3 novembre 2022 | Centre national pour la cybersécurité NCSC

Rapport semestriel 2022/I (janvier – 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

Utilisation de la cybertechnologie dans les conflits armés

Les cyberattaques font de plus en plus souvent partie des conflits armés. Leurs auteurs peuvent aussi bien être des acteurs étatiques que des hacktivistes ou des groupuscules criminels. Le conflit en Ukraine montre l'utilisation qui peut être faite de la cybertechnologie. Le rapport actuel met en évidence ce thème complexe en l'abordant de différents points de vue.

Nette augmentation des courriels de menace

Au cours du premier semestre 2022, le NCSC a enregistré une nette augmentation du nombre de signalements effectués par la population, en recensant 17'186 à la fin de juin. En comparaison avec la même période de l'année précédente (10'234 signalements), cela représente une progression d'environ 70%. Cette augmentation considérable est essentiellement due aux signalements de courriels de menace prétendument expédiés par la police, soit des cas typiques de pseudo-extorsion.

Les cas de fraude toujours en tête du classement national

Pendant la période sous revue, la plupart des signalements enregistrés par le NCSC concernaient les formes de fraude les plus diverses (10'447 signalements). Environ la moitié (5'872 signalements) portait sur des courriels de pseudo-extorsion. D'autres signalements concernaient des fraudes au paiement anticipé (1'834), des pseudo-sextorsions (615) et des fraudes aux petites annonces (419). Les signalements d'hameçonnage et d'attaques fondées sur des logiciels malveillants se sont maintenus au même niveau que l'année précédente à la même période.

Dégâts importants causés par la fraude à l'investissement et à la facturation

Outre les rançongiciels, c'est la fraude à la facturation (piratage d'une messagerie professionnelle) qui, selon le NCSC, représente le potentiel de dommages le plus élevé pour les entreprises. Au cours du premier semestre 2022, le NCSC a reçu 47 signalements à ce sujet, pour des pertes totales de 2,3 millions de francs. La fraude à l'investissement continue ainsi de compter parmi les délits provoquant les pertes financières les plus importantes, en particulier pour les particuliers. À la même période, le montant des dommages dus à l'ensemble des cas annoncés au NCSC s'est élevé à plus de 3 millions de francs.

Légère diminution des signalements de rançongiciels

Bien que les signalements de rançongiciels aient légèrement diminué en passant de 91 à la même période de l'année dernière, à 83 durant le premier semestre 2022, cette forme de cyberattaque reste la plus grande menace à laquelle les organisations suisses sont exposées. Depuis le début de l'année, diverses organisations de secteurs économiques différents ont été victimes de rançongiciels en Suisse.

Progression des cas d'usurpation d'identité

Le NCSC a également enregistré une augmentation considérable des signalements portant sur les falsifications de numéros de téléphone (spoofing). Dans ce cas, des centres d'appel malveillants usurpent le numéro de téléphone de particuliers afin d'inciter leurs victimes à décrocher. Le NCSC a reçu 319 signalements de spoofing durant le premier semestre 2022, alors qu'il n'en avait compté que 17 à la même période de l'année précédente.

Éditorial

Au cours des six derniers mois, la thématique cyber n'a pas pu être abordée sans parler également du conflit en Ukraine. Ce conflit n'a toutefois pratiquement pas eu de répercussions directes dans l'espace cybernétique suisse, si ce n'est que la menace des ransomwares a quelque peu diminué. Il y a deux raisons principales à cela. Des groupes composés de membres russes et ukrainiens ont subis des divisions internes et divers groupes ont commencé à s'engager dans le conflit, ce qui les a occupé.

Le conflit ukrainien montre également où le cyber peut être utilisé comme moyen et où se situent ses limites. Dans les conflits, le cyber est surtout utilisé pour des opérations d'information ou des attaques tactiques, en premier lieu contre des moyens de communication servant à des fins militaires. Les cyberattaques à grande échelle contre les infrastructures n'ont que peu d'effet dans un conflit. Les bombes sont souvent un moyen plus efficace et moins coûteux. De plus, les dommages collatéraux des cyberattaques sont difficilement contrôlables et il existe un risque d'effets dits "spillovers" qui pourraient conduire à une propagation non maîtrisée.

La situation est différente avant le conflit, où des tentatives de paralyser des infrastructures stratégiques de l'Ukraine par des cyberattaques ont été observées. Ces attaques n'ont toutefois eu qu'un succès très limité. Et ce, principalement parce que la cyberdéfense en Ukraine était bien préparée. Les autorités et entreprises civiles ont été un facteur clé à cet égard. Le conflit montre en effet que l'armée doit également se battre dans le cyberespace, mais elle est absorbée par la conduite de la guerre. Il est donc essentiel que les infrastructures numériques puissent être sécurisées par des moyens civils avant et pendant le conflit et qu'en cas de crise, la collaboration entre les services civils et militaires soit assurée. Tout comme dans l'espace physique où, en cas de bombardement, les pompiers doivent également éteindre le feu, car l'armée est absorbée par les combats. Dans sa contribution d'invité, Stéphane Duguin du CyberPeace Institute aborde la problématique des cyberattaques contre les infrastructures civiles. Il s'ensuit une discussion sur les conséquences régionales et mondiales des cyberopérations en Ukraine.

Pour la Suisse, les annonces de fraude en ligne continuent de dominer, avec une augmentation de 70%. Les moyens utilisés par les escrocs sont principalement la fake-extortion, la fraude au paiement anticipé, la fake-sextortion et la fraude aux petites annonces. Dans le présent rapport, nous discutons des modes opératoires actuels et de leurs conséquences.

Dans l'aperçu de la situation, nous traitons principalement de la manière dont l'accès initial aux systèmes est obtenu. Des recommandations sont également formulées sur la manière de rendre ces attaques plus difficiles. Nous constatons malheureusement que de nombreuses mesures de cyber-hygiène de base, telles que la tenue à jour des systèmes, ne sont pas appliquées par tous, ce qui facilite la tâche des pirates. Un aperçu des principales familles de logiciels malveillants et la thématique des ransomwares sont aussi présentés. Enfin, le rapport est complété par la présentation de quelques cas concrets.

Je vous souhaite une bonne lecture. Comme par le passé, nous vous prions, chers lecteurs, de nous faire part de vos réactions. Ce n'est qu'ainsi que nous pourrons adapter en permanence le rapport semestriel à vos besoins.

Florian Schütz, Délégué fédéral à la cybersécurité

2 Contribution d'invité : CyberPeace Institute

Stéphane Duguin est directeur du CyberPeace Institute, une organisation non gouvernementale (ONG) indépendante et neutre qui s'engage pour la paix dans le cyberespace. L'institut suit et analyse les cyberattaques contre des objets civils sur sa plateforme Les cyberattaques en temps de conflit #Ukraine (disponible en anglais uniquement).

Comment un conflit armé déstabilise le cyberespace

Aujourd'hui, en plus des batailles menées au sol, sur les mers et dans les airs, les conflits armés se jouent de plus en plus aussi dans l'espace, dans la sphère de l'information et dans le cyberespace. En l'absence de frontières dans ces domaines, un conflit armé opposant des États peut avoir des répercussions allant bien au-delà des cibles militaires des parties au combat. L'invasion militaire de l'Ukraine en février 2022, qui a précédé toute une série de cyberattaques visant les organisations et établissements publics ukrainiens, a planté le décor d'une guerre qui, aujourd'hui, se déroule autant en ligne qu'au sol. Les attaques et les opérations menées dans le cyberespace dans le cadre du conflit entre la Russie et l'Ukraine ont déstabilisé le monde virtuel et menacent la sécurité et la fiabilité de l'utilisation des technologies.

Stéphane Duguin,
CEO CyberPeace Institute

Quand les infrastructures critiques sont attaquées

Les infrastructures critiques sont des cibles privilégiées pour les cyberattaques – qu'il s'agisse d'un oléoduc (États-Unis, 2021), de stations de pompage (Israël, 2020) ou de services de la santé publique (Royaume-Uni, 2017) – et le conflit en Ukraine le montre une nouvelle fois: en amont de l'invasion et durant les premiers jours de conflit, six souches différentes de maliciels d'effacement des données ont été utilisées contre des organisations ukrainiennes dans des secteurs critiques. Un maliciel peut faire des dégâts considérables s'il compromet des services essentiels pour la population civile. L'attaque du réseau de satellites KA-SAT de ViaSat qui, selon les rapports, visait des éléments de la conduite militaire en Ukraine, a provoqué une perte massive de la communication par Internet pour des utilisateurs à travers toute l'Europe. Une entreprise d'énergie allemande en a notamment subi les conséquences, en perdant l'accès télécommandé à plus de 5800 installations éoliennes. Cette attaque et d'autres maliciels d'effacement des données utilisés pendant le conflit sont attribués à des acteurs étatiques ultraperfectionnés.

Des acteurs non conventionnels qui perturbent le cyberespace

Outre les traditionnelles parties au conflit, d'autres acteurs ont joué un rôle important dans cette guerre, et les frontières qui séparent les deux types de protagonistes sont de moins en moins claires. L'organisation «IT Army of Ukraine», instituée par le gouvernement ukrainien, est un acteur moins conventionnel, dont les attaques DDoS (Distributed Denial of Service) nuisent fortement aux ressources en ligne de la Russie. Des collectifs d'hacktivistes (contraction de «hacker» et «activiste») ont inondé d'attaques DDoS les réseaux d'institutions gouvernementales, d'entreprises étatiques et d'autres organisations. Ces acteurs ont joué un rôle actif dans la perturbation de l'infrastructure en ligne à disposition du grand public, entraînant

des pannes de sites Web et de portails utilisés par la population pour des activités quotidiennes comme l'achat de titres de transport ou le dépôt de déclarations fiscales.

Un grand nombre d'États membres de l'ONU – qui, il faut le préciser, ne sont pas parties au conflit – ont été pris pour cibles ces derniers mois, subissant notamment des cyberattaques de collectifs d'hacktivistes manifestement mécontents des prises de position publiques sur des questions géopolitiques, idéologiques ou économiques de ces États.

Désormais, la publication d'importants volumes de données sensibles pendant un conflit fait partie intégrante du paysage des cybermenaces. Des collectifs ont mené un nombre considérable d'attaques (piratages et fuites de données) au nom de l'activisme antiguerre, donnant librement accès à des données de clients et d'entreprises, y compris à des données personnelles. Ces attaques soulèvent des questions fondamentales sur la protection des personnes, la protection des données et le potentiel d'une utilisation malveillante de ces données dans le futur.

Bien des questions se posent concernant ces acteurs moins traditionnels qui prennent part au conflit armé, notamment en ce qui concerne les tentatives d'attribuer les attaques – c'est-à-dire de déterminer qui a élaboré une cyberattaque, l'a lancée ou l'a autorisée.

Protection de «notre» cyberespace

Les cyberattaques et cyberopérations menées par des acteurs étatiques et non étatiques, que ce soit dans le cadre d'une guerre ou en temps de paix, ont contribué à déstabiliser le cyberespace et en conséquence la société, qui est fortement dépendante de la technologie. Cette déstabilisation a des effets à long terme, et tous n'ont pas encore été étudiés. Un environnement numérique ouvert, libre, stable et sûr requiert impérativement un comportement responsable dans le cyberespace et nécessite l'engagement et la mobilisation de tous les participants:

- Que ce soit en temps de guerre ou en temps de paix, les cyberattaques devraient respecter le droit international et ses normes, et ne pas viser des infrastructures critiques indispensables à la survie de la population civile.
- Les dommages potentiels et les conséquences sur les personnes, ainsi que l'impact humanitaire du recours à des cyberattaques doivent être pris en considération au préalable.
- Les États doivent faire en sorte que les cyberattaques qui enfreignent les lois et les normes internationales soient sanctionnées.
- Les institutions publiques comme les Computer Emergency Response Teams (CERT) sont indispensables pour protéger les systèmes et examiner les attaques grâce à une collaboration efficace et à l'échange d'informations.
- Des entreprises privées peuvent contribuer au développement et à la fourniture de produits et services plus sûrs pour les groupes les plus vulnérables de la société et protéger proactivement les gouvernements et leurs citoyens.
- Par ailleurs, des organisations de la société civile peuvent participer au recensement des cyberattaques, les documenter et analyser leurs répercussions sur les personnes afin de faciliter les enquêtes et soutenir les débats politiques.

3 Thème prioritaire: la dimension cybernétique des conflits armés

Ce chapitre met en lumière les principaux événements rapportés dans le cyberespace depuis le début la guerre actuelle entre la Russie et l'Ukraine. Une grande partie de ce qui se joue dans le cyberespace consiste en activités d'influence, qui ont pour but d'influencer les idées, opinions et motivations de certains groupes cibles et d'intervenir ainsi dans leurs processus décisionnels. Le présent chapitre ne porte pas sur ces activités d'influence, mais sur les activités réalisées dans le cyberespace qui ont un impact direct sur la confidentialité, l'intégrité et la disponibilité des données ou ont des répercussions physiques[1].

