11 mai 2023 | Centre national pour la cybersécurité NCSC

Rapport semestriel 2022/II (juillet à décembre)

Sécurité de l'information

Situation en Suisse et sur le plan international

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF
Centre national pour la cybersécurité NCSC

1 Vue d'ensemble / Sommaire

1 Vue d'ensemble / Sommaire 2
Management Summary 4
Éditorial 5
2 Thème prioritaire: cybersécurité des PME 6
2.1 La numérisation gagne du terrain 6
2.2 Activité de base et outils de soutien 6
2.3 Exploitation informatique et cybersécurité 7
2.4 Recours à des prestataires de services externes 7
2.5 Prévention et préparation aux incidents 7
3 Contributions d'invités: cyberattaques subies 8
3.1 Cyberattaque contre les transports publics lucernois (VBL) 8
3.2 Attaque par rançongiciel: le point de vue de la police 9
4 Annonces émanant d'entreprises ou de particuliers 10
4.1 Aperçu des annonces de cyberincidents reçues 10
4.2 L'escroquerie, incident le plus courant 12
4.2.1 Variantes de faux courriels de menace de la police 12
4.2.2 Attaques visant les administrateurs de sites Internet 13
4.2.3 Fraude à l'investissement 14
4.3 Annonces de phishing 14
4.3.1 L'art d'inventer des histoires plausibles 15
4.3.2 Professionnalisation du phishing basé sur Office365: personnel des entreprises pris pour cible 16
4.4 Annonces de maliciels et de piratages 17
4.4.1 Nombre stable d'attaques par rançongiciel 17
4.4.2 Nouvelle recrudescence des annonces de piratages 18
4.4.3 Faux chantage basé sur des attaques réelles 18
4.5 Annonces diverses 19
4.5.1 Impuissance face à l'usurpation de numéros de téléphone 19
5 Situation 19
5.1 Accès initial 19
5.1.1 Nom d'utilisateur / mot de passe 19
5.1.2 Maliciels (chevaux de Troie) 20
5.1.3 Exploitation des vulnérabilités 21
5.2 Maliciels 22
5.2.1 Diffusion des maliciels 22
5.2.2 Rançongiciels (ransomware) 23

5.3 Systèmes de contrôle industriels (SCI) et technologie opérationnelle (TO) . 27
5.3.1 Tentatives de sabotage dans le cadre de conflits 27
5.3.2 Vulnérabilité de l'approvisionnement énergétique..... 27
5.4 Failles de sécurité 28
5.4.1 Systèmes aux fichiers de configuration publiquement accessibles 28
5.4.2 ProxyNotShell..... 29
5.4.3 Retbleed 30
5.5 Fuites de données..... 31
5.5.1 Métadonnées de fichiers publiés..... 31
5.5.2 Élimination des outils informatiques et des supports de données 32
5.6 Point sur l'Ukraine..... 33
5.6.1 Poursuite des activités dans le cyberespace sans grand succès 33
5.6.2 Des cyberattaques variées aux conséquences multiples 34
5.6.3 Développements à venir..... 35

Management Summary

Thème prioritaire: cybersécurité des PME

La transformation numérique s'opère aussi dans les PME. De nombreux ordinateurs sont aujourd'hui reliés entre eux par des interfaces réseau. Ainsi, des synergies de plus en plus grandes sont créées entre les divers processus, tels que le traitement des commandes, la planification, la production et la logistique, gérés par voie numérique. Cette évolution va de pair avec une augmentation du nombre de systèmes accessibles par Internet, qui requièrent une protection accrue. Or, les PME n'accordent souvent pas assez d'importance à ces questions. C'est pourquoi le rapport du NCSC met l'accent sur la place de la cybersécurité dans les entreprises et sur les points clés de la protection contre les cyberrisques.

L'escroquerie, incident le plus courant

Au deuxième semestre de 2022, le nombre de signalements est resté très élevé, se montant à 17 341, soit un niveau presque identique à celui du premier semestre. Au total, le NCSC a reçu 34 527 annonces l'année dernière. Environ 85 % proviennent de la population, tandis que les 15 % restants émanent d'entreprises, d'associations ou d'autorités. Elles concernent les formes de fraude les plus diverses. Presque un tiers des signalements portent sur des courriels de pseudo-extorsion, soit des courriels de menace prétendument envoyés par les autorités de poursuite pénale. L'arnaque au président et la fraude à la facturation sont également souvent signalées.

Nombre stable d'attaques par rançongiciel

Les annonces relatives à des attaques par rançongiciel sont restées stables et représentent quasiment la moitié des signalements portant sur des maliciels. Sur 76 annonces reçues, un tiers provient de particuliers et deux tiers d'entreprises, lesquelles subissent surtout les assauts du maliciel «Lockbit». Les cybercriminels se servent de ce maliciel non seulement pour chiffrer les données, mais aussi pour les voler et les mettre en ligne si la rançon n'est pas versée. Ces doubles extorsions sont de plus en plus fréquentes. En effet, comme de nombreuses entreprises se protègent désormais contre les rançongiciels en créant des copies de sauvegarde, le simple cryptage des données n'est plus assez lucratif pour les cybercriminels. Dans les cas liés à des rançongiciels, si l'infection initiale n'est pas causée par l'ouverture d'une pièce jointe ou d'un lien transmis par courriel, elle est généralement due à une vulnérabilité ou à une mauvaise configuration.

Nouvelle recrudescence des annonces de piratages

Au deuxième semestre, les annonces de piratages, qui se montent à 276, ont presque doublé par rapport au semestre précédent. Les comptes sur les médias sociaux sont une cible de choix pour les cybercriminels. Ceux-ci se servent par exemple des comptes piratés pour faire chanter les utilisateurs ou diffuser de la publicité pour des offres d'investissement fictives.

Éditorial

On me demande souvent si les PME sont moins sûres que les grandes entreprises. Pour répondre à cette question, il faut d'abord se mettre d'accord sur ce qu'est une PME typique. Une entreprise de marché est réputée être une PME quand elle emploie moins de 250 personnes. En Suisse, 99,7 % des entreprises rentrent dans cette catégorie. Les employés des PME travaillent essentiellement dans la fabrication de marchandises, le commerce, l'entretien et la réparation de véhicules à moteur, la santé ou le social.

On l'aura deviné: il n'existe pas de PME typique, ni de cybersécurité unique pour les PME.. Tout comme dans le cas des grandes entreprises, les conditions offrant une bonne protection face aux cyberattaques sont susceptibles de varier d'une PME à l'autre. Une entreprise de haute technologie de la branche pharmaceutique sera soumise à d'autres conditions qu'une entreprise commerciale à ancrage régional où les facteurs déterminants sont ici les moyens financiers à disposition, le degré de technicité, le modèle d'affaires, la composition du personnel, les structures ainsi que la culture d'entreprise, sans oublier le contexte économique et politique.

Il n'y a donc pas de réponse toute faite à la question posée en amont. Mais il ressort clairement du présent rapport semestriel consacré aux PME qu'elles aussi sont des cibles de cyberattaques. Il pourra s'agir d'attaques opportunistes lancées selon le principe de l'arrosoir, ou d'attaques ciblées contre deses PME intéressantes en termes de droits de la propriété intellectuelle.

Le présent rapport semestriel vise à souligner la vulnérabilité des PME et à indiquer comment les protéger – selon la nature de l'entreprise. Il incombe au Centre national pour la cybersécurité (NCSC) de créer des conditions permettant d'aider encore mieux les PME à assurer leur propre sécurité. N'hésitez donc pas à nous communiquer vos réactions au présent rapport et vos éventuelles idées applicables aux PME et aux cyberrisques.

Aussi différentes les PME soient-elles, elles ont un point commun: leur petit nombre d'employés ne leur permet généralement pas de s'offrir un vaste service de sécurité. Cependant la cybersécurité exige une approche exhaustive, axée sur les affaires. Par conséquent, tant la direction des entreprises que leur personnel doivent posséder des cyberconnaissances dans leur domaine d'activité. Les PME jouiront bientôt d'un avantage non négligeable, dans une économie toujours plus numérisée, pour autant qu'elles acquièrent le savoir requis sans que leur activité économique en pâtisse. Dans ce pays principalement constitué de PME, qu'est la Suisse, il faut pour cela que les autorités, l'économie, le monde scientifique et la société coopèrent. Saisissons donc tous ensemble cette opportunité!

Florian Schütz, délégué fédéral à la cybersécurité

2 Thème prioritaire: cybersécurité des PME

2.1 La numérisation gagne du terrain

Il n'est guère possible d'échapper à la numérisation, bien des gens ne s'imaginent plus vivre sans Internet. Les ordinateurs sont désormais présents dans presque tous les domaines de l'économie et de la société, du moins en matière de communication et d'administration. En outre, la production n'est plus envisageable sans ordinateur dans bien des cas. Un grand nombre de ces appareils sont reliés entre eux par des interfaces réseau et, sous une forme ou une autre, avec les réseaux bureautiques destinés aux tâches administratives. Les commandes, la planification, la production, la logistique et la facturation sont de plus en plus imbriquées dans des processus partiellement ou entièrement automatisés.

Recommandations:

Ne numérisez qu'avec précaution: ne pensez pas qu'aux opportunités et aux avantages promis, mais pensez aux nouvelles situations de dépendance et aux risques qui s'ensuivent. Prenez d'emblée en compte la cybersécurité à chaque étape de votre transformation numérique.

2.2 Activité de base et outils de soutien

La cybersécurité devrait être acquise pour les entreprises offrant des services entièrement numériques – après tout, elles ne peuvent travailler que si leurs systèmes fonctionnent correctement. L'informatique joue cependant un rôle de soutien dans la plupart des entreprises, qui se consacrent en priorité à leur activité de base, soit la fabrication de produits ou la fourniture de services. Tant que l'informatique leur donne satisfaction, les entreprises ne lui accordent guère d'attention et même en cas de dysfonctionnement, il est souvent possible de s'organiser autrement. Une panne totale peut toutefois être lourde de conséquences: si une entreprise ne peut plus gérer sa planification et ses décomptes, une interruption de l'activité et des retards sont à prévoir, ce qui risque à son tour d'affecter le bilan. Par ailleurs, les atteintes à la propriété intellectuelle (espionnage économique) ou un paiement effectué à la mauvaise adresse peuvent entraîner d'importantes répercussions financières.

Conclusion / Recommandation:

Comme pour n'importe quel outil de travail, il faut veiller à l'entretien et à la maintenance des ressources informatiques. Faites-vous conseiller et assister par des spécialistes. La norme minimale pour les TIC et les normes minimales par secteur élaborées par l'Office fédéral pour l'approvisionnement économique du pays (OFAE) en collaboration avec les associations économiques ont valeur de recommandations et fournissent d'utiles points de repère aux entreprises.

2.3 Exploitation informatique et cybersécurité

Dans les PME, les responsables de l'exploitation du parc informatique sont souvent aussi chargés de la cybersécurité. Or dans bien des cas, ils n'accomplissent cette dernière tâche qu'à titre accessoire. Comme l'entretien du parc informatique leur prend déjà beaucoup de temps, la cybersécurité risque d'être négligée. Typiquement, seules les entreprises d'une certaine taille considèrent la cybersécurité comme une fonction à part entière. En informatique, des exigences précises en matière de fonctionnalités sont en place et la performance doit pouvoir être mesurée, tandis que la cybersécurité, elle, relève de la gestion des risques où il incombe à la direction d'en assurer le pilotage. Il est notamment recommandé de prévoir un poste budgétaire spécifique pour la cybersécurité afin que des ressources soient expressément consacrées à la prise de mesures qui s'imposent.

Conclusion / Recommandation:

L'exploitation ainsi que la sécurité de l'infrastructure informatique ont beau être liées, ce sont deux champs d'action différents. Les décisions d'allocation de ressources aux mesures de cybersécurité relèvent de la gestion des risques et doivent être prises dans ce cadre.

