vérifications à effectuer pour contrer une intrusion.[52]

4.2.3 Qakbot

Qakbot (aussi connu sous le nom de Pinkslipbot, Quakbot ou Qbot) était à la base, lors de sa découverte en 2007, un cheval de Troie utilisé principalement pour voler les identifiants bancaires et d'autres informations financières de la victime. Il a évolué depuis en se dotant de multiples modules additionnels. Il peut se propager dans les réseaux du système infecté, collecter et exfiltrer des données (en particulier le contenu des courriels qui sera utilisé lors de

49 Voir rapport semestriel 2021/1 (ncsc.admin.ch), chap. 4.2.3

50 Five affiliates to Sodinokibi/REvil unplugged (europol.europa.eu); Ransomware gang arrested in Ukraine with Europol's support (europol.europa.eu); Arrest in Romania of a ransomware affiliate scavenging for sensitive data (europol.europa.eu); Joint global ransomware operation sees arrests and criminal network dismantled (interpol.int); Ukrainian Arrested and Charged with Ransomware Attack on Kaseya (justice.gov)

51 Protecting Sensitive and Personal Information from Ransomware-Caused Data Breaches (cisa.gov)

52 How ransomware happens and how to stop it (cert.gov.nz)

campagnes ultérieures) ou installer d'autres composants malveillants (*payloads*) sur l'ordinateur concerné. Ces différentes fonctions en font un maliciel redoutable, que le NCSC a observé à plusieurs reprises comme vecteur dans des attaques par rançongiciel en Suisse.[53]

Une analyse a disséqué la chaîne d'attaque de Qakbot en différents modules qui peuvent être assemblés de plusieurs façons selon l'objectif d'une campagne. Cette modularité permet des chaînes d'attaque diverses, qui compliquent la détection d'une campagne Qakbot dans un réseau infecté. Malgré cette modularité, Qakbot arrive presque toujours dans un courriel. Outre les méthodes classiques basées sur une pièce jointe ou un lien, des images sont désormais utilisées à cet effet. Elles indiquent une URL que la victime doit saisir manuellement dans son navigateur. Enfin, l'infection peut provenir d'un document Office contenant des macros pour délivrer Qakbot sur l'ordinateur.[54]

Les courriels envoyés se basent fréquemment sur un fil de discussion existant (thread hijacking), comme l'a observé le NCSC à plusieurs reprises pendant la période sous revue.[55] Ce courriel semblant familier, la victime est plus encline à ouvrir le document et à suivre les instructions qu'il contient. Typiquement, celles-ci font croire que le contenu n'est pas accessible, car les macros sont désactivées. L'utilisateur est alors invité à effectuer différentes étapes pour activer ces macros.[56]

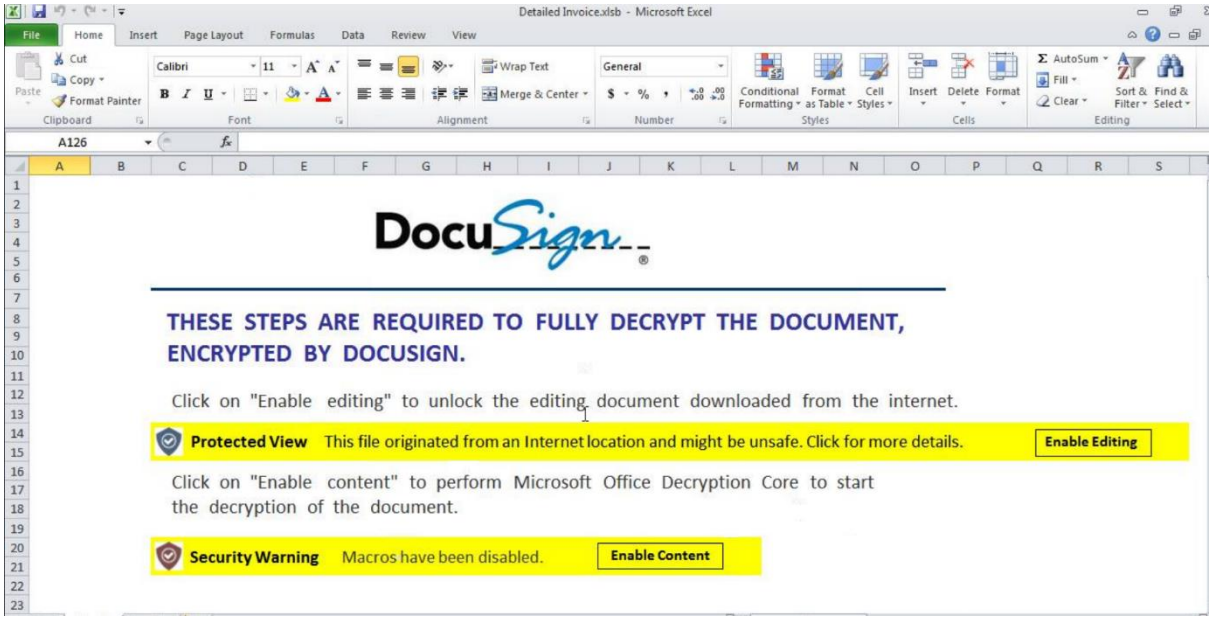

Fig. 6: Fichier Excel comprenant des macros malveillantes

53 QAKBOT - Threat Encyclopedia (trendmicro.com); QakBot (Malware Family) (fraunhofer.de); QakBot, Software S0650 (mitre.org)

54 A closer look at Qakbot's latest building blocks (and how to knock them down) (microsoft.com)

55 Rétrospective de la semaine 44 (ncsc.admin.ch); rétrospective de la semaine 50 (ncsc.admin.ch)

56 Rétrospective de la semaine 20 (ncsc.admin.ch)

On a également observé depuis octobre 2021 que Squirrelwaffle (un maliciel chargeur de logiciels malveillants qui se propage lui aussi par des documents MS Office comprenant des macros malveillantes) installait en plus Qakbot. En outre, l'activité de ce dernier a été marquée au second semestre par l'utilisation de serveurs Exchange compromis.[57]

Conclusion / **Recommandations:**

- Les courriels malveillants peuvent également provenir d'expéditeurs qui semblent connus. Faites preuve de prudence, si une communication déjà effectuée est tout à coup utilisée de manière incohérente.
- Les logiciels malveillants sont souvent diffusés par l'intermédiaire de documents Office et recourent, dans la plupart des cas, aux macros. N'activez jamais les macros.
- Le NCSC recommande aux exploitants de serveurs Microsoft Exchange d'installer sans délai tous les correctifs correspondants et de maintenir les serveurs à jour.
- 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.
- Bloquez au niveau du périmètre réseau les sites Internet utilisés pour propager Qakbot. Une liste de ces sites est fournie gratuitement par URLhaus (abuse.ch).

4.3 Attaques contre des sites ou services Web

4.3.1 Attaques DDoS

La perturbation de la disponibilité de sites Internet en raison d'attaques DDoS (distributed denial of service) est un phénomène régulier en Suisse et à l'étranger. Au second semestre 2021, 17 incidents de ce type ont été signalés au NCSC.

