2 novembre 2023 | Centre national pour la cybersécurité NCSC

Rapport semestriel 2023/I (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

Thème prioritaire: hacktivisme

Les événements politiques importants peuvent susciter la réaction d'activistes, qui vont mener dans le cyberespace des activités illégales, qu'on appelle le hacktivisme. Par leurs actions, les hacktivistes cherchent à attirer l'attention des médias et du grand public. L'administration fédérale en a été la ciblée à deux reprises en juin 2023. Une première attaque par déni de service distribué (DDoS) a été lancée dans le but de surcharger le site Internet des Services du Parlement et de le rendre indisponible, suite à la décision du Conseil des États en lien avec la loi fédérale sur le matériel de guerre. Pour la deuxième attaque, l'élément déclencheur a été l'annonce du discours par vidéo du président ukrainien Volodymyr Zelensky devant l'Assemblée fédérale. Cette deuxième attaque DDoS a touché, outre les sites web de plusieurs offices fédéraux et du Parlement, ceux de plusieurs grandes entreprises en Suisse, de quelques aéroports, de plusieurs villes et cantons ainsi que de l'Association suisse des banquiers. Le rapport semestriel analyse par conséquent les méthodes et les motivations des hacktivistes. Au travers de deux témoignages, il s'intéresse également à la réaction de grandes entreprises ciblées par une attaque DDoS. Simultanément, le NCSC a publié un rapport d'analyse détaillé sur ces attaques DDoS.

Augmentation des annonces au premier semestre 2023

Le NCSC a reçu 19 048 annonces de cyberincidents durant le premier semestre 2023, soit environ 2000 de plus qu'au premier semestre 2022 (16 951 annonces). La majorité des signalements continuent de concerner les formes de fraude les plus diverses. Les annonces relatives à des courriels de menace relevant de la fausse extorsion sont toujours les plus fréquentes; elles représentent environ 30 % des signalements. En règle générale, les destinataires de ces courriels émanant prétendument d'une autorité suisse ou étrangère sont accusés d'avoir commis une infraction. Le NCSC relève que son nom a été de plus en plus souvent utilisé de manière frauduleuse au cours du semestre sous revue.

Forte hausse des annonces d'hameçonnage

Avec une augmentation d'annonces de 40%, l'hameçonnage constitue le deuxième cyberincident le plus signalé et représente ainsi un cinquième des annonces reçues au cours du semestre sous revue. Cette augmentation tient principalement à une vague d'hameçonnage contre les clients SwissPass qui a sévi pendant presque tout le premier semestre 2023. D'une manière générale, le NCSC constate que les tentatives d'hameçonnage sont de plus en plus sophistiquées et que les attaquants testent de nouvelles méthodes pour dissimuler les liens malicieux.

Incidents dus à des rançongiciels: Évolution inverse entre les entreprises et les particuliers

Au cours du premier semestre 2023, le nombre d'attaques par rançongiciel signalées (64) est resté relativement stable par rapport au semestre précédent (76 annonces). Les annonces émanant de particuliers ont fortement reculé (passant de 27 à 8), mais a contrario les entreprises ont signalé davantage de cas (49 contre 56 au semestre précédent). Les attaques engendrent des interruptions opérationnelles de courte durée suite au chiffrement des données ainsi que la potentielle publication des données subtilisées, ce qui rend l'estimation des dommages subis difficile.

Éditorial

Les différentes attaques par déni de service distribué (DDoS) lancées par des hacktivistes prorusses en juin dernier contre des sites Internet suisses, comme ceux des Services du Parlement, de diverses organisations et de plusieurs offices fédéraux, ont fait la une des journaux. Les attaques DDoS ne sont néanmoins pas des événements hors du commun, en ce qu'elles ont lieu presque quotidiennement. Alors pourquoi celles-ci ont-elles fait tant de bruit?

Tout est une question de contexte politique. Par leur action, des hacktivistes prorusses ont voulu faire connaître leur opinion politique et donner l'impression qu'il fallait s'attendre à tout moment à une attaque russe de grande ampleur dans le cyberespace. Lorsque les médias et les experts en cybersécurité relaient cette volonté dans leurs articles, ils contribuent aux objectifs des hacktivistes, qui semblent agir de leur propre initiative selon l'état actuel des connaissances.

En Suisse aussi, les hacktivistes ont réussi à répandre l'incertitude, du moins temporairement, auprès des organisations, personnalités politiques et citoyens non-spécialistes du domaine. Il est par conséquent très important d'analyser sereinement les attaques. Se pose alors la question de l'ampleur réelle des dommages, de la rentabilité économique de renforcer la protection contre les attaques DDoS, du signalement des attaques sans pour autant fournir une plateforme à leurs auteur, ainsi que de la communication auprès du grand public afin qu'ils puissent mieux cerner les enjeux de ces attaques. Le NCSC a élaboré un rapport d'analyse détaillé sur le sujet, qui se trouve à la disposition des personnes intéressées, en complément du présent rapport semestriel.

Les attaques par rançongiciel ont des conséquences bien plus graves pour les entreprises et les autorités que les attaques DDoS. L'attaque qui a eu le plus de retentissement est sans doute celle contre l'entreprise Xplain, qui fournit des services non seulement à des entreprises privées, mais aussi à la Confédération et aux cantons. Une enquête administrative étant en cours, le présent rapport ne revient pas en détail sur cet incident, qui sera traité dans un futur rapport, lorsque toutes les investigations nécessaires auront été menées. Nous souhaitons souligner que nous avons dès le départ décidé de communiquer de la manière la plus transparente possible, sans pour autant mettre en danger les organisations ou les personnes dont les données ont fuité. Cependant la communication transparente, implique aussi automatiquement l'exposition à la critique. Des questions légitimes ont été soulevées, et nous y répondrons au terme des investigations. Les analyses prennent du temps et il ne serait pas pertinent de tirer des conclusions hâtivement.

Le présent rapport comprend également une analyse de la situation en matière de menace ainsi qu'une vue d'ensemble des cyberincidents. La plupart des cyberincidents signalés au NCSC concernent une nouvelle fois les formes de fraude les plus diverses. Restons donc vigilants, surtout lorsqu'il s'agit de communiquer des informations personnelles, telles que les données de notre carte de crédit ou des identifiants. Enfin, le rapport fait le point sur les cybermenaces associées à la guerre en Ukraine.

N'hésitez pas à nous communiquer vos réactions au présent rapport.

Bonne lecture!

Florian Schütz, délégué fédéral à la cybersécurité

2 Thème prioritaire: hacktivisme

De nombreux acteurs s'attaquent à divers systèmes par différents moyens. Le spectre des acteurs de la menace varie selon leurs capacités (à savoir le degré de sophistication) et leurs motivations. Depuis le début de la guerre en Ukraine, les attaques par des groupes d'hacktivistes ont été observées de façon croissante. Ces groupes se caractérisent par deux facteurs: ce ne sont généralement pas des professionnels et leurs activités sont motivées par une idéologie (par ex. sociale, politique ou encore religieuse), contrairement aux criminels, qui eux agissent premièrement par intérêt financier. En conséquence, les hacktivistes peuvent se contenter d'attaques plutôt superficielles (par ex. une interruption de courte durée de la disponibilité d'un site Internet) qui, reprises par les médias, attirent l'attention sur leur cause. Le groupe d'hacktivistes le plus connu est sans doute Anonymous. Sous ce label, des hackers du monde entier s'engagent depuis plus de 15 ans, entre autres, pour la liberté d'expression et l'indépendance d'Internet, ainsi que contre les autorités et les multinationales.

Catalysés par la guerre en Ukraine, de nombreux groupes d'hacktivistes se sont formés ou développés, depuis le mois de février 2022, prenant parti pour l'un ou l'autre des protagonistes, et mènent régulièrement des attaques contre des entités qu'ils jugent nuisibles pour leur camp. Par exemple, les groupes d'hacktivistes prorusses choisissent principalement comme cibles des entités d'États fournissant un appui à l'Ukraine ou infligeant des sanctions à la Russie[1]. On observe moins d'activités et de revendications de la part de groupes d'hacktivistes favorables à l'Ukraine, notamment car ceux-ci sont moins nombreux que ceux soutenant la Russie[2]. En grande majorité, il n'y a pas de lien formel entre un groupe d'hacktivistes et des entités gouvernementales, mais ces groupes peuvent servir de proxy à un État, notamment en agissant comme amplificateur pour de la propagande. De tels liens ont ainsi été mis en évidence dans différents rapports de sociétés de sécurité informatique occidentales[3]. Un cas particulier est celui de l'IT Army of Ukraine. À la différence des groupes d'hacktivistes prorusses, ce groupe a été formé ouvertement à l'initiative d'un gouvernement, le gouvernement ukrainien, qui entreprend des efforts afin de légaliser le statut des membres de l'IT Army of Ukraine, en développant une loi qui devrait permettre de les intégrer officiellement en tant que réservistes[4].

2.1 DDoS: perturbation de la disponibilité de sites et de services Internet

Les attaques affectant la disponibilité d'un service en ligne (*Distributed Denial of Service*, déni de service distribué, en abrégé DDoS) sont des actions par lesquelles les auteurs tentent, en utilisant un grand nombre d'ordinateurs situés dans différents lieux, de rendre un service indisponible pour les usagers réguliers en le saturant de requêtes. De telles attaques n'impliquent ni l'accès non autorisé à des données ni la destruction de systèmes. Une attaque DDoS pourrait être comparée, dans le monde réel, à un grand nombre de personnes qui participe à une conférence de presse publique et qui en créant une cacophonie empêchent les questions légitimes des journalistes d'être entendues et que des réponses aux questions soient apportées.

---

1 Voir chap. 2.1 et 4.7.

2 Russia-Ukraine War - Cybertracker May 03 (cyberknow.medium.com)

3 A year of Russian hybrid warfare in Ukraine (microsoft.com); GRU: Rise of the (Telegram) MinIOns (mandiant.com)

4 Ukraine Scrambles to Draft Cyber Law, Legalizing Its Volunteer Hacker Army (newsweek.com)

Les attaques DDoS qui aboutissent ont donc en général pour seule conséquence de rendre temporairement le site Internet de l'organisation concernée – pour ainsi dire son guichet d'information – inaccessible. Toutefois, quand une partie essentielle des activités opérationnelles est réalisée via le site Internet, comme c'est par exemple le cas pour les boutiques en ligne, une indisponibilité, même brève, peut causer des dommages économiques considérables. Une attaque de ce type peut aussi engendrer également des interruptions de processus en cas de besoins de communication ou d'information urgents.

Les hacktivistes cherchent à attirer l'attention sur eux, ainsi qu'éventuellement à créer de l'insécurité, voire à détruire la confiance dans les organisations qui exploitent les sites. Diverses organisations sont préparées à des attaques DDoS et peuvent rapidement rétablir l'accessibilité à leurs ressources web. Cependant, l'activation des mesures de défense, comme le filtrage du trafic provenant de l'attaque ou l'augmentation de la capacité du trafic, prend un certain temps et entraîne des coûts. Les hacktivistes profitent de ce laps de temps pour prouver qu'un site Internet n'était pas accessible à un certain moment et mettent ce fait en avant sur les réseaux sociaux donnant ainsi l'impression qu'ils ont réussi à «pirater» une entreprise, à «mettre hors service le site Internet» ou même à «tuer le site Internet», même si l'interruption était de très courte durée.

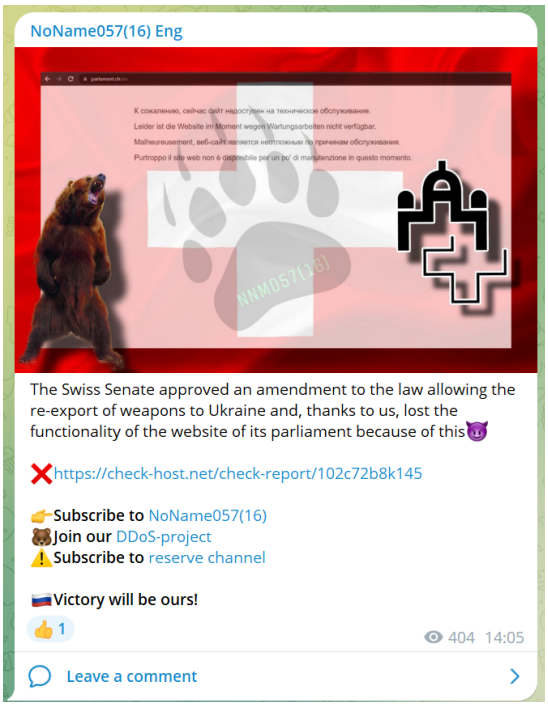


Fig. 1: Revendication des hacktivistes.

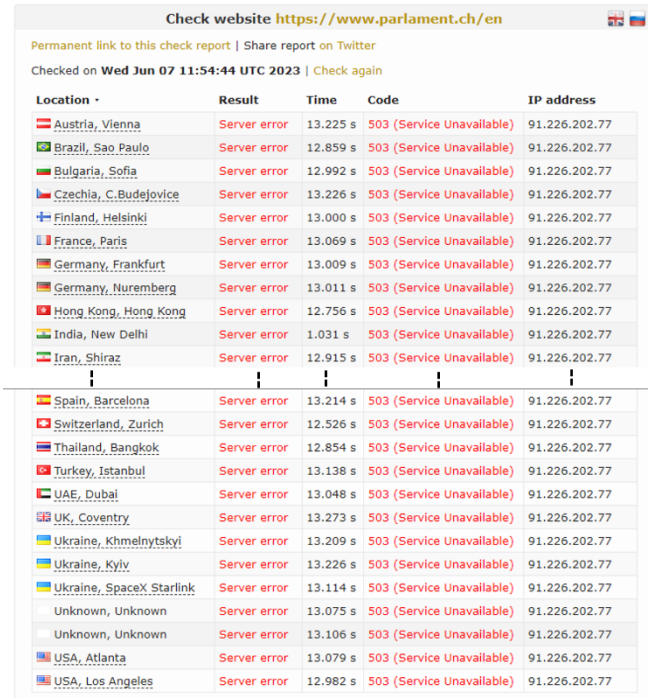


Fig. 2: Capture d'écran d'un examen de l'accessibilité.