2.4 Recours à des prestataires de services externes

Tous les bureaux sont équipés d'ordinateurs, cependant toutes les entreprises n'ont pas leur propre réseau. Lorsque certaines tâches doivent néanmoins pouvoir être accomplies depuis plusieurs appareils, ces entreprises ont aujourd'hui la possibilité d'externaliser le stockage des données et l'exploitation de leurs programmes dans le nuage. Une telle approche peut naturellement aussi être judicieuse pour décharger les réseaux d'entreprises ou accroître la flexibilité des opérations. De plus, les prestataires de services en nuage, spécialisés dans la fourniture de prestations informatiques, possèdent en général de solides connaissances en matière de cybersécurité. Une autre possibilité encore consiste à mandater un fournisseur externe de services de cybersécurité.

Conclusions / Recommandations:

Il convient de veiller à régler la sécurité de façon adéquate dans les contrats avec des prestataires de services externes. Outre l'adoption d'éventuelles mesures spécifiques de protection et de défense contre les cyberattaques (par ex. attaques DDoS, fuites de données et rançongiciels), il faut également aborder la question des copies de sauvegarde des données (*back up*) et de l'obligation de déclarer en cas d'incident.

2.5 Prévention et préparation aux incidents

En plus des mesures de protection à caractère technique, il est important de former les collaborateurs internes, qui constituent un important maillon de la chaîne de défense, à la gestion des cyberrisques. Même s'il n'est pas certain qu'ils reconnaissent d'eux-mêmes tous les courriels malveillants, la sensibilisation aide déjà à limiter les risques. En effet, le risque d'attaque fructueuse diminue fortement si les destinataires, en cas de soupçon ou de doute, ne suivent pas les instructions figurant dans le courriel, ne cliquent pas sur un lien qu'il

renferme ni n'ouvrent de fichier annexé, mais au contraire décident de faire contrôler le courriel suspect à l'interne ou invitent l'expéditeur (présumé) à leur confirmer l'authenticité du message.

En dépit de toutes les mesures de prévention et de sensibilisation, un incident ne peut jamais être exclu. Afin d'être parées à toute éventualité, les entreprises gagnent à élaborer des plans d'urgence à l'interne: les procédures à suivre et les processus d'escalade doivent être définis et testés. Les réflexions préalables sur la communication de crise (interne et externe) allégeront également les pressions subies en cas d'incident: elles permettent de prévenir de nombreuses erreurs et aident ainsi à bien gérer une cyberattaque. Il est également recommandé d'établir à l'avance des contacts avec des prestataires de services susceptibles d'intervenir en cas d'incident informatique (*incident response*), pour ne pas devoir rechercher de tels partenaires dans l'urgence.

Conclusions / Recommandations:

La cybersécurité n'est pas un état susceptible d'être atteint, mais plutôt un processus évolutif, basé sur des mesures techniques, organisationnelles ou relatives au personnel[1] oùla formation des collaborateurs y occupe une place centrale.

Malgré tous les investissements réalisés dans la prévention, un cyberincident ne peut jamais être entièrement exclu. En plus d'élaborer des plans de gestion des incidents, il faut donc aussi réfléchir à l'avance à la communication interne et externe à adopter en pareil cas[2].

3 Contributions d'invités: cyberattaques subies

3.1 Cyberattaque contre les transports publics lucernois (VBL)

Contribution de Franz Theiler, chef informatique de VBL AG

Les transports publics lucernois (VBL) ont été victimes d'une cyberattaque ciblée dans la nuit du samedi 14 mai 2022. Au petit matin, des collaborateurs du centre d'exploitation ont signalé une panne au service de piquet informatique. Les spécialistes ont rapidement compris qu'ils avaient affaire à un événement extraordinaire. Les systèmes informatiques ont été mis hors ligne et le réseau informatique des VBL déconnecté d'Internet.

Le responsable de la gestion des crises a convoqué l'état-major d'urgence. La police lucernoise a été informée des faits désormais prouvés, et l'incident a été signalé au NCSC. Dans la matinée, la cellule de crise et la direction ont encore communiqué la cyberattaque aux principales parties prenantes, soit les autorités, les entreprises de transport et les autres acteurs du secteur, le personnel ainsi que les médias.

Dès le samedi à midi, l'équipe informatique des VBL et des collaborateurs de son prestataire informatique externe se sont retrouvés dans les locaux des VBL afin de se concerter et d'entreprendre les travaux nécessaires. Il convient de souligner que le service informatique

1 Sécurité de l'information: aide-mémoire pour PME (ncsc.admin.ch)

2 Que faire en cas d'incident? (ncsc.admin.ch)

des VBL exploite des systèmes de transports publics critiques nécessitant une disponibilité élevée pour des clients tant internes qu'externes, répartis dans toute la Suisse. Le parc informatique est donc très complexe, développé dans un environnement Windows et Linux. Les activités visant à comprendre et à endiguer la crise ont aussitôt commencé. Le maliciel a pu être identifié et éliminé. Les systèmes de base nécessaires ont ensuite été rétablis et isolés. Les systèmes ont été restaurés par étapes à partir de la dernière sauvegarde, soumis à des vérifications puis remis en production, selon un processus contrôlé et éprouvé. La collaboration parfaite entre les collaborateurs, les fournisseurs et les experts ont permis de maîtriser rapidement la crise et de récupérer toutes les données. La police lucernoise a apporté son soutien compétent sur les questions de science forensique. Enfin, des mesures ciblées ont servi à renforcer ponctuellement la sécurité au cours de la remise en état du système.

La cyberattaque n'a pas affecté la clientèle. Seuls les écrans d'affichage des départs ont dû être éteints pour des raisons de sécurité. Rétrospectivement, on peut dire que l'entreprise était bien préparée à une telle situation de crise. Les unités d'affaires sont parvenues en tout temps à poursuivre l'exploitation sous une forme bien organisée, quoique restreinte. Durant plusieurs semaines, la cellule interne de crise s'est réunie au quotidien, se concertant ensuite avec la direction qui a notamment servi d'intermédiaire entre les services spécialisés.

Dans ces circonstances difficiles, le NCSC a rapidement offert aux VBL le soutien dont ils avaient besoin. Les informations fournies ont apporté aux VBL de précieux indices et des certitudes sur l'identité des auteurs et leur possible mode opératoire. Nous tenons encore à remercier le NCSC pour les deux brillants exposés qu'il a présentés lors de séances d'information des cadres et du personnel, où il a sensibilisé avec enthousiasme et passion les collaborateurs des VBL à la menace des cyberattaques. En tant qu'exploitant d'infrastructures critiques, les VBL peuvent participer aux séances d'échange organisées par le NCSC et profiter des nouveautés régulièrement proposées en matière de sécurité.

3.2 Attaque par rançongiciel: le point de vue de la police

Contribution de la Brigade criminalité numérique, Police cantonale bernoise

Une attaque par rançongiciel consiste à chiffrer des données et à exiger une rançon, généralement en cryptomonnaie. De telles attaques sont automatisées et émanent de groupes cybercriminels bien organisés. Si l'entreprise lésée n'entre pas en matière sur la demande de rançon, elle s'expose à ce que des informations sensibles concernant ses clients soient divulguées et vendues sur le darknet. Ce genre d'attaque a donc aussi des effets sur la réputation de l'entreprise.

Dans un cas récent, la victime avait signalé l'attaque à la centrale téléphonique de la police, qui a informé la Brigade criminalité numérique. Celle-ci a désigné des enquêteurs responsables et fait appel à des spécialistes de la forensique numérique pour définir les premières mesures à prendre. Un cas de rançongiciel requiert toujours la collaboration interdisciplinaire de différents acteurs ainsi que dans le cas présent, des échanges avec l'entreprise concernée pour collecter les informations nécessaires, qui permettront notamment de formuler des instructions concrètes. Une bonne coopération est déterminante à bien des égards. En effet, lors d'une attaque par rançongiciel, l'entreprise s'intéresse moins aux enquêtes et recherches qu'à la restauration de ses données et à la reprise de son activité.

En l'espèce, outre la police, une entreprise de sécurité privée est rapidement intervenue pour aider à remettre en état l'infrastructure. Cette collaboration a porté ses fruits; mais d'ordinaire, le succès d'une telle collaboration dépend de la disposition de l'entreprise concernée à contribuer aux investigations, et de l'importance qu'elle accorde à ces dernières.

Comme une attaque par rançongiciel s'avère techniquement complexe, des entretiens et des séances s'imposent encore pour identifier les points faibles ayant permis l'intrusion.

L'entreprise attendait de notre part des conseils sur les démarches à entreprendre, outre l'investigation du cas, mais surtout aussi des renseignements juridiques, sachant qu'une telle attaque peut léser d'autres parties et affecter des données sensibles.

Globalement, l'entreprise a réagi de façon exemplaire en l'espèce, en signalant aussitôt l'incident à la police et en faisant appel à une entreprise de sécurité privée, ce qui a permis un déroulement sans accroc des opérations entre les spécialistes de la Brigade criminalité numérique et le domaine de la forensique numérique. Nous déconseillons dans tous les cas d'entrer en matière quant à la demande de rançon, ce qui reviendrait à cofinancer le crime organisé. La disposition à payer dépend souvent de la quantité de données chiffrées, de la probabilité d'arriver à les récupérer, mais aussi du montant de la rançon exigée. L'entreprise a agi de manière exemplaire et n'a jamais songé à payer la rançon demandée. Pour éviter un tel scénario, il est conseillé de sensibiliser les collaborateurs aux risques du cyberespace et d'investir dans des cours aussi bien que dans une infrastructure sûre. Si l'entreprise a rapidement pu reprendre son activité commerciale, il lui a fallu plusieurs semaines pour complètement régler l'incident.

4 Annonces émanant d'entreprises ou de particuliers

4.1 Aperçu des annonces de cyberincidents reçues

Cette année encore, le nombre d'annonces a considérablement augmenté. Pour un total de 34 527 annonces, contre 21 714 l'année précédente, on n'observe pas de doublement des cas, cependant la hausse en chiffres absolus (12 813 annonces de plus qu'en 2021) est plus importante qu'en 2021 (10 881 annonces de plus qu'en 2020). Cette progression est due en partie à la notoriété croissante du NCSC et à son formulaire d'annonce. La nouvelle augmentation a toutefois d'autres causes encore, notamment une recrudescence des courriels de menaces prétendument expédiés par la police (voir chap. 4.2.1) et à l'usurpation de numéros de téléphone (*spoofing*) (voir chap. 4.5.1). Le fait qu'au deuxième semestre 2022, avec au total 17 341 cas signalés, le nombre d'annonces ait été quasiment identique à celui du premier semestre, marque toutefois une rupture avec la croissance ininterrompue enregistrée depuis trois ans.

Environ 85 % des annonces proviennent de la population, le solde émanant d'entreprises, d'associations ou d'autorités. Les principaux phénomènes signalés par les entreprises sont l'arnaque au président (190 annonces au deuxième semestre 2022), le piratage de la messagerie professionnelle pour des fraudes à la facturation (45 annonces), les rançongiciels (54 annonces) et les attaques affectant la disponibilité ou attaques DDoS (13 annonces). En outre, les cas de fausse-extorsion (*fake extortion*) observés ne se limitent pas aux particuliers. Il existe des variantes s'adressant directement aux entreprises, à l'instar des faux courriels d'extorsion visant les administrateurs de sites Internet évoqués au chap. 4.4.2. Les tentatives

d'hameçonnage ne se limitent plus aux particuliers depuis longtemps déjà et toujours plus d'employés subissent de telles attaques ciblées au travail. Les données d'accès à Office 365 sont particulièrement convoitées, comme le montre le chap. 4.3.2.

