

7 novembre 2024 | Office fédéral de la cybersécurité OFCS



Rapport semestriel 2024/I (janvier à juin)

Cybersécurité

La situation en Suisse et sur le plan international



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de la défense,
de la protection de la population et des sports DDPS
Office fédéral de la cybersécurité OFCS

Résumé

Le présent rapport semestriel de l'Office fédéral de la cybersécurité (OFCS) passe en revue les principaux phénomènes du contexte cyber actuel en Suisse. Les cyberincidents signalés et les développements apparus au premier semestre 2024 tant en Suisse que sur la scène internationale permettent de démontrer comment divers acteurs malintentionnés opèrent dans le cyberspace. Il conviendra pour cela d'analyser les méthodes auxquels ces derniers recourent pour atteindre leurs objectifs.

Au premier semestre 2024, l'OFCS a reçu au total 34 789 annonces de cyberincidents, soit 15 740 de plus qu'à la même période de l'année précédente. Ce quasi-doublement tient surtout aux signalements dits de « faux appels au nom de la police », de « jeux-concours frauduleux », d'« abonnements pièges » et d'hameçonnage. Parmi ces annonces, près de 90 % d'entre elles émanaient de la population, contre seulement 10 % d'annonces de la part d'entreprises. Comme les années précédentes, les cas de fraude, d'hameçonnage et de pourriels continuent de dominer le classement des cyberincidents.

Escroqueries – incidents les plus souvent signalés

Les cas de fraude restent avec 23 104 annonces le phénomène le plus souvent signalé, totalisant à eux seuls deux tiers des annonces du premier semestre 2024. Leur nombre a largement doublé par rapport à la même période de l'année précédente (11 174). En particulier, 13 730 signalements, soit près de 60 %, concernent des appels frauduleux émanant prétendument d'autorités policières. Ce phénomène consiste à composer un très grand nombre de numéros de téléphone choisis au hasard et à faire croire aux victimes qu'elles sont impliquées dans une procédure pénale. Ensuite ces dernières sont invitées à appuyer sur la touche « 1 » pour discuter des prochaines étapes avec un interlocuteur. Les victimes sont ensuite mises en relation avec un escroc qui va les pousser à télécharger un logiciel d'accès à distance. Celui-ci va se connecter à leurs ordinateurs et effectuer dans leurs systèmes d'e-banking des paiements à leurs dépens.

Forte hausse des annonces d'hameçonnage

Au premier semestre 2024, l'OFCS a reçu 6 643 signalements relatifs à des sites d'hameçonnage, soit 2 800 de plus que l'année précédente à la même période (3 879 annonces). Comme jusqu'à présent, la plupart des tentatives rapportées concernaient des alertes falsifiées de distribution de paquets ainsi que de prétendus courriels de remboursement expédiés au nom de divers fournisseurs, des CFF, respectivement de SwissPass, ou de différentes administrations fiscales. En particulier, des tentatives d'hameçonnage visant des comptes Microsoft 365 sont régulièrement signalées à l'OFCS. Une approche aujourd'hui répandue s'apparente à un système boule de neige, ce qui lui a valu le nom d'« hameçonnage en chaîne » : aussitôt qu'un compte est compromis, des courriels d'hameçonnage sont envoyés à tous les contacts du carnet d'adresses du compte compromis.

Attaques DDoS lors de grands événements et de conférences internationales

Lors d'attaques affectant la disponibilité de sites et de services Internet (*Distributed Denial of Service*, déni de service distribué, *DDoS*), les cybercriminels cherchent à rendre temporairement inaccessible un site ou un service en ligne, en le saturant de requêtes. Trois campagnes *DDoS* ont notamment été observées durant le semestre sous revue : En avril, diverses organisations suisses actives dans le secteur financier ont signalé des attaques

DDoS accompagnées de message de chantage. Ces attaques auraient été revendiquées par un groupe se faisant appeler *Armada Collective* ou *Alpha Jackal*. Indépendamment de toutes considérations financières, des attaques *DDoS* ont à nouveau été menées à des fins politiques lors de grands événements et de conférences internationales organisés en Suisse. Le collectif d'hacktivistes prorusse *NoName057(16)* a visé en janvier 2024 des sites Internet liés au Forum économique mondial (WEF) puis, en juin, des sites d'organisations impliquées dans la Conférence sur la paix en Ukraine organisée à Bürgenstock. Dans l'ensemble, des attaques de ce type étaient attendues durant cette période et l'infrastructure informatique n'a subi que des perturbations mineures. À aucun moment, les systèmes informatiques et les données des deux manifestations ou des organisations participantes n'ont été sérieusement menacés.

Rançongiciels – un défi à la fois national et mondial

Une légère baisse est observable au niveau des entreprises ayant signalé une attaque par rançongiciel à l'OFCS. Durant la période sous revue, les groupes de rançongiciels *Akira*, *8Base* et *Black Basta* ont tous trois revendiqué des attaques contre des entreprises de tailles diverses, actives dans toutes sortes de secteurs. Quant aux particuliers, selon une tendance déjà constatée, ceux-ci se retrouvent de moins en moins dans la ligne de mire des cybercriminels. Le comportement résolument opportuniste des groupes de rançongiciels, qui concentrent désormais leurs efforts sur quelques cibles très lucratives, pourrait expliquer cette évolution. Au niveau international également, les attaques par rançongiciels constituent un défi de taille pour les entreprises privées comme pour les autorités étatiques.

Autres phénomènes

Ce rapport aborde encore les tendances et développements liés aux vulnérabilités, aux maliciels s'attaquant aux appareils mobiles et à l'accès initial. La gestion des données requiert, elle aussi, une grande vigilance. Car après une fuite de données, il est fréquent que des escrocs se servent des informations mises en circulation pour compromettre des systèmes informatiques ou lancer des attaques d'ingénierie sociale dans le cadre de leurs activités frauduleuses. Enfin, le rapport donne un aperçu des activités de cyberespionnage ou de sabotage qui ont été menées dans le contexte des tensions géopolitiques et durant cette année record en échéances électorales. Ce dernier chapitre repose essentiellement sur des observations faites à l'étranger, cependant un tour d'horizon des cybermenaces qui guettent la Suisse serait incomplet sans de telles informations.

Table des matières

Éditorial.....	4
1 Cybermenaces en Suisse – tour d’horizon	6
2 Hameçonnage	8
2.1 Essor de l’hameçonnage en chaîne.....	11
2.2 Le deuxième facteur, cible toujours plus prisée.....	11
3 Maliciels.....	12
3.1 Accès initial au moyen d’un maliciel	13
3.2 Rançongiciels.....	15
3.2.1 Activités des rançongiciels en Suisse	16
3.2.2 Les rançongiciels, un fléau mondial	18
3.3 Maliciels sur des appareils mobiles.....	20
4 Vulnérabilités	21
5 Fraude et ingénierie sociale	23
5.1 Usage de l’intelligence artificielle dans les tentatives d’escroquerie.....	24
5.2 Arnaque à la publicité pour des investissements.....	25
6 Attaques affectant la disponibilité de sites et de services Internet (DDoS)26	
7 Gestion des données, fuites de données et chantage	27
7.1 Fuites de données au niveau des fournisseurs	28
7.2 Commerce légal ou illégal des données.....	30
8 Cyberespionnage et sabotage.....	33
8.1 Cyberespionnage	33
8.1.1 Des institutions politiques sous pression.....	33
8.1.2 Développements internationaux dans le domaine du cybersespionnage.....	34
8.2 Menaces subies par les systèmes de contrôle industriels et par la technologie opérationnelle.....	37

Éditorial

L'Office fédéral de la cybersécurité (OFCS) revient sur ses 182 premiers jours d'activité. Ces six premiers mois ont été particulièrement intenses, entre plusieurs projets ambitieux, des décisions marquantes et le renforcement des nouvelles structures avec celles qui avaient déjà fait leurs preuves. Bien que la voie empruntée ne soit pas toujours facile, l'ensemble des collaborateurs et collaboratrices de l'OFCS veillent au quotidien à rendre la Suisse plus résiliente face aux cybermenaces.

Le développement de l'OFCS est un processus qui se développe à long terme, dont plusieurs étapes ont déjà été franchies. À la Conférence de haut niveau sur la paix en Ukraine à la mi-juin, l'OFCS a prouvé qu'il était en mesure de fournir à bref délai des prestations exceptionnelles, en collaboration avec ses partenaires. Notre office, qui assurait la coordination générale du réseau de suivi de la cybersituation, a su garantir en tout temps la (cyber)sécurité de tous les acteurs concernés et des infrastructures nécessaires à l'organisation de la conférence. Pour gérer au mieux la sécurité d'un événement aussi exposé dans un laps de temps restreint, il nous a fallu adopter une planification rigoureuse basée sur les risques et veiller à ce que toutes les forces d'intervention poursuivent les mêmes objectifs. En outre, toutes les organisations participantes devaient en tout temps avoir accès aux informations nécessaires et pouvoir ainsi agir de façon concertée. Cette performance a été possible grâce aux collaborateurs et collaboratrices de l'OFCS qui, avec leurs solides connaissances et leur bonne compréhension des cyberrisques, ont pu échanger sur un pied d'égalité avec tous nos partenaires et parties prenantes tant, sur le plan suisse qu'international. Outre ce volet de coordination, l'OFCS fut également responsable, en amont, de la gestion des vulnérabilités des infrastructures menacées ainsi que de la sensibilisation des organisations potentiellement exposées, ce qui l'a amené à intervenir dans la gestion des incidents. Je tiens à remercier ici tous nos partenaires pour leur collaboration exemplaire. Mes remerciements vont en particulier aux polices cantonales lucernoise et nidwaldienne, qui ont intégré notre personnel dans leurs propres organisations d'intervention. Mes équipes et moi-même sommes très heureux que cette expérience nous ait encore un peu plus rapprochés. Car ce n'est qu'ensemble que nous parviendrons à améliorer la cybersécurité de la Suisse.

Dans mon précédent éditorial, j'ai notamment parlé de la grande vulnérabilité des systèmes informatiques et de la capacité de réaction bien souvent encore faible, en cas de cyberincident d'importance systémique. Début juin 2024 la société *Synnovis*, qui fournit des prestations à plusieurs hôpitaux londoniens, a subi une attaque par rançongiciel. En raison des pannes informatiques ainsi causées, les établissements touchés ont dû reporter au cours des cinq semaines suivantes près de 6 000 rendez-vous pour des opérations ou des transfusions sanguines. Cela montre une fois de plus à quel point la cybersécurité est un enjeu clé. D'autant plus que de sérieux problèmes risquent d'apparaître, même sans défaillance particulière. Des cyberincidents qui, pris de manière isolée, n'ont pas d'impact direct sur la sécurité étatique peuvent causer des tensions et des pertes financières aux victimes, voire conduire à des faillites. En outre, leur cumul représente tôt ou tard une menace nationale. Il est donc important de ne pas se limiter à la cybersécurité des infrastructures critiques, mais aussi de veiller à ce que toutes les entreprises en Suisse, de la société unipersonnelle aux grands exploitants actifs dans les secteurs critiques, puissent accomplir leur travail sans subir de perturbations majeures.