Le secteur financier reste une cible privilégiée des vagues DDoS utilisées comme moyen de chantage. Des prestataires informatiques, des autorités et des établissements de formation ont également été visés en Suisse au second semestre 2021. Des maîtres chanteurs DDoS se faisant appeler FancyLazarus ont tenté d'extorquer des fonds à plusieurs entreprises et autorités cantonales helvétiques. Les menaces d'attaques graves proférées par les malfaiteurs après des attaques de démonstration ne se sont toutefois pas concrétisées. En juillet et en octobre, l'hébergeur de la ville et du canton de Saint-Gall a été victime d'attaques DDoS qui ont entraîné des défaillances temporaires des sites Internet correspondants.[58]

[57] Voir chap. 4.1.4 précédent

[58] Homepages der St.Galler Behörden durch Hackerangriff lahmgelegt (tagblatt.ch)

Plusieurs fournisseurs VoIP (Voice over IP) internationaux ont signalé des dysfonctionnements provisoires dus à des attaques DDoS, dont Telnyx, Bandwidth et Twilio.[59] En septembre, des services bancaires en ligne ont été indisponibles en Nouvelle-Zélande.[60] Enfin, la branche polonaise de T-Mobile a contré une vaste attaque DDoS en décembre.[61] Selon la presse, des attaques DDoS motivées par des raisons politiques ont été observées en Allemagne dans le contexte des élections au Bundestag.[62]

Les attaques DDoS sont également couplées à d'autres modes opératoires: par exemple, les familles de rançongiciels HelloKitty et Yanluowang opèrent de concert avec des attaques DDoS pour accentuer la pression sur les victimes de leur chantage.[63]

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.

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).

De plus, l'Inter-University Computation Center (IUCC) a publié au semestre dernier un guide détaillé des meilleures pratiques concernant les stratégies de défense contre les attaques DDoS: Best Practices for DDoS Mitigation Strategies (geant.org).

4.3.2 Attaques contre les systèmes VoIP

La téléphonie est désormais presque entièrement numérisée, et la plupart des communications vocales transitent par Internet (VoIP). Les systèmes VoIP au sein des entreprises sont donc raccordés à Internet. Non seulement ils constituent une cible potentielle pour les attaques DDoS (voir chap. 4.3.1 précédent), mais ils peuvent également faire l'objet d'abus, lorsqu'ils sont mal protégés. Ainsi, des criminels ont passé de coûteux appels via les systèmes VoIP d'une entreprise suisse qui n'étaient protégés que par un mot de passe standard. Ces appels vers la Tunisie ont occasionné une facture de plusieurs centaines de milliers de francs.

---

59 DDoS attack takes yet another VoIP provider offline (techradar.com)
60 Government still gauging impact of Wednesday's denial-of-service attacks (stuff.co.nz)
61 Polish T-Mobile unit faces cyber attack, systems not compromised (reuters.com)
62 Bundestagswahl 2021: Hackerangriff auf Website des Bundeswahlleiters (businessinsider.de)
63 Kaspersky Q4 2021 DDoS attack report (securelist.com)

4.4 Systèmes de contrôle industriels (ICS) & technologies opérationnelles (OT)

Les attaques visant directement des systèmes de contrôle industriels pour entraver ou influencer des processus physiques sont restées exceptionnelles pendant la période sous revue. L'impact sur l'exploitation découle bien plus fréquemment des connexions entre les réseaux de ces systèmes et les dispositifs informatiques administratifs qui servent à gérer l'entreprise et ses relations commerciales avec ses clients et ses fournisseurs.

4.4.1 Approvisionnement limité en carburant après une cyberattaque en Iran

En octobre dernier, le fonctionnement de nombreuses stations-service a été perturbé en Iran. Le système de paiement destiné aux carburants subventionnés était tombé en panne[64] à la suite d'une cyberattaque lancée par une puissance étrangère, selon les autorités iraniennes.[65] Les pompes fournissaient certes du carburant, mais le système de paiement pour l'essence subventionnée était inopérant. Pour la plupart des clients iraniens, cela équivaut toutefois à une panne, car ils ne peuvent pas acquérir les carburants sans l'avantage lié aux subventions.

Cette panne s'est produite peu avant le deuxième anniversaire de la dernière grande vague de protestations en Iran, déclenchée elle aussi par une hausse des prix de l'essence. Dans le même temps, le message «Khamenei, où est notre essence?» s'affichait sur les panneaux d'information électroniques des autoroutes. Cela rappelle une cyberattaque similaire qui avait visé les transports ferroviaires iraniens en juillet 2021 et reposait également sur un composant Wiper.[66] Aucun lien direct entre les deux incidents n'a toutefois pu être établi à ce jour.

4.4.2 Gestionnaire exclu du système de commande de la domotique

Le service de sécurité informatique Limes Security a présenté les conséquences de manipulations ciblées non autorisées dans les systèmes de contrôle industriels en prenant l'exemple d'une attaque contre un système de domotique.[67] Une personne malveillante a réussi à accéder à des composants basés sur la technologie KNX et à en modifier la configuration, de sorte que le gestionnaire habituel a perdu le contrôle des appareils.

L'assaillant devait posséder des connaissances techniques spécifiques au fonctionnement de KNX pour que le bâtiment «intelligent» devienne partiellement pilotable manuellement sur place, voire totalement inopérant. Ses intentions demeurent floues, et seul un examen forensique de la mémoire des appareils par des spécialistes externes a permis d'éviter leur remplacement coûteux, certains appareils étant intégrés dans la substance du bâtiment.

---

64 Störung der Benzinversorgung - Schlangen vor Irans Zapfsäulen: «Khamenei, wo ist unser Benzin?» (srf.ch)
65 Iran says Israel, U.S. likely behind cyberattack on gas stations (reuters.com)
66 MeteorExpress | Mysterious Wiper Paralyzes Iranian Trains with Epic Troll (sentinelone.com)
67 KNXlock – an attack campaign against KNX-based building automation systems (limessecurity.com)

Conclusion / Recommandations:

Il est judicieux d'investir dans la sécurisation des accès aux systèmes de contrôle industriels et surveiller l'exploitation et les manipulations pour pouvoir réagir rapidement lorsque des modifications abusives sont suspectées.

Sur son site Internet, le NCSC recommande plusieurs mesures de protection pour les systèmes de contrôle industriels (SCI; ncsc.admin.ch).

4.4.3 Identifications de menaces visant les OT et dommages collatéraux

Les attaques qui perturbent l'exploitation de systèmes de contrôle industriels en utilisant leurs fonctions de manière abusive, comme celles présentées au chapitre précédent, restent une exception parmi les cyberincidents entravant les processus physiques. Il est plus fréquent que les systèmes informatiques employés pour piloter les dispositifs de commande soient infectés par un maliciel très répandu[68] ou que l'on tente d'intégrer des appareils de l'Internet des objets dans des réseaux de *bots* pour des attaques DDoS ou le minage de cryptomonnaies.[69]

En soi, des infections de ce type n'ont souvent aucun effet sur les processus pilotés. Cela change cependant dès qu'un rançongiciel est chargé sur les systèmes. Six familles connues de rançongiciels (Cl0p, MegaCortex, Netfilim, LockerGoga, Maze et EKANS) essaient même, à la suite de l'attaque, d'interrompre explicitement les processus informatiques en relation avec les systèmes OT. Au dernier trimestre 2021, Dragos, une société spécialisée dans la sécurité des SCI, a recensé 176 fuites de données relatives aux SCI qui avaient été publiées sur les pages Darknet de groupes de rançongiciels.[70] Ces fuites concernent principalement l'industrie manufacturière, le transport et le secteur alimentaire.