Annonces au NCSC au deuxième semestre 2022 (par semaine)

Fig. 1: Nombre d'annonces parvenues au NCSC de juillet à décembre 2022, voir aussi Chiffres actuels (ncsc.admin.ch).

Annonces au NCSC au deuxième semestre 2022 (par catégorie)

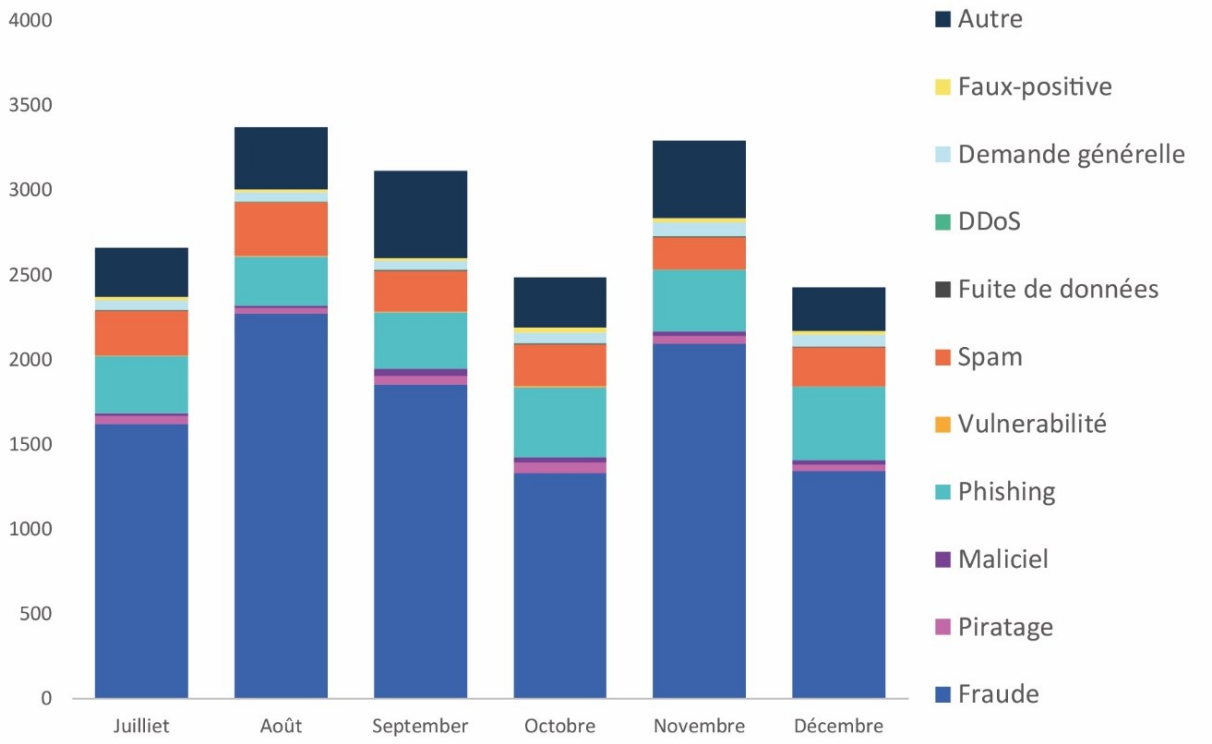

Fig. 2: Annonces effectuées au NCSC au deuxième semestre 2022, par catégorie, voir aussi Chiffres actuels (ncsc.admin.ch).

4.2 L'escroquerie, incident le plus courant

4.2.1 Variantes de faux courriels de menace de la police

Au deuxième semestre 2022, les courriels de menace envoyés au nom d'autorités policières ont à nouveau été les cyberincidents les plus souvent signalés au NCSC, avec 5179 annonces. Il n'est donc pas étonnant que lors de la 36e semaine, soit la période qui a enregistré le plus grand nombre d'annonces en 2022, les faux courriels de menace de la police représentaient 418 des 954 annonces. Les auteurs de ce genre de messages prétendent que le destinataire du courriel est accusé d'un délit grave (typiquement lié à la pédopornographie) et menacent d'engager des poursuites pénales si la personne ne paie pas. Au total, ce sont plus de 11 051 annonces qui rentrent dans cette catégorie en 2022. De ce total, 5179 annonces, soit un tiers des annonces de l'année, ont été enregistrées au second semestre.

Fig. 3: Variantes de courriels de menaces infondées envoyés au nom d'autorités de poursuite pénale avec des noms d'expéditeurs et des logos hétéroclites. En bas à droite, les escrocs ont usurpé le nom du NCSC, mais en se trompant de logo.

Pour conférer un aspect officiel à leur opération de chantage, les escrocs reprennent de manière plus ou moins aléatoire les noms et logos de diverses autorités de poursuite pénale tant suisses qu'étrangères. Parmi les expéditeurs mentionnés au deuxième semestre 2022 figurent par exemple les autorités de police des cantons du Valais, de Vaud et de Genève. Au niveau international, on trouve notamment Europol et Interpol, ainsi que les polices française, belge ou néerlandaise. Le NCSC n'a pas été épargné et apparaît comme expéditeur de tels messages. Les maîtres chanteurs ont toutefois repris par erreur le logo de l'autorité britannique chargée de la cybersécurité, dont l'acronyme est le même. La variante la plus répandue consiste toutefois en courriels censés provenir de l'Office fédéral de la police (fedpol). Les documents annexés portent la signature de sa directrice Nicoletta Della Valle ou celle de l'ex-responsable du Département fédéral de justice et police (DFJP), la conseillère fédérale Karin Keller-Sutter.

4.2.2 Attaques visant les administrateurs de sites Internet

Des cas d'arnaques au chantage visant des administrateurs de sites Internet ont également été observés au deuxième semestre 2022. Au total, 114 annonces concernant cette forme d'attaque sont parvenues au NCSC. Le message des escrocs, généralement expédié à l'aide du formulaire de contact du site Internet mais parfois aussi par courriel, prétend que le site Internet a été piraté et les banques de données qu'il héberge pillées. Il s'achève par une menace de publication des données. Toutes ces requêtes sont rédigées exactement de la même manière et sont conçues comme les faux courriels dits de sextorsion. Ce genre de chantage reprend typiquement les mêmes adresses bitcoin dans tous les courriels envoyés aux entreprises. Si quelqu'un devait effectuer un paiement, les maîtres chanteurs ne seraient donc même pas en mesure d'identifier la victime qui a payé la rançon. Il s'agit d'un mensonge classique.

Une nouvelle variante de cette escroquerie a fait son apparition durant la période sous revue: de soi-disant chercheurs se sont adressés à des responsables de la sécurité pour leur signaler de prétendues vulnérabilités de leurs systèmes. Les auteurs du courriel demandaient, à la fin de leur message, une prime pour le signalement de ladite vulnérabilité dans le cadre du *processus de divulgation responsable*. Les signalements ne se rapportaient toutefois pas à une véritable faille de sécurité, mais simplement à l'absence de la fonctionnalité *HTTP Strict Transport Security (HSTS)*[3] sur le site Internet de l'entreprise. Bien que l'implémentation du HSTS soit fortement recommandée, le fait qu'un site n'utilise pas ce mécanisme peut difficilement être qualifié de faille de sécurité classique. On trouve sur Internet de nombreux sites sur lesquels même les profanes peuvent s'assurer de la présence des éléments de sécurité usuels sur une page donnée. Les escrocs recourent à de tels sites et misent sur le sentiment d'insécurité des administrateurs de sites Internet pour tenter d'obtenir une récompense financière.

[3] Lorsque le service HSTS est activé sur un site, un en-tête supplémentaire est utilisé dans le protocole HTTPS. Ce dernier force les navigateurs à passer par une connexion chiffrée dès leur premier accès au site.

Hi Team,I am a security researcher and found a vulnerability on your website.

Vulnerability : Non - secure requests are not automatically upgraded to HTTPS | HSTS missing

I am hoping to receive a reward for the responsible disclosure of vulnerability.

Looking forward to hearing from you soon.
Kind Regards,

Fig. 4: Courriel signalant une prétendue faille de sécurité du serveur Internet et réclamant une prime.

4.2.3 Fraude à l'investissement

Avec 219 annonces et des dommages qui dépassent 4 millions de francs, la fraude à l'investissement compte au deuxième semestre 2022 aussi parmi les phénomènes signalés au NCSC qui ont causé le plus lourd préjudice financier, sachant que ce montant ne comprend que les dommages signalés par les victimes et que tous les cas ne sont pas communiqués au NCSC. La somme réelle des dommages est donc certainement beaucoup plus élevée. Les victimes sont incitées par différents modes opératoires à investir leur argent sur des sites douteux. Le piège le plus connu consiste en promesses publicitaires fictives, où des célébrités expliquent comment gagner rapidement beaucoup d'argent. En effet il y a quelques années, des interviews fictives de Roger Federer circulaient et des offres frauduleuses ont fait plus tard référence à l'émission télévisée *Die Höhle der Löwen* (équivalent de *Qui veut être mon associé*). Entre-temps, même les noms des conseillers fédéraux sont régulièrement utilisés pour ce genre de publicité. En tout, le NCSC a reçu au deuxième semestre 469 annonces de publicités malhonnêtes promettant des gains importants en peu de temps. Une telle arnaque semble être en perte de vitesse par rapport au semestre précédent, où 619 annonces avaient été reçues. Même si le NCSC continue de recevoir des annonces de victimes s'étant laissées piéger par de telles publicité frauduleuses, le taux de réussite de ces dernières demeurent faibles. Aussi les escrocs doivent donc régulièrement trouver de nouvelles astuces pour convaincre leurs victimes de leur confier leur argent. Une autre méthode répandue consiste à prendre contact de manière anodine via les réseaux sociaux ou les sites de rencontre. Les criminels cherchent patiemment à gagner la confiance de leur victime pour l'amener, dans un second temps, à faire un placement prétendument lucratif. Ils affirment avoir eux-mêmes placé leur argent et s'être enrichis par de tels investissements.

4.3 Annonces de phishing

Au deuxième semestre 2022, le guichet unique géré par le NCSC a reçu 2177 annonces de phishing. Les notifications sont en légère baisse par rapport au semestre précédent, où 2544 cas avaient été signalés. Les courriels de phishing cherchant à obtenir les données de cartes de crédit demeurent certes majoritaires. Mais les pirates convoitent toujours plus d'autres données, comme les identifiants de messagerie. Comme l'explique le chap. 4.3.2, ils s'intéressent surtout aux comptes professionnels, sans dédaigner pour autant les comptes de messagerie privés. Ces derniers sont en effet devenus les sésames permettant d'accéder à une multitude de boutiques et de services sur Internet. En cas d'oubli du mot de passe d'un

prestataire en ligne, il est généralement possible de le réinitialiser à partir d'un tel compte. Par conséquent, il suffit aux escrocs de connaître le mot de passe d'un compte de messagerie pour accéder à de nombreux comptes. Ils pourront ensuite se procurer frauduleusement des biens et des services, en s'introduisant de cette manière sur les comptes de boutiques en ligne. Entre-temps, les escrocs tirent également parti dans leurs arnaques au chantage des comptes de messagerie ou des comptes sur les réseaux sociaux qu'ils ont piratés, dans le but de déstabiliser leurs victimes (voir chap. 4.4.2).