Je me réjouis des défis à relever au deuxième semestre 2024 et j'espère que la lecture du présent rapport semestriel vous apportera beaucoup de nouvelles informations sur la manière de renforcer davantage votre cybersécurité.

Florian Schütz, directeur de l'Office fédéral de la cybersécurité

1 Cybermenaces en Suisse – tour d’horizon

Les cybermenaces font aujourd’hui partie intégrante de l’ensemble des menaces, en Suisse comme à l’étranger. Tandis que les tentatives d’hameçonnage (*phishing*), la diffusion de maliciels ou les activités d’espionnage dans le cyberspace sont des phénomènes qui sont restés constants au fil des ans, les cybercriminels ont recours à des méthodes et à des tactiques toujours plus raffinées pour les mettre en œuvre. Au premier semestre 2024, ce milieu dynamique a par exemple tiré parti de l’apprentissage automatique (*machine learning*, ML)¹ pour ses tentatives de fraude² ou d’hameçonnage³. Les escrocs élargissent constamment la palette des canaux qu’ils utilisent pour lancer leurs attaques et recourent ainsi toujours plus à des services comme Google Ads pour leurs fraudes à l’investissement par exemple. Parfois les innovations observées se répandent très vite, parfois il s’agit d’expériences uniques, l’analyse coûts-bénéfices n’ayant guère été concluante.

Au premier semestre 2024, l’OFCS a reçu au total 34 789 annonces de cyberincidents, soit 15 740 de plus qu’à la même période de l’année précédente. Ce quasi-doublement tient surtout aux signalements dits de « faux appels au nom de la police »⁴, de « jeux-concours frauduleux »⁵, d’« abonnements pièges »⁶ et d’hameçonnage. Les signalements d’appels téléphoniques de personnes se faisant passer pour une autorité de police⁷ ont très fortement augmenté au cours des semaines 10 à 18, comme le montrent les pics du graphique des annonces parvenues à l’OFCS (voir fig. 1). Les mesures adoptées par les opérateurs de télécommunication ont toutefois permis de stopper cette vague d’appels frauduleux en juin 2024, ce qui s’est confirmé par le recul constant du nombre de cyberincidents signalés à la fin de la période de référence.

Parmi les annonces, la majorité (90 %) émanaient de la population, contre seulement 10 % d’annonces de la part d’entreprises⁸. Sans surprise, la plupart des annonces concernaient des cas de fraude, d’hameçonnage et de pourriels (voir fig. 2). Quant aux attaques par rançongiciel⁹ visant les entreprises, le nombre d’incidents signalés a reculé. Ainsi l’OFCS avait reçu 56 annonces de ce type au deuxième semestre 2023, contre 39 durant la période sous revue. De même, moins d’une dizaine de cas de rançongiciel rapportés à l’OFCS ont affecté des particuliers. Bien qu’un écart entre le nombre d’incidents déclarés et la réalité ne puisse être exclu, les cybercriminels réservent visiblement leurs rançongiciels à quelques cibles très lucratives, au lieu de multiplier les attaques contre des victimes ne leur rapportant que peu d’argent.

¹ [Apprentissage automatique \(wikipedia.org\)](https://fr.wikipedia.org/wiki/Apprentissage_automatique)

² Voir [Jeux-concours frauduleux \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/ncsc/fr/ressources/actualites/jeux-concours-frauduleux), [Offres d’emploi frauduleuses \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/ncsc/fr/ressources/actualites/offres-d-emploi-frauduleuses), [Fake-Support \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/ncsc/fr/ressources/actualites/fake-support), ou aussi [Arnaque au président \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/ncsc/fr/ressources/actualites/arnaques-au-president)

³ [Hameçonnage \(phishing\), vishing, smishing \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/ncsc/fr/ressources/actualites/hameconnage-phishing-vishing-smishing)

⁴ [Appels au nom de fausses autorités \(police, douanes\) \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/ncsc/fr/ressources/actualites/appels-au-nom-de-fausses-autorites-police-douanes)

⁵ [Jeux-concours frauduleux \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/ncsc/fr/ressources/actualites/jeux-concours-frauduleux)

⁶ [Abonnements pièges \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/ncsc/fr/ressources/actualites/abonnements-pieges)

⁷ L’OFCS a rédigé un rapport qui a été publié en même temps que le rapport semestriel afin d’approfondir le phénomène des « appels au nom des fausses autorités ». Le rapport met en lumière, entre autres, les derniers développements liés à ce phénomène, les différentes approches et les technologies utilisées à cet effet ainsi que la situation juridique nationale et internationale.

⁸ La catégorie entreprise inclut les associations et les autorités.

⁹ [Rançongiciels \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/ncsc/fr/ressources/actualites/rancongiels)

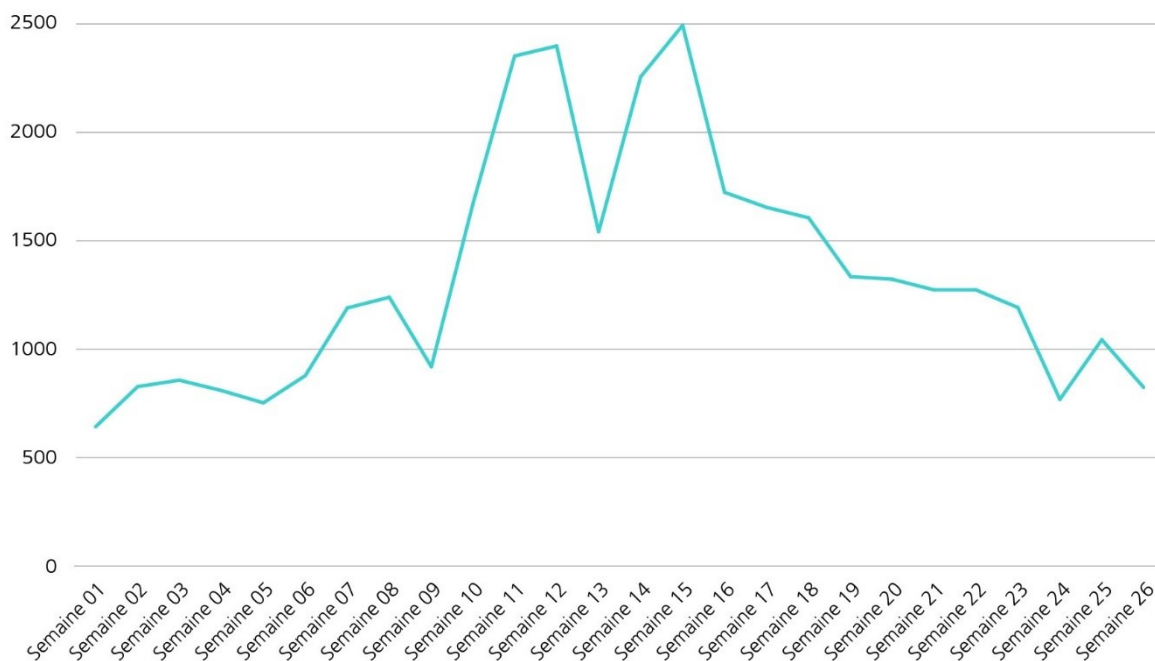


Fig. 1 : nombre d'annonces par semaine parvenues à l'OFCS, de janvier à juin 2024, voir aussi [chiffres actuels \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/chiffres-actuels).

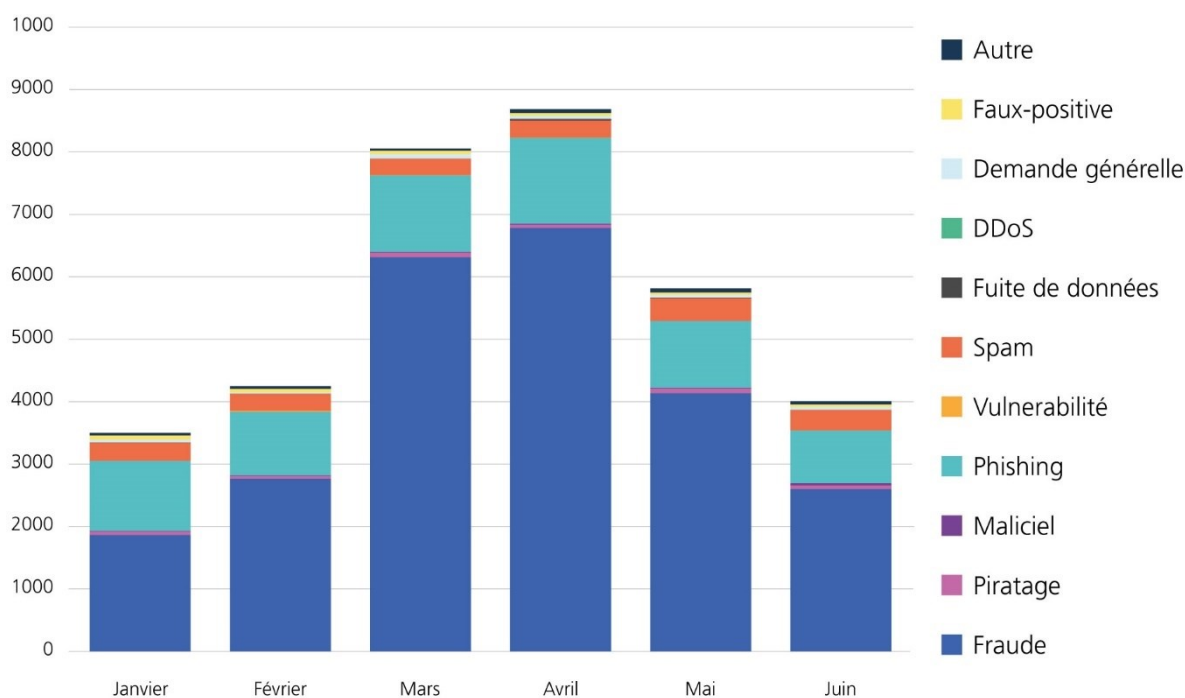


Fig. 2 : annonces parvenues à l'OFCS durant le premier semestre 2024, selon la catégorie, voir aussi [chiffres actuels \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/chiffres-actuels).