Le 7 juin 2023, le groupe prorusse NoName057(16) a perpétré une attaque DDoS contre le site Internet du Parlement suisse. Dans un communiqué de revendication transmis par le service de messagerie instantanée Telegram, il a justifié son acte en invoquant une décision (intermédiaire) du Conseil des États concernant la révision de la loi fédérale sur le matériel de guerre. Le nombre exceptionnellement élevé de requêtes a effectivement saturé le site dès le lancement de l'attaque, jusqu'à la prise de contre-mesures. Pour les usagers normaux, le site était soit inaccessible ou réagissait avec une extrême lenteur. C'est à ce moment-là que les pirates ont fait générer un rapport automatique par un service permettant de vérifier l'accessibilité des sites web au niveau mondial, afin de prouver le succès de l'attaque. Ce rapport ne représente qu'un certain instant, qui n'en dit rien sur la durée de la perturbation. Bien que

l'attaque se soit poursuivie, les contre-mesures prises ont permis de rendre le site à nouveau utilisable dans un délai bref. Dans le scénario évoqué auparavant, cela correspondrait à une courte vidéo de la conférence de presse qui montrerait les perturbateurs en plein acte et qui se terminerait avant que le service de sécurité les expulse de la salle et les empêche d'y revenir.

La semaine suivante, des groupes prorusses se sont attaqués notamment aussi à des aéroports, aux CFF, à la Poste, à l'Association suisse des banquiers, à de nombreux cantons et villes et à plusieurs sites Internet d'offices fédéraux[5]. La Suisse est devenue la cible des hacktivistes principalement car le président de l'Ukraine devait s'exprimer devant l'Assemblée fédérale. La transmission en vidéo du discours n'a cependant pas été perturbée. Tout comme dans le cas d'autres pays qui ont été visés par NoName057(16), les attaques ont cessé après une semaine et les hacktivistes se sont tournés vers d'autres cibles[6]. Le NCSC a élaboré un rapport d'analyse détaillé séparé sur ces attaques.

Outre NoName057(16), le groupe d'hacktivistes prorusse KillNet[7] et le groupe Anonymous Sudan[8], lequel semble être associé au second, ont fait parler d'eux suite à des attaques DDoS contre des cibles se trouvant avant tout en Europe et en Amérique du Nord[9]. Il y a aussi eu des attaques DDoS religieusement motivées, par lesquelles des auteurs ont manifesté leur colère face à des activités qu'ils considéraient comme blasphématoires. Ils ont donc attaqué des sites Internet de pays ou d'organisations qu'ils perçoivent comme ennemis de leur religion[10].

En décembre 2010, la Suisse avait déjà été confrontée à une attaque DDoS politiquement motivée, lors de laquelle des partisans présumés de Wikileaks avaient perturbé le fonctionnement du site Internet de PostFinance pendant des heures[11].

Recommandations:

Le site Internet du NCSC propose dans sa rubrique Attaque affectant la disponibilité (attaque DDoS) (ncsc.admin.ch) diverses mesures de prévention et de défense contre de telles attaques.

Pour les systèmes critiques, il peut être utile de s'abonner à une protection DDoS commerciale (solution de mitigation ou de protection DDoS). De nombreux fournisseurs Internet offrent de tels services.

---

5 Das Gespenst DDoS-Attacke geht um (inside-it.ch)

6 Following NoName057(16) DDoSia Project's Targets (sekoia.io);
DDoSia Project: How NoName057(16) is trying to improve the efficiency of DDoS attacks (avast.io)

7 KillNet Showcases New Capabilities While Repeating Older Tactics (mandiant.com)

8 Microsoft Response to Layer 7 Distributed Denial of Service (DDoS) Attacks (microsoft.com)

9 Le CyberPeace Institute présente sur sa plateforme une vue d'ensemble détaillée des cyberattaques perpétrées dans le cadre du conflit ukrainien. Les attaques peuvent être filtrées selon différents critères (par ex. selon l'Event Type DDoS): Timeline of Cyberattacks and Operations (cyberpeaceinstitute.org).

10 Hacktivists Target Denmark in Ddos Attacks (truesec.com);
Radware Report Ranks Top 15 Most Active Political and Religious Hacktivists (radware.com);
Notable DDoS Attack Tools and Services Supporting Hacktivist Operations in 2023 (cyble.com)

11 Voir Rapport semestriel 2010/2 (ncsc.admin.ch), chap. 3.2.

2.1.1 Les attaques DDoS peuvent être déjouées (Swisscom)

Contribution de Stefan Kuch, Product Owner CSIRT, Swisscom

Le 7 juin 2023, le Parlement suisse a été la cible d'une attaque DDoS. Dès cet instant, l'équipe de cyberdéfense de Swisscom a été en étroit contact avec le NCSC et l'équipe d'exploitation du réseau compétente pour la protection contre les attaques DDoS. L'activation des dispositifs de protection préventive a constitué la première mesure d'urgence.

La semaine suivante, le groupe de hacktivistes prorusse NoName057(16) a de nouveau attaqué diverses cibles en Suisse. Il s'en est notamment pris, le 15 juin, à des clients de Swisscom et à Swisscom-même. À titre d'exemple, nous nous penchons ici plus particulièrement sur une attaque contre le site Internet de l'un de nos clients. Il s'agissait en l'espèce d'une attaque DDoS de couche 7, plus précisément d'une attaque inondation HTTPS (*HTTPS flood*). Dans ce type d'attaque DDoS, des requêtes HTTP GET et HTTP POST d'apparence légitime et changeant constamment déferlent sur le serveur web jusqu'à ce que les ressources soient épuisées et que le serveur ne puisse plus répondre aux requêtes. Cela mène le serveur web à refuser son service (*denial of service*) et tomber en panne. Dans le cas de NoName057(16), ces requêtes provenaient principalement d'«activistes» qui mettent sciemment leur infrastructure à disposition pour des attaques DDoS. Une telle attaque de couche 7 est en général très dynamique et, de ce fait, une prévention complète n'est guère possible. Il est cependant important de disposer d'une infrastructure technique prête à entrer en action pour réagir en cas d'attaque.

L'attaque décrite ici a atteint un volume de 150 000 paquets par seconde (pps), ce qui est beaucoup trop pour le serveur web. En temps normal, le trafic oscille entre 400 et 500 pps, avec des pointes à 1200 pps. En outre, en cas d'attaques intenses, d'autres composants réseau placés en amont du serveur web attaqué peuvent également être affectés..

En guise de contre-mesure, Swisscom a activé un système de mitigation des DDoS et a affiné et adapté en continu les règles correspondantes en collaboration avec le client:

- Le trafic issu des pays dont provenait la plus grande partie des requêtes DDoS a été bloqué (*geofiltering*). Il s'agit de la mesure immédiate la plus simple pour protéger un site Internet auquel la plupart des visiteurs accèdent normalement depuis la Suisse.
- Ensuite, nous avons procédé à une ouverture resp. une adaptation progressive: nous avons autorisé la connexion depuis des plages d'adresses IP et des pays déterminés depuis lesquels le client souhaitait que l'accès soit possible.
- Une limitation de débit (*rate limiting*) a été implémentée sur l'équilibreur de charge connecté en amont pour les connexions au domaine attaqué, ce qui a permis de décharger durablement le serveur web.
- Certaines requêtes de couche 7 ont été bloquées de manière permanente sur le reverse proxy connecté en amont. Nous avons utilisé à cette fin une liste noire établie par le NCSC.

La solution de mitigation DDoS a permis de ramener le volume à environ 500 pps. À cet effet, des requêtes d'environ 2000 adresses IP ont été bloquées. Notons que l'adresse IP la plus active a envoyé une cinquantaine de millions de paquets de données au total sur toute la durée de l'attaque.

En plus de l'attaque du 15 juin décrite ci-dessus, une autre attaque a eu lieu dans la nuit du 18 au 19 juin, mais son volume était sensiblement plus faible (60 000 pps). Comme la mitigation DDoS avait été, à titre préventif, mise en place pour cinq jours, cette attaque n'a toutefois pas eu d'effet négatif.

Après les multiples attaques DDoS de ce mois de juin, quiconque continue à exploiter son service web sans prévoir de mesures de protection efficaces en se contentant de croiser les doigts devrait reconsidérer son attitude. Des mesures de prévention professionnelles contribuent à éviter ou à réduire les dommages possibles en cas d'attaque. La plupart des fournisseurs Internet proposent des services de protection DDoS et peuvent aider leurs clients à se préparer et à se défendre en cas d'attaque.

Grâce à la bonne collaboration entre les différents secteurs opérationnels de Swisscom, comme le réseau et la gestion des incidents majeurs, ainsi qu'au soutien professionnel et à la mise à disposition d'informations par le NCSC, une réaction très rapide aux attaques a été possible et les services de nos clients ont pu être protégés

2.1.2 La préparation et l'entraînement portent leurs fruits (La Poste Suisse)

Contribution du Computer Emergency Response Team, La Poste Suisse (CERT-Post)

La gestion des attaques DDoS fait, depuis de nombreuses années, partie des scénarios prédéfinis de la gestion de crise de la Poste dans le domaine des technologies de l'information. Tandis que l'intensité des attaques DDoS tend à s'accroître, nous renforçons nos capacités de défense, ce renforcement pouvant être consécutif à des attaques ou découler de contrôles réguliers du fonctionnement. Nous vérifions non seulement les performances et configurations techniques, mais nous entraînons aussi régulièrement l'interaction entre les équipes impliquées.

Conséquences de l'attaque de NoName057(16)

La semaine après les premières attaques visant le site du Parlement suisse, une attaque DDoS a été menée le 12 juin 2023 contre des organisations et des entreprises suisses, dont deux applications web de la Poste (portail et login client).

Le service Always-on DDoS Protection que nous fournit notre prestataire de services Internet a filtré peu de trafic d'attaque au début de l'incident, mais nous a alarmés à 8 h 09, avant même que les premiers clients nous signalent des baisses de performance.

Comme les effets de l'attaque étaient mesurables, le Security Operations Center (SOC) de la Poste a activé à 8 h 11 les premiers géofiltres pour les applications web en question, sachant que les auteurs disposaient manifestement d'un réseau zombie (*botnet*) international pour l'exécution des attaques. Nous voulions en premier lieu garantir autant que possible à nos clients l'accès depuis la Suisse. Du fait de ses propriétés (inondation HTTPS avec une bande passante et un volume de paquets relativement modestes), l'attaque n'a pas eu d'autres effets sur la connexion au réseau et sur les autres services de la Poste.

À 8 h 15, le Computer Emergency Response Team (CERT-Post) a pris en charge la coordination de l'incident en collaboration avec le SOC et l'état-major de crise informatique. Pendant les heures et jours suivants, l'équipe a envoyé plusieurs rapports de situation afin que toutes les parties prenantes soient informées des derniers développements. À 8 h 31, le SOC a activé un niveau de défense, afin de pouvoir mieux filtrer le trafic lié à l'attaque dans le Mitigation

Center DDoS prévu à cet effet. Par la suite, l'équipe a procédé, avec ses partenaires externes et internes, au dépouillement des fichiers journaux et à des analyses de renseignement sur les menaces afin d'en savoir autant que possible sur les capacités et les outils des attaquants. Les résultats ont été intégrés dans la défense.

Enseignements tirés de la première vague d'attaques

D'autres attaques ont eu lieu les jours suivants: le 15 juin, le portail de CarPostal SA a été attaqué et, le 17 juin, le portail de la Poste a subi une deuxième vague d'attaques. Lors de ces attaques, nous avons pu bénéficier des enseignements tirés de la première vague et des échanges avec la communauté suisse des CERT: des mesures d'urgence telles que celles qui avaient été prises au début de la première vague n'ont plus été nécessaires. Nous avons sans cesse intégré les connaissances acquises dans notre technique de défense, ce qui nous a permis de repousser avec succès les nouvelles vagues d'attaques.

Alors que, dans la première phase des attaques du 12 juin, le temps de réponse moyen des serveurs attaqués avait augmenté de manière mesurable et nette, un tel effet n'a pas été observé les jours suivants.

Notre préparation régulière et systématique aux attaques DDoS, effectuée depuis des années, a porté ses fruits, même si chaque nouvelle vague d'attaques apporte de nouveaux enseignements. Lors du débriefing, nous avons retenu divers points techniques et organisationnels pour optimiser notre défense.

2.2 Défiguration

La défiguration (*defacement*) désigne la modification d'un site Internet par une cyberattaque. Elle peut être comparée, dans le monde réel, aux graffitis sur la façade d'un immeuble ou sur un mur. Le plus souvent, seule la page d'accueil subit des modifications visuelles, qui visent à diffuser un message politique ou idéologique. Par exemple, le site Internet d'un gouvernement ou d'un mouvement politique est défiguré parce que l'attaquant est en désaccord avec les activités ou objectifs de ces entités[12]. Le contenu du site est remplacé par du texte, une image ou un logo. Les attaques par défiguration restreignent temporairement la disponibilité d'un site et peuvent porter atteinte à la réputation de son exploitant.

Dans le contexte de la guerre en Ukraine, le logo de l'organisation paramilitaire russe Wagner et une prise de position en sa faveur ont été affichés, suite à des attaques par défiguration, sur différents sites Internet russes fin juin 2023, quelques jours après le soulèvement de ce groupe[13]. Les tensions politiques se sont transposées également sur le cyberespace des pays qui assurent leur soutien à l'Ukraine, en particulier ceux qui sont membres de l'OTAN. Ainsi, en mai 2023, un collectif du nom d'UserSec a annoncé vouloir mener, en collaboration avec d'autres groupes d'hacktivistes, une large offensive de défiguration contre les sites Internet

---

12 Par exemple, plusieurs sites Internet de petites entreprises ont été défigurés en Suisse en 2017, après la manifestation contre le gouvernement turc organisée à Berne, lors de laquelle une banderole portant l'inscription «Kill Erdogan with his own weapons!» a été déployée, ce qui a déclenché un incident diplomatique.

13 L'année précédente, le site Internet du groupe Wagner avait lui-même été victime d'une défiguration: des cyberacteurs pro-ukrainiens y avaient publié des photographies de victimes de la guerre et une prise de position de soutien à l'Ukraine.

des États membres de l'OTAN. Ces menaces n'ont cependant pas été suivies d'attaques fructueuses qui auraient fait leur apparition dans les médias.

Recommandations:

Faites surveiller automatiquement votre site Internet afin d'être alerté s'il est modifié. Vous pourrez ainsi réagir rapidement et supprimer les éventuelles manipulations non autorisées. Renseignez-vous auprès de votre hébergeur sur les possibilités existantes.