Nombre de sites de phishing signalés par semaine

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

4.3.1 L'art d'inventer des histoires plausibles

Courriels signalant des factures de Swisscom ou de Sunrise censées avoir été payées à double, SMS mentionnant le remboursement de billets CFF ou la livraison de paquets fictifs: de tels messages ont beau reposer sur des histoires inventées de toutes pièces, leurs destinataires risquent de se faire avoir, car bien des gens attendent un paquet, ont opté pour le recouvrement direct chez Sunrise ou Swisscom, ou ont déposé auprès des CFF une demande de remboursement. En pareil cas, les escrocs procèdent à un calcul des probabilités et privilégient dans leurs histoires des opérations couramment accomplies par la plupart des gens. Un exemple classique vient des fausses notifications des divers services d'expédition, qui amènent la victime à ouvrir une page la priant d'indiquer les données de sa carte de crédit. Avec 532 annonces, près d'un quart des annonces de phishing sont liées à des communications frauduleuses concernant un colis à récupérer. Les commandes en ligne ont explosé depuis la pandémie de coronavirus. La probabilité que quelqu'un attende effectivement un paquet est donc bien réelle. À supposer que 10 % de la population effectue une commande en ligne par semaine, une telle histoire interpellera 10 000 personnes, si les pirates expédient 100 000 courriels par semaine. Dans leurs tentatives de phishing prétextant que des factures télécom ont été payées à double, les escrocs mettent également toutes les chances de leur côté. En adressant les prétendues factures Swisscom payées deux fois aux adresses *bluewin.ch* et celles de Sunrise aux adresses *sunrise.ch*, il y a de fortes probabilités que l'histoire inventée convienne et que les destinataires se laissent duper par la tentative de

phishing. À la fin de l'année 2022, les escrocs se sont concentrés sur de prétendus remboursements des CFF. Là aussi, l'histoire se révèle adaptée dans de nombreux cas, à en juger par les nombreuses annonces au NCSC par des personnes qui attendaient réellement un remboursement de la part des CFF.

Fig. 6: Tentative de phishing basée sur le prétendu remboursement d'un billet CFF.

4.3.2 Professionnalisation du phishing basé sur Office365: personnel des entreprises pris pour cible

Les données d'accès à Office365 intéressent tout particulièrement les cybercriminels, car de tels comptes peuvent servir de point de départ à de nouvelles attaques, par exemple au piratage de messageries professionnelles en vue de l'envoi de factures trafiquées. Avec 45 cas signalés au NCSC durant la période sous revue, dont un où la perte avoisinait un demi-million de francs, il s'agit d'une des fraudes ayant le plus grand potentiel dommageable. Là encore, le montant des dommages non signalés est probablement élevé. Les comptes pillés sont passés au crible, à la recherche des factures envoyées. Les escrocs modifient alors le numéro IBAN à leur profit. La facture est ensuite réexpédiée sous un prétexte quelconque au client, avec la prière d'utiliser le nouveau numéro IBAN. En accédant aux comptes professionnels Office365, les auteurs obtiennent des données internes dont ils pourront se servir pour lancer des attaques d'ingénierie sociale contre d'autres employés ou pour faire chanter l'entreprise. Il arrive souvent que les escrocs mettent également en place une règle de redirection des courriels afin de recevoir automatiquement une copie de tous les messages entrants de la victime. De cette manière, si la personne devait s'apercevoir qu'elle a été victime de phishing et qu'elle modifie ses données d'accès, les auteurs continueront de recevoir tous ses courriels. Il n'est donc pas étonnant que les cybercriminels fassent tout leur possible pour mettre la main sur les données d'accès des collaborateurs. Leurs tentatives dans ce sens témoignent d'un professionnalisme croissant et sont donc toujours plus difficiles à reconnaître. Il faudrait dès lors que les collaborateurs participent à des formations régulières, et que l'on introduise autant que possible une authentification à deux facteurs. Celle-ci offre un niveau de protection supplémentaire contre le piratage des comptes Office365.

Fig. 7: Prétendue proposition de projet à télécharger à partir d'un serveur. Un document flouté s'affiche. Pour l'ouvrir, il faut toutefois commencer par indiquer son mot de passe Office365.

4.4 Annonces de maliciels et de piratages

4.4.1 Nombre stable d'attaques par rançongiciel

Au deuxième semestre 2022, 155 annonces portant sur des maliciels ont été enregistrées. Le recul est significatif par rapport au semestre précédent, où les cas signalés avaient été pratiquement quatre fois plus nombreux, soit 592 annonces. La raison tient à l'absence de grandes vagues. Il y a un an, 405 annonces concernaient le maliciel *Flubot*. Or aucun cas imputable a *Flubot* n'a été notifié durant la période sous revue.

Les annonces portant sur des rançongiciels sont restées stables. Avec 76 cas, elles représentent presque la moitié des annonces dans la catégorie des maliciels. Quant aux entreprises, elles subissent surtout les assauts du maliciel *Lockbit*. Celui-ci est connu pour chiffrer les données ou les voler et les mettre en ligne en cas de non-versement d'une rançon. Ce genre de double extorsion a pris de l'ampleur et risque d'en prendre encore en 2023. De multiples entreprises, visées par des rançongiciels, ont recouru à une stratégie de sauvegarde adéquate. Comme le simple chiffrement des données n'est plus assez lucratif pour les malfaiteurs, ils menacent désormais de les divulguer. Les autres familles de rançongiciels impliquées au semestre écoulé dans les attaques contre des entreprises sont *Play*, *Medusalocker*, *Blackcat*, *Magniber* et *Makop*. La plupart du temps, le vecteur d'infection n'est pas encore connu au moment de l'annonce. Mais l'infection initiale est généralement due à

une vulnérabilité ou à une mauvaise configuration. C'est ce que confirme une étude de Microsoft, selon laquelle des erreurs générales de configuration des logiciels et des appareils expliquent près de 80 % des attaques dues à des rançongiciels[4]. Autrement dit, une gestion en temps utile des correctifs logiciels (*patch management*), le réexamen régulier de la configuration du système ainsi que l'utilisation systématique de l'authentification à deux facteurs pour l'accès aux ressources réduiront significativement les risques d'attaque par un rançongiciel.

Dans leurs attaques contre des particuliers, les pirates continuent de se concentrer sur les appareils de stockage en réseau (NAS). Dans ce contexte, le maliciel *Deadbolt* sort du lot, avec sept annonces. Les appareils accessibles directement depuis Internet sont particulièrement exposés. Ils font l'objet d'analyses systématiques quant à leurs vulnérabilités ou leur mauvaise configuration, qui permettent, par exemple, de repérer les mots de passe faibles. Il est donc primordial de constamment actualiser de tels systèmes et d'en protéger l'accès de manière adéquate.

Qakbot est resté une des familles de maliciels les plus actives: 20 annonces la concernant sont parvenues au NCSC au deuxième semestre 2022. Ce maliciel est propagé par courriel. *Qakbot* a pour particularité de se référer à des conversations électroniques existantes obtenues lors de piratages antérieurs. Les escrocs cherchent ainsi à inspirer confiance à leurs destinataires qui, en reconnaissant l'échange, penseront avoir affaire à un expéditeur connu d'eux. Ces manœuvres visent à inciter la victime à cliquer sur un lien malveillant.

4.4.2 Nouvelle recrudescence des annonces de piratages

Les annonces relevant du piratage ont fortement augmenté. Avec 276 annonces, leur nombre a quasiment doublé par rapport au semestre précédent. Les comptes sur les réseaux sociaux sont très convoités, avec 108 annonces. Les escrocs s'en servent entre-temps pour conférer davantage de poids à leur chantage lors d'attaques de *fake-sextortion* (voir ci-dessous). Souvent aussi, ils utilisent les comptes piratés sur les réseaux sociaux pour promouvoir des investissements frauduleux. Ils privilégient pour de telles pratiques les comptes ayant de nombreux abonnés, afin de diffuser leurs informations sur des transactions douteuses auprès d'un maximum de victimes potentielles.

4.4.3 Faux chantage basé sur des attaques réelles

Les attaques de *fake sextortion* n'ont longtemps été qu'une opération de bluff. Le mode opératoire est le suivant: les escrocs prétendent dans un courriel qu'ils ont rassemblé des photos ou des vidéos sur lesquelles on verrait le destinataire du courriel surfer sur des sites pornographiques. Les maîtres chanteurs demandent une rançon et menacent de publier les images si la somme exigée n'est pas versée dans un délai donné. Durant la période sous revue, le NCSC a reçu 1138 annonces de courriels de *fake sextortion*. Il s'agit normalement d'un bluff, car les escrocs n'ont pas accès à l'ordinateur de la victime mais espèrent l'intimider suffisamment pour qu'elle leur verse la rançon demandée. Au semestre sous revue, il est toutefois arrivé que peu avant de recevoir un tel courriel ou aussitôt après, la victime se soit fait pirater son compte de messagerie et divers comptes sur les réseaux sociaux. Dans 33 cas

[4] Cyber Signals (microsoft.com)

au total, les escrocs y avaient publié du contenu pornographique, ce qui avait abouti au blocage immédiat des comptes et à une notification du réseau dans ce sens. Les escrocs cherchaient ainsi à effrayer leur victime, pour l'amener à leur verser de l'argent. Les données d'accès utilisées provenaient de précédantes fuites de données ou d'attaques de phishing. Il est vrai que la variante basée sur des comptes piratés reste très rare parmi les courriels de *fake sextortion* signalés. Autrement dit, les combinaisons d'identifiants et de mots de passe n'étaient plus actuelles et n'ont pas fonctionné pour chaque victime. Il devait s'agir de paires d'identifiants uniques obtenues à un prix dérisoire sur le darknet.

4.5 Annonces diverses

4.5.1 Impuissance face à l'usurpation de numéros de téléphone

Les annonces de numéros de téléphone usurpés ont tout simplement explosé. Les cybercriminels manipulent le numéro de façon à ce qu'au lieu du vrai numéro, la victime voit s'afficher un autre, susceptible de la mettre en confiance. Alors qu'il en avait enregistré 26 au total en 2021, le NCSC a reçu plus de 781 annonces rien qu'au second semestre 2022. Ce bond est dû à une nouvelle tactique employée par des centres d'appels douteux sis à l'étranger. Afin d'inciter leurs victimes à décrocher, les escrocs utilisent des numéros de téléphone suisses quelconques. Cette démarche en apparence anodine entraîne des conséquences désagréables pour la personne à laquelle appartient le numéro. En cas d'appel manqué, si le numéro s'affiche à l'écran, de nombreuses personnes rappellent, et le propriétaire du numéro se retrouve submergé. Comme les centres d'appels utilisent le même numéro pendant des semaines, voire des mois, la patience de la victime est mise à rude épreuve.

Malheureusement, il est difficile d'agir contre ce tourment. Puisque les centres d'appels sont établis à l'étranger, les opérateurs téléphoniques suisses ne sont pas tenus de vérifier l'attribution des numéros de téléphone. Ceux-ci ne sont en effet soumis à cette contrainte que si les appels proviennent de leur réseau. Si les appels ne cessent pas, il n'y a pas d'autre choix que de changer de numéro.

5 Situation

5.1 Accès initial

Les cybercriminels pratiquent la division du travail et se spécialisent dans certaines étapes des cyberattaques. Obtenir un accès à distance à des systèmes informatiques ou l'accès à des comptes utilisateurs constitue la première étape de la plupart des cyberattaques. Un tel accès initial peut s'obtenir de différentes manières et, une fois établi, être mis à disposition d'autres acteurs pour qu'ils en tirent parti.

5.1.1 Nom d'utilisateur / mot de passe

Les données d'ouverture de session s'obtiennent généralement par phishing (voir chap. 4.3). Autrement dit, ce sont leurs légitimes propriétaires qui les communiquent à leur insu aux escrocs. Par ailleurs, des maliciels (*Keylogger*) peuvent enregistrer de telles paires d'identifiants lorsqu'elles sont saisies sur un appareil infecté.

Les pirates s'introduisent souvent dans les réseaux d'entreprises en subtilisant les données d'accès à distance par les protocoles *Remote Desktop Protocol* (RDP) ou *Virtual Private Network* (VPN).

Recommandation:

L'identification à deux ou plusieurs facteurs offre par exemple une protection contre cette menace. En pareil cas, la combinaison d'un nom d'utilisateur et d'un mot de passe ne suffit plus pour accéder au système ou au compte d'utilisateur sécurisés. Il faut encore indiquer une autre information, comme un code unique envoyé sur le téléphone mobile associé au compte, ou parfois autoriser la demande d'accès via une application d'authentification .