3.1 Cyberactivités avant l'invasion

L'Ukraine doit faire face à des activités de cybersabotage depuis plusieurs années. En voici trois exemples notables:

- En 2015, le maliciel «BlackEnergy3», attribué au cyberacteur russe Sandworm, a provoqué des pannes de courant d'une durée atteignant parfois jusqu'à 6 heures et touchant plusieurs centaines de milliers de consommateurs[2].
- En 2016, Sandworm s'est de nouveau illustré, cette fois avec «Industroyer», un maliciel spécialement développé pour infecter les systèmes de contrôle industriels de l'approvisionnement en électricité. L'attaque a causé des pannes d'environ 1 h dans certains quartiers de Kiev[3].
- Contrairement à 2015 et 2016 qui avaient vu des attaques ciblées sur l'alimentation électrique, en 2017 c'est le maliciel «NotPetya» qui a été massivement propagé. Ce dernier commençait par verrouiller les données du système infecté, avant d'afficher un message réclamant une rançon. La propagation de «NotPetya» s'est faite par la manipulation d'une mise à jour d'un logiciel de comptabilité ukrainien, qui a permis d'infecter un nombre important de systèmes en Ukraine. Le maliciel s'est aussi répandu au-delà des frontières ukrainiennes, infectant des systèmes dans plus de 65 pays. Son mode de fonctionnement, le fait qu'il cible l'Ukraine et l'absence de possibilité de déverrouillage (inhabituelle dans les cas de rançongiciels) suggèrent qu'il ne s'agissait pas de chantage, mais plutôt d'un sabotage[4].

Rien qu'en 2021, le service de renseignement ukrainien SBU a déclaré avoir dû contrer plus de 2000 cyberattaques contre des systèmes gouvernementaux et infrastructures critiques en Ukraine, attaques dont il impute une partie aux services de renseignement russes[5]. Au début de l'année 2022, plusieurs cyberincidents fracassants se sont produits simultanément en Ukraine. Le 15 janvier 2022, Microsoft a ainsi déclaré avoir découvert un maliciel baptisé «WhisperGate»,

---

1 Pour des exemples d'activités d'influence dans le cadre de la guerre en Ukraine, voir chap. 4 du rapport de Microsoft sur la guerre en Ukraine du 22 juin 2022 (microsoft.com); voir également EU vs DISINFORMATION (euvsdisinfo.eu).

2 Voir rapport semestriel 2015/2 (ncsc.admin.ch), chap. 5.3.1

3 Voir rapports semestriels 2016/2 (ncsc.admin.ch), chap. 5.3.1, et 2017/1 (ncsc.admin.ch), chap. 5.3.1

4 Voir rapport semestriel 2017/1 (ncsc.admin.ch), chap. 3

5 SSU neutralizes over 2,000 cyber attacks on government resources in 2021 (ssu.gov.ua)

qui infectait les systèmes des institutions gouvernementales, entreprises informatiques et organisations d'utilité publique en Ukraine depuis le 13 janvier précédent[6]. Si «WhisperGate» se présentait comme un rançongiciel, l'absence de mécanisme de restauration des données permet toutefois de conclure qu'il s'agissait en fait d'un «wiper», soit un maliciel qui écrase toutes les données sur les systèmes infectés et les efface ainsi irrévocablement. Après analyse du maliciel, le gouvernement ukrainien a affirmé qu'il s'agissait d'une opération russe menée fallacieusement sous l'étendard ukrainien dans le but d'attribuer à des cybercriminels du pays la responsabilité de «WhisperGate»[7]. Parallèlement à la propagation de «WhisperGate», d'innombrables sites Web du gouvernement ukrainien ont été modifiés au moyen d'attaques de défiguration[8]. À la mi-février, de nombreuses attaques DDoS ont ensuite perturbé la disponibilité d'énormément de sites Internet et de services en ligne en Ukraine. Des établissements financiers et des autorités nationales en ont notamment été victimes[9].

3.2 Cyberincidents marquants dans le cadre de la guerre actuelle en Ukraine

3.2.1 Perturbation des liaisons satellites

Le 24 février 2022, une heure environ avant le début de l'offensive russe contre l'Ukraine, diverses liaisons avec le satellite KA-SAT de l'entreprise américaine ViaSat ont été interrompues. Un grand nombre d'entreprises, d'autorités et de particuliers recourent à ces satellites de télécommunication en Europe pour accéder à Internet, en particulier dans les régions isolées. L'incident a entraîné des perturbations en Ukraine, mais aussi au-delà des frontières. En Allemagne par exemple, il n'était plus possible d'accéder aux systèmes de surveillance et de télécommande d'installations éoliennes. Le 30 mars 2022, ViaSat a publié une analyse de l'incident. Il en ressort qu'il s'agissait d'une attaque ciblée qui ne visait que la partie du réseau satellitaire assurant la couverture de l'Ukraine[10], mais qui a eu des répercussions bien au-delà. Les criminels ont exploité les lacunes de la configuration d'une connexion VPN pour accéder à l'interface administrateur. Ils ont ainsi pu lancer une mise à jour manipulée d'un micrologiciel sur les appareils de nombreux clients, en conséquence de quoi les systèmes touchés ne pouvaient plus établir de connexion et devaient être restaurés manuellement sur place. Au début mai 2022, l'Union européenne et ses États membres, ainsi que les États-Unis, le Royaume-Uni et d'autres États ont condamné cette attaque, dont la responsabilité a officiellement été imputée à la Russie[11].

---

6 Destructive malware targeting Ukrainian organizations (microsoft.com)

7 Information on the possible provocation (cip.gov.ua)

8 Ukraine hit by 'massive' cyber-attack on government websites (theguardian.com)

9 Ukraine Ministry of Defense confirms DDoS attack; state banks lose connectivity (zdnet.com); DDoS attacks hit Ukrainian government websites (therecord.media)

10 KA-SAT Network cyber attack overview (viasat.com)

11 Cyberopérations russes contre l'Ukraine: déclaration [...] de l'Union européenne (europa.eu); Attribution of Russia's Malicious Cyber Activity Against Ukraine (state.gov); Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion (www.gov.uk)

Commentaire:

Les cyberattaques sur des infrastructures utilisées à des fins militaires, civiles et internationales soulèvent des questions quant aux normes de comportement des États dans le cyberespace. Ces dernières devront faire l'objet de vastes discussions au cours des prochaines années, notamment en matière de dommages collatéraux et de proportionnalité, ainsi qu'en ce qui a trait aux devoirs de considération des agresseurs étatiques.

3.2.2 Tentative de sabotage de l'alimentation électrique: «Industroyer2»

Le 12 avril 2022, le Computer Emergency Response Team ukrainien (CERT-UA), Microsoft et la société informatique slovaque ESET ont fait savoir qu'ils avaient découvert le premier maliciel de cette guerre visant des systèmes de contrôle industriels, «Industroyer2», et l'avaient neutralisé[12]. Il s'agissait là d'une nouvelle version du maliciel «Industroyer» utilisé en 2016, qui avait à l'époque provoqué des pannes de courant à Kiev (voir chap. 3.1). Cette nouvelle version était probablement aussi à attribuer au collectif Sandworm[13]. La cible de cette attaque était un fournisseur d'électricité en Ukraine dont le réseau informatique avait déjà été infiltré par les criminels en février 2022. Les pirates ont réussi à s'introduire dans le réseau du système de contrôle industriel en passant par le réseau informatique et y ont installé le maliciel «Industroyer2». L'attaque aurait ensuite dû déployer ses effets dévastateurs le 8 avril 2022 en coupant du réseau des sous-stations électriques et en paralysant certaines parties de l'infrastructure de l'entreprise. Le wiper «CaddyWiper» aurait dû s'activer en même temps, parallèlement à «Industroyer2», vraisemblablement pour entraver la restauration des systèmes et effacer les traces de l'attaque. Quelques jours après le communiqué du CERT-UA, le gouvernement ukrainien a affirmé que depuis le début de la guerre, plus de 50 attaques similaires avaient pu être déjouées. Les informations d'un rapport confidentiel ont toutefois filtré, contredisant cette déclaration et révélant qu'une cyberattaque survenue peu de temps auparavant avait paralysé neuf sous-stations[14].

Commentaire:

Depuis le début de l'invasion de l'Ukraine, «Industroyer2» est le premier maliciel découvert dont le fonctionnement ne visait pas seulement à détruire des systèmes informatiques, mais à interagir directement avec des systèmes de contrôle industriels afin de nuire à des processus physiques.

---

12 Heavy cyberattack on Ukraine's energy sector prevented (cip.gov.ua);
Industroyer2: Industroyer reloaded (welivesecurity.com)

13 Ukraine Power Grid Cyberattacks (securityboulevard.com);
INDUSTROYER.V2: Old Malware Learns New Tricks (mandiant.com)

14 Russia's Sandworm Hackers Attempted a Third Blackout in Ukraine (wired.com);
Russian hackers tried to bring down Ukraine's power grid to help the invasion (technologyreview.com)

3.2.3 Wiper

Depuis le début de la guerre en Ukraine, un grand nombre de wipers différents sont apparus[15]. Le but des maliciels de ce type est de détruire des données ou de les rendre illisibles soit par chiffrement soit en les écrasant, ce qui les efface de façon irrévocable. Des organisations de divers domaines ont été prises pour cible, par exemple l'administration publique, le secteur de l'énergie ou le secteur financier. On ne dispose toutefois d'aucune information de source officielle concernant l'ampleur concrète et le succès de ces attaques. D'après les analyses, le maliciel est chaque fois programmé pour éviter une propagation hors de contrôle, comme ce fut le cas pour «NotPetya» en 2017. Cependant, le 23 février 2022, le «HermeticWiper» a été détecté en Lituanie et en Lettonie, dans des entreprises fournissant aussi des services au gouvernement ukrainien[16].

Commentaire:

Les acteurs étatiques russes semblent être très soucieux de limiter les effets de leurs cyberattaques à l'Ukraine. Ils ne veulent en aucun cas fournir de prétexte à d'autres pays, et encore moins à l'OTAN, pour intervenir activement dans le conflit.

3.3 Agresseurs non étatiques dans les deux camps

Après l'offensive russe du 24 février 2022, de nombreux acteurs non étatiques (organisations hacktivistes et groupements criminels) ont annoncé prendre part à la guerre dans le cyberespace. Ils revendiquent des attaques ou menacent de représailles ceux qui s'en prennent à «leur» partie au conflit. Au total, on a comptabilisé plus de 80 groupes non étatiques de ce genre.

Du côté russe, l'un des plus importants s'appelle Killnet et a mené de nombreuses attaques DDoS en réponse au soutien accordé à l'Ukraine et aux sanctions prises contre la Russie. Les dommages résultant de ces attaques dépendent dans une large mesure de l'importance de la présence sur Internet de la victime et de sa préparation aux attaques de ce type. La plupart du temps, les attaques DDoS peuvent être contrées ou neutralisées relativement rapidement. Les sites Internet des aéroports, des institutions étatiques et des établissements financiers de nombreux pays européens ont été spécialement pris pour cibles.

Du côté de l'Ukraine, le collectif Anonymous a revendiqué un grand nombre d'attaques contre des organisations russes, mais aussi contre des entreprises occidentales actives en Russie. Le 20 mars 2022, Anonymous a ainsi appelé ces entreprises à se retirer du marché russe dans un délai de 48 heures si elles ne voulaient pas prendre le risque d'être prises pour cibles. Depuis, Anonymous a mené de nombreuses attaques «hack-and-leak», dérobant et publiant des données confidentielles d'entreprises ou de gouvernements, principalement en provenance de Russie.

---

15 An Overview of the Increasing Wiper Malware Threat (fortinet.com)

16 Russia unleashed data-wiper malware on Ukraine (theguardian.com)

Le 26 février 2022, l'Ukraine a annoncé la création d'une «IT Army of Ukraine» et a appelé des volontaires du monde entier à s'y engager pour réaliser des attaques dans le cyberespace au profit de l'Ukraine. L'un des piliers de ce groupement est son canal Telegram, qui lui permet de communiquer les cibles de ses attaques DDoS.

Malgré la fréquence des attaques effectuées par des groupements non étatiques, leur effet sur l'évolution du conflit est resté jusqu'ici marginal.

Commentaire:

Des actes répréhensibles tels que des déprédations sont toujours commis dans le cadre de manifestations politiques dans la rue. Des actes virtuels comparables (défiguration, DDoS) sont aussi commis sur Internet. Cependant, lorsque des hacktivistes s'engagent dans le cadre d'un conflit armé entre États, ils peuvent aussi, dans certaines circonstances, être qualifiés de participants à la guerre (combattants) et devenir de ce fait des cibles légitimes de ripostes. Se pose alors la question de la responsabilité des États (territoire) à partir desquels de telles attaques sont perpétrées.

3.4 Autres aspects du conflit dans le cyberespace

3.4.1 Soutien apporté par des États et des entreprises

Au début de l'année 2022, différentes mesures de soutien à l'Ukraine ont été annoncées dans le domaine de la cybersécurité. Le 14 janvier 2022, le Secrétaire général de l'OTAN a laissé entrevoir la signature d'un accord avec l'Ukraine qui lui octroierait un soutien renforcé en matière de cyberdéfense. La déclaration affirmait également que l'OTAN travaillait avec l'Ukraine depuis des années pour améliorer la cyberdéfense du pays et qu'elle lui apportait aussi un appui sur place. Le 22 février 2022, c'est l'Union européenne qui annonçait la formation d'un groupe d'experts d'une dizaine de personnes représentant divers États européens dans le but d'aider l'Ukraine à gérer les cybermenaces, à la fois sur place et à distance.