68 https://ics-cert.kaspersky.com/publications/reports/2021/12/16/pseudomanuscrypt-a-mass-scale-spyware-attack-campaign/

69 Honeypot experiment reveals what hackers want from IoT devices (bleepingcomputer.com)

70 Dragos ICS/OT Ransomware Analysis: Q4 2021 (dragos.com)

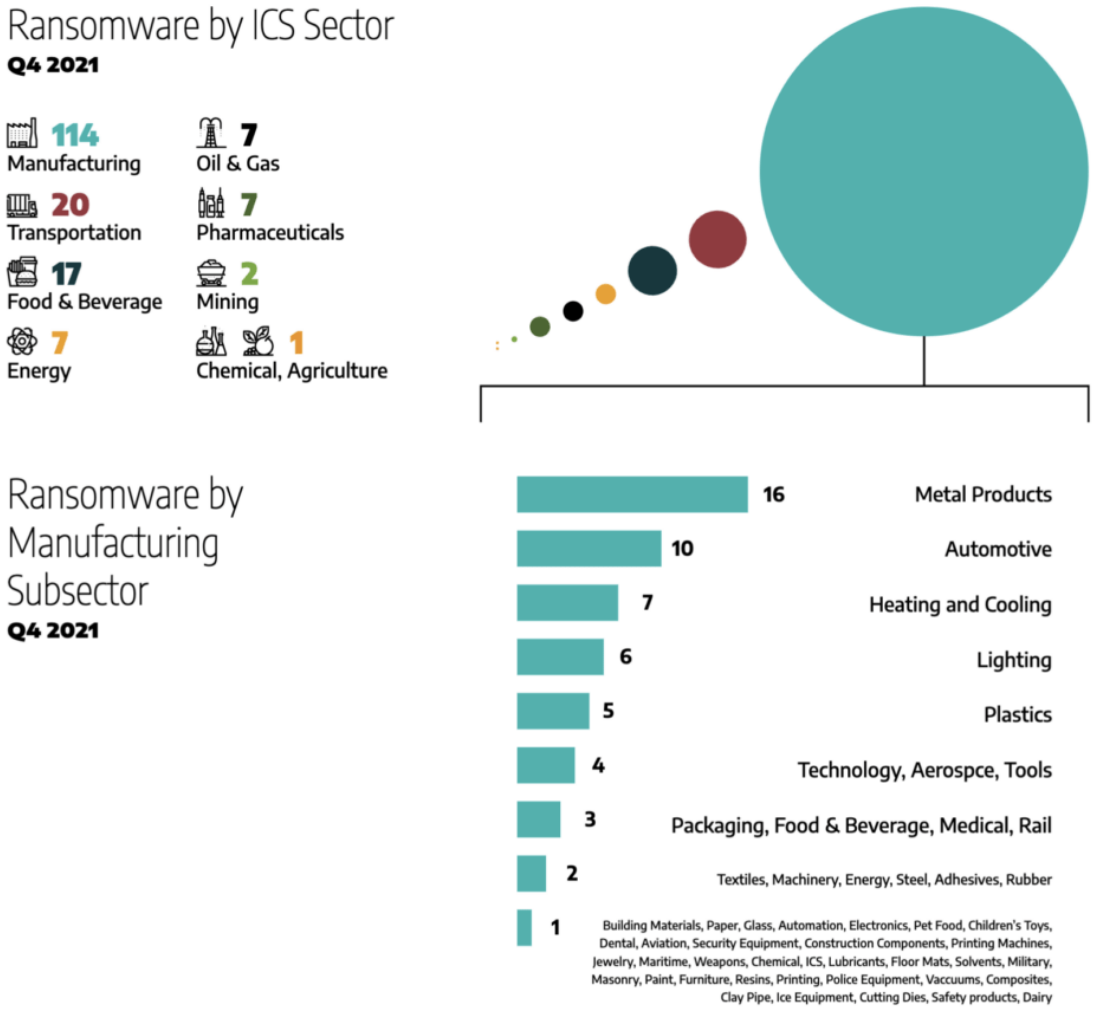

Fig. 7: Données sur les SCI publiées par des groupes de rançongiciels, par secteur (source: dragos.com)

Une enquête[71] de Claroty, entreprise également spécialisée dans la protection OT, a confirmé la vulnérabilité des systèmes face aux rançongiciels: 47 % des 1100 exploitants interrogés ont constaté des effets d'attaques par rançongiciel sur des systèmes OT.

Selon Mandiant, lorsque les données exfiltrées à l'occasion d'attaques par rançongiciel sont publiées, elles comprennent dans un cas sur sept des documents avec des informations sur les systèmes OT (architecture du réseau, matériels et logiciels utilisés, etc.) qui pourraient potentiellement être utilisées pour de futures attaques.

Eu égard aux conflits actuels, des tentatives de sabotage effectives sur des systèmes de contrôle industriels demeurent le scénario le plus vraisemblable.

---

71 Ransomware Often Hits Industrial Systems, With Significant Impact: Survey (securityweek.com)

Ainsi, l'Ukraine a renforcé son dispositif de défense correspondant[72] avec l'aide de spécialistes américains et britanniques dans la perspective d'une invasion par la Russie.

4.5 Vulnérabilités

4.5.1 Atlassian Confluence - CVE-2021-26084 – Exécution de codes à distance

Le 25 août 2021, le fournisseur de logiciels Atlassian a annoncé la publication d'un correctif pour une vulnérabilité critique découverte dans le logiciel Confluence[73], un outil collaboratif de gestion d'espaces de travail et de projets qui est utilisé par de nombreuses entreprises dans le monde et qui contient souvent des données internes. Cette faille permet aux pirates informatiques d'exécuter des codes à distance («Remote Code Execution», RCE). Un attaquant peut alors compromettre entièrement le serveur sur lequel Confluence est opérationnel. Dans plusieurs cas, un crypto miner a été installé[74] ou les entreprises ont été victimes de chantage après le cryptage de leurs données.[75] Selon Atlassian, seule la version locale de son produit était concernée, mais pas la version en nuage.

Conclusion / Recommandations:

Il a été démontré qu'il est facile d'exploiter cette vulnérabilité. Les détails d'exploitation ayant été rendus publics, le risque doit être considéré comme très élevé.

Le public est indirectement affecté lorsqu'une entreprise dont il est client est compromise. Les sociétés qui utilisent des solutions locales doivent être particulièrement prudentes. Il est vivement recommandé à toutes celles qui effectuent elles-mêmes la maintenance de leurs serveurs Confluence d'installer les correctifs nécessaires.[76]

4.5.2 Azure - OMIGOD – Élévation de privilèges, exécution de codes à distance

Le 8 septembre 2021, Microsoft a annoncé un correctif pour de multiples vulnérabilités critiques affectant son offre Azure. La collection de failles baptisée OMIGOD concerne OMI, un outil de gestion des systèmes Linux et UNIX utilisé dans plusieurs services de l'offre Azure. Ces failles permettent l'élévation de privilège d'un utilisateur (CVE-2021-38645, CVE-2021-38648, CVE-202138649) ainsi que l'exécution de codes à distance par un attaquant non authentifié (CVE-2021-38647). Leur gravité se situe entre 7,0 et 9,8 sur un maximum de 10.