5.1.2 Maliciels (chevaux de Troie)

Les maliciels qui créent une porte dérobée après avoir été installés restent une méthode très répandue d'accès initial au système des victimes.

Le vecteur de propagation favori de ces 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 guerre en Ukraine, des catastrophes naturelles ou des manifestations sportives sont parfois utilisées pour piquer la curiosité de la victime. L'urgence est fréquemment simulée pour inciter les destinataires à effectuer des actions sans réfléchir. De tels courriels envoyés en masse sont appelés spams malveillants (malspams). Parfois aussi, les escrocs se réfèrent à d'anciens échanges de courriels interceptés sur des comptes de messagerie compromis ou des serveurs de messagerie piratés pour s'adresser directement aux personnes ayant participé à ces conversations et pour leur envoyer un cheval de Troie. Cette technique de détournement de fils de conversation de courriels porte le nom de *thread hijacking*.

Une autre variante visant à amener les internautes à installer un maliciel consiste à acheter des espaces de publicité en ligne ou à publier des résultats de moteurs de recherche sponsorisés (placement de publicité malveillante ou *malvertising*). Les victimes s'imaginent que l'annonce leur fera obtenir le logiciel qu'elles recherchent, qui peut être un navigateur, une application de communication ou un lecteur vidéo. Or un cheval de Troie s'installe en même temps que le logiciel (gratuit). Une méthode similaire consiste à attirer par un lien publicitaire les utilisateurs sur une page leur signalant que leur navigateur est obsolète et qu'une mise à jour s'impose. Comme ce genre de site reconnaît le navigateur utilisé, la page est adaptée de manière dynamique au type de navigateur. Un clic sur le bouton de mise à jour a pour effet de télécharger un fichier qui, lors de son exécution, installera le cheval de Troie. De telles fausses mises à jour sont également diffusées sur des sites Internet piratés.

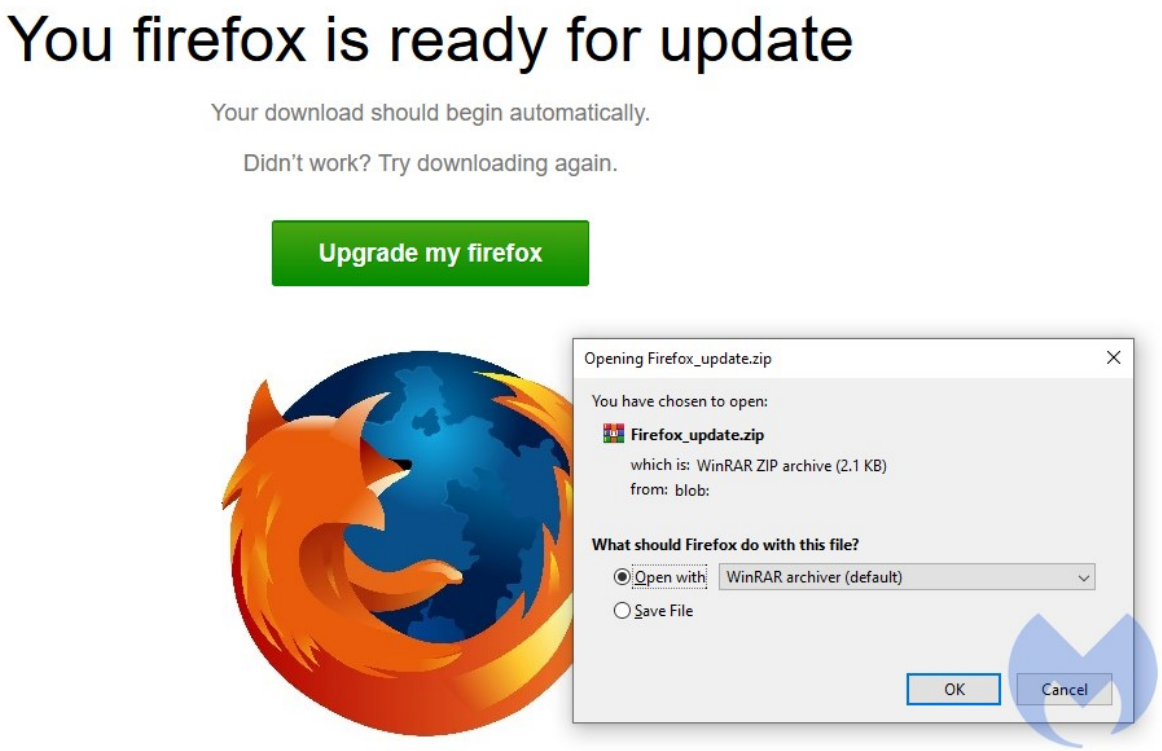

Fig. 8: Fausse mise à jour de navigateur (source: Malwarebytes.com)

Conclusion / Recommandation:

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

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

5.1.3 Exploitation des vulnérabilités

À peine une vulnérabilité d'un produit est-elle connue que différents acteurs passent Internet au crible à la recherche de systèmes vulnérables. La vulnérabilité est déjà exploitée au bout de quelques heures ou de quelques jours. Il est vrai que certaines attaques tirent aussi profit de vulnérabilités connues de longue date et pour lesquels un correctif existe. Aussi le catalogue des vulnérabilités actuellement exploitées de l'agence américaine de cybersécurité (CISA)[5] s'enrichit-il régulièrement d'anciennes failles de sécurité que les utilisateurs auraient pu combler, moyennant une gestion efficace des mises à jour[6].

[5] Known Exploited Vulnerabilities Catalog (cisa.gov)

[6] Adobe, Apple, Cisco, Microsoft Flaws Make Up Half of KEV Catalog (darkreading.com)

Outre les erreurs de programmation des développeurs que des correctifs (*patches)* de sécurité corrigent plus tard, la configuration choisie lors de l'installation de nouveaux produits est parfois à l'origine de vulnérabilités. Divers fabricants publient des instructions de configuration afin renforcer la sécurité de leurs produits.

Recommandations:

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

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

Il est important de remplacer les logiciels arrivés en fin de vie et pour lesquels les fabricants ont renoncé à proposer des mises à jour.

Le NCSC informe régulièrement les organisations en danger en raison de systèmes non mis à jour[7]. 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 ne doivent donc 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[8]. 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 Diffusion des maliciels

Le graphique ci-après indique les familles des maliciels que le NCSC a analysées et identifiées 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.

---

7 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); Une faille de nouveau repérée dans plus de 2800 serveurs Microsoft Exchange en Suisse (*ProxyNotShell*); Encore des serveurs Microsoft Exchange vulnérables en Suisse malgré la mise en garde du NCSC (ProxyNotShell) (ncsc.admin.ch)

8 Cf. rapport semestriel 2021/1 du NCSC (ncsc.admin.ch), chap. 3.2.

Analyse des familles de maliciels réalisée par le NCSC

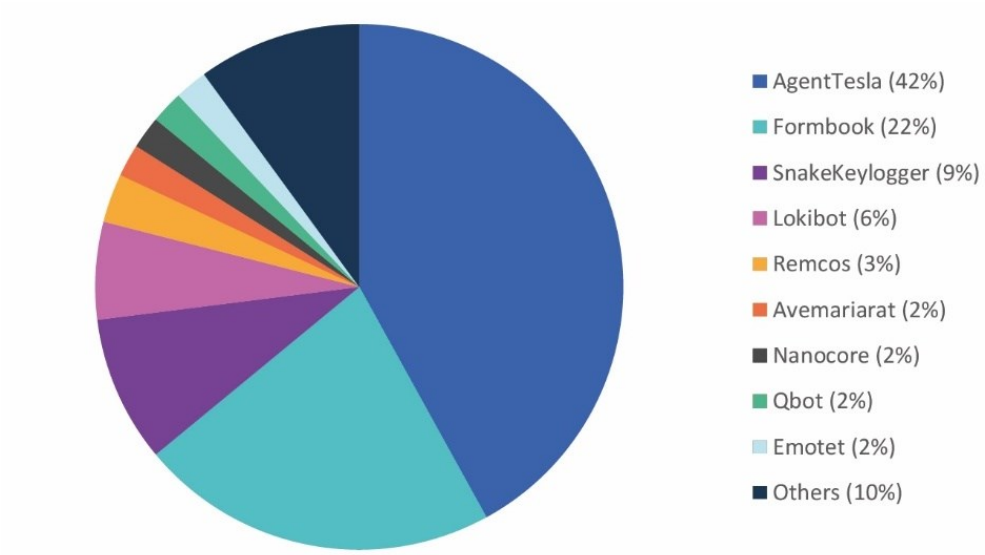

Fig. 9: Analyse par le NCSC des familles de maliciels ayant sévi en Suisse au deuxième semestre 2022.

5.2.2 Rançongiciels (*ransomware*)

Les attaques par rançongiciel demeurent la cybermenace la plus courante, peut-être même celle de plus lourde de conséquences à laquelle les organisations actives en Suisse sont confrontées. Les principales cibles au deuxième semestre 2022 ont été les petites et moyennes entreprises (PME) industrielles et les prestataires de services informatiques. Les développeurs de rançongiciels déploient de nouvelles stratégies ou méthodes pour infiltrer les systèmes et faire du chantage à leurs victimes: nouvelles versions des rançongiciels, conversion du code malveillant en langage de programmation *Rust* pour Windows et Linux, publication des données dérobées sur des sites Internet en clair (et non plus seulement sur le darknet, etc.). Afin de maximiser leurs gains, les cybercriminels recourent souvent à la double extorsion, exfiltrant les données du réseau compromis en amont de leur chiffrement, afin d'accroître la pression sur les victimes en les menaçant de publier leurs données. Face à la recrudescence des attaques par rançongiciel, à l'heure du modèle d'affaires des maliciels sur demande (*Ransomware as a Service*, RaaS) et au vu du nombre croissant de souches et de familles de rançongiciels, les entreprises actives dans la cybersécurité et les services étatiques collaborent toujours plus étroitement afin de trouver des clés de déchiffrement et développer des programmes de déchiffrement.

5.2.2.1 Exemples d'incidents survenus en Suisse

***Play*: quand un incident cause des dommages à des tiers**

À la fin du mois de novembre, un prestataire bernois de services d'informatique en nuage a dû couper ses centres de calcul du réseau suite à une attaque par un rançongiciel peut-être due au groupe *Play*. Les sauvegardes effectuées quatre jours plus tôt ont permis de récupérer une partie des données chiffrées. L'incident a eu des conséquences pour tous les clients de ce prestataire, dont certains qui n'ont plus pu accéder à leurs services en nuage. Ils ne pouvaient notamment plus émettre de factures, ni calculer ou verser les salaires. Cependant aucune donnée n'a été exfiltrée durant l'attaque. D'autres cantons ont également signalé au cours de l'année écoulée des incidents similaires et portant la signature de *Play*.

Double extorsion – attaque entraînant chiffrement et fuite de données

Le 5 septembre 2022, une fabrique de chocolat a subi une attaque de rançongiciel qui a affecté sa production, sa logistique et son administration. En l'espace de deux semaines, les secteurs touchés sont redevenus pleinement opérationnels. L'entreprise a toutefois confirmé que la cyberattaque avait probablement entraîné une fuite de données. Un mois plus tard, le groupe de rançongiciel *BianLian* a publié des fichiers relatifs aux affaires de l'entreprise sur le darknet.

Le groupe *BianLian* utilise un maliciel sur mesure écrit en langage de programmation *Go*[9]. Ses premières activités en ligne remontent à décembre 2021 et le groupe les a intensifiées en juillet 2022, ainsi, le mois suivant, il a considérablement étendu son infrastructure de commande et de contrôle (C2).