2.3 Piratage et divulgation

Dans une opération de piratage et divulgation (*hack and leak*), des hacktivistes pénètrent dans des systèmes informatiques pour y soustraire des données et, ensuite, les publier. Ils cherchent en particulier du matériel compromettant, qu'ils publieront, sous sa forme originale ou sous une forme falsifiée, sur des plateformes telles que Wikileaks ou DDoSecrets, sur des réseaux sociaux ou sur des sites du darkweb, en vue d'obtenir un impact médiatique. Il arrive aussi, selon l'idéologie suivi ou les données volées, que les hacktivistes transmettent les informations à des journalistes d'investigation en vue d'une analyse détaillée et ne les publient pas eux-mêmes.

Le cas d'une pirate suisse a suscité un grand intérêt médiatique au début de 2023. Elle est parvenue à dérober une liste de personnes interdites de vols aux États-Unis datant de l'année 2019 et comprenant quelque 1,5 million d'entrées, sur un serveur d'une compagnie aérienne dont la sécurité était défaillante[14]. Dans un autre cas, des personnes associées au collectif de pirates Anonymous ont publié des données du fournisseur Internet russe Convex censées prouver une surveillance étatique illégale en Russie[15]. Les hacktivistes recourant au rançongiciel *MalasLocker* optent pour un autre modèle. À l'instar des groupes faisant traditionnellement usage de rançongiciels (voir chap. 4.2), ils se procurent une copie des données des systèmes de leurs victimes avant de lancer un rançongiciel. Cependant, ils ne demandent pas de rançon à proprement parler, mais exigent de la victime qu'elle fasse un don à une organisation de bienfaisance en échange de la clé de déchiffrement des données et de la non-publication des données copiées[16].

2.4 Sabotage

Les tentatives de sabotage de systèmes de production constituent sans doute la méthode la plus dangereuse qu'utilisent les hacktivistes pour attirer l'attention sur leurs revendications. Bien que, dans la plupart des cas, les effets réels de leurs actes soient moins importants que prétendu, il faut prêter attention à ce type de menace[17].

---

14 Voir EXCLUSIVE: Leaked TSA No Fly List: File Found on Airline Server (dailydot.com); Schweizer Hackerin stellt USA bloss: Geheime Flugverbots-Liste erbeutet (watson.ch).

15 128GB Of Russian ISP Convex Data Leaked By Anonymous Hacker (informationsecuritybuzz.com)

16 MalasLocker ransomware targets Zimbra servers, demands charity donation (bleepingcomputer.com); Dark Web Profile: MalasLocker Ransomware (socradar.io)

17 We (Did!) Start the Fire: Hacktivists Increasingly Claim Targeting of OT Systems (mandiant.com)

Il convient de citer à cet égard le groupe GhostSec[18], qui est issu du milieu de l'hacktivisme classique d'Anonymous. En janvier 2023, il a annoncé avoir utilisé contre la Biélorussie leur premier rançongiciel spécifiquement destiné aux systèmes de technologie opérationnelle (OT). Le système attaqué reposait sur une plateforme Linux dont la version avait déjà été compromise antérieurement par des rançongiciels. L'attaque a certes eu des effets sur l'exploitation, mais elle ne visait pas directement le processus physique commandé[19].

Les hacktivistes qui ont des intentions de sabotage opèrent le plus souvent dans le contexte de conflits géopolitiques. Par exemple, dans le cadre de la guerre d'agression russe contre l'Ukraine, le groupe OneFist[20] s'est constitué. Il a revendiqué plusieurs incidents ayant eu des conséquences physiques, principalement en Russie[21]. D'autres groupes sont actifs depuis un certain temps, comme c'est le cas de Predatory Sparrow[22] qui est actif dans le contexte des conflits du Moyen-Orient et qui a par exemple revendiqué des dommages physiques à des aciéries iraniennes[23].

Les capacités des hacktivistes se limitent le plus souvent à la manipulation de systèmes de commande non protégés accessibles depuis Internet et à l'utilisation d'outils d'attaque librement accessibles, tels que les modules Metasploit[24].

Il est parfois supposé que, pour des attaques d'une certaine complexité, les groupes d'hacktivistes bénéficient d'une assistance étatique dissimulée. Ainsi, il a été question de possibles liens entre le service russe de renseignement militaire et des groupes d'hacktivistes pro-russes[25]. Il a même été évoqué que, pour les forces de sécurité iraniennes aient été derrière les présumés hacktivistes de Homeland Justice dans le sabotage des systèmes du gouvernement albanais[26]. Récemment, des chercheurs en sécurité ont montré des activités ukrainiennes étaient à l'origine d'une attaque visant un opérateur de satellites russe[27] perpétrée par de prétendus hacktivistes appartenant au groupe Wagner.

Les tentatives de sabotage fructueuses suscitent une attention accrue. Il faut donc s'attendre à ce que d'autres groupes de hacktivistes tentent à l'avenir d'acquérir de telles capacités. Le NCSC britannique met même explicitement en garde contre les intentions destructrices des hacktivistes pro-russes à l'encontre des infrastructures critiques occidentales[28]. Ces derniers pourraient acquérir les compétences nécessaires en étant alimentés par des organisations gouvernementales ou par l'environnement de cybercriminels expérimentés.

---

18 Ghost Security (wikipedia.org)

19 Hacker group discloses ability to encrypt an RTU device using ransomware, industry reacts (industrialcyber.co)

20 About Us | Cyber Security (onefist.org)

21 Meet the hacker armies on Ukraine's cyber front line (bbc.com)

22 Predatory Sparrow (Threat Actor) (fraunhofer.de)

23 Predatory Sparrow massively disrupts steel factories while keeping workers safe (malwarebytes.com)

24 Metasploit | Penetration Testing Software, Pen Testing Security (metasploit.com) – Metasploit Framework est un outil permettant aux responsables de la sécurité de trouver et d'examiner les vulnérabilités de systèmes informatiques. Comme tout outil, il peut être détourné pour des usages malveillants.

25 GRU: Rise of the (Telegram) MinIOns (mandiant.com)

26 Microsoft investigates Iranian attacks against the Albanian government (microsoft.com)

27 Hackers claim to take down Russian satellite communications provider (therecord.media)

28 NCSC warns of emerging threat to critical national infrastructure (ncsc.gov.uk)

Conclusion et recommandation:

La norme minimale pour les TIC et les normes minimales par secteur élaborées par l'Office fédéral pour l'approvisionnement économique du pays (OFAE) en collaboration avec les associations économiques ont valeur de recommandations et fournissent d'utiles points de repère aux entreprises pour se prémunir de manière adéquate également contre les activités des hacktivistes.

3 Annonces émanant d'entreprises ou de particuliers

3.1 Aperçu des annonces de cyberincidents reçues

Annonces au NCSC au premier semestre 2023 (par semaine)

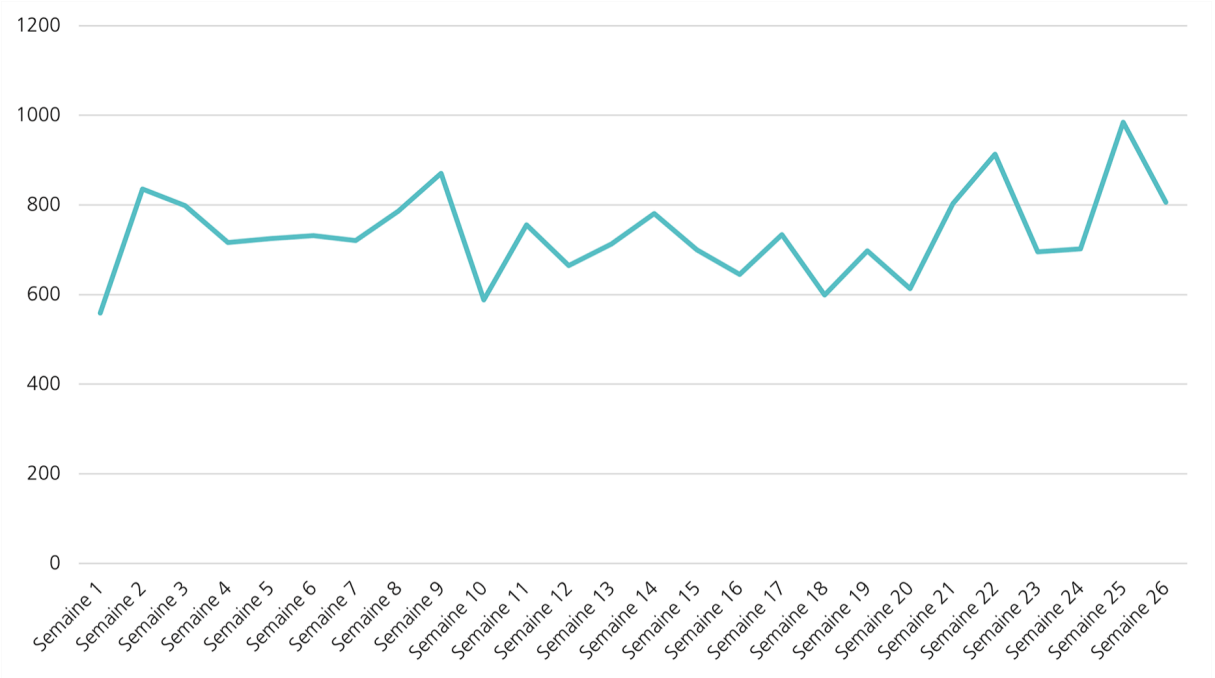


Fig. 3: Nombre d'annonces parvenues au NCSC de janvier à juin 2023, voir aussi Chiffres actuels (ncsc.admin.ch).

Annonces au NCSC au premier semestre 2023 (par catégorie)

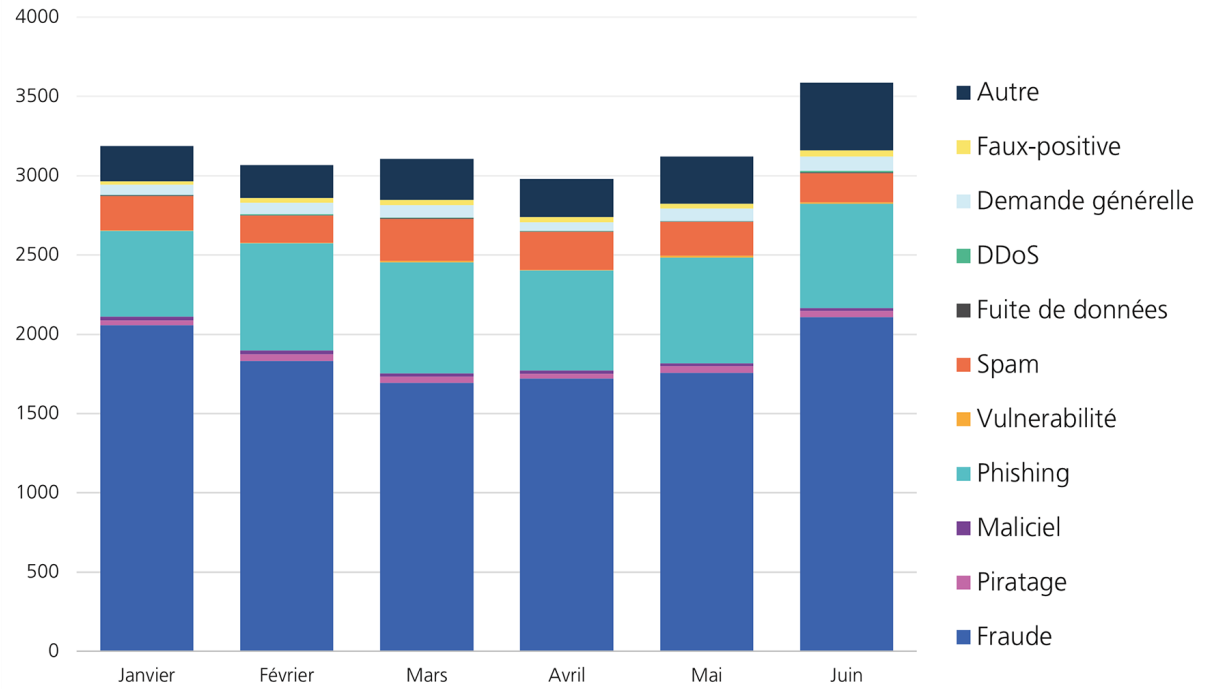


Fig. 4: Annonces effectuées au NCSC au premier semestre 2023, par catégorie, voir aussi Chiffres actuels (ncsc.admin.ch).

Le NCSC a reçu 19 048 annonces de cyberincidents durant le premier semestre 2023, soit environ 2000 de plus qu'au semestre précédent (16 951) et qu'au premier semestre de l'année précédente (16 844). La hausse est donc plus modérée que l'année passée. La part des courriels de menace prétendument expédiés par des autorités (5511) et celle des usurpations de numéros de téléphone *(spoofing*; 543) demeurent pratiquement inchangées c'est-à-dire, comme au semestre précédent, à un niveau élevé. La part des annonces de fraudes (11 168) est en léger recul, passant de 62 à 59 % du total des annonces reçues. En revanche, le nombre d'annonces relatives à des tentatives d'hameçonnage a fortement augmenté par rapport au semestre précédent (près de 1700 annonces supplémentaires), soit un total de 3875 annonces. Cette hausse tient principalement à une vague d'hameçonnage visant les clients SwissPass, qui a sévi pendant tout le premier semestre. Le nombre d'annonces à ce sujet avoisine le millier et a presque décuplé par rapport au semestre précédent.

Fig. 5: Exemple de tentative d'hameçonnage basée sur le prétendu remboursement d'un billet des CFF.