72 U.S. and Britain Help Ukraine Prepare for Potential Russian Cyberassault (nytimes.com)
73 Confluence Security Advisory - 2021-08-25 | Confluence Data Center and Server 7.16 (atlassian.com)
74 Cryptominer z0Miner Uses Newly Discovered Vulnerability CVE-2021-26084 to Its Advantage (trendmicro.com)
75 New Atom Silo ransomware targets vulnerable Confluence servers (bleepingcomputer.com)
76 [CONFSERVER-67940] Confluence Server Webwork OGNL injection - CVE-2021-26084 (atlassian.com)

Six jours après le correctif, l'entreprise ayant découvert les vulnérabilités en a détaillé le fonctionnement dans un article.[77] Le 14 septembre 2021, Microsoft a publié un correctif qui n'était déployé automatiquement que pour certaines offres en nuage.

Les clients qui exploitent leur propre infrastructure Azure doivent appliquer eux-mêmes ce correctif. Microsoft a présenté une liste des services concerné et la marche à suivre.[78]

Conclusion / Recommandations:

Ce type de failles critiques touche indirectement le public lorsque les informations personnelles des entreprises dont il est client peuvent être publiées. Le risque est élevé pour les entreprises qui gèrent leur propre infrastructure Azure. Il leur est recommandé d'examiner et de suivre les indications de Microsoft.

4.5.3 Log4j – CVE-2021-44228 – Log4Shell

Le 9 décembre 2021, une vulnérabilité critique dans la librairie open source Apache «Log4j» a été divulguée (CVE-2021-44228). Les détails nécessaires à l'exploitation ont également été rendus publics. «Log4j» est une librairie Java populaire qui fournit une infrastructure de journalisation à des applications tierces. La faille de sécurité est jugée critique (niveau de gravité de 10 sur 10), car elle permet l'exécution de codes à distance (remote code execution, RCE).

De nombreux produits et logiciels open source reposent sur l'utilisation de «Log4j» comme cadre de journalisation. Beaucoup d'entreprises peuvent donc être affectées sans le savoir lorsqu'elles emploient des produits externes dans certaines parties de leur infrastructure.

Suite au CVE-2021-44228, plusieurs failles de sécurité en rapport avec «Log4j» ont été corrigées. Le NCSC a publié une vue détaillée des événements sur le blog du GovCERT.[79]

Conclusion / Recommandations:

Le NCSC a vivement recommandé d'appliquer aussi rapidement que possible les correctifs disponibles et de suivre étroitement l'évolution de la situation pour les entreprises qui utilisent «Log4j» ou des solutions basées sur «Log4j» dans leur infrastructure.

Cette faille pouvant également affecter des composants d'une infrastructure développée par des tiers, il est fortement recommandé de tenir un inventaire actualisé de ces services et de les mettre à jour régulièrement.

---

77 OMIGOD: Critical Vulnerabilities in OMI Affecting Countless Azure Customers (wiz.io)
78 Additional Guidance Regarding OMI Vulnerabilities within Azure VM Management Extensions (microsoft.com)
79 Zero-Day Exploit Targeting Popular Java Library Log4j (govcert.admin.ch)

Compte tenu de la facilité d'exploitation de cette faille et du volume d'informations correspondantes rendues publiques, le risque reste extrêmement élevé pour les systèmes sur lesquels le correctif n'a pas été appliqué.

Outre les effets indirects sur le public lorsqu'une entreprise est victime d'une attaque, cette vulnérabilité a des conséquences directes sur les particuliers. Les périphériques de stockage connectés au réseau (network attached storage, NAS) qui sont utilisés tant par des entreprises que par des particuliers sont eux aussi vulnérables à ce type d'attaques. QNAP, un fabricant de NAS, a publié des recommandations et des informations sur les produits affectés[80], et plusieurs attaques concluantes par rançongiciel ont été rapportées.

4.5.4 Blacksmith - CVE-2021-42114

Le 15 novembre 2021, des chercheurs de l'EPFZ, de Qualcomm et de l'Université libre d'Amsterdam ont publié une étude sur une vulnérabilité matérielle baptisée Blacksmith.[81] Celle-ci affecte les appareils comprenant un certain type de puce RAM et constitue une nouvelle méthode pour contourner efficacement les systèmes de sécurité mis en place sur les puces DDR4.

Le NCSC ayant été certifié en septembre 2021 pour l'attribution des numéros CVE, il a servi d'intermédiaire entre l'équipe de chercheurs et le fabricant de puce et a donné pour la première fois un numéro CVE à la vulnérabilité Blacksmith.

Conclusion / Recommandations:

Cette vulnérabilité affecte les puces produites par Samsung, SK Hynix et Micron, qui sont utilisées par différentes entreprises technologiques. Ces puces étant employées dans le monde entier, la vulnérabilité est considérée comme critique. Le risque d'une utilisation abusive est néanmoins très faible, car l'exploitation de la faille requiert un effort considérable.

Il n'y a aucun correctif des fabricants dans ce cas précis; les puces RAM DDR4 restent donc vulnérables. Il est recommandé d'utiliser pour les infrastructures critiques un type de puce assurant une meilleure protection contre les attaques Rowhammer (ECC ou DDR5).

80 Multiple Vulnerabilities in Apache Log4j Library - Security Advisory (qnap.com)
81 Blacksmith – Computer Security Group (ethz.ch)

4.6 Fuites de données

4.6.1 Fortinet VPN Credentials

Un pirate dénommé Orange a publié 500 000 données d'accès à des comptes Fortinet VPN sur son nouveau forum clandestin.[82] Celles-ci ont apparemment été obtenues durant l'été grâce à une faille pour laquelle un correctif est désormais disponible.

Le NCSC a identifié quelques 400 entrées en lien avec la Suisse et informé les entreprises concernées.

Conclusion / Recommandations:

Les solutions d'accès à distance vulnérables sont régulièrement utilisées pour diffuser des rançongiciels. Lorsque des criminels détiennent des données d'accès à distance complètes et valables, même des systèmes ayant fait l'objet d'un correctif ne peuvent pas les arrêter.

Dans la mesure du possible, protégez les accès aux données, aux comptes, aux systèmes et aux réseaux avec une authentification à deux facteurs au lieu d'associer simplement un nom d'utilisateur et un mot de passe.

Les données d'accès devraient être modifiées régulièrement, en particulier après la correction d'une faille qui présente un risque de fuite de ces données.

4.6.2 EasyGov

En août 2021, des requêtes massives automatisées ont vraisemblablement permis à des pirates de dérober sur la plate-forme Web www.easygov.swiss, gérée par le Secrétariat d'État à l'économie (SECO), le nom de quelque 130 000 entreprises qui avaient demandé un crédit COVID-19 en 2020. Les pirates n'ont toutefois pas réussi à connaître le montant du crédit ni à obtenir d'autres informations sur ces entreprises. Le SECO a été informé de cet événement le 19 octobre et a pris des mesures immédiates: l'interface Web attaquée a été fermée en l'espace de quelques minutes, les données ont été supprimées du serveur et le processus ciblé sur EasyGov a été intégralement désactivé.[83] Le NCSC a soutenu et conseillé le SECO en la matière. Ce dernier a lancé une enquête correspondante.

Conclusion / Recommandations:

La numérisation permet de simplifier certains processus administratifs. C'est d'ailleurs pour cela que le portail du SECO s'appelle EasyGov. De plus, pendant la pandémie, il était urgent de fournir une aide non bureaucratique aux milieux économiques.