5.2.2.2 Événements survenus à l'étranger: attaques contre le secteur de l'énergie

Dans son précédent rapport semestriel, le NCSC avait présenté quelques exemples d'attaques par rançongiciel ayant touchés la branche économique, en soulignant que les gouvernements, autorités publiques et infrastructures énergétiques semblaient figurer dans le viseur des acteurs criminels. La tendance s'est confirmée au deuxième semestre 2022, durant lequel le secteur énergétique a beaucoup fait parler de lui. Cet intérêt accru tient sans doute au fait que les infrastructures critiques de ce secteur doivent être fonctionnelles à toute heure et qu'elles subissent d'importantes pressions dans le contexte géopolitique actuel. Les attaques par rançongiciel ont touché plusieurs fournisseurs d'énergie européens[10]. Sans surprise, les pirates ayant revendiqué ce genre de méfaits, comme *BlackCat* et *Everest*, sont des groupes pro-russes. Ils ont épargné à ce jour les distributeurs d'énergie suisses, et il paraît peu probable à l'heure actuelle qu'une attaque par rançongicielle ne survienne de manière ciblée contre la Suisse. On ne peut toutefois exclure des attaques opportunistes contre des systèmes vulnérables, ou des dommages collatéraux liés à des attaques contre des opérateurs européens.

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

En 2022, le rançongiciel le plus souvent utilisé en Suisse a été *Lockbit* (dans ses versions 2.0 ou 3.0 alias *Black*), devant *Deadbolt* et *Play* (voir chap. 4.4.1). Le groupe *Lockbit* est toujours le leader au niveau mondial, devant *BlackBasta* et *BlackCat*. D'autres groupes se sont étonnamment hissés à la tête du classement pendant quelques mois, mais sans parvenir à s'y maintenir. On peut citer ici *Hive*, *Sparta*, *Cuba*, *Royal* et *BianLian*.

***Lockbit Black*: grâce à sa nouvelle version, Lockbit reste le numéro un**

Le groupe *Lockbit* avait annoncé en juillet 2022 le développement de la version 3.0 de son rançongiciel. Cette mise à jour s'est faite remarquer en Suisse dès le mois de novembre, la police enregistrant une recrudescence de cas impliquant ce maliciel.

---

9 MalwareHunterTeam on Twitter: "A BianLian x64 ransomware sample (twitter.com)

10 En 2022, d'importantes entrprises gazières italiennes comme GSE SpA et Amalfitana Gas Srl, le géant pétrolier transalpin Eni, la société gestionnaire des réseaux de transport d'électricité et de gaz naturel Creos Luxembourg SA ou l'opérateur du réseau gazier national grec DESFA ont été victimes de rançongiciels.

Il est vrai que certains domaines sont restés épargnés, le code de conduite de *Lockbit* (ou les conditions générales de ce groupe de rançongiciels à la demande ou *RaaS*) interdisant le chiffrement de données d'écoles et hôpitaux. Un hôpital pédiatrique canadien a néanmoins subi une telle attaque, et il s'est avéré que les cybercriminels étaient des partenaires (*affiliates*) de *Lockbit*. Le groupe a présenté ses excuses sur les réseaux sociaux et a signalé avoir exclu ce partenaire. *Lockbit* a encore fourni un outil de déchiffrement gratuitement à l'hôpital pour restaurer ses données.

Dans le cadre de leurs investigations contre *Lockbit*, les autorités françaises et canadiennes sont parvenues à identifier avec le FBI près de 1800 victimes réelles ou présumées de *Lockbit*[11]. Les systèmes infectés comportaient une faille de sécurité dans leurs pare-feu FortiGate ou SonicWall. La police a prévenu les organisations concernées en Suisse.

***Agenda* & *Hive*: Rust apporte un nouveau souffle à d'anciens rançongiciels**

Beaucoup d'acteurs de rançongiciels ont créé une nouvelle version de leur produit à l'aide du langage multiplateforme *Rust*, qui permet de déployer les maliciels sur Windows comme sur Linux. Tel est le cas d'«*Agenda* (aussi appelé *Qilin*), initialement écrit en langage de programmation *Go*. Ses auteurs semblent être actuellement occupés à migrer son code vers *Rust*, car le rançongiciel ne disposait pas de toutes les fonctionnalités dans son code d'origine. *Agenda* procède comme le rançongiciel *Royal* à un chiffrement partiel (ou intermittent). Des paramètres fixés à l'avance déterminent quel pourcentage des fichiers sera chiffré. De cette manière, le chiffrement peut s'effectuer plus rapidement et sa détection, qui est essentiellement basée sur les accès en lecture et en écriture des fichiers, sera retardée. Les auteurs des attaques utilisent toujours plus souvent le langage de programmation *Rust*, car il est plus difficile à analyser et beaucoup d'antivirus ont encore du mal à identifier les maliciels écrits en *Rust*. En Suisse, le rançongiciel *Agenda* a chiffré les ordinateurs d'une administration communale zurichoise. Les copies de sauvegarde ont toutefois permis de restaurer les données.

***BlackCat* & *IceFire*: publication des données volées sur Internet**

Une nouvelle technique de chantage utilisée par le groupe de rançongiciel *ALPHV*/*BlackCat* consiste à créer une copie du site Internet de la victime et à y publier les données exfiltrées afin d'exercer sur elle un maximum de pression. *BlackCat* y remplace les rubriques et les sous-pages d'origine par les siennes, pour faciliter le tri des données exfiltrées. La réplique du site est publiée dans la partie claire d'Internet, où les données sont plus faciles à trouver que sur le darknet. Le site du groupe reprend souvent le nom de domaine de l'adresse originale mais avec une faute de frappe (typosquattage ou *typo domain*)[12]. Une telle façon de procéder est plus problématique pour les victimes qu'une publication sur le réseau Tor, n'importe qui pouvant aisément consulter les données mises en ligne sur un site web normal. La victime d'un tel chantage subit une pression d'autant plus grande qu'elle craint que sa clientèle ou d'autres personnes ne voient les données volées.

L'idée a été reprise par le groupe de rançongiciels *IceFire*, qui a fait son apparition en mars 2022, dans une attaque lancée à la mi-août contre une entreprise suisse, afin d'accroître la pression sur elle.

---

11 Police arrest suspected LockBit operator as the ransomware gang spills new data (techcrunch.com)

12 Exemples de *typo domains*: adimn.ch, adnim.ch ou adrnin.ch au lieu d'admin.ch

***Play* alias *PlayCrypt*: concentration sur des cibles proches du pouvoir**

Dès son entrée en activité en été 2022, le groupe *Play* s'est intéressé aux services étatiques. Un tel mode opératoire est rare, de telles attaques étant poursuivies d'office. Si Play sévit surtout en Amérique latine, il a également fait des victimes sur d'autres continents et dans d'autres secteurs que l'administration.

Play est connu pour sa stratégie de chasse aux trophées (*Big Game Hunting*), consistant à attaquer de grandes organisations résistantes. Les produits utilisés comprennent notamment *Cobalt Strike*, pour la phase d'accès initiale, et *SystemBC RAT* pour les attaques persistantes. Les pirates de *Play* se sont encore récemment mis à exploiter les vulnérabilités *ProxyNotShell* des serveurs Microsoft Exchange. Les analyses ont relevé des parallèles entre les variantes de rançongiciels *Play*, *Hive* et *Nokoyawa*.

***BianLian* & *MegaCortex*: déchiffrement avec des déchiffreurs...**

Un déchiffreur gratuit (programme permettant de récupérer les fichiers chiffrés avec des rançongiciels) est paru pour la souche de rançongiciel *BianLian* en janvier 2023, soit six mois seulement après leur pic d'activité remontant à l'été 2022[13]. Une autre action commune d'Europol et de la police cantonale zurichoise a permis d'arrêter un développeur du rançongiciel *MegaCortex*, et à partir de là de développer un logiciel de déchiffrement pour cette souche. On trouve entre-temps sur Internet de nombreux programmes gratuits de déchiffrement des fichiers[14]. Les entreprises de cybersécurité s'efforcent de les développer rapidement, en réponse à l'essor et à la diversité croissante des souches de rançongiciels.

… et avec des clés de déchiffrement (*Deadbolt*)

La police néerlandaise est parvenue en octobre 2022, grâce à une astuce utilisant le paiement en bitcoins, à s'emparer de 150 clés de déchiffrement du groupe de rançongiciels *Deadbolt*[15]. *Deadbolt*, qui s'en prend surtout aux appareils de stockage en réseau (NAS) fabriqués par l'entreprise QNAP, a fait plusieurs victimes en Suisse. L'obtention de ces clés a été une grande victoire, permettant à plusieurs victimes de déchiffrer leurs données. Il est désormais possible de voir en ligne s'il existe une clé pour un appareil chiffré par *Deadbolt*[16].

Conclusions, perspectives et recommandations:

Lors d'attaques par des rançongiciels, il arrive souvent que des données (parfois sensibles) soient chiffrées et exfiltrées, auquel cas on parle de double extorsion. Cependant certains groupes de rançongiciel ne se donnent même plus la peine de chiffrer les systèmes et se contentent de menacer les victimes de publier leurs données.

Les rançongiciels peuvent causer de sérieux dommages, en particulier si les copies de sauvegarde (*backup*) sont affectées. Des aspects importants de la résolution des incidents sont présentés sur le site Internet du NCSC:

Rançongiciels - que faire? (ncsc.admin.ch) et Fuite de données - que faire? (ncsc.admin.ch)

13 Decrypted: BianLian Ransomware (avast.io)

14 Voir p. ex. The No More Ransom Project (nomoreransom.org)

15 Police tricked a ransomware gang into handing over its decryption keys. Here's how they did it (zdnet.com)

16 Deadbolt Decryption (responders.nu)

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

Comme le rappelle aujourd'hui la guerre en Ukraine, des opérations de cybersabotage sont parfois menées lors de conflits géopolitiques, dans le but d'affaiblir la partie adverse[17]. Une manipulation de la technologie opérationnelle ou des systèmes de pilotage s'impose presque toujours en pareil cas afin de modifier les processus physiques. Il est toutefois rarissime que les processus physiques soient directement pris pour cible, les agresseurs s'attaquant plutôt à l'infrastructure des serveurs et des réseaux afin de perturber l'activité opérationnelle[18].

5.3.1 Tentatives de sabotage dans le cadre de conflits

Au début de la guerre[19], des tentatives de sabotage menées à l'aide de maliciels contre les systèmes d'approvisionnement électrique[20] ont été déjouées, l'infrastructure[21] des agresseurs a été révélée au grand jour et toute une série d'instruments d'attaque[22] ont été publiés avant même d'avoir pu servir. Au deuxième semestre 2022, les activités de sabotage se sont limitées à l'emploi de virus effaceurs (*wiper*)[23] et à des cyberattaques destructrices prenant l'apparence de banals rançongiciels[24]. Aucune trace d'actes de manipulation des systèmes industriels n'a été trouvée, les attaques identifiées visant en particulier les systèmes informatiques d'organisations de transport[25] basées en Ukraine et en Pologne.

Quant aux déclarations de groupes cyberactivistes comme OneFist[26] et Ghostsec[27], qui se vantaient d'avoir provoqué des pannes dans des installations industrielles, elle n'ont pas pu être confirmées ni vérifiées de manière indépendante. Les séquences vidéo présentées par ces groupes indiquent plutôt de simples tentatives de manipuler les tableaux d'affichage et de commande de systèmes de contrôle industriels accessibles par Internet et mal protégés.

5.3.2 Vulnérabilité de l'approvisionnement énergétique

La guerre en Ukraine a eu pour effet collatéral de menacer la sécurité d'approvisionnement énergétique de l'Europe, et donc aussi celle de la Suisse. À commencer par l'approvisionnement en gaz et en électricité. Aussi le Conseil fédéral a-t-il lancé une campagne d'économie d'énergie pour réduire le risque de pénurie[28].