Des informations plus concrètes sur la manière dont les autres pays allaient soutenir l'Ukraine ont été fournies le 10 mai 2022. Dans une déclaration, l'Union européenne et ses États membres ainsi que les États-Unis, le Royaume-Uni et d'autres pays ont condamné les attaques de ViaSat (voir chap. 3.2.1) et ont affirmé qu'ils poursuivraient leur soutien à l'Ukraine afin de renforcer sa cyberrésilience. Au même moment, les États-Unis ont précisé la manière dont ils allaient aider l'Ukraine à garantir son accès Internet et à assurer sa cybersécurité[17].

Le 1er juin 2022, le commandant du US Cyber Command a annoncé qu'en vue de soutenir l'Ukraine, les États-Unis avaient mis en œuvre toute une série d'opérations offensives et défensives, ainsi que des mesures d'information dans le cyberespace[18]. Comme la majeure partie de ces mesures n'a pas été publiée, il est difficile d'en évaluer la portée. L'analyse d'un

17 U.S. Support for Connectivity and Cybersecurity in Ukraine (state.gov)

18 US military hackers conducting offensive operations in support of Ukraine (sky.com)

maliciel conçu pour s'attaquer à des systèmes de contrôle industriels (voir chap. 5.4.1) mais qui n'a pas encore été utilisé jusqu'ici a été publiée en avril 2022 et pourrait bien être liée aux mesures du US Cyber Command précitées. Ce maliciel aurait pu être utilisé pour de futures attaques contre l'Ukraine, mais aussi contre d'autres pays. Une autre opération susceptible d'avoir aidé l'Ukraine a été rendue publique: elle consistait à mettre en partie à l'arrêt l'infrastructure du botnet «CyclopsBlink» (voir chap. 5.2.4) utilisé par le collectif Sandworm.

Beaucoup de sociétés de sécurité informatique accordent une importance particulière à la guerre en Ukraine et consacrent des analyses et des rapports à ce sujet. Ainsi, ESET et Microsoft se sont associés au CERT ukrainien pour rendre publique la découverte de «Industroyer2». Le 22 juin 2022, Microsoft a publié un rapport contenant les observations de l'entreprise en lien avec les cybermenaces associées à la guerre en Ukraine[19]. Ce rapport révèle entre autres que Microsoft et d'autres sociétés technologiques ont aidé l'Ukraine à déplacer la majorité des données et des activités numériques de son gouvernement dans des clouds hors des frontières du pays, le tout en l'espace de dix semaines. Ainsi, lorsque des attaques de missiles ont détruit des centres de calcul ukrainiens au début de l'offensive russe, le pays a pu maintenir son fonctionnement numérique. Le rapport mentionne également l'étroite collaboration des sociétés informatiques avec le gouvernement ukrainien. Microsoft y indique avoir fourni gratuitement à l'Ukraine des services pour une valeur totale estimée à 239 millions de dollars américains. L'aide d'entreprises privées est sans aucun doute essentielle pour l'Ukraine, puisque celles-ci garantissent la protection des systèmes également en conditions normales et connaissent généralement davantage de systèmes et d'événements que n'importe quelle autorité.

3.4.2 Utilisation de cyberinstruments dans le cadre de conflits armés

Les cyberattaques menées en Ukraine depuis le 24 février 2022 et qui ont été rendues publiques jusqu'ici n'offrent pas un tableau complet de la situation et ne permettent pas non plus d'évaluer l'exploitation possible du cyberespace dans le cadre d'un conflit armé.

Comme il s'agit d'une guerre qui dure, de nombreux incidents et leur portée ne sont pas annoncés au grand public. Les protagonistes s'attribuent des attaques réussies ou des parades sans que ces faits soient vérifiés par une tierce partie indépendante. Souvent, les communiqués y relatifs servent à influencer l'opinion publique et l'état d'esprit de la population, dans un sens ou dans l'autre. Aucun cas de cyberattaque contre des systèmes militaires n'a par exemple été rendu public, à l'instar de ce qui s'est produit en 2007 en Syrie lorsque les forces armées israéliennes ont probablement dû utiliser leurs cybercompétences pour neutraliser les systèmes de défense aérienne afin de mener un raid aérien sur des cibles syriennes[20].

Après l'annexion de la Crimée en 2014, le conflit entre l'Ukraine et la Russie ou les régions séparatistes de l'est de l'Ukraine couvait, avec des phases d'activité plus ou moins importante. À cette période, des cyberopérations ont aussi eu lieu (voir chap. 3.1 plus haut), dont les auteurs présumés ont nié être à l'origine, de façon plus ou moins crédible. Depuis le début de

19 Defending Ukraine: Early Lessons from the Cyber War (microsoft.com)

20 Operation Orchard/Outside the Box (2007) - International cyber law: interactive toolkit (ccdcoe.org)

l'offensive russe, l'utilisation de moyens militaires conventionnels pourrait toutefois aussi avoir incité à recourir à des cyberinstruments en arrière-plan. Dans les faits, les moyens militaires conventionnels permettent d'atteindre beaucoup de cibles militaires de façon plus rapide, plus précise, plus simple et plus durable que les cyberattaques.

Il y a plusieurs hypothèses au sujet de l'absence de rapports concernant des cyberattaques russes réussies et dévastatrices (c.-à-d. des attaques ayant pour effet une destruction physique) contre l'Ukraine:

1. La Russie parvient à mener de telles attaques mais ne rend pas ces succès publics notamment parce qu'il s'agit d'une guerre qui dure.
2. La Russie mène des cyberattaques destructrices, mais l'Ukraine parvient à se défendre, en particulier grâce au soutien d'autres États et partenaires privés.
3. La Russie n'effectue pas de cyberattaques destructrices contre l'Ukraine, principalement parce que l'utilisation de moyens militaires conventionnels est plus adéquate pour atteindre ses cibles.

Il y a fort à parier que l'apparente absence de telles attaques soit le résultat d'une combinaison de ces trois hypothèses et qu'il se produise davantage d'événements dans le cyberespace que ce dont le grand public a connaissance.

4 Signalements issus de la population

4.1 Aperçu des annonces de cyberincidents reçues

Au cours du premier semestre 2022, le NCSC a enregistré un total de 17'186 annonces. En comparaison avec la même période de l'année précédente (10'234 annonces), cela représente une augmentation d'environ 70%. Cette hausse considérable s'observe surtout dans les signalements de courriels de fake-extortion qui, durant la période, représentent un tiers du nombre total d'annonces et la moitié des annonces d'arnaques. Les annonces de la catégorie «arnaques» sont de loin les plus fréquentes avec 10'447 cas. Outre les signalements de fake-extortion susmentionnés, les escroqueries les plus courantes sont les fraudes au paiement anticipé (1'834 signalements), les courriels de fake-sextortion (615) et les fraudes aux petites annonces (419). Les annonces d'hameçonnage et de logiciels malveillants se maintiennent quant à elles au même niveau que l'année précédente à la même période.

Annonces au NCSC au premier semestre 2022 (par semaine)

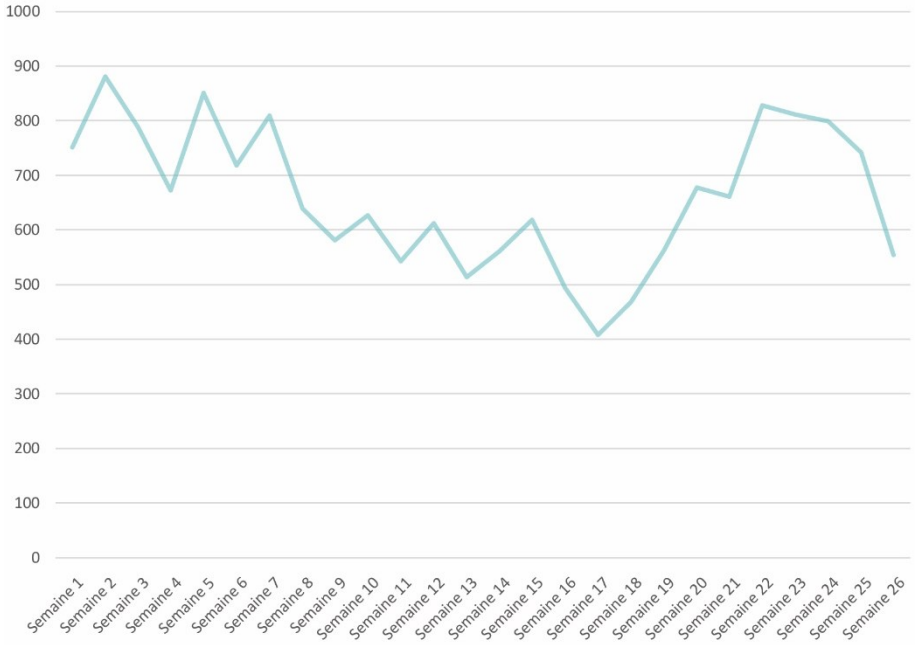


Fig. 1: Nombre d'annonces hebdomadaires parvenues au NCSC du janvier au juin 2022, voir aussi Chiffres actuels (ncsc.admin.ch).

Annonces au NCSC au premier semestre 2022 (par catégorie)

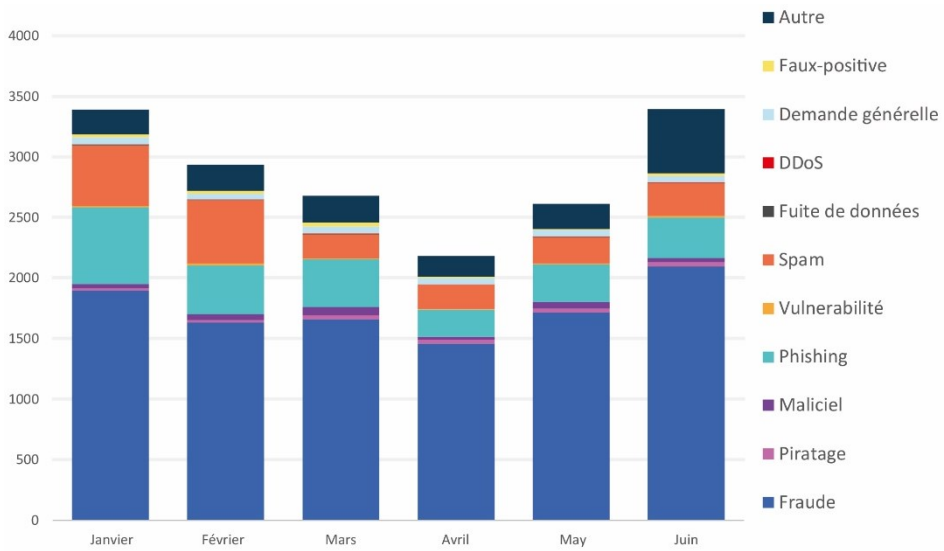
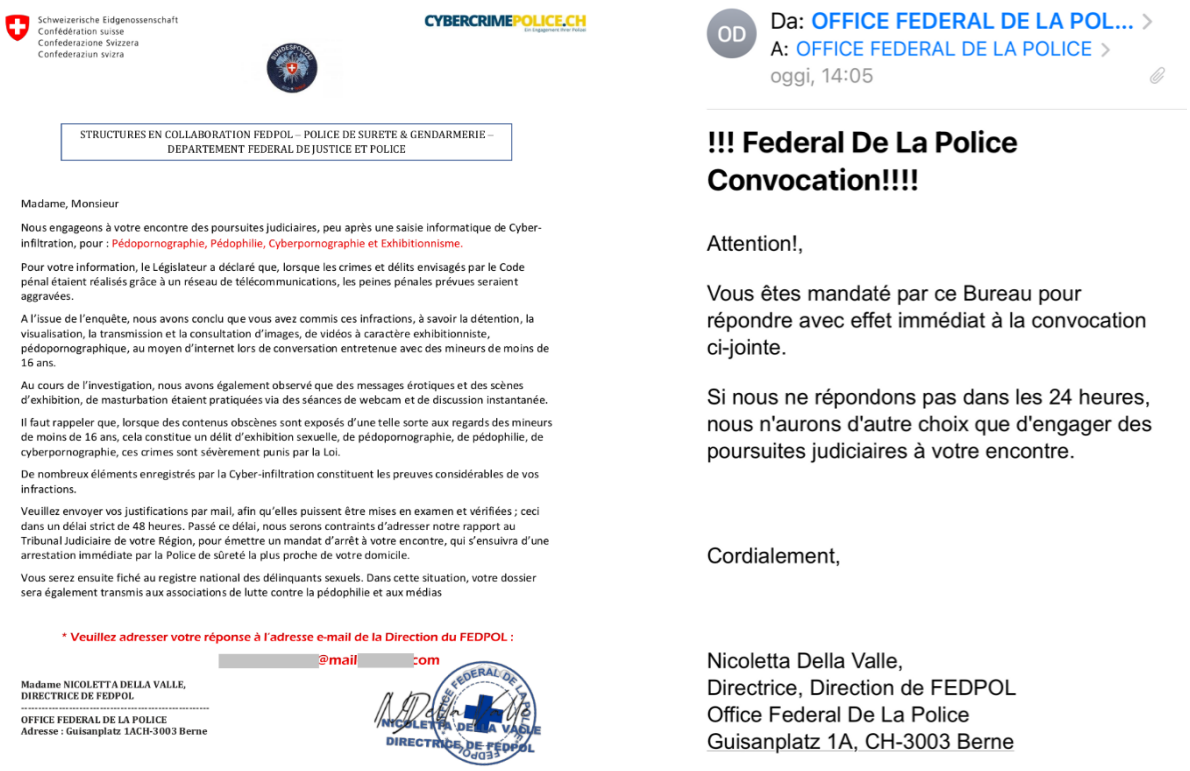


Fig. 2: Signalements effectués au NCSC au premier semestre 2022, par catégorie, voir aussi Chiffres actuels (ncsc.admin.ch).