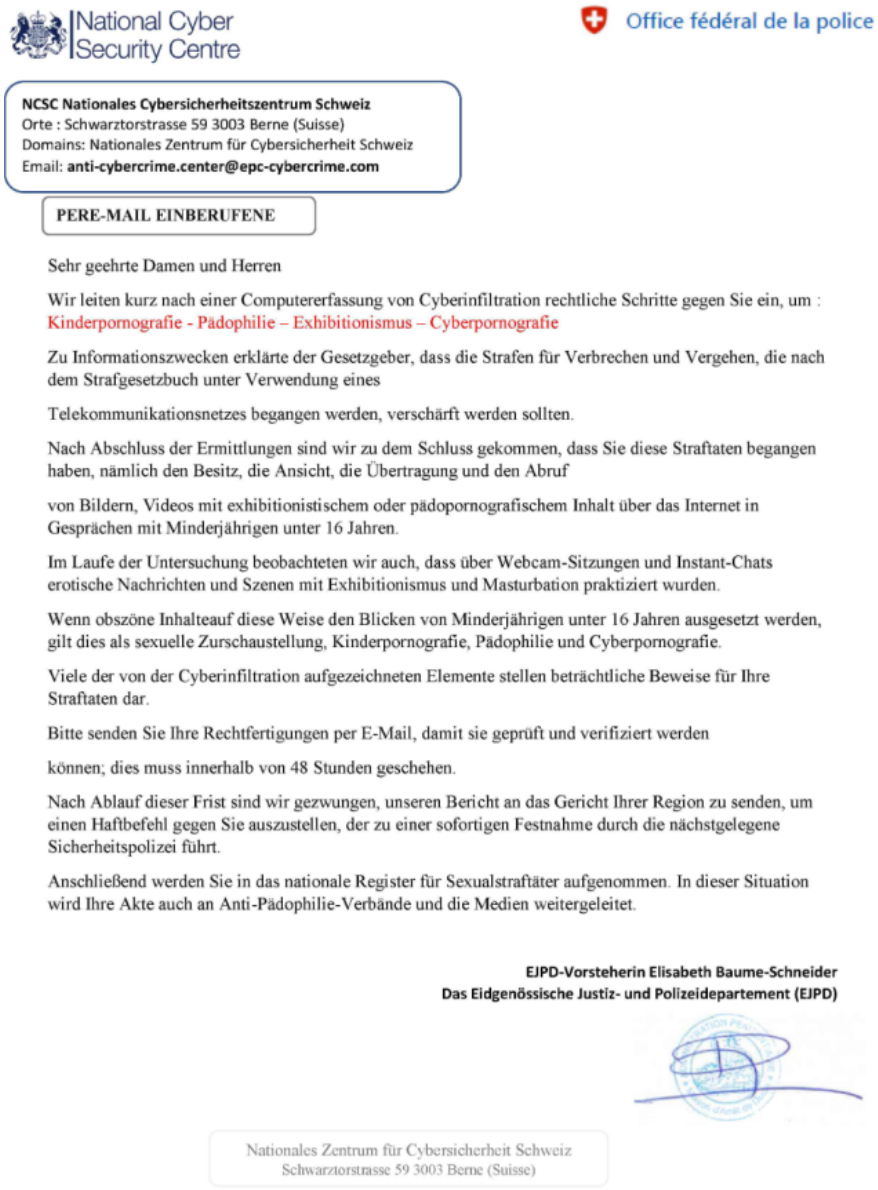
Le nombre de signalements concernant des tentatives d'hameçonnage en lien avec des petites annonces a également augmenté. Dans ce genre de cas, des frais d'une nature quelconque sont exigés lors d'une vente ou alors il s'agit de confirmer une opération. Le but est d'inciter le vendeur à fournir les données de sa carte de crédit. L'hameçonnage par SMS *(smishing)* a également légèrement augmenté et les tentatives qui concernent les fausses alertes de livraison de colis sont restées stables, représentant 600 annonces, soit 15 % des annonces d'hameçonnage.

Le rapport entre les annonces émanant de la population (86 %) et celles qui proviennent d'entreprises, d'associations ou d'autorités est resté stable. En ce qui concerne les annonces typiques des entreprises, tant le nombre d'arnaques au président (116 annonces) que celui des fraudes à la facturation (36) connaissent un léger recul, alors que les attaques par rançongiciel (56) et les attaques affectant la disponibilité (DDoS; 24) ont augmenté. Les entreprises annoncent le plus souvent des courriels de menace émanant prétendument d'une autorité (fausse extorsion; 346). Cette catégorie comprend aussi de nombreuses tentatives de chantage contre des administrateurs de sites Internet: les auteurs attirent leur attention sur une prétendue vulnérabilité du site Internet et affirment qu'il y a eu une fuite de données. Les entreprises annoncent également régulièrement des tentatives d'hameçonnage, qui visent avant tout à mettre la main sur des données de connexion aux comptes Office 365.

3.2 L’escroquerie, l’incident le plus courant

3.2.1 Courriels de menace toujours nombreux

30 % des annonces reçues concernent toujours les courriels de menace émanant prétendument d’une autorité (fausse extorsion*)*. Dans la grande majorité des cas, le destinataire est accusé d’avoir commis une infraction pénale. Ces menaces sont envoyées au nom d’une autorité suisse ou étrangère. Au cours du semestre sous revue, le nom du NCSC suisse a été de plus en plus souvent utilisé de manière frauduleuse, mais de manière erronée en combinaison avec le logo de son homologue britannique. Ces faux portaient généralement la signature falsifiée de la directrice de l’Office fédéral de la police, Nicoletta della Valle, d’un conseiller fédéral ou d’une conseillère fédérale. Les escrocs semblent s’intéresser à la politique suisse puisque, six jours après l’entrée en fonction de la conseillère fédérale Élisabeth Baume-Schneider, des courriels falsifiés portant son nom ont fait leur apparition.



National Cyber Security Centre

Office fédéral de la police

NCSC Nationales Cybersicherheitszentrum Schweiz
Orte : Schwarztorstrasse 59 3003 Berne (Suisse)
Domains: Nationales Zentrum für Cybersicherheit Schweiz
Email: **anti-cybercrime.center@epc-cybercrime.com**

PERE-MAIL EINBERUFENE

Sehr geehrte Damen und Herren

Wir leiten kurz nach einer Computererfassung von Cyberinfiltration rechtliche Schritte gegen Sie ein, um : Kinderpornografie - Pädophilie – Exhibitionismus – Cyberpornografie

Zu Informationszwecken erklärte der Gesetzgeber, dass die Strafen für Verbrechen und Vergehen, die nach dem Strafgesetzbuch unter Verwendung eines

Telekommunikationsnetzes begangen werden, verschärft werden sollten.

Nach Abschluss der Ermittlungen sind wir zu dem Schluss gekommen, dass Sie diese Straftaten begangen haben, nämlich den Besitz, die Ansicht, die Übertragung und den Abruf

von Bildern, Videos mit exhibitionistischem oder pädopornografischem Inhalt über das Internet in Gesprächen mit Minderjährigen unter 16 Jahren.

Im Laufe der Untersuchung beobachteten wir auch, dass über Webcam-Sitzungen und Instant-Chats erotische Nachrichten und Szenen mit Exhibitionismus und Masturbation praktiziert wurden.

Wenn obszöne Inhalteauf diese Weise den Blicken von Minderjährigen unter 16 Jahren ausgesetzt werden, gilt dies als sexuelle Zurschaustellung, Kinderpornografie, Pädophilie und Cyberpornografie.

Viele der von der Cyberinfiltration aufgezeichneten Elemente stellen beträchtliche Beweise für Ihre Straftaten dar.

Bitte senden Sie Ihre Rechtfertigungen per E-Mail, damit sie geprüft und verifiziert werden

können; dies muss innerhalb von 48 Stunden geschehen.

Nach Ablauf dieser Frist sind wir gezwungen, unseren Bericht an das Gericht Ihrer Region zu senden, um einen Haftbefehl gegen Sie auszustellen, der zu einer sofortigen Festnahme durch die nächstgelegene Sicherheitspolizei führt.

Anschließend werden Sie in das nationale Register für Sexualstraftäter aufgenommen. In dieser Situation wird Ihre Akte auch an Anti-Pädophilie-Verbände und die Medien weitergeleitet.

EJPD-Vorsteherin Elisabeth Baume-Schneider
Das Eidgenössische Justiz- und Polizeidepartement (EJPD)

Nationales Zentrum für Cybersicherheit Schweiz
Schwarztorstrasse 59 3003 Berne (Suisse)

Fig. 6: Courriel de fausse extorsion au nom du NCSC avec le logo de son homologue britannique, prétendument signé par la conseillère fédérale Élisabeth Baume-Schneider. Le courriel a été annoncé au NCSC le 6 janvier 2023, soit peu après l’entrée en fonction de la nouvelle conseillère fédérale.

3.2.2 Autres phénomènes relevant de l'escroquerie

Le NCSC continue à recevoir de nombreuses annonces relatives à des fraudes au paiement anticipé (1660). Aux messages classiques, qui font miroiter un héritage ou un coffre d'or sans propriétaire, sont désormais venues s'ajouter des variantes modernes. Le destinataire reçoit par courriel un nom d'utilisateur et un mot de passe qui lui permettent de voir, en cliquant sur le lien indiqué, une importante somme en cryptomonnaie qui se trouve sur «son» compte. Le montant promise lui sera versé, s'il s'acquitte régulièrement des frais, qui se renouvellent et augmentent toujours, cependant le paiement n'intervient évidemment jamais.

Les signalements de cas de *fake sextortion*, (fausse sextorsion), d'abonnement piège et de fraude aux petites annonces sont restés aussi fréquents qu'au semestre précédent. Concernant les petites annonces, le phénomène de l'arnaque s'est transformée en hameçonnage, en ce que lors du processus de paiement, un lien d'hameçonnage est envoyé à la victime.

Le NCSC a enregistré 245 annonces concernant de la fraude à l'investissement en ligne. C'est un peu plus qu'au semestre précédent, au cours duquel il en avait reçu 219. Cependant, le montant total des dommages indiqués a plus que doublé et a atteint 9,5 millions de francs. Les ressources en personnel engagées par les escrocs semblent considérables. En effet, ils répondent rapidement et personnellement aux victimes potentielles. Outre la prise de contact "personnelle" avec les futures victimes par le biais de divers canaux de médias sociaux, où la confiance est établie sur une longue période, les sites web mis en place pour l'escroquerie en ligne offrent, par exemple, une assistance 7j/7 et 24h/24 par chat ou téléphone. Ils proposent également des vidéos de formation qui expliquent le fonctionnement de la fausse plateforme d'investissement.

Une fois de plus, la rapidité avec laquelle les escrocs réagissent aux actualités a pu être observée. Par exemple, pour le lancement de la fusée Starship, une fausse action «give away» a été lancée avec une fausse vidéo (*deepfake)* d'Elon Musk[29].

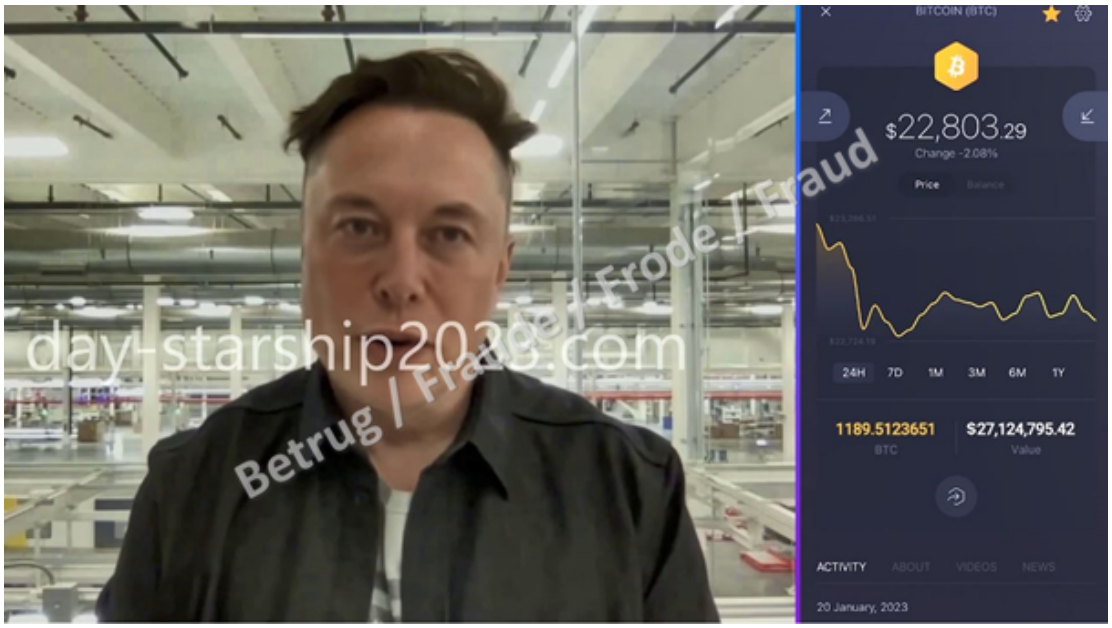


Fig. 7: Vidéo truquée d'Elon Musk, dans laquelle ses traits et sa voix sont imités.

29 Semaine 17: vidéo de promotion truquée pour une fausse action «give away» (ncsc.admin.ch)

3.3 Annonces d'hameçonnage

Avec une augmentation d'annonces de 40%, l'hameçonnage constitue le deuxième cyberincident le plus signalé et représente ainsi un cinquième des annonces reçues au cours du semestre sous revue.

De manière générale, le NCSC constate que les tentatives d'hameçonnage sont de plus en plus sophistiquées et que les attaquants testent de nouvelles méthodes pour dissimuler les liens malicieux.

L'envoi de messages d'hameçonnage par SMS (*smishing*) a été assez fréquemment observé. Il s'agissait notamment de fausses alertes de livraison de colis. Le destinataire reçoit apparemment un avis de la Poste, de DHL, de DPD ou de Fedex l'informant qu'un colis ne peut pas être délivré parce que des indications manquent ou que des frais n'ont pas été réglés. La page d'hameçonnage est conçue de façon à ne s'afficher qu'en cas de consultation à partir d'un téléphone mobile (par ex. un navigateur Chrome sur un système d'exploitation Android). En revanche, le destinataire qui la consulte à partir d'un ordinateur est automatiquement redirigé vers le bon site (par ex. celui de la Poste). Les escrocs tentent ainsi de faire croire aux autorités de sécurité que le message et le lien contenu ne sont pas frauduleux et qu'il n'y a pas lieu de prendre de mesures. Les annonces relatives à des tentatives d'hameçonnage au moyen de codes QR restent plutôt rares.

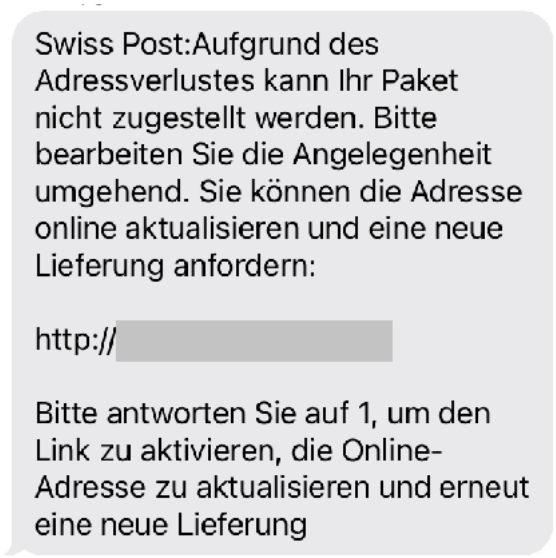


Fig. 8: Tentative typique d'hameçonnage par SMS avec une fausse notification relative à un colis au nom de la Poste suisse. Après avoir cliqué sur le lien, le destinataire sera invité à saisir les données de sa carte de crédit.