---

17 Voir notamment à propos de *Stuxnet* le rapport semestriel 2010/2 (ncsc.admin.ch), chap. 4.1 et 5.1) et à propos de Triton/Trisis le rapport semestriel 2017/2 (ncsc.admin.ch), chap. 5.3.2.

18 How Many ICS-OT Directed Attacks In 2022? (linkedin.com)

19 Rapport semestriel 2022/1 du NCSC, chap. 3 et 5.4

20 Industroyer2: Industroyer reloaded (welivesecurity.com)

21 New Sandworm malware Cyclops Blink replaces VPNFilter (ncsc.gov.uk)

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

23 Russian APT groups continue their attacks against Ukraine with wipers and ransomware (eset.com)

24 RansomBoggs: New ransomware targeting Ukraine (welivesecurity.com)

25 New "Prestige" ransomware impacts organizations in Ukraine and Poland (microsoft.com)

26 The Increasing Threat Posed by Hacktivist Attacks (forescout.com)

27 Country-Specific ICS Targeting: Shining a Light on GhostSec (otorio.com)

28 Energie: Le Conseil fédéral lance la campagne d'économies d'énergie (admin.ch)

Dans une situation aussi tendue, une cyberattaque réussie contre les dispositifs de commande des systèmes d'approvisionnement aurait des effets bien plus dévastateurs que s'il y avait pléthore d'alternatives pour compenser. Mais à moins d'une extension du conflit au reste de l'Europe, il reste peu probable qu'un État étranger déploie des activités ciblées de cybersabotage[29] contre les systèmes suisses d'approvisionnement énergétique. Les attaques de rançongiciels présentent un danger beaucoup plus grand[30]. Si les chiffrements qui s'ensuivent devaient paralyser des systèmes intervenant dans la gestion de l'approvisionnement énergétique, des restrictions voire des interruptions seraient à craindre dans l'exploitation productive[31].

La sécurité physique des systèmes s'avère elle aussi déterminante dans ce contexte. Ainsi, le sectionnement mécanique de câbles en fibre optique indispensables à la circulation des trains de la Deutsche Bahn[32] a provoqué une panne massive, montrant le risque bien réel d'opérations de sabotage menées sur le terrain[33]. Une telle action confirme encore l'importance de prévoir des mesures visant à la remise en service des installations afin de renforcer la résilience du système tout entier.

Conclusion / Recommandations:

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

Des mesures adéquates figurent dans la norme minimale pour les TIC élaborée par l'OFAE et dans les normes minimales par secteur qui en découlent:

Norme minimale pour les TIC (ncsc.admin.ch)

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

5.4 Failles de sécurité

5.4.1 Systèmes aux fichiers de configuration publiquement accessibles

Des chercheurs en sécurité signalent régulièrement des failles au NCSC à l'aide du formulaire destiné à la divulgation coordonnée d'une vulnérabilité (*Coordinated Vulnerability Disclosure*, CVD)[34]. Au cours du semestre sous revue, le NCSC a ainsi été informé de différentes vulnérabilités dues à une mauvaise configuration logicielle: des fichiers de configuration non protégés étaient accessibles sans restriction dans un répertoire situé sur un serveur Internet.

29 «La Sécurité de la Suisse 2022»: le Service de renseignement de la Confédération publie son nouveau rapport de situation (admin.ch)

30 Dragos Industrial Ransomware Analysis: Q4 2022 (dragos.com)

31 Cybersecurity Research Report January 2023 (nozominetworks.com)

32 Sabotage bei der Bahn: Viele vertrauliche Infos sind offen zugänglich (heise.de)

33 BfV-Sicherheitshinweis für die Wirtschaft 04/2022 (wirtschaftsschutz.info)

34 Annonce d'une faille ou divulgation coordonnée d'une vulnérabilité (Coordinated Vulnerability Disclosure, CVD) (ncsc.admin.ch)

Un exemple très répandu vient des fichiers créés à partir de l'outil de gestion des versions *Git*. Ce logiciel crée un dossier portant l'extension *.git*, qui renferme tout le code source de l'application ou du système. Si ce dossier est accessible et consultable sur un serveur Internet, un agresseur averti pourrait accéder à des données potentiellement sensibles, telles que les données d'accès ou les mots de passe.

Le NCSC est parvenu à identifier en Suisse 1300 systèmes concernés et à alerter leurs exploitants.

Or *Git* n'est pas le seul logiciel à générer de tels fichiers de configuration et des dossiers cachés; on peut encore citer les pages de profil PHP faisant partie de l'environnement de développement (*framework)* Symfony[35] ou les fichiers de texte *.env*, souvent employés pour enregistrer les clés d'accès et les mots de passe qu'un système utilise. Si les droits d'accès n'ont pas été correctement définis, un pirate pourra lire et utiliser de tels fichiers à mauvais escient.

Le NCSC collabore activement avec les chercheurs en sécurité afin d'informer les exploitants concernés et de les sensibiliser aux risques et dangers qu'impliquent de telles erreurs de configuration[36].

Conclusion / Recommandations:

Les fichiers de configuration tels que le dossier *.git* ne devraient jamais être accessibles par Internet. Le cas échéant, s'il n'est pas possible de le supprimer rapidement, il est nécessaire d'en protéger et d'en limiter au moins l'accès (par exemple à l'aide de règles .htaccess ou, selon la technologie utilisée, à l'aide de restrictions d'accès techniques similaires).

Plus efficaces encore seraient des mesures préventives, telles que la vérification et l'adaptation du processus de développement afin que seules les données souhaitées et destinées au projet en question (mentionnées dans le fichier *build*) figurent dans le répertoire. Les données sensibles ou confidentielles, c'est-à-dire les mots de passe, clés API, etc., ne devraient jamais être intégrées directement au code source ou à l'application (codé en dur, *hardcoded)*. En tout cas, elles ne devraient pas être enregistrées dans le répertoire *Git*, mais dans le dossier *gitignore* pour être ignorées. Il faudrait absolument respecter ces mesures élémentaires de sécurité et s'inspirer des bonnes pratiques en place.

5.4.2 ProxyNotShell

À la fin du mois de septembre 2022, une entreprise de cybersécurité vietnamienne[37] a signalé des attaques déployées le mois précédent contre des infrastructures critiques du monde entier. Son analyse a permis d'identifier deux failles dites *zero day* des serveurs Microsoft Exchange ayant servi à mener les opérations. La première (CVE-2022-41040) est une faille permettant de lire des fichiers sur le serveur local, appelée *server-side request forgery* (SSRF), grâce à laquelle un agresseur s'étant authentifié peut tirer parti de la seconde faille (CVE-

35 Covid-Center & andere Webseiten: Bedienen Sie sich! (dnip.ch)

36 Dépôts Git non protégés sur Internet: attention danger! (ncsc.admin.ch)

37 Two Microsoft Exchange zero-days exploited by attackers (helpnetsecurity.com)

2022-41082), soit une vulnérabilité de type exécution de code arbitraire (*remote code execution* ou RCE). Cette dernière permet d'exécuter à distance, par Internet, du code malveillant. En combinant ces deux failles, un intrus pourra par exemple accéder à des systèmes vulnérables.

Microsoft a confirmé peu après les failles des serveurs Microsoft Exchange 2013, Microsoft Exchange 2016 et Microsoft Exchange 2019 et recommandé de prendre des mesures immédiates. La faille critique a été appelée *ProxyNotShell*, car elle découle d'une vulnérabilité d'Exchange appelée *ProxyShell* (CVE-2021-34473, CVE-2021-34523, CVE-2021-31207, découverte en 2021 et présentant certaines similitudes.).

Le 10 novembre 2022, Microsoft a publié des mises à jour logicielles comblant ces deux failles de sécurité. Or le 18 novembre 2022, le NCSC a identifié en Suisse 2800 serveurs présentant une porte d'entrée pour les cybercriminels, faute d'avoir appliqué entre-temps les correctifs de sécurité actuels[38]. Au début du mois de décembre 2022, le NCSC a de nouveau avisé par lettre recommandée les entreprises n'ayant toujours pas appliqué les correctifs de sécurité.

Conclusion / Recommandations:

La vulnérabilité *ProxyNotShell* était déjà activement exploitée par les cybercriminels avant que le correctif officiel de Microsoft ne soit disponible. Dans de tels cas, il est important de réagir rapidement et de suivre les recommandations – qui peuvent aller jusqu'à la désactivation du système vulnérable – en attendant, par exemple, 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 d'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 un peu de répit jusqu'à l'adoption de mesures de défense. Mais une telle mesure ne saurait remplacer la mise à jour du système et l'installation de correctifs dès leur parution.

5.4.3 Retbleed

Le 12 juillet 2022, l'EPF de Zurich[39] a publié une vulnérabilité des microprocesseurs d'Intel et d'AMD. Nommée *Retbleed*, cette faille pourrait être utilisée par un pirate informatique pour accéder à n'importe quelle zone mémoire. *Retbleed* est un nom créé à partir de *RET* et de *bleed* (saigner en anglais). Il se fonde sur l'analogie avec des vulnérabilités antérieures comme *Heartbleed*, qui permettaient déjà de récupérer les informations stockées dans la mémoire des serveurs. RET est l'abréviation de RETURN, instruction de programmation des processeurs. Une prudence particulière s'impose dans le cas des infrastructures partagées (*shared infrastructure*) et lors de l'exécution de logiciels peu fiables.

---

38 Une faille de nouveau repérée dans plus de 2800 serveurs Microsoft Exchange en Suisse (ProxyNotShell) (ncsc.admin.ch)

39 Spekulative Berechnungen öffnen eine Hintertür zum Informationsklau (ethz.ch); Speculative calculations open a backdoor to information theft (ethz.ch)

Le NCSC a soutenu les chercheurs de l'EPF de Zurich en vue de la divulgation coordonnée des deux vulnérabilités et de l'attribution des numéros CVE. *Retbleed* a ainsi obtenu les numéros CVE-2022-29900 (pour les processeurs du fabricant AMD) et CVE-2022-29901 (processeurs du fabricant Intel).

Conclusion / Recommandations:

Retbleed est une faille de sécurité très complexe, qui n'a pas été exploitée jusqu'ici ou du moins dont aucun cas d'utilisation n'est connu.

Comme des conditions spécifiques doivent être réunies en vue de l'exploitation de cette vulnérabilité, le risque est minime pour les utilisateurs.

Tant Intel qu'AMD préparent des correctifs pour réduire et combler cette vulnérabilité. Il est plus important que jamais de faire uniquement fonctionner sur son système des logiciels dignes de confiance et d'installer avec scepticisme les logiciels tiers. En outre, il est essentiel d'installer au plus vite les mises à jour et les correctifs des fabricants et de prendre en compte leurs recommandations.

5.5 Fuites de données

La sécurité des données est l'un des enjeux majeurs de la transformation numérique, tant pour les propriétaires des données que pour les personnes ou entreprises qui retrouvent leurs propres informations dans des jeux de données. Or malgré la prise de conscience croissante de l'importance de la sécurité ainsi que de la protection des données dans l'espace numérique, les fuites de données sont restées un sujet de préoccupation au deuxième semestre 2022, pour différentes raisons. En dehors des cas où la protection et la maintenance des systèmes laissaient à désirer, la négligence humaine et surtout les cyberattaques ont contribué à la publication de données sensibles. En effet, les cybercriminels dérobent volontiers des données – en plus de les chiffrer (voir chap. 5.2.2 Rançongiciels) – pour faire pression sur leurs propriétaires ou les revendre au plus offrant.

Même si les médias parlent surtout des attaques de rançongiciels, il est nécessaire de souligner qu'une meilleure gestion des données aurait permis d'éviter dans bien des cas la publication de données sensibles. Les paragraphes qui suivent reviennent sur deux cas où, dans l'un, des informations ont été involontairement publiées et, dans l'autre, des données confiées à des tiers ont été divulguées sans autorisation.