4.2 L’arnaque, annonce la plus fréquente

4.2.1 Tendance continue à la hausse des cas de fake-extortion

La tendance à la hausse de courriels de menace envoyés au nom de la police, qui s’était dessinée à la fin de l’année dernière déjà, s’est poursuivie durant le premier semestre 2022. Ces courriels dits de fake-extortion représentent sur la période environ un tiers (5'872) de toutes les annonces reçues et environ la moitié des signalements d’arnaques. La fake-extortion est un type d’escroquerie dans lequel le destinataire du courriel est accusé d’un délit grave (typiquement lié à la pédopornographie). Le courriel menace d’engager des poursuites pénales si la personne ne paie pas. L’astuce a été observée en France depuis plusieurs années déjà et a ensuite traversé la frontière. Au début, les courriels frauduleux n’existaient qu’en français. Ils ont ensuite commencé à apparaître en allemand et depuis la mi-mai 2022, les premiers courriels de ce genre en italien ont été annoncés au NCSC. Dans la variante la plus courante, le courriel prétend provenir de l’Office fédéral de la police ou plus précisément de sa directrice Nicoletta Della Valle.



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

CYBERCRIMEPOLICE.CH

STRUCTURES EN COLLABORATION FEDPOL – POLICE DE SURETE & GENDARMERIE – DEPARTEMENT FEDERAL DE JUSTICE ET POLICE

Madame, Monsieur

Nous engageons à votre encontre des poursuites judiciaires, peu après une saisie informatique de Cyber-infiltration, pour : Pédopornographie, Pédophilie, Cyberpornographie et Exhibitionnisme.

Pour votre information, le Législateur a déclaré que, lorsque les crimes et délits envisagés par le Code pénal étaient réalisés grâce à un réseau de télécommunications, les peines pénales prévues seraient aggravées.

A l’issue de l’enquête, nous avons conclu que vous avez commis ces infractions, à savoir la détention, la visualisation, la transmission et la consultation d’images, de vidéos à caractère exhibitionniste, pédopornographique, au moyen d’internet lors de conversation entretenue avec des mineurs de moins de 16 ans.

Au cours de l’investigation, nous avons également observé que des messages érotiques et des scènes d’exhibition, de masturbation étaient pratiquées via des séances de webcam et de discussion instantanée.

Il faut rappeler que, lorsque des contenus obscènes sont exposés d’une telle sorte aux regards des mineurs de moins de 16 ans, cela constitue un délit d’exhibition sexuelle, de pédopornographie, de pédophilie, de cyberpornographie, ces crimes sont sévèrement punis par la Loi.

De nombreux éléments enregistrés par la Cyber-infiltration constituent les preuves considérables de vos infractions.

Veuillez envoyer vos justifications par mail, afin qu’elles puissent être mises en examen et vérifiées ; ceci dans un délai strict de 48 heures. Passé ce délai, nous serons contraints d’adresser notre rapport au Tribunal Judiciaire de votre Région, pour émettre un mandat d’arrêt à votre encontre, qui s’ensuivra d’une arrestation immédiate par la Police de sûreté la plus proche de votre domicile.

Vous serez ensuite fiché au registre national des délinquants sexuels. Dans cette situation, votre dossier sera également transmis aux associations de lutte contre la pédophilie et aux médias

* Veuillez adresser votre réponse à l’adresse e-mail de la Direction du FEDPOL :

[redacted]@mail[redacted]com

Madame NICOLETTA DELLA VALLE,
DIRECTRICE DE FEDPOL

OFFICE FEDERAL DE LA POLICE
Adresse : Guisanplatz 1ACH-3003 Berne

NICOLETTA DELLA VALLE
DIRECTRICE DE FEDPOL

OD

Da: OFFICE FEDERAL DE LA POL...
A: OFFICE FEDERAL DE LA POLICE
oggi, 14:05

!!! Federal De La Police Convocation!!!!

Attention!,

Vous êtes mandaté par ce Bureau pour répondre avec effet immédiat à la convocation ci-jointe.

Si nous ne répondons pas dans les 24 heures, nous n'aurons d'autre choix que d'engager des poursuites judiciaires à votre encontre.

Cordialement,

Nicoletta Della Valle,
Directrice, Direction de FEDPOL
Office Federal De La Police
Guisanplatz 1A, CH-3003 Berne

Fig. 3: Courriels typique de menace au nom de la directrice de fedpol Nicoletta Della Valle.

Les expéditeurs de l’autorité invoquée qui sont mentionnés dans les courriels de menace changent toutefois souvent et sont aussi cités successivement sans le moindre lien. D’autres variantes ont aussi été envoyées au nom de diverses polices cantonales ou du portail de la police Cybercrimepolice.ch. Même le nom du NCSC a été utilisé pour donner une touche officielle à des courriels d’arnaque. Pour communiquer avec les victimes, les auteurs de ces attaques se servent souvent de comptes de messagerie piratés appartenant à des étudiants de différentes

universités en Europe et au Brésil. Le NCSC a annoncé des centaines de comptes de messagerie falsifiés ou piratés aux fournisseurs concernés afin que ces derniers puissent prendre des mesures contre leur utilisation abusive.

4.2.2 Dégâts importants dus à la fraude à l'investissement ou à la facturation

La fraude à l'investissement continue d'être parmi les délits provoquant les pertes financières les plus importantes. Au cours du premier semestre 2022, le montant des dommages provoqués par les cas annoncés au NCSC s'est élevé à plus de trois millions de francs suisses. Des pertes à six chiffres par cas ne sont pas rares dans ce domaine. Il semble qu'en période d'augmentation du renchérissement et de taux d'intérêt bas, de telles offres d'investissement soient en plein essor. Aveuglés par des promesses de rendement élevé (et suspect), les victimes font fi de tous les signes montrant qu'il s'agit d'une arnaque. Par exemple, dans la plupart des cas, les sites Web d'investissement douteux n'ont que quelques mois d'existence.

Outre les rançongiciels, c'est la fraude à la facturation (piratage d'une messagerie professionnelle) qui, selon le NCSC, représente le potentiel de dommages le plus élevé pour les entreprises. Durant la période sous revue, il a reçu 47 annonces relevant de cette catégorie. Cette forme de fraude s'appuie toujours sur un échange de messages entre deux parties liées par un contrat, qui contient une facture ou ordre de paiement. Les fraudeurs modifient le numéro de l'IBAN sur lequel le montant doit être versé. Pour pouvoir intervenir dans la communication électronique, les escrocs doivent avoir accès soit au compte de messagerie de l'expéditeur, soit à celui du destinataire. Ce sont surtout des sous-traitants qui sont pris pour cibles, d'une part parce que les montants de leurs factures sont souvent élevés, d'autre part parce que plusieurs factures sont généralement envoyées en même temps, ce qui multiplie les chances de succès des criminels. Le montant des pertes annoncées au NCSC dans cette catégorie atteignait 2,3 millions de francs suisses.

4.2.3 L'usurpation d'identité a le vent en poupe

Les annonces de numéros de téléphone usurpés ont tout simplement explosé. En comparaison avec le même semestre l'année dernière, elles sont passées de 17 à 319! En toile de fond, on trouve les appels de centres d'appels douteux utilisant des numéros de téléphone appartenant en réalité à des particuliers. Pour les appels frauduleux ou les centres d'appels douteux, c'est une pratique courante de falsifier le numéro d'appelant qui s'affiche et d'utiliser un numéro suisse anodin pour inciter le destinataire à prendre l'appel. Si ce sont toujours les mêmes numéros usurpés qui sont utilisés, le vrai propriétaire du numéro peut se voir littéralement submerger de rappels. Certaines personnes ont ainsi signalé recevoir jusqu'à 50 appels par jour. Normalement, les centres d'appels changent régulièrement de numéros falsifiés, de sorte que les rappels cessent d'eux-mêmes. Dans quelques cas cependant, les mêmes numéros ont été utilisés pendant des semaines voire des mois. C'est une pratique agaçante pour les vrais propriétaires de ces numéros, d'autant plus qu'il n'y a rien à faire pour y remédier[21].

[21] Voir à ce propos FF **2017** 6185 – Message concernant la révision de la loi sur les télécommunications (admin.ch), 6207 et 6221.

4.3 Annonces de phishing

Les annonces d'hameçonnage ont un niveau plus ou moins similaire à celui du même semestre de l'année précédente. 2'308 cas ont été signalés au moyen du formulaire d'annonce, soit 100 de moins, mais 4'535 sites au total ont été traités directement via le portail spécialisé antiphishing.ch. Les courriels contenant de fausses annonces de colis envoyés au nom de diverses sociétés de livraison restent majoritaires. 464 annonces sont à mettre sur le seul compte de cette variante. Dans la catégorie hameçonnage, une autre tentative d'escroquerie qui reste d'actualité est l'indication de factures soi-disant payées à double, envoyée par des fournisseurs Internet comme Swisscom ou Sunrise. Le courriel informe que le montant excessif sera remboursé à condition que le destinataire fournisse son numéro de carte de crédit.

Les tentatives d'hameçonnage liées à des petites annonces ont augmenté au premier semestre 2022, avec au total 145 annonces. Dans cette variante, l'escroc simule son intérêt pour un produit. Une fois le prix de vente convenu, il indique qu'il va organiser le transport et virer le montant, qui comprendra à la fois le prix de vente et les coûts de transport. De son côté, le vendeur devra payer la société de livraison. Pour ce faire, il doit s'inscrire sur le site Web d'une société de livraison donnée, payer avec sa carte de crédit et donc fournir toutes les données de cette dernière. Ces sites Web sont parfois extrêmement personnalisés et contiennent non seulement le nom et l'adresse du vendeur, mais aussi souvent une photo de l'objet de la vente, que l'escroc a repris de la plateforme de petites annonces. Cela représente donc un investissement relativement important de la part de ce dernier, mais qui au final semble s'avérer payant.

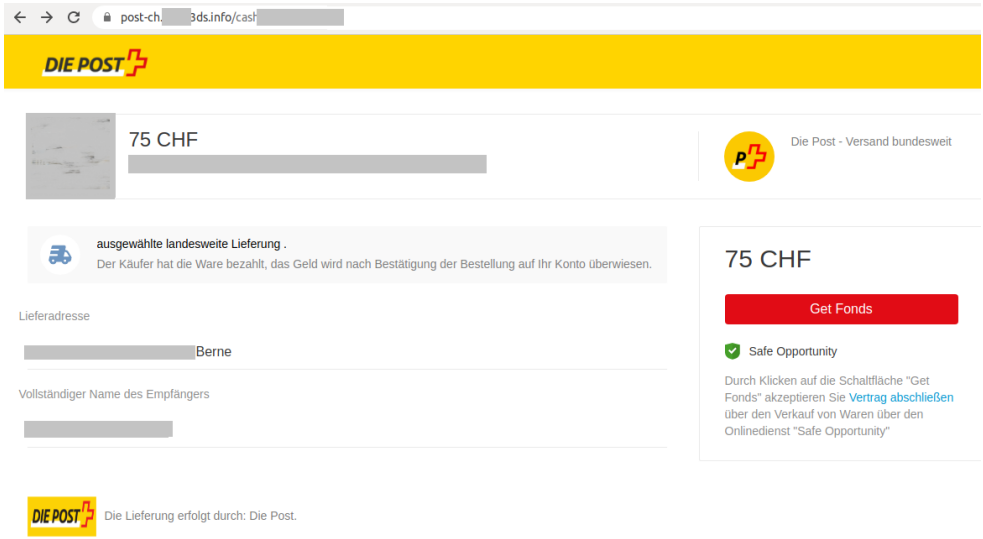


Fig. 4: Site Web personnalisé avec l'adresse du vendeur et une photo de l'article vendu.