Cette statistique montre que la cybersécurité et la protection de la Suisse face aux cyberrisques constituent un défi permanent pour l'économie, l'État et la société. Avec la création au 1^{er} janvier 2024 de l'Office fédéral de la cybersécurité (OFCS), la structure du

rapport semestriel, publié deux fois par an, a également été remaniée¹⁰. Le rapport semestriel aborde désormais, dans chaque chapitre, des phénomènes au cœur de l'ensemble des cybermenaces que connaît la Suisse, à savoir l'hameçonnage, les maliciels, les vulnérabilités, les cas de fraude et d'ingénierie sociale¹¹, les attaques affectant la disponibilité (*DDoS*) des services exposés à Internet, les fuites de données ainsi que le cyberespionnage et le cybersabotage. La priorité reste d'informer le grand public sur les questions de cybersécurité. Le rapport semestriel vise à exposer, à partir d'incidents réels, les cybermenaces et les défis actuels, ainsi qu'à formuler des recommandations pour la population. Selon le principe de la responsabilité individuelle, il incombe à tout un chacun de contribuer, dans les limites de ses capacités et possibilités, à une Suisse sûre dans le cyberspace.

2 Hameçonnage

Les sites d'hameçonnage comptent avec les cas d'escroquerie parmi les éléments les plus fréquemment signalés à l'OFCS. Ils permettent à des acteurs malveillants de collecter des données d'accès, des informations financières et/ou confidentielles d'internautes trop confiants. Souvent, l'hameçonnage vise à tromper les utilisateurs et utilisatrices par des techniques d'ingénierie sociale, afin de les inciter à installer des maliciels. Dans ces cas, les logiciels malveillants n'y jouent qu'un rôle secondaire¹². Tandis que l'envoi de courriels à grande échelle reste la méthode privilégiée en la matière, d'autres approches misent sur un contact de vive voix (*voice phishing* ou *vishing*) ou sur l'envoi de SMS (*smishing*) pour accéder à des informations sensibles.

L'OFCS a reçu au premier semestre 2024, via son formulaire d'annonce, beaucoup plus de signalements¹³ de sites d'hameçonnage (6 643) qu'un an plus tôt à la même période (3 879). La plupart des modes opératoires décrits dans les signalements ne changent pas. Les alertes falsifiées de distribution de colis continuent d'être une méthode très employée par les auteurs. Le répertoire habituel des hameçonneurs comprend aussi les prétendus courriels de remboursement expédiés au nom de divers fournisseurs, des CFF respectivement de SwissPass, ou de différentes administrations fiscales. D'autres données statistiques documentant les campagnes d'hameçonnage menées en Suisse livrent des résultats similaires. Le nombre d'URL de phishing vérifiées et confirmées par l'OFCS est également en hausse. Alors qu'au premier semestre 2023, 4 765 URL de *phishing* uniques lui avaient été signalées, ce chiffre a largement doublé durant la période sous revue (11 505 URL de *phishing*). La fig. 3 illustre l'évolution hebdomadaire. Afin de rendre leurs sites d'hameçonnage aussi crédibles que possible, les escrocs usurpent régulièrement des noms de marques et d'entreprises connues. Au premier semestre 2024, de tels abus se sont concentrés principalement sur le secteur financier (26 %), les services postaux (24 %), les transports

¹⁰ Les rapports semestriels sont tous publiés dans la rubrique [Rapports sur la situation \(ncsc.admin.ch\)](https://ncsc.admin.ch).

¹¹ [Ingénierie sociale \(social engineering\) \(ncsc.admin.ch\)](https://ncsc.admin.ch)

¹² Au niveau international, le phénomène d'hameçonnage ne recouvre pas partout la même réalité. D'autres définitions incluent la diffusion de maliciels (voir [Phishing \(attack.mitre.org\)](https://attack.mitre.org)). L'OFCS exclut expressément cet aspect dans sa définition d'hameçonnage.

¹³ Outre les cas d'hameçonnage qui lui sont directement signalés, l'OFCS en inclut d'autres reçus par le biais de l'initiative antiphishing.ch. Cette source constitue une précieuse source d'informations en la matière. Par conséquent, les chiffres indiqués ici peuvent différer du nombre d'annonces directes de cas d'hameçonnage.

publics (23 %), les télécommunications (11 %) et le secteur informatique (8 %). Ces pourcentages sont restés plus ou moins constants au fil des mois (voir fig. 4).

Afin de protéger la population au maximum, l'OFCS s'efforce de faire bloquer au plus vite les sites d'hameçonnage. De leur côté, les escrocs mettent tout en œuvre pour empêcher cette désactivation rapide. Ils sont constamment à l'affût de nouvelles méthodes visant à empêcher les autorités de sécurité d'apprendre l'existence de leurs sites. Entre-temps, certains sites d'hameçonnage ne peuvent être consultés qu'avec une configuration spécifique. Une variante très prisée consiste à réserver l'accès à de tels sites frauduleux aux smartphones, tous les accès à partir d'ordinateurs ou d'autres appareils étant redirigés vers les sites Internet légitimes. La plupart des internautes ne naviguent en effet sur Internet plus que depuis des smartphones, alors que les autorités de sécurité utilisent des ordinateurs.

Une autre approche basée sur un mécanisme autosélectif est apparue durant la période sous revue¹⁴. Au lieu d'envoyer directement un courriel qui contiendrait un lien à leur site d'hameçonnage, les escrocs expédient un courriel inoffensif en priant la victime d'y répondre. Dans un second temps, après avoir reçu une réponse, ils lui renvoient par courriel le lien d'hameçonnage. Il s'agit dès lors d'un courriel préparé et transmis automatiquement à l'expéditeur, indépendamment de ce qu'il a pu écrire. Cette approche vise à éviter une diffusion à large échelle du lien vers le site d'hameçonnage et à retarder ainsi son signalement aux autorités de sécurité, telles que l'OFCS. Autrement dit, seules les personnes n'ayant pas reconnu la tentative d'escroquerie et qui ne la dénonceront probablement pas non plus reçoivent un tel lien. Cette précaution accroît la probabilité que le site frauduleux reste plus longtemps en ligne et touche ainsi davantage de victimes potentielles afin de leur soutirer les données de leur carte de crédit ou leur mot de passe.

Une campagne d'hameçonnage visant la clientèle de PostFinance et tirant parti d'un canal de diffusion rarement utilisé¹⁵ a encore retenu l'attention des médias. En mai 2024, les escrocs ont envoyé par courrier des lettres contenant un code QR renvoyant à un site frauduleux. Leur missive s'intitulait « Réactivation de votre accès e-banking nécessaire ». L'entreprise PostFinance a rappelé dans sa communication qu'elle n'envoyait jamais de telles lettres et qu'il fallait donc ignorer les prétendues instructions qu'elles renferment¹⁶.



Recommandations

Signalez à l'OFCS les sites présentant un risque d'hameçonnage via reports@antiphishing.ch ou directement sur la plateforme antiphishing.ch. Ceci est un processus automatique. Pour obtenir un suivi de votre annonce, vous pouvez aussi signaler un tel incident à nos spécialistes au moyen du [formulaire d'annonce](#) ou par courriel à incidents@ncsc.ch. Avec votre aide, l'OFCS pourra lancer des mises en garde ciblées et adopter les mesures nécessaires afin que ces sites soient retirés d'Internet.

¹⁴ [Semaine 11 : Le recyclage, c'est bien, mais pas pour les mots de passe \(ncsc.admin.ch\)](#)

¹⁵ Voir notamment [Phishing: Brief von Postfinance entpuppt sich als Betrugsversuch \(srf.ch\)](#), [Phishing: Postfinance met en garde contre des nouvelles lettres d'arnaque \(blick.ch\)](#)

¹⁶ [Des lettres de phishing avec un faux code QR en circulation \(postfinance.ch\)](#)



Fig. 3 : nombre d'URL de phishing vérifiées et confirmées par l'OFCS par semaine au cours du premier semestre 2024.

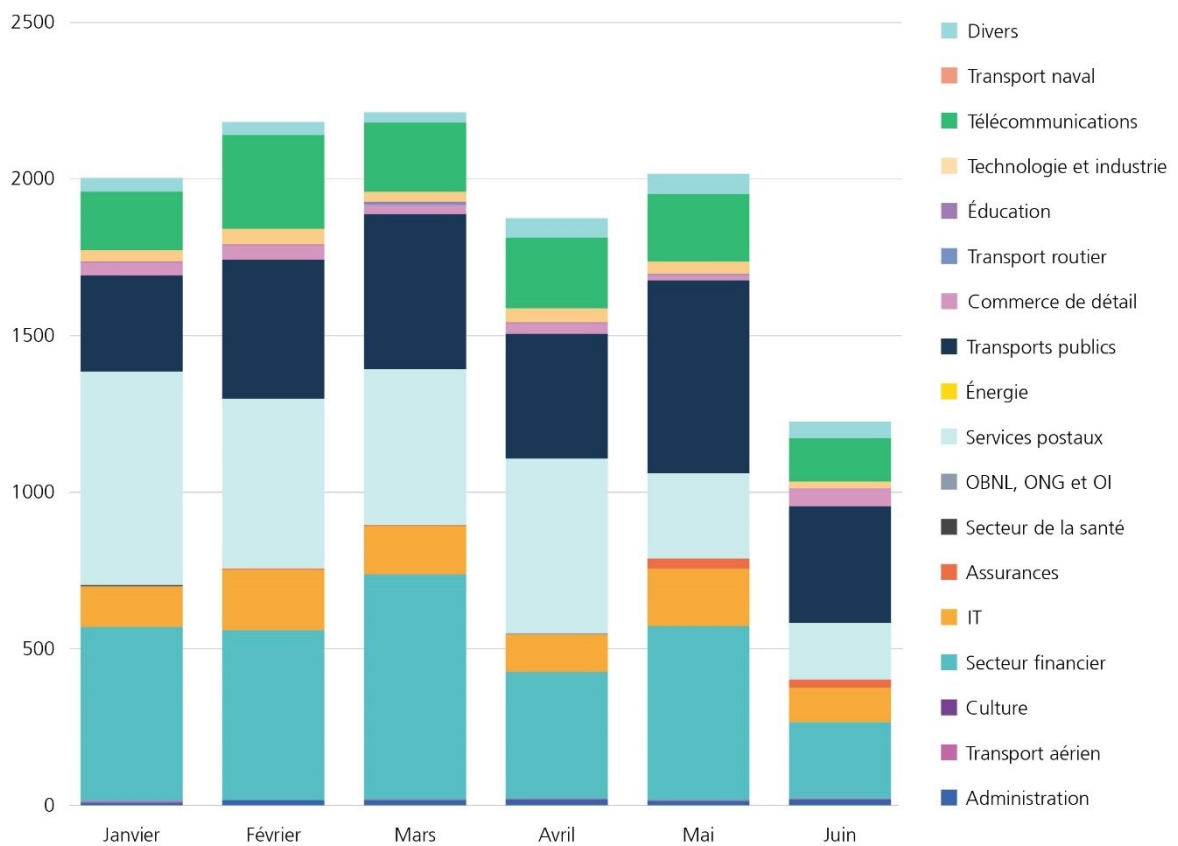


Fig. 4 : nombre d'URL de phishing vérifiées et confirmées par l'OFCS au cours du premier semestre 2024, ventilées par secteur sur la base des noms de marques usurpés.