En outre, une vague d'hameçonnage par téléphone (*voice phishing,* en abrégé *vishing)* a été observée. Les auteurs se sont fait passer pour des collaborateurs d'une entreprise de télécommunication et ont essayé, par divers moyens, d'obtenir le code de sécurité envoyé par SMS dans le cadre d'une authentification multifactorielle. Ils ont ensuite acheté des cartes Paysafe dans les boutiques en ligne de l'entreprise de télécommunication[30].

Au cours du premier trimestre 2023, des tentatives d'hameçonnage en temps réel de comptes Office 365 ont été fréquemment et avant tout annoncées par des entreprises. Souvent, ces

[30] Semaine 5: hameçonnage sophistiqué par téléphone (ncsc.admin.ch)

hameçonnages recouraient à un document HTML joint au courriel. La page d'hameçonnage ouverte en local sur le navigateur affichait même les logos exacts des entreprises, lesquels étaient téléchargés en arrière-plan de façon dynamique par des scripts à partir du véritable site Internet de l'entreprise. Dès qu'une victime saisissait son nom d'utilisateur et son mot de passe sur une page d'hameçonnage, il convenait d'intercepter le code de sécurité de l'authentification multifactorielle, dont la durée de validité est limitée. Afin de gagner du temps sur les activités ultérieures en arrière-plan, les pirates simulaient un dysfonctionnement temporaire du réseau après la connexion de la victime[31].

Nombre de sites d'hameçonnage signalés par semaine

Fig. 9: Nombre d'adresses URL d'hameçonnage examinées et confirmées par le NCSC chaque semaine, au premier semestre 2023.

3.4 Annonces de maliciels et de piratages

3.4.1 Incidents dus à des rançongiciels: Évolution contraire entre les entreprises et les particuliers

Au premier semestre 2023, 124 annonces portant sur des maliciels ont été enregistrées, soit à nouveau moins que le semestre précédent (155). Comme lors du semestre précédent, il n'y a pas eu de grandes vagues d'envois de maliciels par courriel.

Bien que le nombre d'annonces concernant des rançongiciels soit passé de 76 à 64, il ne faut en aucun cas baisser sa garde. En effet, ce recul n'est pas imputable aux entreprises mais aux particuliers (passage de 27 à 8 cas). Les systèmes de stockage en réseau (NAS), particulièrement visés chez les particuliers, ne sont attaqués plus que sporadiquement[32]. En revanche, le nombre de cas annoncés par les entreprises, les administrations et les associations est passé de 49 à 56. Des entreprises importantes sont aussi visées, comme le montrent de nombreux exemples du premier semestre 2023 (voir chap. 4.2.1). Le rançongiciel *Lockbit* a

31 Semaine 6: comptes Office 365 sécurisés visés par des tentatives d'hameçonnage en temps réel (ncsc.admin.ch)

32 Voir Semaine 4: faille de sécurité sur les appareils NAS de QNAP […] (ncsc.admin.ch).

été particulièrement actif également au cours de la période sous revue. Des rançongiciels des familles *Play*, *BlackCat*, *Medusalocker*, *Phobos*, *BlackByte*, *BlackBasta*, *Babuk*, *ECh0raix* et *Akira* ont également été signalés. Étant donné que, dans de nombreux cas, la famille de rançongiciels responsable n'est pas encore connue au moment de l'annonce, le NCSC ne peut pas fournir de chiffres fiables sur ce point. Il travaille actuellement sur l'élaboration d'un formulaire qui sera envoyé aux entreprises après un incident, afin de requérir systématiquement ces informations.

3.4.2 Annonces de piratages

Les annonces relevant du piratage sont passées de 276 à 225. Près de la moitié des signalements concernent des comptes de médias sociaux. Dans cette catégorie, le nombre d'annonces (101) est resté stable par rapport au semestre précédent (108). Les escrocs se servent de comptes piratés sur les médias sociaux pour conférer davantage de poids à leur chantage lors d'attaques de fausse sextorsion. Souvent aussi, ils utilisent les comptes piratés pour promouvoir des investissements frauduleux. Ils privilégient pour de telles pratiques les comptes ayant de nombreux abonnés, afin de diffuser leurs informations sur des transactions douteuses auprès d'un maximum de victimes potentielles.

3.5 Annonces diverses

3.5.1 Optimisation du référencement dans les moteurs de recherche au moyen de domaines abandonnés et de sites piratés

L'utilisateur qui fait une recherche dans un moteur de recherche courant ne clique en général que sur les résultats de la première page. S'il n'est pas satisfait du résultat, il va probablement affiner sa recherche plutôt que se donner la peine de chercher de meilleurs résultats sur la deuxième ou la troisième page.

Les exploitants de sites Internet douteux l'ont aussi remarqué et ils tentent, en recourant à toutes les astuces imaginables, de manipuler la recherche à leur profit afin que leurs offres s'affichent sur la première page de résultats. Ce procédé augmente la probabilité que des victimes potentielles ouvrent la page piratée et qu'elles accèdent ainsi à des sites frauduleux.

Les deux modes opératoires suivants ont été annoncés au NCSC au cours du premier semestre.

Dans la première variante, des domaines non entretenus sont utilisés de façon frauduleuse. Beaucoup de propriétaires connaissent le problème: ils n'ont plus besoin de leur nom de domaine et envisagent de le résilier, puisqu'il génère des frais annuels. Or peu d'entre eux se préoccupent du fait qu'après sa résiliation, n'importe qui peut se l'approprier et l'utiliser pour le contenu de son choix. Par le passé, plusieurs anciens propriétaires de domaines ont signalé au NCSC que l'adresse de leur ancien site Internet menait désormais à des boutiques en ligne suspectes ou à des sites pour adultes. Les domaines qui disposent d'un cercle de visiteurs certes restreint mais néanmoins intéressants pour les escrocs sont particulièrement visés. Ceux-ci tirent parti de la position obtenue par le site Internet d'origine dans les moteurs de recherche. Si un mot-clé correspondant est recherché, ce n'est pas le site d'origine mais le site associé au nom de domaines des escrocs qui apparaît.

Dans une deuxième variante, les cybercriminels tentent de manipuler les résultats des moteurs de recherche en se servant de sites Internet piratés. Au début de l'année, le NCSC a constaté que, lors d'une recherche sur Google de sites Internet dont le piratage lui avait été annoncé, le titre exact s'affichait dans les résultats, mais que l'extrait du contenu du site figurant sous le titre ne correspondait pas avec celui du site Internet et qu'il comprenait divers liens dissimulés sous des combinaisons de lettres et de chiffres. Cette liste de liens douteux s'affichait aussi lors de l'ouverture du site au moyen de Google Cache (une copie du site temporairement enregistrée par Google). En revanche, l'ouverture de la page au moyen de l'URL fonctionnait correctement. Dans le cas en question, le NCSC soupçonnait que des contenus différents apparaissent à l'ouverture de la page en fonction de l'agent utilisateur (*user agent*). Ce dernier est transmis au serveur d'un site web à chaque consultation de la page et lui fournit des informations concernant le système d'exploitation et le navigateur utilisés. Ces données sont exploitées à des fins de relevés statistiques, mais elles peuvent également servir à optimiser les contenus d'une page pour un navigateur donné. Comme Google parcourt le plus souvent le web avec l'agent utilisateur "Googlebot", il est possible d'identifier ses requêtes de recherche. Cette fonction peut toutefois être détournée pour présenter à Google un contenu de site préparé. Comme ce sont toujours les mêmes liens qui s'affichent sur les différents sites piratés, Google part du principe que les sites liés sont intéressants et les juge plus pertinents qu'ils ne le sont en réalité. Ils apparaissent par conséquent plus haut dans les résultats de recherche, ce qui augmente leur visibilité. Pour tous les autres visiteurs du site piraté et ainsi aussi pour son propriétaire, le contenu normal s'affiche. Ainsi, cette manipulation passe plus inaperçue et peut générer ses effets sur une longue période.

4 Situation

4.1 Accès initial

Obtenir un accès à distance à des systèmes informatiques ou l'accès à des comptes utilisateurs constitue la première étape de la plupart des cyberattaques. Un tel accès initial peut s'obtenir de différentes manières[33] et, une fois établi, être mis à disposition d'autres acteurs pour qu'ils en tirent parti.

4.1.1 Nom d'utilisateur et mot de passe

Les identifiants de connexion s'obtiennent généralement par hameçonnage (voir chap. 3.3). Les utilisateurs sont donc trompés et transmettent leurs données d'accès à des cybercriminels. La qualité des messages d'hameçonnage augmente sans cesse, et il est de plus en plus difficile de les démasquer[34]. Les cybercriminels réagissent également aux mesures de sécurité

[33] Voir aussi Initial Access, Tactic TA0001 (mitre.org).

[34] Semaine 25: des tentatives d'hameçonnage toujours plus difficiles à démasquer (ncsc.admin.ch); voir aussi chap. 3.3.

supplémentaires et ont développé des méthodes pour attaquer aussi les comptes protégés par une authentification à deux ou plusieurs facteurs[35].

Conclusion et recommandations:

Même si les mesures de sécurité n'offrent pas une protection absolue, il vaut la peine de ne pas rendre la vie trop facile aux cybercriminels. Il est conseillé de choisir des mots de passe forts et, si possible, de protéger les comptes importants avec une authentification à deux ou plusieurs facteurs[36].

Vérifiez toujours la cible (adresse, URL) d'un lien[37]. Un logo ou une autre image ne prouvent pas l'authenticité d'un courriel ou d'un site Internet. Soyez sur vos gardes lorsque vous devez saisir des mots de passe ou d'autres informations.

4.1.2 Maliciels (chevaux de Troie)

Les chevaux de Troie, qui une fois installés créent une porte dérobée, restent une méthode courante pour obtenir un accès initial au système de la victime. L'installation n'est normalement pas automatique, mais requiert une action. Les cybercriminels recourent donc à diverses astuces pour inciter la victime à effectuer l'action nécessaire. Le code qui installe le maliciel est souvent intégré dans un autre programme ou caché d'une autre façon, si bien que l'utilisateur ne se rend pas compte de son exécution.

Il arrive très fréquemment que des maliciels soient diffusés par courriel. Le code de l'infection peut être directement contenu dans une pièce jointe ou accessible via un lien figurant dans le courriel. Le contexte du courriel incite le destinataire à exécuter le fichier contenant le code malveillant. Par exemple, le courriel fait référence à des affaires courantes, telles que des offres, des livraisons ou des factures, ou promet des informations exclusives sur des événements d'actualité. Certains cybercriminels accroissent la crédibilité du courriel contenant le maliciel en s'appuyant sur des échanges de courriels antérieurs authentiques obtenus frauduleusement auprès d'autres organisations. C'est notamment le cas pour *QakBot*, un maliciel qui débouche régulièrement, une fois l'infection initiale réalisée, sur des infections par rançongiciel[38]. Souvent, le cybercriminel crée un sentiment d'urgence pour inciter le destinataire à agir sans réfléchir. Le NCSC a exposé, dans une rétrospective hebdomadaire, un exemple concret dans lequel ces différents éléments (incitation par courriel, dissimulation de l'installation du logiciel dans un autre programme, invitation à réagir immédiatement) sont présents[39].

---

35 Semaine 6: comptes Office 365 sécurisés visés par des tentatives d'hameçonnage en temps réel (ncsc.admin.ch); Semaine 8: SMS de la part du Conseil fédéral et autres tentatives d'hameçonnage (ncsc.admin.ch); Semaine 9: courriels de menace envoyés au nom du NCSC et hameçonnage en temps réel (ncsc.admin.ch); Semaine 19: le «SIM swapping», une méthode pour voler des cartes SIM en ligne (ncsc.admin.ch)

36 E comme Equiper (s-u-p-e-r.ch); Protégez vos comptes (ncsc.admin.ch)

37 Mythe: liens (ncsc.admin.ch)

38 Semaine 24: le maliciel QakBot s'adapte pour mieux circuler (ncsc.admin.ch)

39 Semaine 18: un loup déguisé en agneau, ou lorsqu'une prétendue mise à jour cache un logiciel malveillant (ncsc.admin.ch)

Les cybercriminels peuvent aussi inciter les internautes à installer un maliciel en achetant des espaces de publicité en ligne ou en publiant des résultats de recherche sponsorisés (*malvertising*). Ces annonces font croire que le logiciel recherché peut être téléchargé via l'annonce en question. Cependant, un maliciel est installé en même temps que le logiciel souhaité (le plus souvent gratuit)[40].

Enfin, des criminels utilisent également des clés USB pour diffuser leurs maliciels. Celles-ci peuvent d'une part être développées spécialement pour une infection initiale de l'environnement visé[41]. D'autre part, des maliciels peuvent être copiés sur une clé USB lorsque celle-ci est insérée dans un ordinateur déjà infecté, pour infecter ensuite les autres systèmes auxquels la clé sera branchée. Ce mode opératoire, qui était un peu tombé dans l'oubli, est cependant toujours utilisé[42].

Conclusion et recommandations:

Ne cliquez jamais sur un lien dans un courriel suspect et n'ouvrez jamais de fichiers joints. En cas de doute, interrogez le prétendu expéditeur en utilisant un moyen de contact fiable pour savoir si le courriel émane réellement de lui.

Si vous êtes à la recherche d'un logiciel sur Internet, contrôlez avant de le télécharger que vous êtes bien sur le site du fabricant ou sur un autre site digne de confiance (par ex. revue informatique connue). La prudence s'impose chaque fois qu'une fenêtre de téléchargement s'ouvre. Veillez autant que possible à ce que les programmes se mettent à jour automatiquement. Utilisez sinon toujours la fonction de mise à jour intégrée, ou téléchargez la dernière version directement sur le site du fabricant.

Ne branchez pas à votre ordinateurs des périphériques USB inconnus ou que vous avez trouvés.