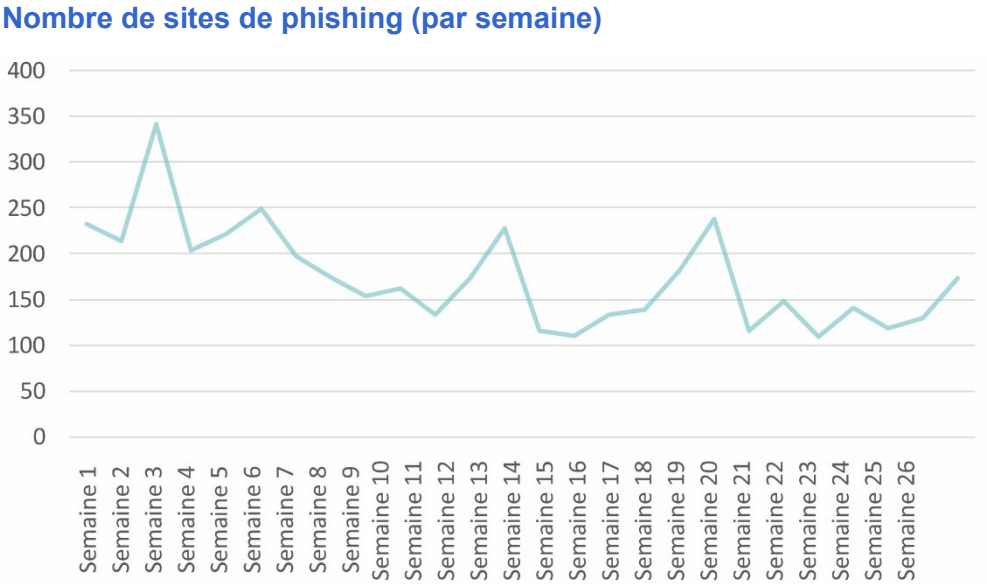


Fig. 5: Nombre d'adresses URL de phishing examinées et confirmées par le NCSC par semaine, au premier semestre 2022. Les données actuelles sont publiées sous: https://www.govcert.admin.ch/statistics/phishing/.

4.4 Annonces de maliciels et de piratages

Durant le premier semestre 2022, un total de 255 annonces de maliciels ont été enregistrées, ce qui représente un recul de 20 % par rapport à la même période de l'année précédente. Si l'on a échappé aux grosses vagues, deux vagues plus petites de «Flubot» ont été observées en mars et en mai avec 56 annonces au total. Dans ces cas, ce sont des SMS qui annoncent des livraisons de colis avec différentes variantes de texte. Le lien figurant sous le texte amène sur un site Web demandant à la victime de télécharger un logiciel de la société de livraison sur son smartphone Android et de l'installer. En juin 2022, des services d'enquête internationaux ont réussi à paralyser le réseau à l'origine du cheval de Troie «Flubot» (voir chap. 5.2.3).

Une autre vague comptant 30 annonces concernait le maliciel «QakBot» (aussi connu sous les noms de «QuakBot» ou «Qbot»). Ce maliciel est propagé par courriel. Pour inciter les destinataires à ouvrir le document joint malveillant, les cybercriminels se servent souvent de conversations électroniques existantes de l'entreprise (p. ex. avec des fournisseurs ou des clients) que des piratages antérieurs ont permis d'obtenir. Le maliciel ainsi installé va leur servir de porte d'entrée pour pénétrer les réseaux de l'entreprise (voir chap. 5.1.2) et y placer des chevaux de Troie verrouillant les données (appelés rançongiciels).

Par rapport au même semestre de l'année précédente, les annonces de rançongiciels ont légèrement reculé, de 91 à 83 cas signalés. Les annonces portaient principalement sur les familles de rançongiciels «QLocker» et «Deadbolt» contre des appareils NAS, ainsi que «LockBit 2.0», «Sodinokibi» et «Conti». Les incidents de piratage ont par contre augmenté de 139 à 184 annonces. Ce sont surtout les comptes de médias sociaux qui sont visés. 91 annonces concernaient ainsi des réseaux sociaux comme Facebook, Instagram ou Twitter.

5 Événements survenus / situation

5.1 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. Ce sont en effet ces accès qui permettent au pirate d'atteindre son but, qu'il s'agisse d'abuser du système ou du compte pour commettre des escroqueries, d'obtenir des données sans autorisation ou d'introduire clandestinement des maliciels de chiffrement (rançongiciels). L'accès initial peut être obtenu de différentes manières:

5.1.1 Nom d'utilisateur / mot de passe

Le plus simple pour accéder à un système ou à un compte, c'est lorsque celui-ci n'est sécurisé que par un nom d'utilisateur (souvent l'adresse de courriel) et un mot de passe. Un simple hameçonnage de l'adresse de courriel permet dans ce cas de trouver le mot de passe recherché et d'accéder au compte ou au système convoité. Le pirate dispose alors d'un accès total et peut exécuter les mêmes opérations que l'utilisateur légal, que celui-ci soit justement en ligne ou non.

Les accès sécurisés uniquement par un nom d'utilisateur et un mot de passe renferment en outre le risque de voir plusieurs comptes piratés si l'utilisateur a utilisé plusieurs fois le même mot de passe. Les cybercriminels utilisent souvent pour ce faire le bourrage d'identifiants, un processus qui consiste à tester les données d'accès obtenues sur tous les sites de services courants (prestataires de messagerie, Twitter, Facebook, Instagram, Amazon, etc.). Les données d'accès ainsi vérifiées sont ensuite revendues.

Conclusion / Recommandation:

L'identification à deux ou plusieurs facteurs offre par exemple une protection contre cette menace.

Le préposé fédéral à la protection des données et à la transparence (PFPDT) a collaboré à la rédaction d'un rapport[22] et de lignes directrices[23] de la Global Privacy Assembly sur le sujet du bourrage d'identifiants.

5.1.2 Maliciels (chevaux de Troie)

Une autre méthode permettant d'obtenir un accès non autorisé consiste à utiliser un maliciel, qui crée une porte d'entrée dissimulée dans le système. Comme dans la légende grecque du cheval de Troie, le maliciel est introduit clandestinement dans un système et ouvre une voie par laquelle les pirates peuvent ensuite installer d'autres maliciels. Pour amener les utilisateurs à cliquer sur le lien malveillant ou à ouvrir le fichier «troyen», diverses méthodes d'ingénierie

22 22-06-27-Credential-Stuffing-General-Public-Awareness.pdf (globalprivacyassembly.org)

23 22-06-27-Credential-stuffing-guidelines.pdf (globalprivacyassembly.org)

sociale peuvent être utilisées. Ces tentatives de manipulation recourent souvent à des techniques typiques: susciter la curiosité ou la crainte d'avoir manqué quelque chose, ou encore donner un sentiment d'urgence.

À l'heure actuelle, la plupart des chevaux de Troie contiennent des fonctionnalités pour le téléchargement ultérieur et l'installation d'autres maliciels (par exemple «Emotet»[24], «Qakbot»[25] ou «Formbook/XLoader»[26]). Il existe toutefois encore des chevaux de Troie qui prennent surtout des captures d'écran et enregistrent les saisies du clavier (appelés Keylogger) pour obtenir les noms d'utilisateurs et les mots de passe (ainsi que les données de cartes de crédit et autres informations). Le cheval de Troie envoie ensuite les données, à intervalles réguliers et de manière autonome, à son exploitant ou à l'auteur de l'attaque, ou les enregistre sur Internet à des emplacements appelés dropzones, où les criminels peuvent les récupérer. «SnakeKeylogger»[27] est un cheval de Troie de ce type qui a été très actif durant la période sous revue.

Conclusion / Recommandation:

Le vecteur de propagation favori des chevaux de Troie est encore et toujours le courrier électronique. Souvent, le texte utilisé dans les courriels infectés se rapporte aux affaires courantes comme des offres, des livraisons ou des factures. Des informations exclusives sur des événements d'actualité tels que la pandémie, la guerre en Ukraine, des catastrophes naturelles ou des manifestations sportives sont parfois utilisées comme point de départ pour piquer la curiosité. L'urgence est aussi fréquemment simulée pour inciter les destinataires à effectuer des actions sans y réfléchir.

Ne cliquez jamais sur un lien dans un courriel suspect et n'ouvrez jamais de fichiers joints.

5.1.3 Exploitation des vulnérabilités

Les vulnérabilités ou failles de sécurité des logiciels ainsi que les configurations incorrectes permettent à un agresseur de s'introduire directement dans un système, ou de se procurer à partir de là l'accès voulu. Les systèmes directement accessibles depuis Internet sont particulièrement menacés, faute d'être toujours protégés par une autre couche de sécurité.

Les vulnérabilités du logiciel Microsoft Exchange ont régulièrement défrayé la chronique depuis le début de l'année 2021.[28] D'autres failles ont été rendues publiques depuis la première, qui avait fait grand bruit en mars 2021. Comme les entreprises sont très nombreuses à utiliser ce logiciel pour serveur de messagerie, les agresseurs ont l'embarras du choix quant aux victimes, d'autant plus que tous les responsables de systèmes n'activent pas tout de suite les mises à

[24] Emotet (fraunhofer.de); Emotet Botnet C&Cs (abuse.ch); URLhaus | emotet (abuse.ch)

[25] QakBot (fraunhofer.de); Qakbot Botnet C&Cs (abuse.ch); URLhaus | Qakbot (abuse.ch); voir aussi rapport semestriel 2021/2 (ncsc.admin.ch), chap. 4.2.3.

[26] Formbook (fraunhofer.de); Xloader (fraunhofer.de); URLhaus | Formbook (abuse.ch)

[27] 404 Keylogger (fraunhofer.de); URLhaus | SnakeKeylogger (abuse.ch)

[28] Voir Rapport semestriel 2021/1 (ncsc.admin.ch), chap. 3.1.1.

jour disponibles. Les produits d'accès à distance et les pare-feu non actualisés sont également des portes d'entrées appréciées des cyberacteurs afin de s'introduire dans les réseaux.[29]

Les plateformes en nuage ne sont guère mieux loties et risquent de subir des cyberattaques en cas de protection insuffisante, de configuration incorrecte ou de vulnérabilités logicielles. Il en va de même pour les interfaces utilisateur graphiques (interfaces web) des systèmes dont la surveillance et le pilotage s'effectuent à distance.

Conclusion / Recommandation:

À peine une vulnérabilité d'un produit est-elle connue que différents acteurs passent au crible Internet à la recherche de systèmes vulnérables. La vulnérabilité est déjà exploitée au bout de quelques heures ou de quelques jours.

Tant les particuliers que les entreprises feraient bien de maintenir constamment à jour les logiciels de tous leurs appareils, de préférence à l'aide de la fonction de mise à jour automatique.

Le NCSC informe régulièrement les organisations en danger en raison de systèmes non mis à jour.[30] Des indices dans ce sens lui parviennent des chercheurs en sécurité en quête de systèmes mal protégés reliés à Internet. Or des criminels peuvent aussi bien rechercher et attaquer des systèmes vulnérables. Les exploitants de systèmes feraient donc bien de ne pas attendre de recevoir une mise en garde du NCSC. Il leur est vivement recommandé d'instaurer une gestion efficace des logiciels, avec des processus d'inventaire et de mise à jour.[31] Enfin, il est nécessaire que les organisations agissent rapidement, au plus tard quand elles reçoivent une lettre recommandée du NCSC.

5.2 Maliciels

5.2.1 Situation générale

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

---

29 Voir Rapport semestriel 2021/1 (ncsc.admin.ch), chap. 3.1.2.

30 Il est grand temps de combler les failles de sécurité de Microsoft Exchange Server (ncsc.admin.ch); Certaines failles de sécurité de MS Exchange n'ont toujours pas été comblées (ncsc.admin.ch)

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

Analyse des familles de maliciels

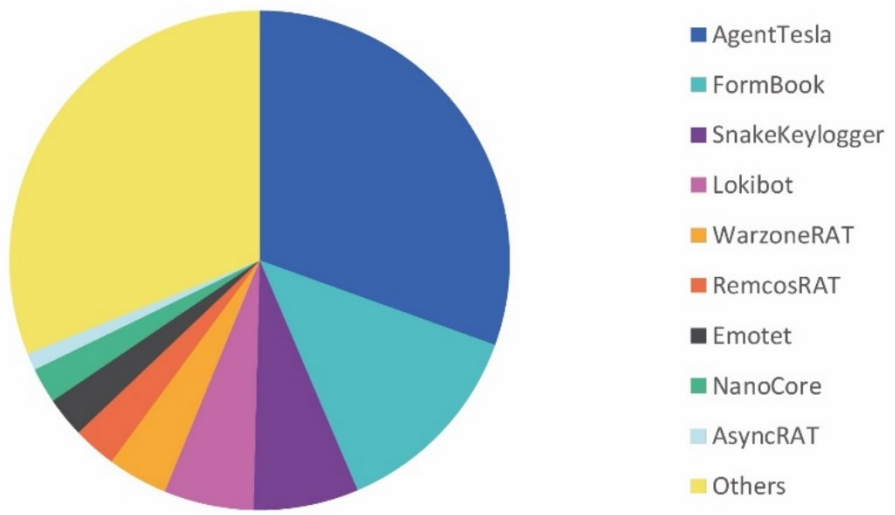


Fig. 6: Analyses du NCSC des familles de maliciels actifs en Suisse au premier semestre 2022.

Le graphique ci-après indique les familles de maliciels dont la présence a été constatée en Suisse durant la période sous revue à l'aide d'analyses des données collectées par les gouffres DNS (*DNS sinkhole*). Un tel dispositif sert à rendre les maliciels inopérants, en empêchant ceux-ci d'accéder aux noms de domaine prévus et en réenregistrant ces derniers pour le compte d'une organisation de sécurité. Il devient ainsi possible d'identifier les appareils infectés qui, au lieu de se connecter avec les serveurs des exploitants du maliciel, s'adresseront aux serveurs de l'organisation de sécurité. Le NCSC reçoit ces données de divers partenaires internationaux couvrant tout l'espace d'adressage suisse, et informe les propriétaires des appareils ayant subi une infection par l'intermédiaire de leur fournisseur d'accès.