2.1 Essor de l'hameçonnage en chaîne

Des tentatives d'hameçonnage visant des comptes Office 365 sont régulièrement signalées à l'OFCS. Dans bien des cas, l'approche observée s'apparente à un système boule de neige. Dès qu'une victime a dévoilé son mot de passe sur un site frauduleux, les cybercriminels piratent son compte et envoient le même courriel d'hameçonnage à tous ses contacts. Si l'un des destinataires se fait piéger à son tour, le processus continue grâce à cette personne. Ce mode opératoire aboutissant très vite au piratage de nombreux comptes, il a reçu le nom d'« hameçonnage en chaîne ». Le but n'est toutefois pas d'emblée clair, car à première vue, aucun dommage direct n'est visible. Et comme tous les contacts figurant dans le carnet d'adresses du compte piraté reçoivent à leur tour un message, il est probable que l'un des destinataires détecte le piège, qu'il en informe la victime et signale la campagne d'hameçonnage. La victime n'a plus alors qu'à réinitialiser ses mots de passe, et la valeur du compte piraté semble dès lors nulle pour les escrocs. Une telle approche peut néanmoins s'avérer lucrative pour les cybercriminels, s'ils téléchargent tous les courriels de la victime aussitôt après avoir piraté son compte. Ils n'auront plus qu'à les passer au crible, à la recherche de matériel exploitable pour de futures attaques ciblées. En effet, ce genre d'attaque par courriel abuse souvent de la référence à un précédent échange. Il se peut encore que les pirates mettent en vente les courriels dérobés sur des forums criminels (voir chap. 7.2). Une autre possibilité consiste à créer une règle de redirection pour que tous les courriers entrants parviennent aux escrocs. Cette règle demeurera valable même après un changement de mot de passe et il arrive souvent qu'elle passe inaperçue. Les escrocs pourront ainsi accéder plus tard à d'autres comptes – généralement les réseaux sociaux – grâce à la fonction de réinitialisation du mot de passe.

2.2 Le deuxième facteur, cible toujours plus prisée

L'OFCS recommande systématiquement d'activer si possible à l'avenir l'authentification multifactorielle, à chaque fois qu'un incident d'hameçonnage lui est signalé. L'authentification multifactorielle (MFA) est une méthode exigeant que l'utilisateur s'identifie de deux manières différentes ou plus pour accéder à la ressource souhaitée¹⁷. Il peut s'agir typiquement d'une information connue de l'utilisateur (par ex. mot de passe), d'un objet en sa possession (par ex. un smartphone ou jeton d'authentification¹⁸) ou encore de certains traits physiques (par ex. données biométriques, comme une empreinte digitale ou la reconnaissance faciale).

L'activation de l'authentification multifactorielle rend un compte beaucoup plus sûr. La sûreté n'en n'est cependant pas garantie. Même après avoir activé la MFA, la prudence s'impose en ligne. Si des utilisateurs et utilisatrices réagissent à des requêtes, courriels ou appels téléphoniques falsifiés et révèlent ainsi leurs autres facteurs d'authentification, la MFA peut elle aussi être contournée. L'OFCS a ainsi observé au premier semestre 2024 que toujours plus de sites d'hameçonnage tentent d'accéder au facteur de sécurité supplémentaire, à l'instar du mot de passe à usage unique. Des appels frauduleux sont également lancés à cet effet (voir chap. 5). Les escrocs convainquent la victime de télécharger un logiciel d'accès à

¹⁷ [S-U-P-E-R.ch – Double protection \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/s-u-p-e-r.ch)

¹⁸ Un jeton d'authentification est un dispositif de sécurité servant à valider l'identité d'un utilisateur, voir aussi [Jeton d'authentification \(wikipedia.org\)](https://fr.wikipedia.org/wiki/Jeton_d'authentification).

distance et une fois cela fait, ils incitent la victime à se connecter à son compte, leur donnant dès lors accès en temps réel à l'ordinateur et le compte de la victime. Les cybercriminels peuvent ainsi suivre les activités à l'écran de leur victime et manipuler discrètement l'ordinateur. De tels cas révèlent que la méthode multifactorielle ne garantit pas une protection absolue contre les accès indésirables. Il réduit surtout le temps dont dispose un cybercriminel pour agir. Partout où l'authentification multifactorielle est en place, les escrocs ne peuvent accéder au compte de leur victime qu'au moment précis où celle-ci s'y connecte. Tout accès ultérieur est impossible. À titre de comparaison, un pirate peut utiliser comme bon lui semble un compte protégé uniquement par mot de passe, jusqu'à ce que le mot de passe piraté ait été modifié.

Bien que l'usage au quotidien de nombreux services numériques se soit généralisé – de la messagerie aux comptes bancaires, en passant par les réseaux sociaux – la MFA reste un mal nécessaire aux yeux de nombreuses personnes. Or, plus les utilisateurs sont invités à activer des options d'authentification supplémentaires, plus ce surcroît d'efforts risque d'être mal perçu. Certaines personnes auront tendance à se montrer moins prudentes et à négliger les bonnes pratiques de sécurité. Ce phénomène a été baptisé *MFA fatigue*. Les invitations constantes à ouvrir des applications d'authentification, à saisir des codes SMS ou à utiliser des jetons de sécurité peuvent finir par être agaçantes et lassantes. À cela s'ajoute que bien des méthodes d'authentification multifactorielle ne sont pas toujours fiables¹⁹. Des codes SMS peuvent ainsi arriver tardivement ou des applications d'authentification peuvent présenter des problèmes techniques. Les escrocs savent entre-temps exploiter cette situation à leur profit. Ils bombardent les titulaires d'un compte de demandes de vérification, jusqu'à ce que la personne lassée ou dans le feu de l'action, donne accès à leur compte.



Recommandations

Activez autant que possible l'**authentification multifactorielle (MFA)** pour accroître la sécurité de vos comptes. Elle réduit significativement le risque de compromission, mais ne protège pas des techniques d'ingénierie sociale²⁰. Méfiez-vous donc des demandes frauduleuses, transmises par courriel ou SMS, vous invitant à confirmer vos coordonnées d'accès ou à divulguer la clé générée par votre jeton d'authentification. N'oubliez pas non plus qu'il est facile de falsifier l'adresse de l'expéditeur d'un courriel ou un numéro de téléphone.

3 Maliciels

En comparaison à d'autres sources qui recensent la distribution de maliciels en Suisse²¹, l'OFCS n'a reçu qu'assez peu d'annonces (92) en rapport direct avec cette cybermenace. Un maliciel (*malware*)²² est conçu pour exécuter à l'aide d'autres programmes des fonctions

¹⁹ Voir [Zweiter Faktor SMS: Noch schlechter als sein Ruf \(ccc.de\)](#)

²⁰ [Ingénierie sociale \(social engineering\) \(ncsc.admin.ch\)](#)

²¹ Voir [Statistics \(abuse.ch\)](#)

²² [Logiciels malveillants \(ncsc.admin.ch\)](#)

indésirables et généralement malveillantes sur des systèmes informatiques. Comme ce genre d'activité intervient généralement à l'insu de l'utilisateur légitime²³, cela peut expliquer le nombre plutôt faible de cas signalés par la population, notamment pour les maliciels diffusés par courriel. En outre, les méthodes de filtrage employées par les fabricants de logiciels sont aujourd'hui d'un tel niveau que seul un faible pourcentage des courriels renfermant des contenus malveillants parvient à destination. De plus, les mesures de sécurité prévues sur les terminaux ont été perfectionnées à un tel point que plusieurs interactions de l'utilisateur sont désormais nécessaires, avant qu'un fichier malveillant ne puisse être installé. Toutes ces interactions constituent également des éléments de mises en garde que l'utilisateur pourraient remarquer. Tout indique que les pirates privilégient d'autres approches pour installer des maliciels, par exemple en dissimulant leurs programmes malveillants dans des logiciels gratuits, des plugiciels ou des applications n'offrant pas la même transparence à l'utilisateur. De tels incidents sont donc plus rarement signalés. Une vaste campagne a néanmoins été observée durant la période sous revue, avec un maliciel du nom de *Poseidon Stealer*, qui touchait les utilisateurs de MacOS (voir chap. 3.1). Fin juin 2024, de nombreux citoyens de Suisse alémanique ont reçu un courriel intitulé « À partir du mois de juillet 2024, l'accès AGOV sera obligatoire pour tous les services publics »²⁴. Il visait à amener les destinataires à installer un logiciel censé leur garantir un accès sans faille à l'administration publique. Comme pour l'hameçonnage, la diffusion des maliciels dépend souvent du facteur humain. Plus le prétexte semble crédible, plus la probabilité que les acteurs mal intentionnés réussissent à installer leur maliciel est grande.

3.1 Accès initial au moyen d'un maliciel

Pour accéder à un système informatique, les cybercriminels ont souvent recours à des logiciels malveillants, par exemple à des chevaux de Troie. Comme il faut en général que l'utilisateur accomplisse une action spécifique, ils ont mis au point divers mécanismes de tromperie. Par exemple, le maliciel peut être dissimulé dans un autre programme, dans un document annexé ou dans un lien transmis par courriel, qu'un utilisateur non averti croira inoffensif. Bien des maliciels observés au niveau international ont également été repérés en Suisse, comme *AgentTesla*, *DarkGate*, *FakeUpdates*, *Formbook*, *Gootloader*, *GuLoader*, *PikaBot* ou *Poseidon Stealer*²⁵. Le présent sous-chapitre revient plus en détail sur les deux derniers de cette liste, où les méthodes de diffusion employées en Suisse ainsi que les facteurs susceptibles d'en maximiser l'impact seront exposés.

En début d'année, il est apparu à diverses reprises que pour diffuser leur maliciel *PikaBot*, les escrocs aient d'abord lancé des attaques ciblées en détournant des conversations de courriels (*e-mail thread hijacking*). Ils ont ainsi pu se servir d'anciennes correspondances dérobées dans d'autres comptes de messagerie (voir chap. 2.1) afin de tromper leurs victimes (voir fig. 5).