---

82 Hackers leak passwords for 500,000 Fortinet VPN accounts (bleepingcomputer.com)
83 EasyGov victime d'une cyberattaque (seco.admin.ch)

Les entreprises pouvaient dès lors ouvrir un formulaire de demande de crédit en indiquant simplement leur identifiant (IDE). Aucun formulaire ne s'ouvrait lorsqu'un (premier) crédit avait déjà été demandé pour une IDE. Des requêtes massives comportant des IDE, qui figurent dans le registre du commerce, ont été exécutées pour découvrir abusivement les entreprises ayant sollicité un crédit.

L'activation de possibilités de consultation ou de contenus reliés à une base de données comporte toujours un risque d'abus. Il faut donc se demander quels résultats obtiendrait une personne curieuse non autorisée en effectuant diverses saisies – même une réponse négative permet de tirer des conclusions. Dans tous les cas, il est primordial d'empêcher les requêtes massives pour éviter que des personnes non autorisées n'obtiennent de grands volumes de données en très peu de temps.

4.7 Espionnage

4.7.1 Pegasus

Au second semestre 2021, la presse, les chercheurs, les organisations non gouvernementales et l'opinion publique se sont fortement intéressés à l'utilisation du logiciel d'espionnage Pegasus après la publication en juillet 2021 d'un rapport d'Amnesty International sur l'usage de ce logiciel contre des militants des droits humains et des journalistes dans le monde.[84] En 2018 déjà, la plate-forme de recherche canadienne CitizenLab avait publié une information sur l'emploi de Pegasus dans 45 pays entre 2016 et 2018.[85] Développé par l'entreprise israélienne NSO, Pegasus est un logiciel de surveillance des appareils mobiles qui, d'après les informations du fabricant, a été conçu pour lutter contre le terrorisme et est vendu à des autorités étatiques. Des solutions similaires sont utilisées à travers le monde pour enquêter sur des personnes ciblées par des enquêtes pénales et lors de mesures d'approvisionnement des services de renseignements. Les autorités de sécurité recourent à ce procédé, car un nombre croissant de canaux de communication et d'applications employés par les suspects sont cryptés de bout en bout, de sorte qu'il n'est plus possible d'écouter ou de lire les messages pendant la transmission. Une industrie proposant aux autorités étatiques des produits de surveillance ciblant les terminaux s'est développée ces dernières années. Le problème est que ces moyens de surveillance sont employés conformément au cadre juridique local, qui varie d'un pays à l'autre. En septembre 2021, Apple a corrigé dans son service de chat iMessage une faille qui avait été exploitée par Pegasus.[86]

---

84 Projet Pegasus: révélations de l'espionnage de grande ampleur du logiciel israélien de NSO Group (amnesty.ch)

85 HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries (citizenlab.ca)

86 Analyzing Pegasus Spyware's Zero-Click iPhone Exploit ForcedEntry (trendmicro.com)

4.7.2 Vol de données grâce à l'API Slack

Supposément soutenu par l'État iranien, le groupe de pirates informatiques MuddyWater.[87]déploie une porte dérobée récemment découverte nommée Aclip, qui abuse de l'interface API de Slack, un service de messagerie instantané basé sur le Web, pour des communications internes. Aclip tire son nom du script batch Windows via lequel elle s'exécute (aclip.bat). La porte dérobée demeure sur un appareil infecté en ajoutant une clé de registre; elle se lance donc automatiquement au démarrage du système. Aclip reçoit des commandes PowerShell du serveur C2 par l'intermédiaire des fonctions de l'API Slack et peut être utilisée pour exécuter d'autres commandes, envoyer des captures d'écran du bureau Windows actif et exfiltrer des données. D'après un rapport d'IBM, les opérateurs ont utilisé cette technique contre des compagnies aériennes.[88]

4.7.3 Nobelium

Les chercheurs ont baptisé Nobelium les pirates à l'origine de l'attaque contre la chaîne d'approvisionnement de SolarWinds. Plusieurs services rattachent Nobelium au groupe APT29 ou au SVR, le service des renseignements extérieurs de Russie.[89] Nobelium a de nouveau opéré au second semestre 2021. Selon Microsoft, il visait notamment des prestataires informatiques ainsi que des fournisseurs de services gérés et de services en nuage aux États-Unis et en Europe pour pouvoir accéder à leurs clients. Microsoft a constaté que les pirates ciblaient des comptes avec des droits privilégiés pour pouvoir se propager dans les environnements en nuage et exploiter les relations clients.[90] Cette campagne souligne l'importance des relations de confiance et des relations clients dans les risques d'espionnage, en particulier au niveau des prestataires informatiques.

4.7.4 Nickel / K3chang

Les acteurs du cyberespionnage continuent d'exploiter fortement les solutions d'accès à distance n'ayant pas fait l'objet de correctifs: Microsoft a dévoilé une campagne du groupe Nickel qui procédait ainsi.[91] Nickel semble opérer depuis la Chine et a été rattaché au groupe K3chang.[92] La campagne décrite par Microsoft avait différents objectifs, dont des organismes gouvernementaux, des représentations diplomatiques et des organisations non gouvernementales sur plusieurs continents, y compris en Suisse.

---

87 MuddyWater (Threat Actor) (fraunhofer.de)
88 Nation State Threat Group Targets Airline with Aclip Backdoor (securityintelligence.com)
89 APT29, NobleBaron, Dark Halo, StellarParticle, NOBELIUM, UNC2452, YTTRIUM, The Dukes, Cozy Bear, CozyDuke, Group G0016 (mitre.org)
90 NOBELIUM targeting delegated administrative privileges to facilitate broader attacks (microsoft.com)
91 NICKEL targeting government organizations across Latin America and Europe (microsoft.com)
92 Ke3chang, APT15, Mirage, Vixen Panda, GREF, Playful Dragon, RoyalAPT, Group G0004 (mitre.org)

4.8 Ingénierie sociale et phishing

4.8.1 Aperçu du phishing

Pendant la période sous revue, 90 046 URL ont été vérifiées après leur signalement sur le portail antiphishing.ch, géré par le NCSC, ou auprès du guichet unique à l'aide du formulaire d'annonce. Parmi elles, 3991 se sont révélées être des sites d'hameçonnage, que le NCSC a annoncés à l'hébergeur concerné, aux différents fabricants de navigateurs et aux groupes de travail luttant contre le phishing. Ce nombre a légèrement fléchi par rapport aux 4682 sites d'hameçonnage identifiés au premier semestre 2021.