Infections par des logiciels malveillants

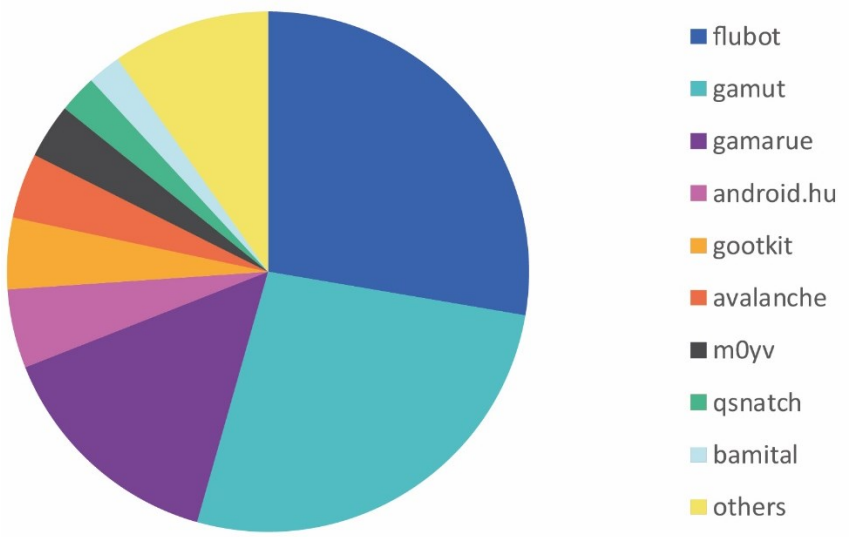


Fig. 7: Répartition des infections par logiciels malveillants en Suisse détectées par le NCSC au premier semestre 2022.

5.2.2 Rançongiciels

Cette année aussi, les cybercriminels mènent des campagnes de rançongiciels. Toutes les branches d'activité en font désormais les frais dans le monde entier[32], et les rançongiciels[33] demeurent la plus grave cybermenace pesant sur les organisations en Suisse.

5.2.2.1 Événements survenus en Suisse

Depuis le début de l'année, diverses organisations actives dans des secteurs économiques différents ont subi en Suisse des cyberattaques.[34]

Dans les cas survenus dans le secteur de la santé, les agresseurs ont souvent utilisé la méthode de la double extorsion, où le rançongiciel «LockBit 2.0»[35] commence par copier des données sensibles de la victime, avant de les verrouiller dans ses systèmes. De nombreuses institutions du secteur suisse de la santé ont ainsi été confrontées au verrouillage de leurs serveurs ainsi qu'à des fuites de données. Les informations dérobées ont souvent abouti dans l'Internet clandestin. De telles attaques portent préjudice non seulement aux institutions, mais aussi indirectement aux patients, car les informations dérobées contiennent souvent, en plus de leurs coordonnées, des données sensibles, telle l'anamnèse.[36]

Dans des secteurs comme les transports et la logistique, qui revêtent une importance systémique pour beaucoup d'autres secteurs, les pirates cherchent à perturber autant que possible la marche des affaires pour mettre leurs victimes sous pression et les amener à payer une rançon.[37] Dans le cas de Swissport, les dispositifs de continuité d'activité ainsi que les sauvegardes effectuées ont aidé à limiter les retombées pour d'autres entreprises.[38]

Dans le secteur de la formation, l'Université de Neuchâtel a subi en février 2022 une attaque due à un rançongiciel. L'incident a eu pour effet d'accélérer la mise en œuvre des nouvelles mesures de sécurité que le canton avait déjà prévues en réponse aux cyberattaques survenues peu avant dans les communes vaudoises de Rolle et Montreux.[39] De telles mesures comprennent en particulier des tests de pénétration réguliers et une meilleure détection précoce des attaques[40].

---

32 2021 Trends Show Increased Globalized Threat of Ransomware (cisa.gov)

33 Rançongiciels (ncsc.admin.ch); What Is Ransomware? (trellix.com)

34 Hackerangriff auf Schweizer Spitalverband (inside-it.ch); Hackerangriff auf Swissport sorgt für Verspätungen im Flugbetrieb (computerworld.ch); Cyberangriff auf Luzerner ÖV bleibt ohne grössere Folgen (inside-it.ch); Cyberattaque contre Emil Frey: des données publiées sur le darkweb (ictjournal.ch); Ransomware-Attacke: «BlackByte» hackt Schweizer Logistikkonzern (watson.ch); Le pire est survenu: les données volées à l'Université de Neuchâtel ont été publiées (letemps.ch)

35 Hacker veröffentlichen erneut sensible Schweizer Gesundheitsdaten (inside-it.ch)

36 Des hackers diffusent les données médicales de Neuchâtelois (watson.ch)

37 The future of cyber security: Ransomware groups aim for maximum disruption (darktrace.com)

38 BlackCat ransomware gang claims responsibility for Swissport attack (computerweekly.com)

39 Neuchâtel a amélioré sa cybersécurité (rtn.ch)

40 Cyberattaque: le canton a pris des mesures (swissinfo.ch)

Les exemples qui précèdent n'ont aucune prétention à l'exhaustivité. Divers médias ont publié une liste plus complète des attaques dues à des rançongiciels qui se sont produites 2022 en Suisse ou à l'étranger[41].

5.2.2.2 Événements survenus à l'étranger

Attaques visant des gouvernements ou des autorités

Depuis avril 2022, plusieurs autorités gouvernementales d'Amérique latine ont été victimes d'attaques de rançongiciels auxquelles des agresseurs russophones semblent avoir pris part[42]. Le Costa Rica, le Pérou, le Mexique, l'Équateur, le Brésil et l'Argentine font partie des États ayant condamné, à l'assemblée générale des Nations Unies, l'invasion de l'Ukraine par la Russie. Le Costa Rica a même dû décréter l'état d'urgence national suite à ces attaques. Les opérations lancées contre des gouvernements sud-américains impliquaient notamment des groupes de rançongiciels comme Conti, ALPHV/BlackCat, LockBit et BlackByte. Le 24 mai, les systèmes informatiques du Land autrichien de Carinthie ont subi une attaque de rançongiciel due à BlackCat, qui a temporairement perturbé les services de l'État[43].

Attaques contre des infrastructures dans le secteur de l'énergie

En Europe, plusieurs terminaux pétroliers situés aux Pays-Bas et en Belgique (Amsterdam, Rotterdam et Anvers) ainsi qu'en Allemagne (Oiltanking GmbH) ont subi dès la fin de janvier 2022 des problèmes informatiques[44]. Les spécialistes de la cybersécurité de ces pays ont expliqué qu'ils n'avaient aucune raison de supposer que ces attaques soient liées entre elles.[45] En tout, les incidents ont touché dans le monde une dizaine de terminaux pétroliers, qui ont fait état de dysfonctionnements opérationnels[46]. Les groupes de rançongiciels russes BlackCat et Conti ont été pointés du doigt[47].

5.2.2.3 Aperçu des acteurs les plus actifs

Conti et ses successeurs

Le puissant groupe russe Conti[48] a suspendu ses activités en mai 2022[49]. Après avoir assuré de son soutien à la Russie qui venait d'envahir l'Ukraine, ce groupe a surtout fait parler de lui

---

41 The terrifying list of cyber attacks worldwide (konbriefing.com);
Hacker schlagen in der Schweiz zu: Die unfassbar lange Opfer-Liste (watson.ch)

42 Latin American Governments Targeted By Ransomware (recordedfuture.com)

43 Hackerangriff auf Land Kärnten: "Black Cat" will fünf Millionen Dollar in Bitcoin (derstandard.at)

44 Des cyberattaques signalées contre des sites portuaires en Allemagne, en Belgique et aux Pays-Bas (lemonde.fr)

45 String of cyberattacks on European oil and chemical sectors likely not coordinated, officials say (therecord.media)

46 Oil terminals in Europe's biggest ports hit by a cyberattack (securityaffairs.co)

47 BlackCat ransomware implicated in attack on German oil companies (zdnet.com)

48 The Conti Enterprise: ransomware gang that published data belonging to 850 companies (group-ib.com);
The hateful eight: Kaspersky's guide to modern ransomware groups' TTPs (securelist.com)

49 Conti ransomware finally shuts down data leak, negotiation sites (bleepingcomputer.com);
Ransomware-Gang Conti schließt Leak- und Verhandlungsplattform (heise.de)

au printemps[50], quand un initié a rendu publiques des discussions internes de ses membres, révélatrices du mode opératoire d'un tel gang[51]. La fuite baptisée «Conti-Leaks»[52] ainsi que des divergences politiques ont probablement eu raison du groupe. Différents membres se sont organisés par la suite en plus petits groupes spécialisés dans une phase spécifique des attaques de rançongiciels, comme l'intrusion dans le réseau ou le vol des données[53]. On trouve par exemple des similitudes entre les tactiques, techniques et procédures (TTP) de Conti et celles des nouveaux groupes BlackBasta[54] et BlackByte[55]. BlackBasta est entré dès avril sous les feux de la rampe en infectant de son maliciel, en l'espace de quelques semaines, une bonne douzaine d'entreprises situées dans le monde entier[56]. Ce groupe présente de nombreux points communs avec Conti, qu'il s'agisse des blogs de fuite des données, des sites de paiement, des portails de restauration, de la communication avec les victimes ou encore des méthodes de négociation[57]. Quant à BlackByte, son rançongiciel dispose de fonctions et de caractéristiques offrant de grandes similitudes avec Conti[58].

BlackCat fait peau neuve

Le rançongiciel BlackCat ou ALPHV, dont les opérateurs faisaient auparavant partie de la sulfureuse organisation BlackMatter/DarkSide[59], est apparu pour la première fois en novembre 2021. Ce rançongiciel particulièrement adaptable offre diverses méthodes et options de verrouillage, qui permettent d'attaquer quantité d'entreprises (à commencer par les plus grandes)[60]. Le modèle d'affaires utilisé a pour particularité de ne pas publier d'emblée sur la page de fuite des données le nom des victimes, mais de s'en tenir à une description de l'organisation concernée. Ou alors une page Web cachée est créée dont l'adresse n'est communiquée qu'aux victimes, à des fins de vérification. De cette façon, les agresseurs leur donnent l'occasion de négocier discrètement leur rançon et maintiennent la pression avec leur menace de publication[61]. Si le groupe décide finalement de publier les données, il le fait sur un site Web ordinaire et non dans l'Internet clandestin. Cela lui permet de toucher un public plus large. De cette façon, même les personnes ayant peu de connaissances techniques et qui sont concernées par la fuite de données (comme les employés ou les clients) peuvent vérifier si leurs données ont été compromises, voire télécharger la totalité des données et documents dérobés à l'entreprise[62].

---

50 Conti ransomware gang backs Russia, threatens US (techtarget.com)
51 Inside Conti leaks: The Panama Papers of ransomware (therecord.media)
52 Conti-nuation: methods and techniques observed in operations post the leaks (nccgroup.com)
53 Conti ransomware shuts down operation, rebrands into smaller units (bleepingcomputer.com); Former Conti Members Are Now BlackBasta, BlackByte and Karakurt Members (spiceworks.com)
54 Shining the Light on Black Basta (nccgroup.com)
55 Threat Spotlight: The BlackByte ransomware group is striking users all over the globe (talosintelligence.com)
56 New Black Basta ransomware springs into action with a dozen breaches (bleepingcomputer.com)
57 New Black Basta Ransomware Possibly Linked to Conti Group (securityweek.com)
58 Former Conti Members Are Now BlackBasta, BlackByte and Karakurt Members (spiceworks.com)
59 Aggressive BlackCat Ransomware on the Rise (darkreading.com)
60 Threat Assessment: BlackCat Ransomware (paloaltonetworks.com)
61 Ransomware gangs now give victims time to save their reputation (bleepingcomputer.com)
62 Ransomware gang publishes stolen victim data on the public Internet (helpnetsecurity.com)

Retour de REvil et de Cl0p

Le début de l'année 2022 a été marqué par l'apparition de nouveaux groupes de rançongiciels, alors que d'autres refaisaient parler d'eux.

La redoutable organisation REvil a de nouveau sévi depuis la fin du mois d'avril, avec une nouvelle infrastructure et un rançongiciel plus sophistiqué[63]. Ce gang avait cessé toute activité en octobre dernier. En janvier 2022, Une intervention policière coordonnée avec Washington avait même permis d'arrêter en Russie des membres de REvil[64]. Selon des sources russes, la communication entre les deux pays aurait pris fin après l'invasion de l'Ukraine, et d'ailleurs le gouvernement américain n'aurait pas fourni assez d'informations pour que des inculpations soient possibles[65].

Le groupe Cl0p s'est lui aussi manifesté à nouveau en avril, après quelques mois d'inactivité présumée. Les chercheurs s'en sont d'autant mieux rendu compte qu'en un mois, il a ajouté 21 nouvelles victimes à son site sur les fuites de données[66].