²³ [BSI - Malware \(bsi.bund.de\)](https://www.bsi.bund.de)

²⁴ [Des cybercriminels diffusent des maliciels pour macOS au nom d'AGOV \(ncsc.admin.ch\)](https://www.ncsc.admin.ch)

²⁵ [Brève analyse technique du maliciel « Poseidon Stealer » \(ncsc.admin.ch\)](https://www.ncsc.admin.ch)

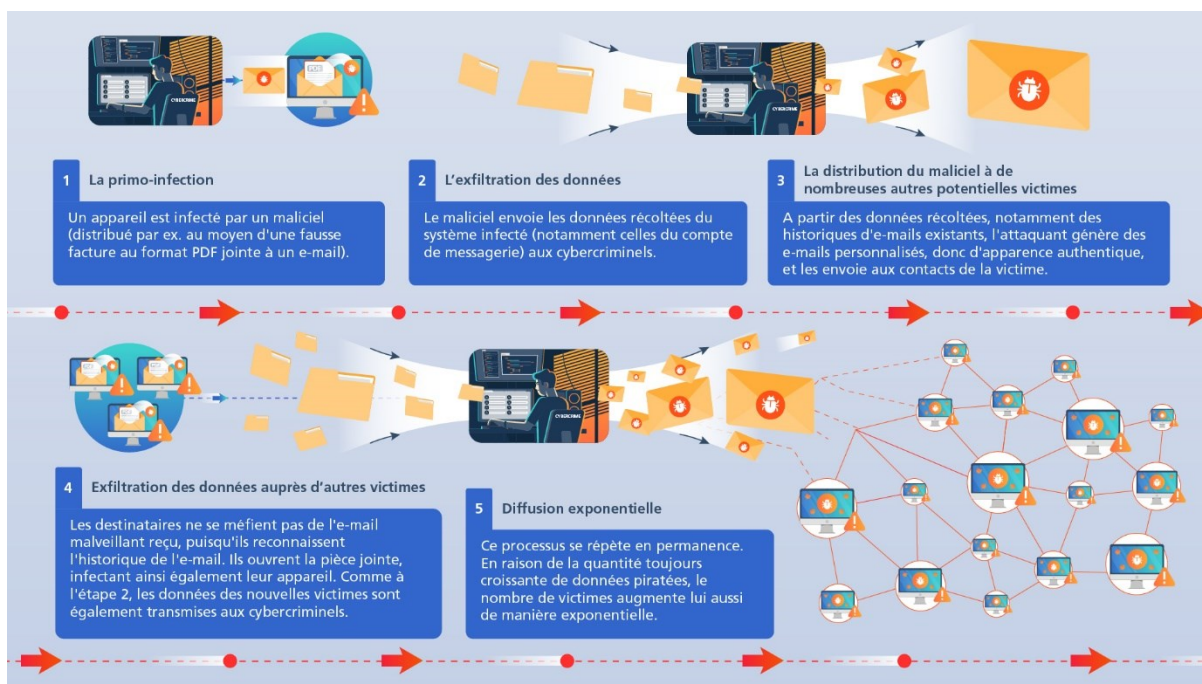


Fig. 5 : détournement de conversations en vue de la diffusion de maliciels.

Par exemple, le document annexé à l'email est un fichier Excel, signalant à l'utilisateur que des fichiers sont à sa disposition en ligne et qu'il faut cliquer sur un certain bouton pour les afficher²⁶. Or, ce bouton masque un script qui conduit à une infection par *PikaBot*. En effet une telle infection peut être d'autant plus lourde de conséquences que, depuis le deuxième semestre 2023, ce maliciel a fréquemment été employé en combinaison avec différents rançongiciels²⁷. En mai 2024, dans le cadre de la coopération judiciaire internationale, les autorités de poursuite pénale de divers pays ont déployé une vaste opération baptisée *Endgame* visant au démantèlement de plateformes criminelles de services d'accès initial et de distribution de maliciels (*malware-as-a-service*)²⁸. Ce coup de filet visait notamment l'infrastructure de *PikaBot*. À court terme, on peut considérer que l'opération a réduit cette menace en Suisse. Mais de tels effets ne sont que rarement durables, car d'une part tant que les auteurs de maliciels n'ont pas été arrêtés, ils s'empressent de reconstruire leur infrastructure. D'autre part les criminels qui y recourent s'adressent rapidement à d'autres fournisseurs si une infrastructure est démantelée.

Fin juin 2024, l'OFCS a communiqué qu'une campagne de *malspam*²⁹ censée émaner d'AGOV cherchait à infecter les utilisateurs de MacOS en Suisse alémanique avec le maliciel *Poseidon Stealer*³⁰. Le lien figurant dans un courriel conduisait à un site Internet invitant le destinataire à télécharger un fichier avec l'extension .dmg. Ce fichier présenté comme une application de bureau AGOV était en réalité le maliciel *Poseidon Stealer*. Une fois installé, il

²⁶ [TA577 introduced a rather interesting new approach to distribute their Pikabot malware \(x.com\)](#)

²⁷ [The Emerging Threat of PikaBot Malware \(flashpoint.io\)](#)

²⁸ [Largest ever operation against botnets hits dropper malware ecosystem \(europol.europa.eu\)](#)

²⁹ [Qu'est-ce qu'un spam : le guide essentiel de détection et de prévention des spams \(avast.com\)](#)

³⁰ [Des cybercriminels diffusent des maliciels pour macOS au nom d'AGOV \(ncsc.admin.ch\)](#)

dérobait des informations présentes sur l'ordinateur de la victime pour les transmettre aux cybercriminels. Il est intéressant de noter que cette campagne suisse coïncidait avec une autre menée à l'étranger. Quelques jours plus tôt, des publicités frauduleuses (*malvertising*)³¹ pour le nouveau navigateur *Arc* avaient servi au déploiement d'une campagne internationale de distribution de ce même maliciel³². Dans cette attaque ciblée, les internautes ayant souhaité accéder par un moteur de recherche à *Arc* étaient incités à cliquer sur le résultat « sponsorisé » par les escrocs plutôt que sur le lien officiel.



Recommandations

Ne cliquez pas sur les liens dans les courriels suspects et n'ouvrez aucun fichier joint que vous n'attendriez pas de l'expéditeur. En cas de doute, demandez à l'expéditeur supposé, par d'autres canaux, si le courriel en question émane bien de lui.

Lorsque vous recherchez des logiciels sur Internet, vérifiez avant de les télécharger que vous vous trouvez sur le site officiel du fabricant ou sur un autre site de confiance (par ex. magazine informatique connu). Lorsque vous utilisez des moteurs de recherche, vérifiez si le site Internet affiché est déclaré ou non comme publicité payante.

Faites preuve de prudence chaque fois qu'une fenêtre de téléchargement s'ouvre.

Laissez si possible les programmes s'actualiser automatiquement. Servez-vous toujours de la fonction de mise à jour intégrée, ou téléchargez la dernière version en date directement chez le fabricant.

Ne connectez pas d'appareil USB inconnu ou trouvé à votre ordinateur.

3.2 Rançongiciels

Les attaques par rançongiciels³³ font régulièrement la une des journaux, donnant lieu à de nombreuses analyses³⁴. Dans ce genre d'opération, les cybercriminels chiffrent les données

³¹ La publicité frauduleuse (*malvertising*) est une technique de cyberattaque consistant à injecter dans des publicités numériques un code malveillant qui s'installera ensuite sur l'appareil des visiteurs, voir [NCSC For Startups: taking on malvertising \(ncsc.gov.uk\)](https://www.ncsc.gov.uk/startups-taking-on-malvertising).

³² ['Poseidon' Mac stealer distributed via Google ads \(malwarebytes.com\)](https://malwarebytes.com/blog/news/2023/01/poseidon-mac-stealer-distributed-via-google-ads)

³³ [Rançongiciels \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/ranconware)

³⁴ Voir le compte rendu consacré par la Neue Zürcher Zeitung (NZZ) à l'incident de 2023 dû au rançongiciel *Play* : [Kriminelle Hacker greifen die NZZ an: das Protokoll der Krise \(nzz.ch\)](https://www.nzz.ch/kriminele-hacker-greifen-die-nzz-an-das-protokoll-der-krise), Interview avec le directeur de la société *Xplain* sur l'incident de 2023 dû au rançongiciel *Play* : [Xplain-CEO: «Es war nicht vorgesehen, dass wir produktive Daten bei uns haben» \(inside-it.ch\)](https://www.inside-it.ch/news/2023/01/15/xplain-ceo-es-war-nicht-vorgesehen-dass-wir-produktive-daten-bei-uns-haben), Rapport de l'OFCS concernant les analyses de données effectuées après l'attaque lancée en 2023 par le rançongiciel *Play* contre l'entreprise *Xplain* : [Cyberattaque contre l'entreprise Xplain : publication du rapport de l'Office fédéral de la cybersécurité sur l'analyse des données \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/office-federal-de-la-cybersécurité-sur-lanalyse-des-données) Rapport final de l'enquête administrative sur l'incident de 2023 dû au rançongiciel *Play* : [Clôture de l'enquête administrative concernant la cyberattaque contre Xplain SA : le Conseil fédéral adopte des mesures \(admin.ch\)](https://www.admin.ch/gov/fr/accueil/document/ADM_73333)

des systèmes informatiques de leur victime à l'aide d'un maliciel et en bloquent ainsi l'accès. Parallèlement, ils exfiltrent généralement aussi les données. Après quoi les escrocs demandent à leur victime de leur verser une rançon en échange d'un outil de déchiffrement (clé de déchiffrement) et de la non-publication ou de la non-revente des données dérobées. L'ampleur des dommages peut varier. Si les attaques ne causent guère de dommages aux entreprises ayant une bonne cyberhygiène, elles peuvent mettre en péril celles mal préparées³⁵. Au-delà des coûts à payer pour la restauration des données, les entreprises doivent poursuivre leur activité opérationnelle pendant plusieurs jours voire plusieurs semaines avec des services informatiques fonctionnant de manière limitée ou qui sont totalement indisponibles. En outre, la publication des données dérobées peut causer un grave préjudice à la réputation des entreprises.

3.2.1 Activités des rançongiciels en Suisse

Le nombre de signalements à l'OFCS relatifs à des attaques par rançongiciel contre des entreprises est en légère baisse. Au premier semestre 2024, seules 39 annonces sont parvenues à l'OFCS, contre 56 à la même période un an plus tôt. De même, la tendance actuelle se poursuit en ce qui concerne les particuliers : Ceux-ci sont de moins en moins dans la ligne de mire des cybercriminels. Cinq annonces seulement émanent de particuliers, contre huit à la même période de l'année précédente. Une meilleure sensibilisation des utilisateurs et la mise en place de sauvegardes (hors ligne) pourraient avoir contribué à cette évolution. Une autre explication réside dans le fait que les attaques se concentrent toujours plus sur des cibles très lucratives. Si l'objectif est d'exercer une pression maximale afin d'obtenir le paiement de la rançon demandée, il en résulte un surcroît d'efforts et les cybercriminels auront tendance à réduire le nombre de cyberattaques avec les ressources à leur disposition. Quant aux victimes jugées peu intéressantes, mais dont ils auraient réussi à pirater les systèmes, elles leur feront également gagner de l'argent grâce à la revente illégale des informations dérobées (voir chap. 0).