4.1.3 Exploitation des vulnérabilités

Dès qu'une vulnérabilité d'un produit est connue, différents acteurs commencent à fouiller Internet à la recherche de systèmes vulnérables. La vulnérabilité est déjà exploitée au bout de quelques heures ou de quelques jours. Certaines attaques tirent aussi profit de vulnérabilités connues de longue date et pour lesquels un correctif existe mais n'a pas encore été implémenté[43]. Parfois, les cybercriminels exploitent les failles n'ayant fait l'objet d'aucune publication ou n'ayant aucun correctif connu (failles *zero-day*)[44]. Début juin, le groupe de rançongiciel CI0p a commencé à exploiter une faille d'injection SQL alors inconnue sur le logiciel de transfert de données MOVEit Transfer. Les applications web accessibles à partir d'Internet ont été

40 Void Rabisu's Use of RomCom Backdoor Shows a Growing Shift in Threat Actors' Goals (trendmicro.com)

41 Cyberconseil: les clés USB peuvent servir de porte d'entrée pour les cyberattaques (ncsc.admin.ch)

42 Beyond the Horizon: Traveling the World on Camaro Dragon's USB Flash Drives (checkpoint.com)

43 Voir par exemple Semaine 7: systèmes VMware ESXi bloqués (ncsc.admin.ch).

44 Une faille du jour zéro est une vulnérabilité pour laquelle il n'existe pas encore de mise à jour ou de correctif permettant de la supprimer.

infectées par un code encoquillé (*web shell*)[45] permettant d'enregistrer les banques de données de MOVEit Transfer sous-jacentes[46].

Outre les erreurs de programmation des développeurs que des *patchs* de sécurité ou des mises à jour ont corrigé plus tard, la configuration choisie lors de l'installation de nouveaux produits est parfois à l'origine de vulnérabilités. Plusieurs fabricants fournissent des instructions sur la manière de configurer ou de renforcer leurs produits en toute sécurité.

Recommandations:

En cas d'utilisation de nouveaux produits, vérifiez leur configuration en matière de sécurité et de protection des données. Veillez à n'activer que les fonctionnalités dont vous avez besoin.

Tant les particuliers que les entreprises devraient maintenir constamment à jour les logiciels de tous leurs appareils, de préférence à l'aide de la fonction de mise à jour automatique[47]. Il est vivement recommandé d'instaurer une gestion efficace des logiciels, avec des processus d'inventaire et de mise à jour[48].

Il est important de remplacer les logiciels arrivés en fin de vie pour lesquels les fabricants ne fournissent plus de mises à jour.

4.2 Rançongiciels

Le nombre d'incidents dus à des rançongiciels a également été important au premier semestre 2023. Divers domaines ont été concernés, allant du petit commerce local à la grande entreprise internationale. Les quelques exemples suisses et internationaux ci-après exposent non seulement la situation dans le cyberespace, mais aussi les évolutions des groupes et des modes opératoires qui ont eu lieu durant le premier semestre 2023.

4.2.1 Exemples d'incidents survenus en Suisse

En Suisse, *Lockbit* demeure le rançongiciel le plus répandu. Les acteurs qui en sont à l'origine lancent des campagnes finement élaborées d'hameçonnage ou exploitent les vulnérabilités pour s'introduire dans les systèmes. Par ailleurs, les activités des groupes *Play* et *BlackBasta* ont particulièrement retenu l'attention du NCSC ce semestre.

Les attaques ambitieuses du groupe Play

Le groupe *Play* a été très actif: il s'en est notamment pris à Energy Pool Suisse[49] en février 2023, à CH Media et à la NZZ, deux grandes entreprises de médias, en mars 2023[50], à la

---

45 Un code encoquillé est une interface qui permet d'accéder à distance à un serveur web via un navigateur web.

46 Faille critique du logiciel de transfert de fichiers «MOVEit» (ncsc.admin.ch);
CL0P Ransomware Gang Exploits MOVEit Vulnerability (cisa.gov); voir aussi chap. 4.4.1, 4.5.1 et 4.5.2.

47 Voir U comme Utiliser ses mises à jour (s-u-p-e-r.ch).

48 Voir Rapport semestriel 2021/1 (ncsc.admin.ch), chap. 3.2.

49 Ransomware-Angriff auf Schweizer Energie-Firma (inside-it.ch)

50 Daten von CH Media nach Cyberangriff veröffentlicht (chmedia.ch);
Cyberkriminelle veröffentlichen erneut Daten von CH Media (chmedia.ch);
Cyberangriff auf das Unternehmen NZZ: Veröffentlichung von NZZ-Daten im Darknet (nzz.ch)

commune valaisanne de Saxon en avril 2023[51] et au prestataire de services informatiques Unico[52] ainsi qu'au fournisseur de logiciels Xplain[53] en mai 2023. Les perturbations que les attaques ont provoquées et, aussi, la publication ultérieure, par les cybercriminels, des données qu'ils ont subtilisées ont fait largement connaître le groupe *Play*.

Le rançongiciel BlackBasta affecte l'exploitation d'une entreprise

L'acteur *BlackBasta* a su également se démarquer au premier semestre. Il compte parmi ses victimes l'entreprise ABB[54] ainsi que le fournisseur de machines et de services industriels Bobst[55]. Dans les deux cas, les incidents ont impacté les activités de l'entreprise.

BlackBasta fonctionne comme un rançongiciel en tant que service (RaaS) sans pourtant qu'il y ait d'indications que le groupe ait fait de la publicité sur les forums traditionnels du darknet ou sur des plateformes de commerce illicite ou qu'il ait tenté d'une manière ou d'une autre de recruter des affiliés. Les indices récents suggèrent que les auteurs du logiciel développent eux-mêmes leur boîte à outils et qu'il agit seul ou en collaborant qu'avec un nombre limité d'affiliés de confiance.

L'évolution du groupe _BianLian_

Dans le rapport semestriel précédent, le NCSC avait déjà fait part d'un incident lié au groupe *BianLian*[56]. Ce dernier avait fait une première victime suisse en septembre 2022, soit deux mois après son apparition. Le NCSC avait alors énoncé qu'à l'instar de beaucoup d'auteurs de maliciels, *BianLian* appliquait le principe de la double extorsion. Il commençait par exfiltrer les données, c'est-à-dire par les copier, avant de les chiffrer. Cependant depuis janvier 2023, le groupe semble avoir renoncé au chiffrement des données et n'effectuer qu'une exfiltration. Il convient néanmoins de souligner qu'à ce même moment de l'année, un déchiffreur gratuit est paru pour le maliciel *BianLian*.

Cela n'a pas empêché le groupe de poursuivre ses activités. Au printemps 2023, le département de l'instruction publique du canton de Bâle-Ville a subi une attaque de *BianLian* et a vu ses données publiées sur le darknet peu après[57]. L'absence de chiffrement semble être à la mode également chez d'autres groupes de rançongiciel, tels que *BlackCat* et *Cl0p,* qui appliquaient jusque-là la double extorsion[58]. A contrario, d'autres groupes, tels que *Karakurt,* n'ont jamais recouru au chiffrement.

4.2.2 Situation à l'étranger

Dans le domaine des rançongiciels, l'état de la situation en Suisse ne diffère que peu de celle au niveau international. À l'étranger aussi *Lockbit*, *BlackCat/AlphV* et *Royal* dominent le

---

51 Cyberattaque contre le service de la curatelle de Saxon (policevalais.ch)

52 Ransomware-Attacke auf IT-Dienstleister Unico Data: viele Betroffene (watson.ch)

53 Cyberattaque contre l'entreprise Xplain: l'administration fédérale est également touchée (admin.ch)

54 Multinational tech firm ABB hit by Black Basta ransomware attack (bleepingcomputer.com); ABB provides details about IT security incident (abb.com)

55 Cyberattaques ciblées: Bobst résiste à deux piratages informatiques (24heures.ch); Mutmassliche ABB-Hacker stecken auch hinter Angriff auf Bobst (inside-it.ch)

56 Rapport semestriel 2022/2 (ncsc.admin.ch), chap. 5.2.2.1

57 Grosser Cyberangriff - Kinder betroffen: Daten des Basler Erziehungsdepartements gehackt (srf.ch)

58 Voir chap. 4.5.1.

classement quant au nombre d'attaques, et les principales cibles sont des entreprises industrielles et des prestataires de services[59]. Parmi les incidents majeurs figure le cas du service postal britannique Royal Mail, qui a dû interrompre ses services d'expédition internationale en janvier 2023 en raison d'une infection par le rançongiciel *LockBit*[60].

Outre la persistance des attaques conduites par ces groupes réputés, de nouveaux rançongiciels (comme *Akira*) et de nouveaux groupes (comme *MalasLocker*, voir chap. 2.1.1) sont apparus, tandis que certains groupes ont été dissous (*Hive*) et d'autres sont réapparus (*Cl0p*)[61].

4.2.3 Aperçu des groupes les plus actifs et des principaux vecteurs d'infection

Surfer sur la vague de la tendance

Au cours du premier semestre, la plupart des incidents sont dus aux maliciels *Lockbit*, *BlackCat/AlphV* et *Cl0p*. Les vecteurs d'infection apparaissent et disparaissent au rythme des découvertes de failles et des publications de correctifs. Les cybercriminels savent rapidement s'adapter aux nouvelles tendances technologiques, comme nous avons pu l'observer avec les langages *Go* ou *Rust*[62], la vulnérabilité *ESXi VMware*[63] ou encore la technique de distribution de maliciel au moyen de fichiers OneNote[64]. Parfois il n'est pas nécessaire de changer son mode opératoire technique, car les méthodes traditionnelles reposant sur l'ingénierie sociale continuent à se suffisre à elles-mêmes. L'erreur humaine reste une faille inestimable pour les cybercriminels.

Attaquer les prestataires de services informatiques

Les prestataires de services informatiques figurent également dans la liste des victimes de rançongiciels. En effet, lorsqu'un rançongiciel touche une société de services informatiques, il peut ainsi affecter plusieurs clients à la fois. Les prestataires de services informatiques jouent un rôle d'interface ou de point de connexion avec de nombreux réseaux de clients. Cet effet multiplicateur rend ces entreprises intéressantes pour les auteurs, qui y voient une opportunité d'exiger des rançons multiples ou élevées. Un plan de continuité des activités (incluant la sauvegarde des données et la capacité de répliquer l'infrastructure des serveurs à l'aide d'images et de l'informatique en nuage [*cloud computing*]) a été un élément clé pour les sociétés de services informatiques qui ont pu reprendre rapidement leurs activités après une attaque par rançongiciel.

S'écarter du chiffrement

La double extorsion était pendant longtemps un mode opératoire presque standard pour les groupes et leurs affiliés usant de rançongiciels. Dans certains cas, il arrivait de même retrouver de la triple extorsion: non seulement les criminels exfiltraient puis chiffraient les données, mais ils s'en prenaient également aux parties tierces et aux personnes liées à la victime, en utilisant les données obtenues pour les extorquer également. Cependant, le NCSC observe que divers

---

59 March 2023 broke ransomware attack records with 459 incidents (bleepingcomputer.com); Ransomware Trends 2023, Q2 Report (cyberint.com);

60 LockBit leaks more Royal Mail data after ransomware attack (techmonitor.ai)

61 Voir chap. 4.4.1 et 4.5.2.

62 Voir Rapport semestriel 2022/2 (ncsc.admin.ch), chap. 5.2.2.

63 Semaine 7: systèmes VMware ESXi bloqués (ncsc.admin.ch)

64 Qakbot evolves to OneNote Malware Distribution (trellix.com)

groupes commencent à s'écarter du chiffrement en se contentant d'exfiltrer les données et d'extorquer de l'argent à la victime sous menace de publier les données obtenues (voir chap. 4.5.1).

Conclusions, perspectives et recommandations:

Les groupes et modes opératoires en matière de rançongiciel évoluent et se transforment de plus en plus rapidement. Il est donc important de prendre autant que possible des mesures de prévention tant sur le plan technique qu'humain[65].

Des aspects importants de la résolution des incidents sont présentés sur le site du NCSC:

Rançongiciels – Que faire? (ncsc.admin.ch) et Fuite de données – Que faire? (ncsc.admin.ch)

4.3 Systèmes de contrôle industriels et technologie opérationnelle

Au premier semestre 2023, les attaques opportunistes contre les réseaux d'organisations qui exploitent aussi des systèmes de contrôle industriels et de la technologie opérationnelle sont demeurées la plus grande menace pour l'exploitation sûre de ces systèmes. En Suisse, l'exploitation des installations du groupe industriel ABB[66] et du fabricant de machines romand Bobst[67] a été affectée, au moins temporairement, par des attaques en lien avec le rançongiciel *BlackBasta*. Dans le domaine de l'approvisionnement en énergie, Energy-Pool Suisse[68] a été victime du rançongiciel *Play* (voir chap. 4.2.1).

Au niveau international, l'emploi, croissant depuis le début de l'année, de maliciels effaceurs (*wipers)* a provoqué des interruptions d'exploitation dans des organisations en Ukraine[69]. *NikoWiper*[70] a notamment été utilisé contre une entreprise du secteur de l'énergie. La hausse de l'utilisation de maliciels effaceurs est notamment imputable à un nouvel acteur, appelé Cadet Blizzard[71] ou Frozen Vista[72], qui a été responsable, au début de la guerre, notamment d'attaques avec le maliciel effaceur *WhisperGate*. Hors de cette zone de conflit, un cyberincident a provoqué des interruptions de transport pour un gazoduc canadien[73]. Selon des extraits de documents classifiés américains qui ont fuité (*Pentagon leaks*), il a été revendiqué par le groupe d'hacktivistes prorusse Zarya. D'autres actes potentiellement destructeurs sont évoquées au chap. 2.4 (thème prioritaire).

Le prestataire de services de sécurité Mandiant a publié fin mai des informations sur le maliciel spécifique au système de contrôle industriel *CosmicEnergy*[74], qui attaque les appareils qui

65 Voir les méthodes et mesures décrites au chap. 4.1.
66 Multinational tech firm ABB hit by Black Basta ransomware attack (bleepingcomputer.com); ABB provides details about IT security incident (abb.com)
67 Mutmassliche ABB-Hacker stecken auch hinter Angriff auf Bobst (inside-it.ch)
68 Ransomware-Angriff auf Schweizer Energie-Firma (inside-it.ch)
69 Ukraine Suffered More Wiper Malware in 2022 Than Anywhere, Ever (wired.com)
70 New Report Reveals NikoWiper Malware That Targeted Ukraine Energy Sector (thehackernews.com)
71 Cadet Blizzard emerges as a novel and distinct Russian threat actor (microsoft.com)
72 Fog of war: how the Ukraine conflict transformed the cyber threat landscape (blog.google)
73 Russian hacktivist threat on Canada's pipelines is 'call to action,' top cyber official says (therecord.media)
74 CosmicEnergy: New OT Malware Possibly Related To Russian Emergency Response Exercises (mandiant.com)

fonctionnent selon le standard d'alimentation électrique IEC-104. Tant Mandiant que d'autres spécialistes des systèmes de contrôle industriels[75] pensent qu'il s'agit d'un outil qui a été développé pour des scénarios d'exercice, car il n'a pas le potentiel destructeur de certains maliciels comme *Industroyer 2.0* ou *Pipedream*, connus depuis le premier semestre 2022[76].