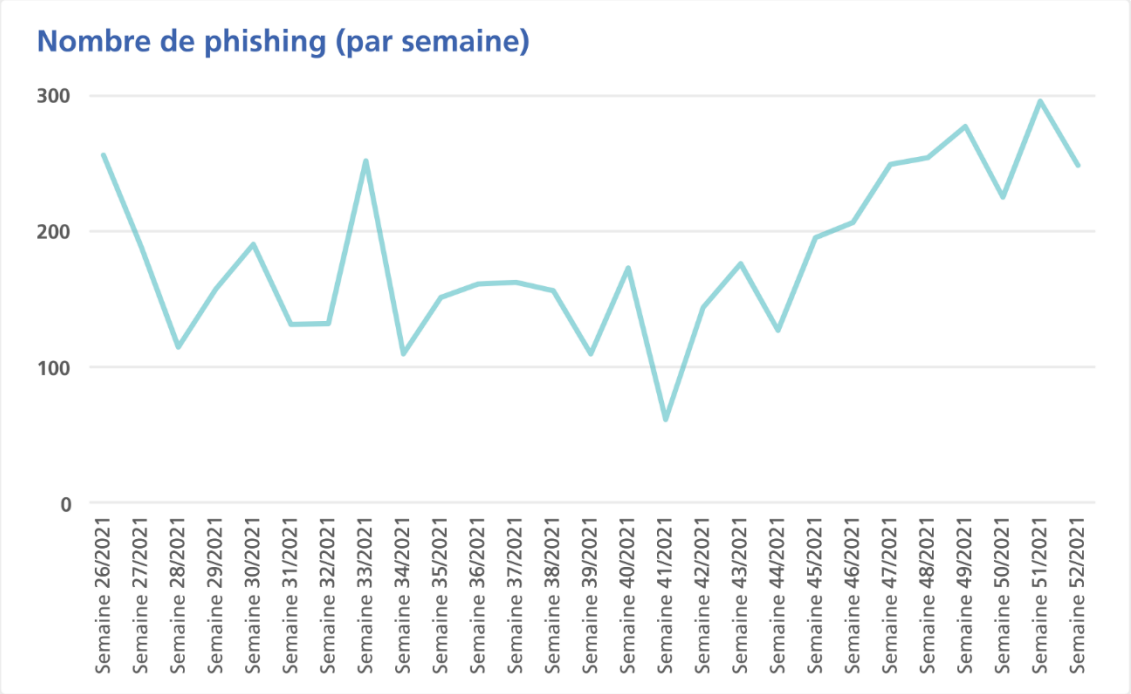

Fig. 8: Nombre d'adresses URL de phishing examinées et confirmées par le NCSC chaque semaine, au deuxième semestre 2021. Les données actuelles sont publiées sous: https://www.govcert.admin.ch/statistics/phishing/

Le NCSC observe une mutation dans les tentatives d'hameçonnage: au lieu que de grandes marques internationales soient usurpées, les identités visuelles d'entreprises locales, qui opèrent parfois exclusivement sur le marché suisse, sont détournées à des fins abusives, les données d'accès aux prestataires de services financiers et aux services Web restant des cibles privilégiées. Pour obtenir les données de cartes de crédit, les criminels utilisent les logos des entreprises les plus variées et des prétextes divers.[93]

Le phishing était à l'origine un phénomène de masse, mais les malfaiteurs s'attaquent parfois désormais à des cibles très spécifiques. Pendant le semestre sous revue, une tentative d'ha-

[93] Voir précédent chap. 4.1.2 et chap. 5.2 ci-après

meçonnage visait les entreprises clientes de la Banque Migros. Quiconque cliquait sur la rubrique «Particuliers» du site de phishing était redirigé vers le véritable site Web de la Banque Migros. Les malfaiteurs ciblaient les données pouvant leur permettre d'accéder aux logiciels de comptabilité des entreprises.

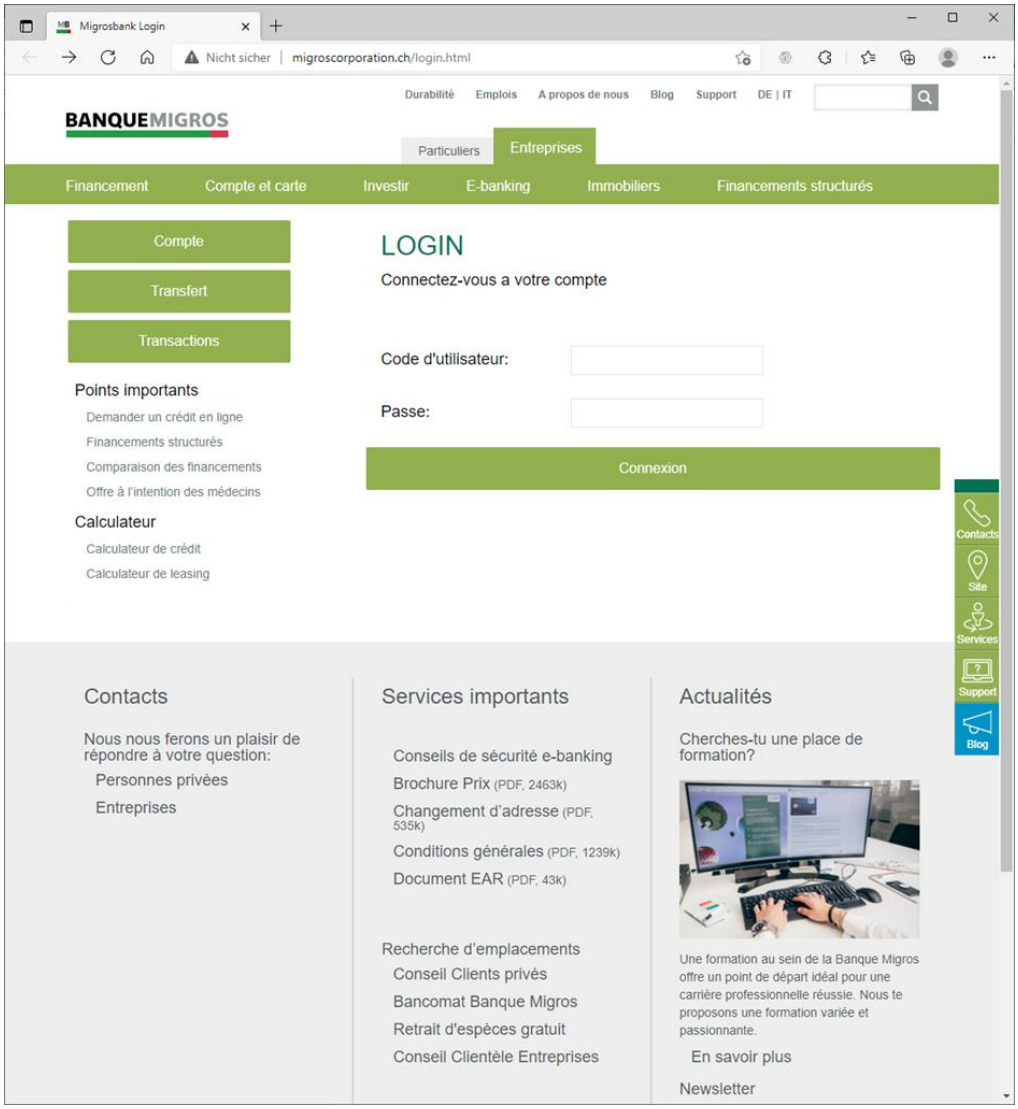

Fig. 9: Site d'hameçonnage visant la clientèle entreprises de la Banque Migros

En outre, de l'hameçonnage en temps réel visant les clients d'établissements financiers suisses a de nouveau été constaté au second semestre, même si son volume était extrêmement faible par rapport aux autres attaques par phishing. Déjà présentée dans le rapport semestriel 2019/1[94], cette technique élude l'authentification à deux facteurs, mais requiert une intervention plus active du malfaiteur, car celui-ci doit se connecter au système d'e-banking en même temps que la victime.