Les groupes de rançongiciels *Akira*, *8Base* et *Black Basta* ont tous trois revendiqué des attaques contre des entreprises de tailles diverses et actives dans toutes sortes de secteurs. En particulier, au moins neuf infections par rançongiciel signalées par des entreprises suisses à l'OFCS concernent le rançongiciel *Akira*, trois d'entre elles sont survenues durant le mois de mars. Ce groupe se caractérise par ses attaques opportunistes, perpétrées contre un nombre relativement élevé de victimes, de tailles diverses et actives dans différents secteurs. Alors même que ce groupe n'est actif que depuis mars 2023, on estime qu'il aurait déjà attaqué jusqu'au début de cette année près de 250 organisations situées en Europe, en Amérique du Nord et en Australie³⁶. *Akira* adopte une approche novatrice : selon le NCSC finlandais, ce groupe a tiré par exemple profit d'une faille de sécurité du VPN de CISCO pour chiffrer

Rapport d'enquête du Préposé fédéral à la protection des données et à la transparence (PFPDT) sur l'incident de 2023 dû au rançongiciel *Play* : [Le PFPDT clôt les enquêtes contre l'entreprise Xplain, ainsi que les offices fédéraux fedpol et OFDF \(edoeb.admin.ch\)](#)

³⁵ Voir notamment *Akumin Inc.*, *CloudNordic*, *KNP Logistics*, *MediSecure*, *Travelex*, *United Structures*

³⁶ [#StopRansomware: Akira Ransomware \(cisa.gov\)](#)

systématiquement les systèmes NAS (stockage en réseau) et les sauvegardes de sauvegardes³⁷.

Le rançongiciel *8Base* a fait un peu moins de victimes qu'*Akira*, avec trois cas seulement signalés en Suisse. *8Base* s'est fait connaître en novembre 2023, lorsqu'il était parvenu à compromettre l'entreprise informatique suisse *Concevis SA*³⁸. Ce groupe recourt au chiffrement des données et à des techniques d'extorsion (de type *name and shame*), afin de pousser ses victimes issues de différentes branches d'activité à payer une rançon³⁹. Des échantillons de ce rançongiciel révèlent qu'il s'agit d'une version adaptée du rançongiciel *Phobos v2.9.1*⁴⁰, distribuée au moyen du maliciel *SmokeLoader*⁴¹. Deux des victimes suisses ont ainsi été mises au-devant de la scène malgré elles en 2024, suite à la parution de données dérobées sur la page du groupe consacrée aux fuites d'informations. La première victime, *Nexus Telecom Switzerland AG*⁴², n'a subi que peu de conséquences de la publication de 23 gigaoctets (Go) de données : Il s'agissait essentiellement de données d'archives et cette société n'avait pas de client suisse. La deuxième victime, *Mikrona*, fournisseur d'orthodontistes, de dentistes et de prothésistes dentaires, n'a pas eu d'interruption de son activité de production, selon ses propres dires. Grâce aux copies de sécurité disponibles, les systèmes opérationnels touchés ont à nouveau été en état de complètement fonctionner après quelques jours. Bien que *Mikrona* ait réagi très vite, on peut toutefois supposer que des données aient été compromises⁴³.

Le groupe de rançongiciel *Black Basta*⁴⁴ s'est fait remarquer par ses opérations menées en Suisse entre février et avril 2024, affectant trois grandes entreprises, dont un fournisseur pour des infrastructures critiques entre autres. En février et mars 2024, *Black Basta* a ainsi déclaré l'agence de recrutement *Das Team AG* et le marchand de jouets *Franz Carl Weber* comme nouvelle victime sur sa page de fuites de données. Ces deux sociétés n'ayant visiblement pas cédé à leur chantage, les escrocs ont publié des données, lesquelles étaient parfois sensibles⁴⁵. À la différence d'*Akira* ou de *8Base* par exemple, *Black Basta* se montre particulièrement sélectif dans le choix de ses victimes. Ce groupe compromet régulièrement de prestigieuses entreprises ou organisations, pour leur réclamer des rançons élevées. Cela s'est vérifié en avril 2024 lors de l'incident affectant le groupe *Swisspro*⁴⁶. *Black Basta* a revendiqué la cyberattaque et publié, selon ses propres dires, 700 Go de données, lorsque la victime a refusé tout paiement. Cependant comme l'attaque ne concernait qu'une infrastructure informatique désuète, les conséquences néfastes sont restées minimales et *Swisspro* a pu continuer de fournir ses services en permanence.⁴⁷

³⁷ [Finland warns of Akira ransomware wiping NAS and tape backup devices \(bleepingcomputer.com\)](#)

³⁸ [Cyberattaque contre l'entreprise Concevis: l'administration fédérale est également concernée \(ncsc.admin.ch\)](#)

³⁹ [Ransomware Spotlight: 8Base \(trendmicro.com\)](#)

⁴⁰ [#StopRansomware: Phobos Ransomware \(cisa.gov\)](#)

⁴¹ [8Base \(sentinelone.com\)](#)

⁴² [Daten von Nexus Telecom im Darkweb veröffentlicht \(inside-it.ch\)](#)

⁴³ [Cyberangriff auf Schweizer Medtech-Firma \(inside-it.ch\)](#)

⁴⁴ [#StopRansomware: Black Basta \(cisa.gov\)](#)

⁴⁵ [Haufenweise Kundendaten von Schweizer Personalvermittler gestohlen \(inside-it.ch\)](#), [Cyberkriminelle stehlen schützenswerte Daten von Franz Carl Weber \(inside-it.ch\)](#)

⁴⁶ [Basta bekennt sich zum Angriff auf BKW-Tochter Swisspro \(inside-it.ch\)](#)

⁴⁷ [Russischer Hackerangriff: Attacke auf Schweizer Stromkonzern wirft Fragen auf \(bernerzeitung.ch\)](#)

3.2.2 Les rançongiciels, un fléau mondial

Les infrastructures critiques demeurent dans le radar des groupes de rançongiciels. En effet ces organisations se retrouvent sous pression, au vu de leur rôle majeur dans la vie quotidienne et des conséquences importantes que pourraient engendrer une éventuelle interruption de ces systèmes et services (notamment des effets en cascade sur d'autres fonctionnalités critiques). Cette observation a également été faite par le *Federal Bureau of Investigation (FBI)*, qui a constaté une augmentation générale des attaques de rançongiciels contre les infrastructures critiques⁴⁸. Si quelques groupes prétendent suivre certains principes éthiques dans le choix de leurs victimes, la majorité des groupes n'hésitent pas à attaquer les infrastructures critiques. C'est bien parce que cette pression liée à la prestation existe, que les criminels estiment que les infrastructures critiques sont plus enclines à payer la rançon. C'est ainsi que les entreprises *Veolia North America*⁴⁹ et *Southern Water*⁵⁰, actives dans l'approvisionnement en eau potable et l'élimination des eaux usées, ont toutes deux subi des attaques par rançongiciel. De même, un développeur allemand de logiciels destinés aux systèmes de contrôle des infrastructures critiques a été victime d'une attaque par rançongiciel⁵¹. Le secteur de la santé est lui aussi une cible de choix des cybercriminels. Aux États-Unis, les autorités fédérales ont spécifiquement mis ce secteur en garde contre les activités des rançongiciels *Phobos* et *Akira* (voir chap. 3.2.1)⁵².

Début juin 2024, un cas disruptif et très médiatisé a touché plusieurs hôpitaux londoniens lorsque *Synnovis*, un fournisseur de prestations de ces entités, a été victime d'une attaque par le rançongiciel *Qilin*. En raison de cette cyberattaque et des pannes informatiques qui s'en sont suivies, les hôpitaux ont dû reporter au cours des cinq semaines suivantes près de 6 000 rendez-vous, des opérations ou des transfusions sanguines⁵³. Les services d'urgences n'ont toutefois jamais cessé d'être opérationnels. Le groupe de rançongiciel a publié quelques semaines plus tard 400 Go de données sensibles touchant à la santé⁵⁴. Dans une interview ultérieure, les escrocs ont admis qu'ils étaient bien conscients des conséquences de leurs actes et qu'ils ne regrettaient rien⁵⁵.

Face à la menace croissante que les rançongiciels font peser à travers le monde entier, diverses autorités de poursuite pénale ont mis en place plusieurs mesures : L'opération dite *Cronos*, lancée à la mi-février 2024, sous la direction de la *National Crime Agency (NCA)* britannique, a permis aux autorités policières de neutraliser le groupe *LockBit*, encore très influent à l'époque⁵⁶. Par exemple, *LockBit* fut à l'origine du quart voire du tiers des attaques par rançongiciel lancées en 2023 au niveau mondial⁵⁷. En plus d'arrêter certains membres du

⁴⁸ [Federal Bureau of Investigation : Internet Crime Report 2023 \(ic3.gov\)](https://www.ic3.gov)

⁴⁹ [Veolia Responds to Cyber Incident \(mywater.veolia.us\)](https://mywater.veolia.us)

⁵⁰ [Black Basta claims hack on Southern Water \(computing.co.uk\)](https://computing.co.uk)

⁵¹ [Critical infrastructure software maker confirms ransomware attack \(bleepingcomputer.com\)](https://bleepingcomputer.com)

⁵² Voir [CISA, FBI, and MS-ISAC Release Advisory on Phobos Ransomware \(cisa.gov\)](https://www.cisa.gov), [Feds Warn Health Sector About Akira Again, Amid New Attacks \(bankinfosecurity.com\)](https://www.feds.gov)

⁵³ [NHS Trusts cancelled over 6,000 appointments after Qilin cyber attack \(computerweekly.com\)](https://computerweekly.com), [Cyber-attack on London hospitals declared critical incident \(bbc.com\)](https://www.bbc.com)

⁵⁴ [NHS England confirm patient data stolen in cyber attack \(bbc.com\)](https://www.bbc.com)

⁵⁵ [Qilin has 'no regrets' over the healthcare crisis it caused \(theregister.com\)](https://www.theregister.com)

⁵⁶ [The NCA announces the disruption of LockBit with Operation Cronos \(nationalcrimeagency.gov.uk\)](https://www.nationalcrimeagency.gov.uk)

⁵⁷ [Auswirkungen der Operation Cronos auf LockBit \(trendmicro.com\)](https://www.trendmicro.com)

plus modernes se basent certes sur cette règle, mais améliorent les aspects de redondance, d'accès et de distance géographique. Cela intègre entre autres les fournisseurs de cloud qui proposent des services de cloud correspondants⁶⁶.

Vous trouverez sur le site de l'OFCS une [liste de mesures préventives](#) pour se protéger des rançongiciels et des [consignes à suivre en cas d'incident](#). De manière générale, l'OFCS déconseille aux victimes de payer une rançon, car il n'y a aucune garantie que les criminels tiennent parole. De plus, toute rançon payée rehausse l'attrait de nouvelles opérations menées avec des rançongiciels.