5.5.1 Métadonnées de fichiers publiés

Les sites Internet représentent des plateformes essentielles pour les entreprises et les institutions, qui s'en servent afin de communiquer des informations ou de les rendre accessibles au monde extérieur. Il leur arrive toutefois de publier malgré elles des informations internes dans les métadonnées de fichiers[40]. Il s'agit pour les externes d'une mine de

[40] Toutes sortes de fichiers comportent des métadonnées (informations caractérisant le contenu d'un fichier). Il peut s'agir d'informations sur l'auteur, dans le cas des documents Word ou PDF, alors que les fichiers photo incluent notamment des données de localisation (GPS) dans leurs métadonnées.

renseignements (noms des employés, noms d'utilisateurs, adresses électroniques, structures de dossiers, logiciel utilisé et numéro de version, etc.). Les auteurs de cyberattaques souhaitent en particulier connaître la version des applications utilisées, afin de déterminer les vecteurs d'attaque pertinents pour leurs victimes potentielles.

Ce problème lié aux métadonnées n'a pas échappé à l'administration fédérale, qui a mis en place des mesures de sensibilisation des collaborateurs.

Conclusion / Recommandation:

Dans un premier temps, il faudrait que les organisations effectuent un bilan actuel et contrôlent les métadonnées de tous les fichiers qu'elles ont publiés. Le cas échéant, elles les republieront après les avoir nettoyées. En outre, il est recommandé de nettoyer les fichiers selon un processus défini d'avance avant toute diffusion ou publication. Il convient de sensibiliser l'ensemble du personnel à ces questions et de le former en la matière.

5.5.2 Élimination des outils informatiques et des supports de données

En décembre 2022, les médias ont révélé que pendant plusieurs années, la Direction de la justice du canton de Zurich n'avait pas éliminé dans les règles de l'art ses périphériques de stockage. C'est ainsi qu'entre 2006 et 2012, des données sensibles et non chiffrées sont tombées entre de mauvaises mains. Les supports de données renfermaient notamment les numéros de téléphone et les adresses confidentielles de procureurs et de juges, des dossiers pénaux, des expertises psychologiques ainsi que des plans de bâtiments[41].

Un rapport d'enquête externe sur ces incidents a encore signalé que comme leur système d'information juridique central n'étant pas au point, les collaborateurs installaient sur leur disque dur local des dossiers parallèles afin de traiter plus efficacement les cas. Or ces lecteurs n'étaient pas suffisamment protégés, les données qu'ils renfermaient n'étant pas systématiquement chiffrées[42].

Conclusion / Recommandation:

L'incident montre à quel point, dans le sillage de la numérisation, la sécurité des données requiert une attention particulière. Il faut concevoir des processus de conservation sécurisée des données facile à utiliser, afin que tout le personnel se conforme aux instructions en place.

Il existe plusieurs possibilités de détruire correctement les supports de données, à savoir l'écrasement des données, la démagnétisation des supports de données et leur destruction physique. En cas d'externalisation de la destruction des données, choisissez avec soin votre prestataire, optez pour une procédure appropriée et assurez-vous qu'il existe une preuve écrite du processus de destruction.

Le NCSC propose des informations pratiques destinées aux entreprises sur les mesures à prendre en cas de fuite de données.

41 Schweiz aktuell - Datenleck bei Justizdirektion Kanton Zürich: GPK stellt Antrag auf PUK (srf.ch)

42 Datenskandal Justizdirektion: Zürich setzt die Prioritäten falsch (nzz.ch)

5.6 Point sur l'Ukraine

5.6.1 Poursuite des activités dans le cyberespace sans grand succès

La guerre en Ukraine est demeurée l'un des principaux événements géopolitiques au deuxième semestre 2022. Le précédent rapport semestriel avait déjà passé en revue les incidents survenus dans le cyberespace, à la lumière du conflit actuel en Ukraine et de ses antécédents[43]. Entre-temps, il n'y a pas eu de changement majeur dans la typologie des cyberincidents, mais leur nombre a augmenté[44]. Les services de sécurité ukrainiens ont ainsi signalé avoir neutralisé en 2022 quelque 4500 cyberattaques, soit trois fois plus qu'un an plus tôt[45]. La Russie continue de faire pression sur l'Ukraine dans le cyberespace, sans succès significatif à ce jour. Trois hypothèses avaient été émises dans le précédent rapport semestriel pour expliquer l'absence de cyberattaque très destructrice d'origine russe:

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.

Les informations obtenues sur les activités déployées dans le cyberespace dans le cadre de la guerre en Ukraine depuis le dernier rapport, font plutôt pencher pour la deuxième hypothèse. La Russie demeure très active et aurait même multiplié depuis octobre 2022 les opérations contre les infrastructures ukrainiennes du secteur de l'énergie, mais sans parvenir à s'imposer dans le cyberespace, l'Ukraine s'étant défendue avec succès[46]. Ces cyberattaques ne sont manifestement pas considérées comme une alternative aux moyens militaires conventionnels mais sont souvent lancées en parallèle, à l'occasion de tentatives de prise d'influence. La campagne d'octobre-novembre 2022 contre les centrales électriques ukrainiennes est un bon exemple de cette multidimensionnalité des opérations. Les attaques de missiles étaient accompagnées de cyberattaques et d'activités de propagande. Les cyberattaques avaient pour but d'accroître la pression sur un secteur déjà astreint à se contenter de ressources limitées, après les dégâts infligés par les moyens militaires conventionnels. Quant à la propagande, elle visait à imputer la responsabilité des nuisances occasionnées (pannes comprises) à l'État ukrainien, aux collectivités locales ou aux grandes entreprises ukrainiennes[47]. Mais comme l'Ukraine avait prévu un tel scénario, les cyberopérations n'ont pas eu le succès escompté. Cette situation met d'ailleurs en lumière une potentielle explication au peu de succès de la Russie dans le cyberespace: il n'y a pas eu de nouveaux types

---

43 Rapport semestriel 2022/1 du NCSC (ncsc.admin.ch), chap. 3.

44 The number of cyberattacks on Ukraine keeps increasing (cip.gov.ua)

45 SSU neutralized over 4,500 cyberattacks on Ukraine in 2022 (ssu.gov.ua)

46 SSU neutralized hundreds of cyberattacks on Ukrainian cogeneration plants and energy companies in 2022 (ssu.gov.ua)

47 Cyber, Artillery, Propaganda. General overview of the dimensions of Russian aggression (cip.gov.ua); Preparing for a Russian cyber offensive against Ukraine this winter (microsoft.com)

d'attaques. Les cyberattaques observées ont été menées selon des schémas déjà connus, et donc il a été possible de leur opposer des stratégies de défense éprouvées[48].

5.6.2 Des cyberattaques variées aux conséquences multiples

Il a été question de nombreuses cyberattaques liées à la guerre en Ukraine, y compris dans la presse non spécialisée. Certains articles ne précisent hélas pas le genre d'attaques menées ou leurs conséquences, ce qui rend impossible toute approche différenciée des événements. La description qui suit de quelques cyberattaques montre qu'elles peuvent avoir un impact très variable et rappelle que la prudence s'impose, à la lecture d'articles employant des termes vagues.

5.6.2.1 Attaques affectant la disponibilité (attaques DDoS ou *Distributed Denial of Service*)

Les attaques DDoS survenues durant la période sous revue comptaient parmi les plus flagrantes[49]. De telles cyberattaques visent à paralyser des sites Internet ou d'autres services en ligne, en les inondant de requêtes. Elles proviennent surtout de groupes d'hacktivistes prenant fait et cause pour l'une des parties belligérantes. Ainsi, des groupes prorusses comme KillNet choisissent les pays et les cibles à attaquer en fonction du soutien qu'ils accordent à l'Ukraine ou des sanctions qu'ils prononcent contre la Russie. Les dommages causés par de telles opérations sont à ce jour marginaux dans le contexte de la guerre en Ukraine, et consistent principalement en des atteintes à la réputation.

Par exemple, les attaques DDoS lancées en octobre 2022 par KillNet contre les sites Internet d'aéroports américains[50] ont rendu certaines pages temporairement inaccessibles. Les passagers n'ont plus pu s'informer par ce biais sur le statut actuel de leur vol. Ces attaques n'ont toutefois eu aucun impact sur les activités opérationnelles de ces aéroports.

5.6.2.2 Diffusion des maliciels

Pendant la période sous revue, les nombreuses campagnes de diffusion de maliciels principalement déployées contre des institutions ukrainiennes ont fait couler beaucoup d'encre[51]. Ces campagnes ont pour but d'accéder à des systèmes en les infectant au moyen de maliciels. En temps de guerre, de tels accès sont exploités à des fins d'espionnage (vol d'informations) ou de sabotage (dysfonctionnement du système). Les auteurs distribuent souvent le maliciel par courriel en usurpant l'identité d'organismes officiels. Un thème actuel est à chaque fois abordé afin d'amener les destinataires à effectuer la manipulation nécessaire pour infecter leur système. Une autre approche observée consiste à créer de faux sites Internet en reprenant l'identité de services officiels et d'y dissimuler le maliciel dans un programme que l'utilisateur est censé installer. Enfin, on peut également diffuser un maliciel en exploitant les vulnérabilités existantes d'un système. En pareil cas, aucune interaction n'est généralement nécessaire de la part des utilisateurs du système pris pour cible. Les effets de telles

---

48 Cyber, Artillery, Propaganda. General overview of the dimensions of Russian aggression (cip.gov.ua)

49 Timeline of Cyberattacks and Operations (cyberpeaceinstitute.org)

50 Coverage of Killnet DDoS attacks plays into attackers' hands, experts say (therecord.media)

51 Timeline of Cyberattacks and Operations (cyberpeaceinstitute.org)

campagnes varient beaucoup, en fonction du type de logiciel malveillant et du système infecté. Pour prendre un exemple simplifié à l'extrême, un maliciel ayant subtilisé des informations figurant sur l'ordinateur d'un étudiant d'une école n'aura pas le même impact que s'il avait perturbé l'exploitation du système d'un hôpital.

C'est ainsi par exemple qu'en juillet 2022, le maliciel *GammaLoad* a été envoyé à diverses autorités ukrainiennes. La campagne est attribuée au groupe APT (*Advanced Persistent Threat*) russe Gamaredon[52]. Lors de cette campagne, le maliciel *GammaLoad* était propagé dans une prétendue fiche d'information annexée à des courriels qui semblaient provenir de l'Académie nationale des services de sécurité d'Ukraine. Aussitôt que le système pris pour cible était infecté avec *GammaLoad*, le groupe Gamaredon pouvait en extraire des informations ou charger sur ce système d'autres maliciels comportant des fonctions supplémentaires, par exemple à des fins de sabotage.

Dans un autre cas, trois entreprises de transport et de logistique basées en Ukraine ou en Pologne ont été infectées en quelques heures seulement par le rançongiciel *Prestige*»[53]. Ce rançongiciel est attribué au groupe APT russe Sandworm. Un incident dû à un rançongiciel peut perturber l'exploitation des entreprises touchées, ce qui en l'occurrence aurait pu affecter le transport des marchandises. Une intervention rapide a toutefois permis de limiter les dommages dus à cette cyberattaque.

5.6.3 Développements à venir

Rien n'indique une diminution, dans le cyberespace, des activités liées à la guerre en Ukraine. Tant que la guerre durera, la Russie continuera très probablement de lancer des attaques dans ce domaine et de saisir toutes les occasions pour parvenir à ses fins, en les combinant ou non avec des activités déployées dans d'autres sphères opérationnelles.

---

52 Кібератаки групи UAC-0010 (Armageddon) з використанням шкідливої програми GammaLoad.PS1 v2 (CERT-UA#5003,5013,5069,5071) (cert.gov.ua)

53 New "Prestige" ransomware impacts organizations in Ukraine and Poland (microsoft.com)