[94] Rapport semestriel 2019/1 (ncsc.admin.ch), chap. 4.4.2

Les réseaux sociaux peuvent également servir à l'hameçonnage. Ainsi, à la mi-novembre, la fonction de Facebook qui permet d'afficher les pages sur lesquelles une personne a été identifiée a été détournée en vue d'un phishing ciblé.[95]

4.8.2 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. En général, ces messages proviennent prétendument d'expéditeurs dignes de confiance, tels que des détaillants ou des entreprises de logistique connus. Ils prennent parfois la forme de concours. Un lien conduit généralement à une page spécialement préparée par les escrocs, sur laquelle il faut indiquer ses données personnelles ou les détails de sa carte de crédit.

Par exemple, pendant la période sous revue, Coop a lancé un avertissement sur les réseaux sociaux à propos d'un message d'hameçonnage circulant sur WhatsApp qui informe le destinataire qu'il aurait gagné à un concours organisé par le détaillant.

Fig. 10: Avertissement de Coop concernant des jeux-concours frauduleux organisés en son nom. [96]

4.8.3 SIM Swapping

L'échange (ou *swap*) de cartes SIM est une technique permettant de rediriger le trafic réseau d'un abonné mobile sans avoir accès à son appareil.[97] Grâce à ce piratage, le malfaiteur contraint un opérateur de téléphonie mobile à émettre une nouvelle carte SIM et à la lier à un

95 Rétrospective de la semaine 45 (ncsc.admin.ch)
96 coop_ch auf Twitter: "#Phishing-Nachricht auf WhatsApp." (twitter.com)
97 Network Effects, Tactic TA0038 - Mobile (mitre.org)

numéro de téléphone et à un compte existants. La personne qui obtient cette nouvelle carte SIM peut, par exemple, recevoir des SMS comportant un code pour une authentification à deux facteurs afin d'accéder à certains services, ou réinitialiser le mot de passe d'un compte, car cette opération requiert souvent la saisie d'un code envoyé par SMS.[98]

L'ingénierie sociale auprès des collaborateurs d'une entreprise de téléphonie mobile est l'une des techniques employées par les criminels pour se faire remettre une nouvelle carte SIM. Une fuite de données de l'entreprise concernée peut fournir des informations utiles en la matière. T-Mobile US Inc., la filiale américaine de Deutsche Telekom, a été confrontée à plusieurs fuites de données ces dernières années. T-Mobile a rendu public le dernier incident datant de décembre 2021 après le signalement de plusieurs utilisateurs victimes de SIM Swapping.[99]

Une autre tactique consiste à amener les collaborateurs d'une entreprise de télécommunication à installer un logiciel d'accès à distance ou à communiquer les données de connexion à un service d'accès à distance utilisé dans l'entreprise. Les criminels ont ainsi un accès externe à l'ordinateur et peuvent émettre une nouvelle carte SIM, envoyée à l'adresse de leur choix.[100]

4.8.4 Faux support technique e-banking via un lien Google Ad

Les appels d'un faux support technique[101], au cours desquels l'appelant prétend que l'ordinateur est infecté, sont un phénomène connu de longue date. En général, les criminels se présentent comme des collaborateurs d'une entreprise informatique et tentent d'infecter le système de la victime ou souhaitent lui vendre une prestation pour obtenir les données de sa carte de crédit. Dans la variante observée entre fin août et fin septembre par le NCSC[102] et les autorités de police cantonale[103], les escrocs avait mis en ligne des annonces Google qui s'affichaient en premier lors de la recherche de plates-formes e-banking de certaines banques suisses. Le lien figurant dans l'annonce conduisait à un site d'hameçonnage. Après avoir saisi l'identifiant et le mot de passe, un message d'erreur apparaissait et invitait à appeler un numéro de téléphone suisse. Un prétendu collaborateur de la banque répondait à l'appel et convainquait la victime de télécharger un logiciel d'accès à distance pour qu'il puisse accéder à l'ordinateur et résoudre le «problème». Le soi-disant collaborateur prenait alors le contrôle de l'ordinateur et exécutait un supposé paiement test avant de s'évaporer dans la nature avec l'argent.

98 SIM Card Swap, Technique T1451 - Mobile (mitre.org)
99 T-Mobile says new data breach caused by SIM swap attacks (bleepingcomputer.com)
100 Hackers Are Breaking Directly Into AT&T, T-Mobile, Sprint to Take Over Customer Phone Numbers (vice.com)
101 Fake Support (ncsc.admin.ch)
102 Rétrospective de la semaine 32 (ncsc.admin.ch); Rétrospective de la semaine 34 (ncsc.admin.ch)
103 Raiffeisen Meldung "Aufgrund verdächtiger Aktivitäten wurde Ihr Konto gesperrt" ist Betrug (cybercrimepolice.ch)