3.3 Maliciels sur des appareils mobiles

Les appareils mobiles, soit les smartphones ou les tablettes, sont devenus des outils quotidiens. Performants et connectés en permanence, ces appareils miniaturisés renferment toujours plus de données personnelles, allant des photos, aux contacts, courriels et applications contenant des données sensibles, telles que l'e-banking ou les outils MFA. La plupart des appareils mobiles utilisent les systèmes d'exploitation *Android* ou *iOS* pour proposer ces fonctionnalités. Cette convergence d'information vers un seul appareil mobile conduit à l'apparition des « maliciels mobiles », catégorie à part entière de logiciels malveillants, car ils sont spécifiquement conçus pour viser les systèmes d'exploitation de ce type d'appareils. Durant la période sous revue, divers incidents et développements ont été observés dans ce domaine, bien qu'aucun d'eux n'ait eu de lien exclusif avec la Suisse.

En Finlande, l'agence *Traficom* a signalé en mai 2024 une campagne qui visait à diffuser des maliciels s'attaquant aux comptes d'e-banking d'utilisateurs *Android*⁶⁷. Des SMS frauduleux incitaient les victimes à installer une fausse application antivirus. Pour convaincre les utilisateurs, le message paraissait émaner d'une banque ou d'un service de paiement et évoquait une prétendue activité bancaire suspecte ou une demande de recouvrement. Les escrocs les avaient rédigés en finnois, en recourant à l'usurpation d'identité (*spoofing*)⁶⁸ pour donner l'impression de provenir d'opérateurs de télécommunication locaux. Les destinataires étaient ensuite priés d'appeler un numéro spécifique. À cette occasion, les victimes étaient amenées à installer un antivirus ne provenant pas du magasin d'applications officiel. Il s'agissait en fait du maliciel pour smartphones *Vultur*⁶⁹. Une fois installé, les escrocs pouvaient notamment accéder aux applications de l'appareil infecté, dont celles d'e-banking. C'est ainsi que les cybercriminels ont pu vider les comptes bancaires de plusieurs victimes.

Outre *Vultur*, de nombreux maliciels ont été conçus pour les systèmes d'exploitation des appareils mobiles, un marché en constante évolution. Des chercheurs en cybersécurité ont ainsi analysé en avril 2024 un nouveau logiciel pour appareils mobiles appelé *Brokewell*. Les victimes téléchargent ce maliciel destiné aux systèmes d'exploitation Android sur d'autres sites que la boutique d'applications officielle, en croyant avoir affaire à une mise à jour de Google

⁶⁶ [What's the Diff: 3-2-1 vs. 3-2-1-1-0 vs. 4-3-2 \(backblaze.com\)](#)

⁶⁷ [The National Cyber Security Centre Finland's weekly review – 18/2024 \(kyberturvallisuuskeskus.fi\)](#)

⁶⁸ [Usurpation d'identité \(spoofing\) \(ncsc.admin.ch\)](#)

⁶⁹ [Android Malware Vultur Expands Its Wingspan \(fox-it.com\)](#)

rendue publique en avril 2024, en est un bon exemple. Elle permettait à un pirate d'exécuter du code à distance sur les appareils vulnérables et, ce faisant, de compromettre les systèmes de ses victimes⁷⁵.

En dehors de cette vulnérabilité, l'OFCS a signalé à plusieurs reprises aux exploitants d'infrastructures critiques, durant la période sous revue, des failles de sécurité de produits en circulation. Dans 85 % des cas, il s'agissait de fabricants connus mondialement. Seuls 15 % des avis de sécurité se rapportaient à des fournisseurs moins connus et peu répandus en Suisse. De façon générale, on constate que les vulnérabilités rencontrées sont les mêmes pour les entreprises suisses que pour leurs concurrents à l'étranger et qu'elles doivent absolument être corrigées. Le présent chapitre explique pourquoi des produits de fournisseurs aussi renommés se retrouvent régulièrement dans la presse, pour des failles de sécurité aux conséquences potentiellement très graves.

Premièrement, les produits logiciels complets sont en principe très complexes. Ils comportent de multiples fonctions avec des interdépendances dans leur code-même (à l'intérieur du logiciel), mais aussi des dépendances avec le système d'exploitation (à l'extérieur). Cette complexité peut conduire à des erreurs de code difficiles à identifier et à corriger. Toute nouvelle fonction ou intégration peut générer de nouvelles vulnérabilités, qui passeront d'abord inaperçues. Deuxièmement, les grands fournisseurs de logiciels doivent constamment améliorer leurs produits pour rester concurrentiels. Or, ce développement continu s'accompagne souvent de pressions liées à la date de déploiement, les nouveaux produits ou les mises à jour devant pouvoir être rapidement mis sur le marché. Dans de telles conditions, il se peut que des vulnérabilités ne soient pas d'emblée découvertes. Troisièmement, les logiciels les plus répandus dans le commerce comptent de très nombreux utilisateurs, ce qui les transforme en cible convoitée des cybercriminels. Une cyberattaque contre un logiciel populaire peut donner accès à des millions d'appareils et d'utilisateurs, ce qui accroît considérablement le préjudice potentiel d'une telle opération. Ces facteurs et d'autres encore font que les noms de grands fournisseurs de logiciels renommés apparaissent souvent dans le contexte de la gestion des défaillances et que leurs produits semblent présenter continuellement des vulnérabilités.



Conclusion / Recommandations

Plus un logiciel est répandu et utilisé, plus il est probable que des vulnérabilités soient régulièrement découvertes. Cela s'explique notamment par le grand nombre d'utilisateurs et à la complexité d'un tel logiciel.

Les fabricants des logiciels les plus répandus doivent, par conséquent, eux aussi, instaurer une forte culture de la sécurité et répondre de la sécurité de leurs produits. Diverses mesures envisageables à cet effet méritent d'être citées, comme la réalisation de tests de sécurité, la mise en œuvre de bonnes pratiques en vue d'un développement sûr et finalement, par-dessus tout, une réaction rapide et efficace aux failles de sécurité nouvellement découvertes.

⁷⁵ [CVE-2024-3400 PAN-OS: Arbitrary File Creation Leads to OS Command Injection Vulnerability in GlobalProtect \(paloaltonetworks.com\)](#), [Vulnérabilité critique dans des pare-feux de Palo Alto \(ncsc.admin.ch\)](#)

Il serait faux de croire que les logiciels de fournisseurs mondiaux réputés sont automatiquement plus sûrs à l'utilisation et qu'ils fonctionnent mieux que des produits moins connus. Même les produits logiciels de fabricants les plus connus comportent des vulnérabilités.

Un produit dont une faille de sécurité vient d'être corrigée n'est pas pour autant durablement sûr à l'usage. De nouvelles vulnérabilités peuvent apparaître **en tout temps**, parfois **immédiatement** après l'installation du dernier correctif de sécurité. Ne perdez donc jamais de vue la nécessité de mises à jour régulières.

Par conséquent, **actualisez** vos logiciels sans attendre, quand une mise à jour de sécurité est publiée. Anticipez la **fin du cycle de vie** d'un logiciel et remplacez-le à temps.

5 Fraude et ingénierie sociale

Les cas de fraude ou escroquerie restent avec 23 104 annonces le phénomène le plus souvent signalé, totalisant à eux seuls deux tiers des annonces du premier semestre 2024. Leur nombre a largement doublé par rapport à la même période de l'année précédente (11 174). 13 730 signalements, soit près de 60 % d'entre eux, concernent des appels frauduleux émanant de prétendues autorités policières. Encore inexistant il y a un an, ce phénomène n'a fait son apparition qu'au deuxième semestre 2023. Même si dans la deuxième moitié de la période sous revue, les annonces concernant ce phénomène ont fortement diminué, elles représentent toujours la majorité des incidents signalés. Un robot appelle un maximum de numéros de téléphone choisis au hasard. Si la victime décroche, elle entend un message enregistré en anglais lui annonçant qu'elle est impliquée dans une procédure pénale et l'invitant à appuyer sur la touche « 1 » pour discuter des prochaines étapes avec un policier. Ce n'est qu'en appuyant sur la touche que la victime va finalement être mise en relation avec un escroc. Celui-ci va la persuader, en recourant à des techniques d'ingénierie sociale⁷⁶, de télécharger un logiciel d'accès à distance, qui lui permettra accéder à son ordinateur. Ensuite il pourra effectuer des paiements au détriment de la victime dans le système d'e-banking⁷⁷.

Les courriels de menace envoyés au nom d'autorités de poursuite pénale se situe en deuxième place de la liste des signalements, avec un total de 2 252 annonces. Un an plus tôt, cette variante d'escroquerie figurait encore en tête de cette catégorie d'annonces à l'OFCS, avec plus de 5 500 signalements. Le mode opératoire est similaire à celui des appels de menace précédemment décrits. Là encore, la victime est accusée d'avoir commis un délit. La communication s'effectue toutefois ici non par téléphone, mais par écrit. La victime est invitée à répondre à une adresse électronique, et les escrocs tenteront ensuite d'obtenir d'elle le paiement d'une caution.

Outre les cas de fraude classique au paiement anticipé⁷⁸, qui arrivent en troisième position avec 1 135 annonces, l'OFCS a surtout reçu durant la période sous revue des annonces de

⁷⁶ [Ingénierie sociale \(Social Engineering\) \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/ingénierie-sociale)

⁷⁷ [Semaine 15 : Les appels de fausses autorités atteignent un niveau record - mais ce n'est pas seulement un signe négatif \(ncsc.admin.ch\)](#)

⁷⁸ [Fraude au paiement anticipé \(ncsc.admin.ch\)](#)

jeux-concours frauduleux (1 111 annonces). Seuls 281 signalements lui étaient parvenus à la même période de l'année précédente. Le phénomène a connu un essor marqué en fin de période. Entre-temps, les noms de la plupart des entreprises connues du secteur de l'alimentation ou technique ont été mêlés à ces prétendus jeux-concours. Comme il s'agit de recruter un maximum de participants, les questions posées sont d'une grande simplicité. Pour obtenir le prétendu gain, il faut ensuite indiquer sur un site web frauduleux des données personnelles (telles que des données de carte de crédit, nom, adresse électronique, numéro de téléphone portable, etc.). L'envoi de telles informations amène la victime à souscrire, à son insu, à un abonnement de plusieurs années, dont les frais seront aussitôt débités de sa carte de crédit.

On constate également une augmentation des attaques visant les comptes de médias sociaux. Le nombre de signalements est passé de 101, à la même période l'année dernière, à 178. Ce type d'incident est d'autant plus impactant, car il est difficile de récupérer un compte piraté, comme le confirment divers témoignages de victimes. L'OFCS reçoit régulièrement des messages de personnes lui signalant avoir rempli les formulaires nécessaires au blocage et n'avoir jamais reçu de réponse des exploitants de réseaux sociaux, ou d'avoir reçu un refus. Il est donc fréquent de ne pas retrouver un compte piraté, malgré des demandes répétées dans ce sens.