LockBit

LockBit, groupe spécialisé dans le rançongiciel à la demande (ransomware as a service, RaaS)67, a déjà signé de nombreux méfaits en 202268. Son site de fuites de données indique à chaque fois les victimes supposées, avec un compte à rebours pour la publication des données dérobées. Il s'est toutefois avéré à plusieurs reprises que LockBit prend des libertés avec les faits. Ainsi contrairement à ce qui a été dit, ce n'est pas le site du Ministère français de la justice, mais celui d'une étude d'avocats basée à Caen qui a été piraté69. De même, l'expert en cybersécurité américain Mandiant ne s'était pas fait dérober de données70. LockBit semble parfois chercher à faire parler de lui. Il ne faut pas pour autant sous-estimer la force de frappe d'un tel groupe qui, au semestre sous revue, a fait une centaine de victimes par mois dans toute l'Europe71.

Le rançongiciel fait l'objet de mises à jour régulières, comme tout logiciel normal. Après la parution en juin 2021 de la version 2.0[72], il existe déjà entre-temps une version 3.0[73].

---

63 REvil ransomware returns: New malware sample confirms gang is back (bleepingcomputer.com)

64 Russia takes down REvil hacking group at U.S. request - FSB (reuters.com)

65 REvil prosecutions reach a 'dead end,' Russian media reports (cyberscoop.com)

66 Clop ransomware gang is back, hits 21 victims in a single month (bleepingcomputer.com)

67 *Ransomware as a Service* (RaaS) est un modèle d'affaires adopté par les exploitants de rançongiciels et leurs partenaires. Les partenaires paient, afin que des attaques soient lancées au moyen du rançongiciel développé par les exploitants. On peut y voir une variante du modèle d'affaires des logiciels à la demande (*Software as a service* [SaaS]); Ransomware as a Service (RaaS) Explained (crowdstrike.com)

68 LockBit overtakes Conti as most active ransomware group so far in 2022 (scmagazine.com)

69 Ministère de la Justice: Le groupe Lockbit publie des données, mais pas les bonnes (zdnet.fr)

70 Mandiant: "No evidence" we were hacked by LockBit ransomware (bleepingcomputer.com)

71 Ransomware LockBit : une centaine de victimes par mois au premier semestre (lemagit.fr)

72 LockBit 2.0: How This RaaS Operates and How to Protect Against It (paloaltonetworks.com)

73 LockBit 3.0: Significantly Improved Ransomware Helps the Gang Stay on Top (darkreading.com)

Conclusions, perspectives et recommandations:

Le nombre d'attaques de rançongiciels devrait augmenter encore cette année et toucher davantage d'infrastructures critiques. L'Agence américaine de la cybersécurité et de la sécurité des infrastructures (CISA) a constaté dès 2021 une recrudescence d'attaques raffinées contre les infrastructures critiques, avec les graves conséquences qui s'ensuivent[74]. Les stratégies et les techniques utilisées par les rançongiciels ont évolué en 2021, comme en attestent les progrès technologiques accomplis et les menaces accrues auxquelles s'exposent toutes sortes d'organisations dans le monde[75].

L'éclatement de la guerre en Ukraine a beau avoir entraîné des réorganisations dans l'écosystème de la cybercriminalité, les acteurs sur la scène du rançongicel font preuve de résilience. Des groupes se défont pour réapparaître sous une nouvelle forme, changent de nom ou remplacent au besoin leurs cadres, par exemple quand les autorités répressives exercent sur eux de trop fortes pressions ou si, comme dans le contexte de la guerre en Ukraine, les divergences d'opinions entravent le travail commun.

Outre les mesures de cybersécurité protégeant les systèmes face aux maliciels en général et aux rançongiciels en particulier, d'autres mesures sont encore envisageables derrière cette première ligne de défense. Ainsi, les chercheurs ont découvert dans certains rançongiciels des «points faibles», dont il est possible de tirer parti pour empêcher tout au moins le verrouillage final des données[76].

Les rançongiciels peuvent causer de sérieux dommages, en particulier si les copies de sauvegarde (*backup*) sont affectées. La page du site du NCSC intitulée Rançongiciels – que faire? (ncsc.admin.ch) aborde les diverses facettes de la prévention des incidents.

Par ailleurs, l'Agence américaine de la cybersécurité et de la sécurité des infrastructures (CISA) a publié à l'intention des entreprises un document expliquant comment prévenir les fuites de données lors d'attaques de rançongiciels, et comment réagir le cas échéant[77].

74 2021 Trends Show Increased Globalized Threat of Ransomware (cisa.gov)
75 Ransomware: Over half of attacks are targeting these three industries (zdnet.com)
76 Conti, REvil, LockBit ransomware bugs exploited to block encryption (bleepingcomputer.com)
77 Protecting Sensitive and Personal Information from Ransomware-Caused Data Breaches (cisa.gov)

5.2.3 Maliciels pour smartphones

Après sa dernière grande vague d'attaques datant de l'automne 2021, «Flubot» est réapparu en Suisse le 18 mars 2022. Des SMS invitaient les victimes à installer le maliciel sur leur smartphone. Cette vague d'ampleur internationale78 visait les appareils Android. En Suisse, la plupart des SMS diffusés contenaient de fausses notifications de livraison de colis. Au niveau international, «FluBot» se cachait également dans des SMS du type «C'est toi dans la vidéo?», ou dans de fausses invitations à mettre à jour le navigateur ou le système d'exploitation en place. Le NCSC a consacré à l'incident sa rétrospective de la semaine 1279.

«FluBot» s'est spécialisé notamment dans le vol de SMS sur les téléphones mobiles. Le but étant de trouver parmi les SMS dérobés des mots de passe à usage unique. Une fois le smartphone infecté, l'ensemble de son carnet d'adresses était envoyé au serveur de contrôle des malfaiteurs. Le smartphone recevait ensuite une liste de numéros de téléphone provenant d'autres appareils piratés, auxquels il devait envoyer le SMS malveillant. Le NCSC a reçu 56 annonces concernant «Flubot» au premier semestre 2022.

Au début du mois de mai, la police néerlandaise a démantelé l'infrastructure de «Flubot», désactivant cette souche de maliciel. Cette action policière avait été précédée d'une enquête complexe, impliquant les autorités de poursuite pénale d'Australie, de Belgique, de Finlande, de Hongrie, d'Irlande, d'Espagne, de Suède, de Suisse, des Pays-Bas et des États-Unis. Le Centre européen de lutte contre la cybercriminalité (EC3) d'Europol assurait la coordination des activités déployées au niveau international80. Depuis lors, «Flubot» n'a plus donné signe de vie en Suisse.

Recommandations:

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

5.2.4 Réseau de zombies «CyclopsBlink» – désactivation du successeur de «VPNFilter»

En mai 2018, la communauté de cyberchercheurs Cisco Talos avait publié ses dernières découvertes sur le maliciel «VPNFilter»[81], qui infectait surtout les routeurs de particuliers et de petites entreprises (*small office home office, SOHO*) et les périphériques de stockage en réseau (*network attached storage, NAS*). Les activités attribuées au groupe de pirates d'élite

78 New FluBot and TeaBot campaigns target Android devices worldwide (bleepingcomputer.com)

79 Semaine 12: FluBot circule de nouveau en Suisse (ncsc.admin.ch)

80 Takedown of SMS-based FluBot spyware infecting Android phones (europol.europa.eu)

81 New VPNFilter malware targets at least 500K networking devices worldwide (thalosintelligence.com)

Sandorm[82] avaient cessé après le démantèlement couronné de succès de l'infrastructure de «VPNFilter» par la justice américaine[83].

La veille au soir de l'invasion de l'Ukraine par la Russie, les autorités de sécurité britanniques[84] et américaines ont publié des informations détaillées sur son apparent successeur «CyclopsBlink», qui prenait essentiellement pour cibles les appareils des fabricants Watchguard et Asus[85].

Les exploitants d'appareils infectés, dont certains se trouvaient en Suisse, ont été prévenus par leurs fournisseurs Internet ou par les CERT nationaux[86]. Dans plusieurs cas d'appareils de commande du réseau de zombies, comme les exploitants n'avaient pas effectué le nettoyage demandé, le Département américain de la justice est lui-même intervenu et a éliminé les maliciels après une décision de justice[87].

La communauté de la cybersécurité occidentale est ainsi parvenue à neutraliser l'infrastructure d'attaque de Sandworm et à prévenir ou du moins entraver d'autres attaques potentielles, comme indiqué dans le thème prioritaire (chap. 3.1 et 3.2) ou ci-après au chapitre sur les systèmes de contrôle industriels (chap. 5.4.1).

Recommandations

Le NCSC donne sur son site des recommandations visant à une utilisation sûre des appareils, qui s'adressent à la fois aux utilisateurs privés et aux exploitants d'appareils IdO (appareils connectés à Internet, Internet des objets).

5.3 Attaques lancées contre des sites et des services Web

Les interruptions de disponibilité de sites Web dues aux attaques par déni de service distribué (*distributed denial of service, DDoS*) restent d'actualité tant en Suisse qu'à l'étranger. Au premier semestre 2022, le NCSC a pris connaissance de dix incidents de ce genre, signalés par des PME suisses issues de différentes branches d'activité. Les mobiles de telles attaques relèvent du chantage, de la volonté de causer du tort à un concurrent, ou peuvent encore être politiques.

Selon les rapports d'entreprises de sécurité actives au niveau mondial, même si l'on trouve ponctuellement des attaques toujours plus virulentes (record: 1,4 Tbit/s) et plus complexes (combinaison de différentes méthodes d'attaque)[88], la plupart des attaques DDoS sont de faible intensité (moins de 10 Gbit/s) [89]. Outre le taux de transfert des données, il faut aussi

82 Sandworm (Threat Actor) (fraunhofer.de); voir aussi chap. 3.1 et 3.2.2
83 Justice Department Announces Actions to Disrupt Advanced Persistent Threat 28 Botnet of Infected Routers and Network Storage Devices (justice.gov)
84 New Sandworm malware Cyclops Blink replaces VPNFilter (ncsc.gov.uk)
85 Cyclops Blink Sets Sights on Asus Routers (trendmicro.com)
86 Shadowserver Special Reports – Cyclops Blink (shadowserver.org)
87 Justice Department Announces Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate (GRU) (justice.gov)
88 DDoS attacks becoming larger and more complex, finance most targeted sector (helpnetsecurity.com)
89 DDoS threats growing in sophistication, size, and frequency (helpnetsecurity.com)

prendre en considération des facteurs comme les paquets par seconde (pps) ou les requêtes par seconde (rps). Cloudflare a par exemple enregistré une attaque de 26 millions de requêtes par seconde émanant d'un réseau de zombies certes petit, avec 5067 machines seulement, mais très performant[90].

Depuis avril 2022, un groupe de pirates prorusse ou anti-OTAN se faisant appeler Killnet multiplie les attaques DDoS contre les pays qui soutiennent l'Ukraine par des livraisons d'armes, des aides financières ou des sanctions contre la Russie. Il s'en est ainsi pris aux sites de l'ONU, de l'OSCE, de l'OTAN ainsi que d'organisations basées en Ukraine, en République tchèque, en Estonie, en Lettonie, en Lituanie, en Allemagne, en Norvège, en Pologne, en Roumanie, en Grande-Bretagne, en Italie et aux États-Unis. Parmi leurs victimes figuraient beaucoup d'aéroports[91], de nombreuses autorités étatiques, des banques, des compagnies de chemin de fer, des groupes énergétiques et des fournisseurs d'accès Internet (voir aussi chap. 3.3).

Conclusion / Recommandations:

Le NCSC recommande aux systèmes critiques de s'abonner à une protection DDoS commerciale (solution de mitigation DDoS). De nombreux fournisseurs Internet offrent de tels services.

Le site Web du NCSC propose à sa rubrique Attaque affectant la disponibilité (attaque DDoS) diverses mesures de prévention et de défense contre de telles attaques.

5.4 Systèmes de contrôle industriels (SCI) et technologie opérationnelle (TO)

Des actes de cybersabotage sont ponctuellement observables lors de conflits géopolitiques[92]. Des manipulations au niveau de la technologie opérationnelle ou des systèmes de pilotage s'imposent presque toujours en pareil cas, afin de modifier les processus physiques. Or si de telles attaques requièrent du temps et des ressources, elle s'avèrent plus aisées à mener lors de conflits ayant dégénéré en violences armées avec usage de moyens cinétiques (voir thème prioritaire du chap. 3.2.2 à propos d'«Industroyer2»).

5.4.1 Pipedream / Incontroller: outils visant la technologie opérationnelle

Le lendemain de l'annonce des attaques menées avec le maliciel «Industroyer2» (voir chap. 3.2.2), plusieurs autorités américaines communiquaient dans une mise en garde commune des détails sur un autre maliciel modulaire[93], utilisable à des fins de cybersabotage contre des appareils intervenant dans l'approvisionnement énergétique ou dans des secteurs voisins. La

90 Cloudflare mitigates 26 million request per second DDoS attack (cloudflare.com)

91 Russia-Ukraine: malicious cyber activity targeting aviation entities (ospreyflightsolutions.com)

92 Voir en particulier les analyses consacrées à «Stuxnet» dans le rapport semestriel 2010/2 (ncsc.admin.ch), chap. 4.1 et 5.1) et à Triton/Trisis dans le rapport semestriel 2017/2 (ncsc.admin.ch), chap. 5.3.2

93 APT Cyber Tools Targeting ICS/SCADA Devices (cisa.gov)

publication avait un caractère préventif, aucun cas de déploiement opérationnel de l'une des variantes de maliciels décrites n'ayant été observé jusque-là.