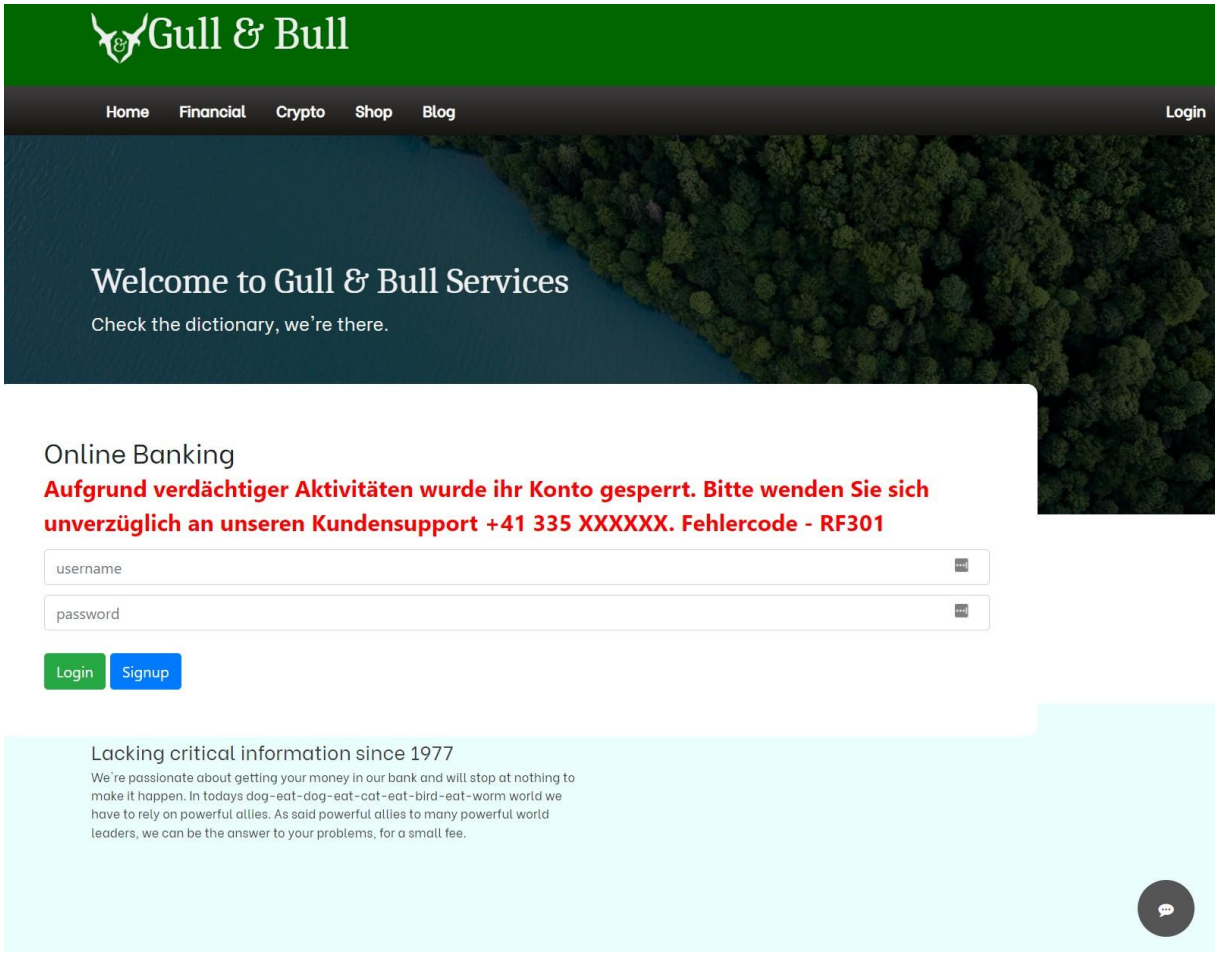

Fig. 11: Imitation de la page de connexion d'un institut financier

5 Phénomènes combinés dans l'ingénierie sociale

5.1 Tendance aux attaques ciblées plutôt qu'aux opérations de masse

La fraude au paiement anticipé, la fake sextortion ou le faux support technique ne représentent qu'une petite partie des phénomènes observés par le NCSC en 2021. Un aperçu de ces quelque 45 phénomènes figure sur la page «Cybermenaces»[104] du NCSC. Il arrive de plus en plus souvent qu'une catégorisation claire soit impossible, car les escrocs tentent toujours plus de combiner plusieurs phénomènes. Cela tient au fait qu'ils ont davantage de mal à tromper leurs victimes avec de «simples» courriels frauduleux et doivent dès lors redoubler d'efforts pour parvenir à leurs fins.

104 Cybermenaces (ncsc.admin.ch)

Ces dernières années, les tentatives de fraude constituaient surtout des opérations de masse. Les escrocs envoyaient automatiquement des centaines de milliers de courriels à des destinataires quelconques en espérant qu'une partie d'entre eux se laisserait piéger.

Malgré une faible charge pour les malfaiteurs, leur taux de réussite était minime. Ce modèle d'affaires semble néanmoins avoir fait recette par le passé, puisque l'on observe régulièrement de nombreux envois massifs de ce type.

La sensibilisation des internautes va cependant croissant et le taux de réussite diminue régulièrement en défaveur des escrocs. La plupart des tentatives d'attaque grossières sont identifiées. Les escrocs doivent donc appliquer d'autres méthodes pour inciter une victime potentielle à faire ce qu'elle ne ferait pas en temps normal. Il convient dès lors de susciter la confiance pendant un certain temps. La prise de contact se produit, par exemple, sur des plates-formes que le destinataire juge fiables et sur lesquelles il a déjà eu des expériences positives. Cela réduit son scepticisme tout en augmentant la probabilité que cette personne soit victime d'une escroquerie somme toute simple.

Certaines publications sur des sites de petites annonces renvoient vers des sites d'hameçonnage. Un supposé soldat souhaitant investir en Suisse répond à des annonces sur des portails immobiliers. Quant aux sites de rencontre usuels, les escrocs essaient de convaincre leurs victimes de «placer» leur argent sur des plates-formes douteuses.

5.2 Hameçonnage à la suite d'une petite annonce

De nombreux escrocs rodent sur les plates-formes de petites annonces. La fraude correspondante fait d'ailleurs partie des délits les plus fréquemment signalés. Outre les scénarios classiques consistant à vendre des marchandises inexistantes ou à ne pas livrer le produit payé, le NCSC observe de plus en plus souvent des variantes combinées dans lesquelles les données de carte de crédit des annonceurs sont volées sur ces plates-formes. Les escrocs se donnent du mal et créent des sites Web d'entreprises de livraison de colis qui semblent officiels. Ces sites ne sont toutefois pas génériques; ils sont personnalisés et comprennent non seulement le nom présumé du destinataire, mais également une description et une image de l'article à vendre. Les malfaiteurs conçoivent une page Web individuelle pour chaque vendeur. Ce travail sert uniquement à surmonter le scepticisme de la victime et à l'inciter à indiquer ses données de carte de crédit.

5.3 Héritage au lieu de la vente d'un logement

La fraude au paiement anticipé est un classique des courriels frauduleux qui sont envoyés en grand nombre. De supposés héritages et gains au loto sont censés éveiller la curiosité des destinataires et les amener à répondre. Toutefois, la plupart de ces derniers identifient désormais ces courriels comme frauduleux et les suppriment. Les escrocs testent donc de nouvelles variantes susceptibles de mieux réussir. Dans l'une d'elles, ils répondent à une annonce immobilière. Un prétendu soldat stationné en Afghanistan et en quête d'un nouveau foyer en Suisse se montre intéressé par une offre immobilière. Après un long échange de courriels destiné à attirer la confiance et en lien avec le futur achat, le pseudo-soldat oriente la discussion vers une somme d'argent qu'il souhaite investir en Suisse. Le militaire fait miroiter au

propriétaire immobilier une récompense pécuniaire considérable s'il contribue à l'investissement. Dans ce cas également, il demande tôt ou tard à la victime de payer des émoluments. L'histoire est inventée d'un bout à l'autre, et ni le soldat ni son pactole n'existent.

5.4 Investir plutôt que prêter

L'arnaque aux sentiments (romance scam ou love scam), c'est-à-dire la forme numérique de l'escroquerie au mariage, existe depuis des années. Dans ce type de fraude, les escrocs créent de faux profils sur les réseaux sociaux et les sites de rencontres en ligne, puis feignent le grand amour avec leurs victimes pour obtenir ensuite une aide financière de leur «partenaire». Là encore, ils ont de plus en plus de mal à inciter la victime à faire un versement, que ce soit pour une mère prétendument malade ou pour des dettes que le partenaire doit régler urgemment sous peine de se retrouver à la rue. Ces variantes sont elles aussi connues et alertent les victimes potentielles. Les malfaiteurs recherchent donc de nouvelles opportunités. Ils tentent fréquemment de convaincre la victime d'investir sur une plate-forme de placement. Un «partenaire» ou une «connaissance» des escrocs travaille dans ce secteur ou ceux-ci affirment avoir déjà gagné beaucoup d'argent sur une plate-forme. La tactique est claire: l'escroc détourne l'attention et laisse croire qu'il est riche. Au lieu de demander de l'argent, il fait bénéficier la victime de ses «connaissances», lui faisant ainsi miroiter un gain important. La victime ne peut guère se douter que les gestionnaires de la supposée plate-forme et le rabatteur sont de mèche.

Conclusion / Recommandations:

Les escrocs se détournent parfois des opérations de masse pour tenter des attaques personnalisées. Toutes ces variantes ont une chose en commun: les malfaiteurs s'efforcent au préalable de gagner la confiance de leur cible au moyen d'une première prise de contact. Il est donc primordial de rester prudent, même si l'on a la sensation de connaître son interlocuteur. Internet est un lieu où quiconque peut prendre l'identité de son choix, y compris dans les profils postés sur des plates-formes renommées. Communiquer virtuellement avec une personne depuis un certain temps ne signifie pas pour autant qu'elle est digne de confiance.