Le risque d'attaques ciblées contre des processus contrôlés par la technologie opérationnelle reste le plus élevé dans le contexte de conflits existants, tels que la guerre en Ukraine ou les tensions au Moyen-Orient. L'autorité de cybersécurité des États-Unis CISA[77] met en garde contre les activités de l'acteur étatique Volt Typhoon, qui a développé, selon Microsoft[78], des capacités disruptives, susceptibles d'être mises en œuvre par exemple en cas d'escalade des tensions à Taïwan[79].

Dans le monde entier, des efforts sont menés pour protéger les systèmes contrôlant les processus des infrastructures critiques. L'Union européenne a adopté la directive SRI 2, qui exige des exploitants des mesures de sécurité adéquates[80]. Aux États-Unis, la CISA a publié un livre blanc pour accroître la résilience des infrastructures critiques cybernétiques[81]. Du côté de l'industrie, le projet "ETHOS" a été créé en tant qu'initiative du secteur privé pour promouvoir l'échange d'alertes et d'informations sur les menaces spécifiques aux technologies opérationnelles[82].

Conclusion et recommandations:

Les réflexions sur la résilience des systèmes et des organisations s'avèrent précieuses pour maintenir le bon fonctionnement des installations industrielles même dans des situations tendues. Il en va de même de la formation et du perfectionnement continus du personnel.

Des mesures adéquates figurent dans la norme minimale pour les TIC publiée par l'Office fédéral pour l'approvisionnement économique du pays (OFAE), mise à jour en 2023, ainsi que dans les normes minimales par secteur: Norme minimale pour les TIC (ncsc.admin.ch).

Le NCSC recommande sur son site des mesures de protection pour les systèmes de contrôle industriels (SCI) (ncsc.admin.ch).

75 COSMICENERGY Malware Is Not an Immediate Threat to Industrial Control Systems (dragos.com)
76 Voir Rapport semestriel 2022/1 (ncsc.admin.ch), chap. 5.4.1.
77 People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection (cisa.gov)
78 Volt Typhoon targets US critical infrastructure with living-off-the-land techniques (microsoft.com)
79 Chinese Malware Hits Systems on Guam. Is Taiwan the Real Target? (nytimes.com)
80 Directive […] visant à assurer un niveau élevé commun de cybersécurité […] (directive SRI2) (ec.europa.eu)
81 Research, Development, and Innovation for Enhancing Resilience of Cyber-Physical Critical Infrastructure: Needs and Strategic Actions (cisa.gov)
82 ETHOS | Emerging Threat Open Sharing (ethos-org.io)

4.4 Failles de sécurité

4.4.1 MOVEit (CVE-2023-34362 | CVE-2023-35036 | CVE-2023-35708)

Fin mai 2023, une faille critique du jour zéro (CVE-2023-34362) a été découverte dans le logiciel de transfert de données MOVEit Transfer et MOVEit Cloud du fabricant Progress. Elle concernait toutes les versions de l'application, qui est utilisée par de nombreuses entreprises du monde pour le partage et l'échange de fichiers.

Le fabricant a publié le 31 mai 2023 une alerte[83] décrivant la faille en détail et expliquant les mesures nécessaires pour y remédier. À ce moment-là, des acteurs criminels exploitaient déjà activement la faille de sécurité.

La faille touchait les serveurs Windows sur lesquels était exploitée une version vulnérable du logiciel MOVEit. Un cybercriminel pouvait détecter les systèmes vulnérables relativement facilement, à l'aide de services d'indexation Internet publics ou d'un balayage de ports et ainsi identifier des cibles.

L'application web MOVEit, qui permet à ses utilisateurs de gérer et de partager des fichiers de façon simple et pratique, autorisait une injection SQL. Un cybercriminel pouvait, en exploitant cette faille de sécurité, accéder au système cible, en l'occurrence à la banque de données de MOVEit Transfer, exécuter des commandes système et soustraire des données de l'entreprise concernée. Une telle attaque est réalisée en premier lieu afin de voler des données et d'extorquer une rançon aux victimes. Elle donne cependant également la possibilité à des tiers de modifier des données existantes dans le système visé et d'y introduire de nouveaux fichiers et donc aussi des maliciels.

Peu après la divulgation de la faille du jour zéro, le groupe de rançongiciel CI0p a revendiqué la responsabilité de centaines d'attaques contre des organisations du monde entier. Des criminels ont également exécuté avec succès ce scénario d'attaque dans des entreprises suisses de différentes branches avant que les correctifs mis à disposition par le fabricant aient pu être installés.

Lors de la publication de son alerte relative à la faille CVE-2023-34362, le 31 mai 2023, le fabricant Progress a mis à disposition des correctifs accompagnés d'instructions détaillées qui permettaient de supprimer immédiatement la faille. En même temps, il a chargé une entreprise tierce de soumettre le code de l'application MOVEit à une vérification dans le cadre de l'analyse de cette faille. Quelques jours plus tard cette revue de code a débouché sur l'identification de deux autres failles critiques, pour lesquelles des correctifs ont été mis à disposition du public le 9 juin 2023 (CVE-2024-35036) et le 15 juin 2023 (CVE-2023-35708).

Les deux failles publiées ultérieurement (CVE-2023-35036 et CVE-2023-35708) appartiennent à la même catégorie que la première (CVE-2023-34362). Les trois correctifs mis à disposition par le fabricant visent à supprimer les injections SQL.

---

83 MOVEit Transfer Critical Vulnerability (May 2023) (CVE-2023-34362) (progress.com)

Conclusion et recommandations:

Lorsqu'il est établi qu'une faille a déjà été exploitée à la date de sa publication, il est non seulement important de se conformer immédiatement aux mesures d'urgence préconisées par le fabricant et d'appliquer au sein de l'entreprise un processus efficace de gestion des correctifs, mais il est aussi capital de rechercher activement et soigneusement des signes d'attaques antérieures sur les systèmes susceptibles d'avoir été touchés. L'identification rapide d'indicateurs de compromission peut aider à endiguer une attaque à un stade précoce et, de ce fait, réduire les conséquences négatives sur l'activité et les processus d'affaires d'une entreprise.

4.4.2 Fortinet (CVE-2022-39952 | CVE-2021-42756)

Le 16 février 2023, Fortinet a publié deux failles critiques identifiées par son équipe de Product Security Incident Response (PSIRT) interne.

Le numéro CVE-2021-42756[84] concerne FortiWeb et le numéro CVE-2022-39952[85] décrit une faille de sécurité dans FortiNAC.

FortiNAC identifie et protège les appareils connectés au réseau d'une entreprise à l'aide de différentes fonctions en contrôlant l'accès aux ressources du réseau et en réagissant de façon automatisée aux événements de sécurité, alors que FortiWeb se concentre sur la protection des applications web et des API contre les attaques DDoS, les menaces répertoriées dans le top 10 de l'OWASP[86] et les activités de bots malveillants.

Dans les deux cas, il était possible pour un cybercriminel, sous certaines conditions, d'exécuter du code ou des commandes système sur le système cible vulnérable et ainsi de parvenir à exécuter des codes à distance.

Les deux failles n'avaient pas été exploitées activement à la date de la publication, ou tout au moins, une exploitation n'était pas publiquement connue. Toutefois, le 21 février 2023, soit quelques jours après que Fortinet ait informé le public des failles, des chercheurs en sécurité informatique ont publié le code d'exploitation (*exploit code*) de la faille CVE-2022-39952, ce qui a accru considérablement la probabilité d'une exploitation par des acteurs criminels. Quelques heures à peine après la publication de ce code, plusieurs tentatives d'exploitation actives ont été rapportées.

Les deux failles critiques ont attiré l'attention des cybercriminels et revêtaient pour eux un intérêt particulier notamment vu que les produits de Fortinet sont largement répandus et utilisés dans le monde entier. Fortinet dispose d'un portefeuille très étendu en matière de cybersécurité, ses solutions équipant plus de 10 millions d'appareils. Cette situation rend les produits de Fortinet présentant des failles connues très attrayants pour les cybercriminels. En effet, lorsqu'un grand nombre de produits est employé dans le monde, la probabilité d'identifier des appareils non mis à jour, et donc vulnérables, est élevée.

---

84 PSIRT Advisories FG-IR-21-186 (fortiguard.com)

85 PSIRT Advisories FG-IR-22-300 (fortiguard.com)

86 OWASP Top Ten (owasp.org)

Le 21 février 2023, Fortinet a communiqué, simultanément à la publication des deux alertes relatives aux numéros CVE-2021-42756 et CVE-2022-39952, des mesures nécessaires pour corriger les deux failles critiques. Dans les deux cas, une mise à niveau des produits FortiWeb et FortiNAC est requise pour se protéger durablement contre la menace.

Conclusion et recommandations:

Les failles sont souvent déjà exploitées très peu de temps après leur divulgation, et parfois même déjà auparavant. Il est donc extrêmement important de mettre les produits et les services à jour aussi rapidement que possible et d'installer les correctifs selon les recommandations et prescriptions du fabricant. Informez-vous régulièrement, de manière proactive, des nouvelles failles éventuelles. De nombreux fabricants mettent à disposition de leurs clients divers canaux permettant d'obtenir les informations pertinentes. Outre les informations publiées sur le site Internet, ils proposent, par exemple, de s'abonner à des flux RSS ou à des newsletters par courriel. Il est ainsi possible d'intégrer les connaissances relatives aux nouvelles failles au processus de gestion des vulnérabilités d'une entreprise et de combler ces dernières dans les meilleurs délais.

4.5 Fuites de données et gestion des données

En 2023, la sécurité des données reste un enjeu majeur pour les entreprises et les particuliers. Cela vaut pour les responsables de données (qui possèdent, stockent ou font stocker des données), tous les fournisseurs participant au stockage sous une forme ou une autre ainsi que pour les personnes que les données concernent. Bien que le thème suscite davantage d'attention et que la prise de conscience se renforce par conséquent, des cyberattaques continuent d'être à l'origine de fuites de données. Les cybercriminels se détournent de plus en plus du schéma classique (chiffrement des données et extorsion) pour se limiter à la soustraction des données et à la menace de les publier pour extorquer de l'argent aux victimes (voir chap. 4.2). Des attaques contre un fournisseur tiers peuvent aussi entraîner des fuites de données critiques. Dans un tel cas, il peut être difficile pour le client du fournisseur tiers d'obtenir des informations détaillées sur l'incident et sur les conséquences exactes de la fuite de données.

4.5.1 Des attaques par rançongiciel au pur chantage aux données

Fin janvier 2023, le département de l'instruction publique du canton de Bâle-Ville a été touché par une cyberattaque perpétrée par le groupe de rançongiciel *BianLian*[87]. La rançon exigée n'ayant pas été payée, environ 1,2 To de données soustraites ont été publiées sur le darknet au mois de mai. À la différence du mode opératoire habituel de *BianLian*, les systèmes du département n'ont pas subi de chiffrement.

87 Grosser Cyberangriff - Kinder betroffen: Daten des Basler Erziehungsdepartements gehackt (srf.ch)

Ce cas illustre l'adaptation de la stratégie de certains groupes de rançongiciels, qui remplacent de plus en plus la tactique de la double extorsion[88], dominante jusqu'à présent, par un pur chantage aux données. Après l'exfiltration des données, les auteurs ont renoncent au chiffrement des systèmes et parient sur le fait que les dommages que causerait la publication des données soient suffisamment importants pour inciter les victimes à payer. Il s'avère en effet, qu'au cours du premier semestre 2023, la propension à payer une rançon diminuait progressivement après une attaque de rançongiciel utilisant systématiquement le chiffrement[89], ce qui s'explique notamment par une meilleure sensibilisation aux problèmes de sécurité, par des mesures efficaces dans ce domaine (par ex. sauvegardes hors ligne)[90] et par des efforts entrepris par les prestataires de services de sécurité informatique pour mettre à disposition des logiciels de déchiffrement[91].

Les groupes de rançongiciels doivent aussi tenir compte des questions financières et les cyberattaques incluant un chiffrement mobilisent des ressources importantes. De plus, il faut ensuite s'occuper des victimes: les criminels doivent nouer un contact avec elles, mener des négociations et les soutenir dans le déchiffrement après le paiement. En simplifiant leur modèle d'affaires, les cybercriminels peuvent réduire leurs coûts et consacrer du temps à des attaques supplémentaires. La façon dont le groupe CI0p a exploité une faille du logiciel de transfert de documents MOVEit[92] pour une compromission de masse (voir chap. 4.4.1) illustre parfaitement le changement de mode opératoire: les noms de quelque 500 organisations concernées ont été publiés sur le site de divulgation du groupe CI0p jusqu'à fin juin 2023. Les données volées contiennent des informations sur environ 30 millions de personnes du monde entier. La maîtrise d'une attaque d'une telle ampleur aurait mobilisé des ressources très élevées pour les cybercriminels si celle-ci avait été liée à un chiffrement. Le mode opératoire reste financièrement intéressant pour le groupe même si peu de victimes paient la rançon demandée.

Lors d'une exfiltration de données sans chiffrement, la victime conserve en principe sa capacité d'action sur le plan technique. Cependant, une fuite de données personnelles sensibles ou de données sensibles d'entreprise peut porter atteinte à la réputation de celle-ci et enfreindre la protection des données. En outre, de telles données peuvent être réutilisées à d'autres fins criminelles. Même après le paiement de la rançon, rien ne garantit que les données seront effectivement effacées et qu'elles ne seront pas publiées ou revendues. Diverses victimes tentent néanmoins de dissimuler l'incident en payant la rançon.

---

88 Dans une cyberattaque avec double extorsion, l'auteur combine le vol de données avec un chiffrement afin d'extorquer de l'argent aux propriétaires des données ou de vendre les données. Une rançon est exigée, d'une part, pour le déchiffrement des données ou des sauvegardes et, d'autre part, pour l'effacement et la non-publication des données.

89 Big Game Hunting is back despite decreasing Ransom Payment Amounts (coveware.com)

90 Improved Security and Backups Result in Record Low Number of Ransomware Payments (coveware.com)

91 *BianLian*, par exemple, a modifié son mode opératoire et opté pour le simple vol de données après la publication par une entreprise de sécurité informatique, début 2023, d'un programme gratuit de déchiffrement pour le rançongiciel employé par le groupe.