La publication par le gouvernement américain des outils de cybersabotage découverts avait été préparée avec le concours de deux entreprises de cybersécurité américaines spécialisées dans les systèmes industriels, qui ont baptisé ce maliciel évolué «Pipedream»[94] et «Incontroller»[95]. Ce rapport préventif faisait suite à d'autres publications concernant surtout les infrastructures d'attaque russes. L'administration Biden a ainsi fait d'une pierre deux coups, en stoppant dans leur élan les nouveaux maliciels et en soulignant, à partir de cet exemple des dommages que des agresseurs potentiels sont susceptibles d'infliger aux exploitants d'infrastructures critiques américains, l'urgence de réaliser les mesures qu'elle préconise dans sa campagne «Shields Up»[96].

5.4.2 ICEFALL: 56 failles dans la technologie opérationnelle

L'appel à prévoir des dispositifs de défense à plusieurs niveaux ne repose pas seulement sur les nouvelles connaissances relatives aux aptitudes des agresseurs[97] des systèmes de contrôle industriels, mais tient également à la technologie utilisée, dont l'architecture de sécurité est parfois obsolète. La société de cybersécurité Forescout a ainsi publié sous le titre «ICEFALL»[98] une liste de 56 failles de sécurité de produits connus relevant de la technologie opérationnelle. L'équipe d'intervention compétente de la CISA (ICS-CERT) publie en outre régulièrement les nouvelles recommandations de sécurité[99] des différents fabricants. De même, le Cyber-Defence Campus d'armasuisse s'est allié à son pendant allemand, le BSI afin de développer le Common Security Advisory Framework (CSAF), de façon à garder la vue d'ensemble de la situation[100].

Conclusion / Recommandations:

Les outils d'attaque et les failles de sécurité nouvellement découverts montrent qu'il est nécessaire d'investir pour sécuriser l'accès aux systèmes de contrôle industriels ainsi que de surveiller les manipulations effectuées afin de pouvoir réagir rapidement, en cas de soupçon de modifications abusives.

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

94 CHERNOVITE's PIPEDREAM Malware Targeting Industrial Control Systems (ICS) (dragos.com)
95 INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple ICS (mandiant.com)
96 Shields Up (cisa.gov)
97 Three new ICS threat groups discovered, one primed to disrupt energy targets (scmagazine.com)
98 OT:ICEFALL: 56 Vulnerabilities Caused by Insecure-by-Design Practices in OT (forescout.com)
99 ICS-CERT Advisories (cisa.gov)
100 Collaboration entre le CYD Campus et le BSI (admin.ch)

5.5 Failles de sécurité

5.5.1 Log4Shell

La faille de sécurité Log4Shell affectant la bibliothèque Java Log4j, déjà mentionnée dans le rapport semestriel 2021/2 du NCSC, reste d'actualité. Au premier semestre 2022, elle a notamment servi à attaquer et compromettre des serveurs VMware, sur lesquels les correctifs de sécurité n'avaient pas été installés[101].

De par sa nature, cette faille de sécurité peut parfaitement affecter une application ou un système n'étant pas placés sous la responsabilité directe de l'équipe de sécurité d'une organisation. Elle est d'autant plus difficile à repérer et à corriger.

Le Cyber Safety Review Board du Département américain de la sécurité intérieure fait le constat suivant, dans un récent rapport: «L'incident Log4j est loin d'appartenir au passé. Selon cette commission, Log4j constitue une "faille endémique" et le cas échéant, on trouvera encore pendant des années, sinon plus d'une décennie, des objets vulnérables à Log4j. Le risque reste par conséquent bien réel[102].»

Conclusion / Recommandations:

En réponse à ce genre de faille de sécurité, susceptible d'apparaître dans l'infrastructure d'un logiciel mis à disposition par des tiers, il est recommandé de prévoir dans chaque organisation les capacités requises pour tenir un inventaire précis des actifs ou applications informatiques, de donner la priorité à l'installation des mises à jour logicielles et d'investir dans les capacités de détection des systèmes vulnérables. Le rapport du Cyber Safety Review Board renferme aussi des recommandations plus détaillées sur Log4Shell.

5.5.2 Follina

Le 31 mai 2022, Microsoft a attribué le numéro CVE-2022-30190 à une faille de sécurité baptisée «Follina». Cette faille permet d'exécuter un code à distance à l'aide de msdt (outil servant à l'assistance de Microsoft), même si la fonction macro est désactivée, quand un utilisateur ouvre ou visualise en mode aperçu un document infecté dans une application de la suite Office. Microsoft connaissait depuis mars 2021 cette faille de sécurité, qui n'a reçu un numéro CVE qu'au moment où elle a commencé à être utilisée.

Les chercheurs en sécurité ont publié sur Internet plusieurs techniques de défense et de détection, mais la défaillance n'a été corrigée que le deuxième mardi de juin 2022 («Patch Tuesday»). Une chronologie détaillée des événements survenus entre la détection de la vulnérabilité et la mise en œuvre des mesures de défense documente la manière dont cette faille de sécurité a été exploitée avant d'être rendue publique[103].

---

101 Log4Shell Vulnerability Targeted in VMware Servers to Exfiltrate Data (threatpost.com)

102 CSRB Report on Log4j - Public Report - July 11 2022_508 Compliant (cisa.gov)

103 Follina — a Microsoft Office code execution vulnerability (doublepulsar.com)

Conclusion / Recommandations:

Dans le cas de Follina, les détails nécessaires à la réalisation d'un exploit avaient été publiés avant qu'un correctif officiel ne soit disponible, et divers acteurs avaient déjà exploité cette vulnérabilité. En pareil cas, les entreprises ou organisations ont tout intérêt à s'informer régulièrement, à analyser les dernières recommandations et, le cas échéant, à adopter des mesures permettant de réduire les risques, jusqu'à ce qu'un correctif officiel soit disponible et qu'il puisse être installé.

Il est recommandé comme toujours de se conformer aux bonnes pratiques en matière de sécurité informatique. Le personnel pourra contribuer à déjouer ce type de cyberattaques, à condition d'avoir reçu une formation sur la manière d'identifier les courriels malveillants et de ne pas télécharger ou exécuter leurs annexes[104].

5.5.3 Confluence

Le 2 juin 2022, Atlassian a publié un bulletin de sécurité sur une vulnérabilité critique de son logiciel de wiki Confluence, qui a reçu le numéro CVE-2022-26134[105]. Un exploit permettait d'exécuter à distance n'importe quel code sur les serveurs Confluence. Aucun correctif n'était disponible au moment de la publication du bulletin, alors même que les détails rendant un exploit possible étaient accessibles à tout le monde et que des attaquants exploitaient déjà la faille. Ainsi, il a été vivement recommandé de restreindre l'accès des produits Confluence à Internet, ou de les désactiver jusqu'à ce qu'une mise à jour soit fournie.

Le correctif est paru le lendemain. En Suisse, la faille a été exploitée par un rançongiciel dans un cas au moins.

104 Gestion sûre du courrier électronique (ncsc.admin.ch)

105 Confluence Security Advisory 2022-06-02 | Confluence Data Center and Server 7.18 (atlassian.com)

Conclusion / Recommandations:

Comme dans le cas de Follina, la faille de sécurité CVE-2022-26134 a été activement utilisée, avant même la parution d'un correctif officiel. Il est par conséquent important de réagir rapidement et de suivre les recommandations – qui peuvent aller jusqu'à la désactivation du système vulnérable – en attendant la publication d'un correctif officiel.

Une stratégie claire relative à l'accès direct depuis Internet aux interfaces de gestion et aux applications internes permet de réduire la surface d'attaque offerte par une organisation. Si des applications sensibles doivent être accessibles depuis Internet, il convient d'en protéger soigneusement l'accès (par ex. VPN avec authentification multifactorielle, liste des hôtes IP dont l'accès est autorisé pour la maintenance, etc.). À supposer qu'il n'y ait pas encore de correctif pour une faille de sécurité activement exploitée, une gestion avisée des accès externes offre au besoin un peu de répit jusqu'à l'adoption de mesures de défense. Mais une telle mesure ne saurait remplacer l'installation de correctifs dès leur parution.

5.6 Fuites de données

5.6.1 Protection des données: importance de la sécurité des données

Une fuite de données met tout le monde dans l'embarras. Personne n'a envie que des informations personnelles ou sensibles soient divulguées sans son accord, ou de devoir expliquer à des tiers que c'est ce qui leur est arrivé. Or des fuites de données se produisent à tout moment, par la faute de systèmes mal protégés ou mal entretenus, en raison d'erreurs humaines ou lors d'attaques à mobile criminel. Les données dérobées dans un système au cours d'une attaque de rançongiciel offrent en effet un moyen de chantage supplémentaire. Les personnes concernées s'exposent le cas échéant à recevoir des menaces directes de la part des criminels. On parle ici de «triple extorsion»: si l'entreprise pirate ne veut rien payer ni pour le déverrouillage de ses données, ni pour en empêcher la publication, les maîtres-chanteurs risquent de s'en prendre directement aux individus concernés, en les menaçant à leur tour de publier leurs données ou lors d'attaques bien ciblées d'ingénierie sociale. Un tel risque existe surtout avec les données personnelles sensibles, comme les données de patients. Le NCSC a publié sur son site un guide à l'usage des entreprises en cas de fuite des données.

Commentaire:

Il n'existe à ce jour en Suisse aucune obligation légale de signaler les violations de la sécurité des données ou les fuites de données. Cependant, les exploitants d'infrastructures critiques devraient à l'avenir signaler les cyberattaques subies aux autorités, et une obligation de notifier ou d'informer est également prévue dans la nouvelle loi sur la protection des données (LPD).

5.6.2 Lapsus$

Le groupe cybercriminel Lapsus$ s'est illustré à la fin de 2021 par de nombreuses attaques lancées en Amérique du Sud et au Portugal. L'une d'elles a abouti au vol de plus de 50 TB de données, extraites des systèmes du Ministère de la santé brésilien où elles ont été effacées[106]. Une autre attaque a touché Impresa, le plus grand conglomérat de médias au Portugal, dont les sites Web ont été défigurés par une demande de rançon montrant que ce gang avait obtenu l'accès au Cloud de l'entreprise[107]. Dans les deux cas, Lapsus$ a fait chanter ses victimes, exigeant le versement d'une rançon afin que leurs données leur soient restituées ou qu'elles ne soient pas publiées. Le groupe a gagné en visibilité dans les premiers mois de 2022, où il a mené de fructueuses attaques contre des entreprises technologiques internationales comme NVIDIA[108], Samsung,[109] Vodafone[110], Ubisoft[111], Microsoft[112] ou encore Okta[113]. Ces attaques ont abouti à la publication de données confidentielles de ces sociétés. Par la suite, Lapsus$ aurait subi une contre-attaque de NVIDIA et se serait plaint de ce que ses propres données ont été verrouillées[114]. À la fin du mois de mars 2022, sept personnes âgées de 16 à 21 ans soupçonnées de faire partie de ce gang ont été arrêtées en Grande-Bretagne. Deux d'entre elles ont été mises en accusation au début d'avril. Les activités du groupe ont cessé et plus aucun autre incident n'a été signalé au premier semestre 2022. Au début de son activité, Lapsus$ passait pour être un groupe opérant avec un rançongiciel. En réalité, le gang ne faisait qu'exfiltrer ou parfois effacer des données, et faisait chanter ses victimes en les menaçant de publier les données dérobées. Pour accéder aux systèmes de ses victimes, Lapsus$ recourait souvent à des techniques d'ingénierie sociale, qui lui permettaient d'accéder aux informations de connexion[115]. Certaines attaques pourraient avoir abouti avec la coopération d'employés des sociétés attaquées (initiés, menace interne). Le groupe avait ainsi publié sur son canal Telegram une annonce promettant une forte récompense aux employés d'entreprises faisant partie des branches les intéressant, en échange de leur code d'accès à distance VPN[116]. Ce canal Telegram était d'ailleurs la seule plateforme publique du groupe: ses membres y parlaient de leurs activités, parfois en temps réel, et plus de 60 000 abonnés suivaient leurs faits et gestes. En conclusion, on peut dire que Lapsus$ n'a pas sévi longtemps mais a très vite su lancer, avec des moyens modestes et des techniques rudimentaires, de fructueuses attaques contre de nombreuses entreprises renommées pour exfiltrer leurs données.

---

106 Brazilian Ministry of Health suffers cyberattack and COVID-19 vaccination data vanishes (zdnet.com)
107 Lapsus$ ransomware gang hits SIC, Portugal's largest TV channel (therecord.media)
108 NVIDIA confirms data was stolen in recent cyberattack (bleepingcomputer.com)
109 Hackers leak 190GB of alleged Samsung data, source code (bleepingcomputer.com)
110 Vodafone Investigating Source Code Theft Claims (securityweek.com)
111 Ubisoft Cyber Security Incident Update (ubisoft.com)
112 DEV-0537 criminal actor targeting organizations for data exfiltration and destruction (microsoft.com)
113 Updated Okta Statement on LAPSUS$ (okta.com)
114 vx-underground on Twitter (twitter.com)
115 LAPSUS$: Recent techniques, tactics and procedures (nccgroup.com)
116 Lapsus$ Ransomware Group Announced Recruitment of Insiders (securityaffairs.co)