92 Faille critique du logiciel de transfert de fichiers «MOVEit»: appliquer un correctif de toute urgence (ncsc.admin.ch)

Conclusion et recommandations:

Quelques acteurs tendent de plus en plus à renoncer au chiffrement des données et à passer au simple vol de données avec extorsion. Des mesures bien pensées peuvent réduire les dommages, telles que la sensibilisation et la formation des utilisateurs selon des directives internes ou encore une culture positive de l'erreur qui permet d'optimiser les processus internes en collaboration avec le personnel avant qu'une fuite de données se produise.

Gestion adéquate des données

Règle générale: classer les données par catégorie en fonction de leur sensibilité et les protéger en tenant compte de ces catégories. Dans la mesure du possible, les données devraient être chiffrées lors de leur enregistrement.

Règles de conservation: définir **qui** stocke **quelles données**, **où** et sous quelle **forme**, ainsi que les personnes **avec qui** les données sont partagées. Conserver uniquement les données nécessaires à l'exploitation de l'entreprise. Examiner périodiquement si les données qui sont obsolètes ou ne sont plus activement nécessaires ont été effacées. Un archivage numérique hors ligne des données peut aussi entrer en ligne de compte.

Mesures statistiques

Jeux de données: anonymiser ou pseudonymiser les données statistiques provenant, par exemple, d'enquêtes ou celles à des fins de test. Une conservation séparée des identificateurs sous forme chiffrée est également judicieuse. Les données brutes doivent, dans l'idéal, être conservées dans une sauvegarde hors ligne.

Mesures techniques et cyberhygiène

Gestion des mots de passe: introduire des directives sur les mots de passe et une authentification à plusieurs facteurs.

Respecter le principe du moindre privilège.

Mettre en œuvre la segmentation du réseau.

Gestion des correctifs: lors de la divulgation d'une faille, implémenter les correctifs nécessaires aussi rapidement que possible et tenir compte des cycles de vie des produits.

Mesures organisationnelles

Élaborer et tester un plan d'urgence pour la maîtrise des incidents, tout en fixant clairement les responsabilités.

En cas de fuite de données, implémenter le plus rapidement possible des mesures d'urgence techniques et, éventuellement, faire appel à des spécialistes externes. Une communication interne et externe transparente et cohérente s'impose. Idéalement, élaborer une stratégie de communication au préalable.

Examiner également dans quelle mesure il est nécessaire d'informer en temps utile les personnes et les organisations concernées par la fuite de données. Il faut tenir compte ici de la nouvelle loi fédérale sur la protection des données (entrée en vigueur le 1er septembre 2023). Les cas de violation de la protection des données doivent être annoncés dans les meilleurs délais au Préposé fédéral à la protection des données et à la transparence (PFPDT).

4.5.2 Fuite de données lors de cyberattaques *contre* ou *via* la chaîne logistique

Les organisations et les entreprises acquièrent souvent des services et des biens de production auprès de fournisseurs tiers pour mettre leurs propres biens et services à disposition. Dans ce contexte, des attaques peuvent être perpétrées *contre*[93] la chaîne logistique ou *via*[94] cette chaîne. Les processus d'affaires étant de plus en plus interconnectés et la numérisation devenant croissante, ces attaques peuvent entraîner des perturbations ou des interruptions de l'exploitation. Mise à part cette atteinte au cœur de métier, les conséquences, telles que des fuites de données, peuvent être dévastatrices. Lorsque des fournisseurs sont victimes d'une cyberattaque, il arrive souvent que des informations d'accès et des données de leurs clients soient également subtilisées. D'autre part, les systèmes ou les logiciels compromis du fournisseur peuvent être utilisés pour soustraire directement des données chez les clients.

Plusieurs incidents impliquant la fuite de données de tiers ou relatives à des tiers se sont produits en Suisse et dans le monde entier au cours du premier semestre 2023. Dans plusieurs cas survenus en Suisse[95], des cybercriminels ont volé des données de fournisseurs tiers, qu'ils ont ensuite soit vendues sur le darkweb, soit qu'ils ont utilisées comme moyen de pression en menaçant la victime de publier les données sur des sites de divulgation (voir chap. 4.2.1). Ces fuites ont touché non seulement des informations concernant les fournisseurs en question, mais aussi des données des clients qui utilisent au moins une partie de l'infrastructure de ces fournisseurs de services informatiques. Au niveau international, des acteurs pécuniairement motivés ont également recouru à l'extorsion de données pour faire pression tant sur les fournisseurs que sur les clients[96]. Le nombre de clients concernés était très élevé, en particulier dans le contexte de failles dans des logiciels de transfert de documents[97].

---

93 Dans une cyberattaque *contre* la chaîne logistique, l'auteur de la menace se concentre en premier lieu sur le fournisseur tiers, mais les clients de celui-ci peuvent subir des dommages collatéraux.

94 Une attaque *via* la chaîne logistique combine deux attaques, mais l'auteur de la menace a pour cible principale les clients du fournisseur. Tandis que la première attaque vise un fournisseur, la seconde utilise l'infrastructure compromise du fournisseur pour atteindre la victime principale, à savoir le client.

95 Sont notamment survenus en Suisse les incidents suivants:
- CH Media/NZZ: Cyberkriminelle veröffentlichen erneut Daten von CH Media (chmedia.ch); Cyberangriff auf das Unternehmen NZZ: Veröffentlichung von NZZ-Daten im Darknet (nzz.ch);
- imprimeur de la Revue Suisse: Une fuite de données touche jusqu'à 425'000 Suisses de l'étranger (swissinfo.ch);
- Xplain AG: Cyberattaque contre l'entreprise Xplain: l'administration fédérale est également touchée (admin.ch).

96 Sont notamment survenus au niveau international les incidents suivants:
- Capita: UK pension funds warned to check on clients' data after Capita breach (therecord.media);
- Alliance Healthcare: Cyberattack cripples Spanish drug giant Alliance Healthcare (cybernews.com); Un ciberataque impide […] medicamentos […] a las farmacias (elpais.com)
- Managed Care of North America: Nearly 9 million people affected by data breach from cyberattack on dental insurer (therecord.media).

97 Voir Progress et faille de MOVEit (chap. 4.4.1), ainsi que Fortra et faille de GoAnywhere: Summary of the Investigation Related to CVE-2023-0669 (fortra.com).

Conclusion et recommandations:

Les chaînes logistiques constituent un défi central pour la cybersécurité et nécessitent une gestion active des risques. L'évaluation des conséquences d'une fuite de données mobilise de nombreuses ressources. Les organisations et les entreprises devraient prendre des mesures en vue d'une gestion sûre des données et d'une bonne cyberhygiène (voir les recommandations du chap. 4.5.1), mais aussi généralement partager les données avec des tiers selon un principe similaire à celui du « besoin d'en connaître » (c'est-à-dire partager autant que nécessaire, mais aussi peu que possible). En outre, il s'agit pour elles d'identifier dans un premier temps leur paysage cyber spécifique en matière de menace et de risques critiques, puis dans un deuxième temps de les synthétiser dans un plan de réduction des risques régulièrement mis à jour. Elles devraient à cet effet examiner, pour tous leurs domaines d'activité, la criticité des dépendances aux fournisseurs et aux services et, en se fondant sur ce profil des risques, fixer par contrat un droit d'auditer les fournisseurs tiers et une obligation d'annoncer les incidents, surtout en cas de criticité élevée. Les organisations et les entreprises de taille modeste peuvent faire appel au soutien d'associations ou de conseillers spécialisés pour un examen indépendant.

Troisièmement, il est important de prendre des mesures techniques de surveillance des systèmes propres, afin d'analyser les connexions et les autres activités, pour introduire des contre-mesures en cas d'irrégularités. Cela inclut la meilleure protection possible des canaux de communication entre l'organisation et ses fournisseurs. Les organisations devraient finalement établir un plan d'urgence, le tenir à jour et le tester. Les scénarios des exercices devraient aussi prendre en compte les relations avec les fournisseurs et les effets indirects des fuites de données.

4.6 Piratage de sites Internet

Les sites Internet piratés peuvent être employés abusivement pour une multitude d'activités: ils peuvent être utilisés non seulement pour la diffusion de messages politiques (voir chap. 2.2), pour l'optimisation du référencement dans les moteurs de recherche (voir chap. 3.5.1) ou alors comme sites d'hameçonnage, mais il est aussi possible de s'en servir pour diffuser des maliciels. Les chercheurs en sécurité ou d'autres personnes qui constatent des changements non autorisés sur un site Internet essaient normalement d'en informer l'exploitant, afin que le site soit nettoyé. Or, il est généralement difficile, voire impossible, de retrouver les contacts correspondants sur les sites Internet. Pour résoudre ce problème, l'Internet Engineering Task Force (IETF) a développé une norme prévoyant que les exploitants enregistrent les principaux contacts sur leur site Internet, dans un fichier texte portant le nom «security.txt» dans le répertoire prédéfini «/.well-known»[98].

[98] RFC 9116 - A File Format to Aid in Security Vulnerability Disclosure (ietf.org)

Recommandations:

Enregistrez un contact de sécurité sur votre site Internet[99].

Protégez votre site Internet en suivant les recommandations du NCSC.

Notifications à des exploitants de sites Internet par semaine

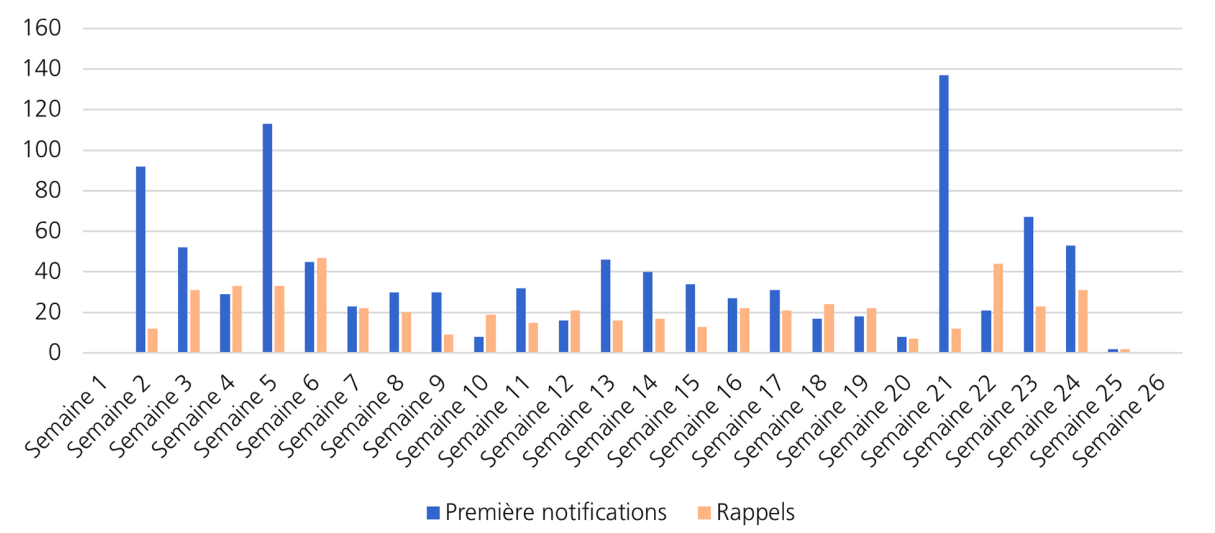


Fig. 10: Notifications du NCSC à des exploitants de sites Internet concernant un piratage ou une modification non autorisée.

4.7 Point sur l'Ukraine

Le premier semestre de l'année 2023 a été marqué par l'anniversaire de l'offensive russe contre l'Ukraine du 24 février 2022. Les deux derniers rapports semestriels ont traité des activités en lien avec cette guerre observées dans le cyberespace jusqu'à la fin de l'année 2022[100].

Développements principaux observés depuis le début de l'année 2023

Les acteurs liés au gouvernement russe sont principalement actifs dans le domaine de l'espionnage, mais également du sabotage. Ces activités sont notamment liées à la diffusion par courriel de maliciels, qui ont pour but d'obtenir un accès initial à un système, ainsi que de campagnes d'hameçonnage, qui ont pour objectif d'obtenir les données de connexion des victimes à certains systèmes. Elles ont été observées principalement en Ukraine, mais des campagnes d'espionnage ont également été rapportées dans d'autres pays, majoritairement des alliés de l'Ukraine et des membres de l'OTAN.

Les groupes d'hacktivistes exécutent principalement des attaques ayant pour objectif de perturber la disponibilité (attaques DDoS) de sites Internet. Les groupes d'hacktivistes prorusses choisissent les États cibles principalement en fonction des appuis qu'ils fournissent à l'Ukraine

99 Enregistrez un contact de sécurité sur votre site Internet (ncsc.admin.ch)

100 Voir Rapport semestriel 2022/1 (ncsc.admin.ch), chap. 3, et Rapport semestriel 2022/2 (ncsc.admin.ch), chap. 5.6.

ou des sanctions qu'ils prononcent contre la Russie. Ces activités ont été observées de manière récurrente en dehors de l'Ukraine, principalement dans les pays de l'Union européenne ou membres de l'OTAN. La Suisse a quant à elle été prise pour cible pendant plus d'une semaine par le groupe d'hacktivistes prorusses NoName057(16) au début du mois de juin, période précédant l'allocution du président de l'Ukraine devant l'Assemblée fédérale par vidéoconférence le 15 juin 2023[101]. Les dégâts occasionnés par les attaques de ces groupes sont marginaux, mais servent toutefois à des fins de propagande.

Développements à venir

Rien n'indique une diminution dans le cyberespace des activités malveillantes en lien avec la guerre en Ukraine. Tant que la guerre durera, la Russie continuera très probablement de lancer des attaques dans ce domaine et de saisir toutes les occasions pour parvenir à ses fins, en les combinant ou non avec des activités déployées dans d'autres sphères opérationnelles. Un facteur de risque important pour le futur concerne les activités des groupes d'hacktivistes. Différents groupes ont fait part de leur intention de mener des attaques plus destructrices que les attaques DDoS observées jusqu'à présent. Pour l'instant, aucun groupe n'a toutefois prouvé avoir les capacités nécessaires pour concrétiser ces nouvelles intentions, mais si cela devait être le cas, les dommages collatéraux pourraient gagner en importance.

[101] Voir chap. 2.1.