5.1 Usage de l'intelligence artificielle dans les tentatives d'escroquerie

Le précédent rapport semestriel⁷⁹ s'était déjà intéressé de près à l'utilisation de l'intelligence artificielle (IA) dans les tentatives d'escroquerie. L'évolution s'est poursuivie sans changement notable au cours des six derniers mois. Il est difficile de déterminer au cas par cas dans quelle mesure l'apprentissage automatique (*ML*)⁸⁰ ou les grands modèles de langage (*LLM*)⁸¹ ont été utilisés à des fins criminelles. En règle générale, on ne peut que faire des conjectures quant à l'utilisation ou non d'outils de traduction. Mais parfois, il est clair que l'intelligence artificielle a joué un rôle. Le meilleur exemple est le cas d'une arnaque au président⁸² : Dans ce genre d'escroquerie, un ordre de paiement prétendument urgent du patron parvient au service financier. Les escrocs négligent d'ordinaire de s'adresser de façon ciblée à leur victime ou de personnaliser leur requête. Loin d'être spécifiques, leurs messages sont généralement interchangeables. Ils cherchent à dissuader la victime de s'adresser à son responsable hiérarchique. Mais dans le cas présent, le responsable des finances avait reçu auparavant un appel téléphonique d'un prétendu avocat l'invitant à une vidéoconférence avec son supérieur. La réunion devait commencer quelques minutes plus tard⁸³. Puis, un courriel avec les données d'accès à la réunion lui était parvenu à cet effet. Quand le responsable des finances s'est connecté à la conférence en ligne, il a pu voir son chef à l'écran et interagir avec lui. Pendant l'entretien, son prétendu supérieur a cherché à obtenir son numéro de téléphone portable et à lui faire effectuer des transactions financières. En l'occurrence, les escrocs avaient réalisé la vidéo du chef à l'aide d'algorithmes *deepfake*. La source exacte du matériel ayant servi à créer

⁷⁹ Voir [Rapport semestriel 2023/2 \(ncsc.admin.ch\)](#)

⁸⁰ [Apprentissage automatique \(wikipedia.org\)](#)

⁸¹ [Grand modèle de langage \(wikipedia.org\)](#)

⁸² [Arnaque au président \(ncsc.admin.ch\)](#)

⁸³ [Semaine 14 : Réunion en ligne avec un faux chef \(technique de deep fake\) : fraude au CEO 2.0 \(ncsc.admin.ch\)](#)

ces fausses vidéos n'a pas pu être établie avec certitude. L'OFCS considère toutefois qu'il s'agissait de matériel en libre accès.

5.2 Arnaque à la publicité pour des investissements

Pour inciter les internautes à soi-disant investir leur argent sur un site Internet douteux⁸⁴, des escrocs misent sur l'aura de personnes connues qui auraient réalisé d'énormes profits en très peu de temps, grâce à leurs offres lucratives. Des célébrités suisses ou internationalement connues comme Sandra Boner, Beatrice Müller, Roger Federer, Nemo ou Alain Berset apparaissent malgré elles dans de telles arnaques. Ces publicités, parfois de très mauvais goût, sont une source d'irritation croissante, alors que paraissent chaque jour de nouvelles annonces cherchant à attirer le chaland par de fausses promesses.

Le schéma de ces publicités pour des investissements frauduleux est toujours le même : les criminels prétendent que la personnalité connue n'était pas autorisée à parler d'un investissement aussi rentable et sûr, sous peine de se faire licencier. Une variante parle de déclaration faite par mégarde et qui n'aurait jamais dû être rendue publique. Même la mort d'une personnalité est parfois utilisée comme prétexte. L'investissement initial est généralement fixé à 250 francs. Quelques jours plus tard, des gains mirobolants sont annoncés à la victime, pour l'encourager à investir davantage. Sa modeste mise de 250 francs est ainsi rapidement suivie d'autres versements se chiffrant en milliers de francs, le seuil des 10 000 francs étant dépassé dans certains cas. Puis quand la victime cherche à se faire verser les gains et le montant investi, elle est priée de patienter, voire de régler des frais supplémentaires. Le principe de cette fraude consiste à appâter la victime par un montant de départ relativement bas, puis à instaurer une relation de confiance avec elle. Les offres spéculatives s'adressent en priorité à des néophytes du placement. Beaucoup d'entre elles « investissent » et y perdent toutes leurs économies.



Conclusions / Recommandations

À l'ère des applications basées sur des algorithmes, des acteurs mal intentionnés parviennent ainsi à générer du contenu pour des courriels ou messages courts qui paraissent crédibles et qui ressemblent à s'y méprendre à du courrier légitime, tant du point de vue de la langue que de la présentation. Cette compétence n'est pas très différente de ce qu'une personne polyglotte aurait pu effectuer. Il est d'autant plus difficile aux destinataires de ce genre de contenus d'y déceler une tentative d'escroquerie. Les applications en question permettent par ailleurs de fabriquer des photos, des vidéos et des voix très réalistes (*deepfakes*), qui pourront servir au lancement d'attaques d'ingénierie sociale. Par exemple, des voix bien imitées ont de bonnes chances de convaincre les victimes d'attaques ciblées qu'elles ont affaire à une personne qu'elles connaissent, et donc qu'un versement d'argent ou une autre forme d'aide s'imposent.

Les escrocs imaginent sans cesse de nouveaux scénarios afin de pousser leurs victimes à des actions irréfléchies. Ils recourent à des contenus générés par l'intelligence artificielle ou à

⁸⁴ [Fraude à l'investissement \(ncsc.admin.ch\)](https://www.ncsc.admin.ch/fraude)

des méthodes d'ingénierie sociale pour faire baisser la garde de leur victime et pour la faire exécuter certaines opérations sous leur conduite. Restez vigilant. Prenez le temps de réfléchir et dans le doute, adressez-vous à d'autres personnes ou à l'OFCS, pour obtenir leur avis sur la question.

6 Attaques affectant la disponibilité de sites et de services Internet (DDoS)

Lors d'attaques affectant la disponibilité de sites et de services Internet (*Distributed Denial of Service*, déni de service distribué, *DDoS*)⁸⁵, les cybercriminels cherchent à rendre un service ou un système en ligne temporairement inaccessible, en le saturant de requêtes. De telles attaques n'impliquent ni accès non autorisé à des données, ni de dommages durables sur les systèmes. Les attaques *DDoS* fructueuses ont donc généralement pour seul effet de paralyser provisoirement le service pris pour cible, d'habitude un site Internet. Le présent chapitre s'intéresse à trois campagnes *DDoS* observées durant le semestre sous revue. Tandis que l'une d'elles se caractérisait par une motivation financière, les deux autres relèvent de l'activisme dans le cyberspace (hacktivisme)⁸⁶.

En avril 2024, diverses organisations suisses actives dans le secteur financier ont signalé des attaques *DDoS* accompagnées de message de chantage⁸⁷. Ces attaques, émaneraient d'un groupe se faisant appeler *Armada Collective*⁸⁸ ou *Alpha Jackal* et suivaient toutes le même schéma : l'organisation prise pour cible reçoit tout d'abord un courriel lui annonçant des perturbations de ses services en ligne, si elle ne verse pas une rançon. La menace est aussitôt suivie d'une brève attaque *DDoS* pouvant déjà conduire à une surcharge ou à l'interruption de ces services. Le cybercriminel accroît alors la pression sur l'organisation afin qu'elle paie, en la menaçant par courriel d'intensifier ses attaques. Dans certains cas, la menace a été mise à exécution et les attaques ont augmenté en durée et en intensité. Des adresses IP légitimes d'organisations financières ont même été détournées, apparaissant comme sources dans des cyberattaques visant d'autres institutions. Mais dans la grande majorité des cas signalés, les conséquences sont restées limitées et les mesures usuelles destinées à endiguer les attaques *DDoS* en sont venues à bout. En Suisse, la dernière activité d'*Armada Collective*, ou du moins d'un pirate prétendant faire partie de ce groupe, remontait à 2020.

Indépendamment de toutes considérations financières, des attaques *DDoS* ont à nouveau été menées à des fins politiques⁸⁹, dans le contexte de conférences ou grands événements internationaux organisés en Suisse. Le collectif d'hacktivistes prorusse *NoName057(16)* a

⁸⁵ [Attaque affectant la disponibilité \(attaque DDoS\) \(ncsc.admin.ch\)](#)

⁸⁶ Voir le thème prioritaire du rapport semestriel 2023/01 : [Rapport semestriel du NCSC: gros plan sur l'hacktivisme \(ncsc.admin.ch\)](#)

⁸⁷ [Attaques DDoS et extorsion : une combinaison très actuelle \(ncsc.admin.ch\)](#)

⁸⁸ En 2015 et 2016, le groupe *Armada Collective* utilisait déjà le même mode opératoire selon l'analyse de MELANI, organisation qui a précédé l'OFCS. Mais les données techniques n'indiquent pas s'il s'agit en 2024 des mêmes acteurs qu'à l'époque.

⁸⁹ Voir [Rapport semestriel 2023/2](#), chap. 3.6.1 ; [Rapport semestriel 2023/1](#), chap. 2.

attaqué en janvier 2024 des sites Internet liés au Forum économique mondial (*WEF*) et en juin 2024 des sites d'organisations impliquées dans la Conférence sur la paix en Ukraine organisée à Bürgenstock. L'OFCS avait publié auparavant un aide-mémoire avec des recommandations à l'intention des organisateurs dont les infrastructures étaient particulièrement exposées⁹⁰. Pendant ces deux manifestations, l'OFCS a analysé les cibles choisies par les hacktivistes et a étroitement collaboré avec les exploitants des infrastructures malmenées. Dans l'ensemble, des attaques de ce type étaient attendues durant cette période et l'infrastructure informatique n'a subi que des perturbations mineures. À aucun moment, les systèmes informatiques et les données des deux manifestations ou des organisations impliquées n'ont été sérieusement menacés⁹¹. Les cyberattaques se sont concentrées sur la couche application du modèle OSI (attaque *DDoS* de couche 7)⁹², ce qui s'est traduit par une inondation de requêtes *HTTP/s GET*⁹³. La plupart des adresses IP utilisées appartenaient à des fournisseurs de services *VPN* privés et avaient été détournées par *NoName057(16)* en vue de cette attaque *DDoS*.



Recommandations

Le site Internet de l'OFCS propose dans sa rubrique [Attaque affectant la disponibilité \(attaque *DDoS*\) \(ncsc.admin.ch\)](#) diverses mesures de prévention et de défense contre de telles attaques. Préparez-vous à une attaque potentielle, en coopération avec votre fournisseur de services ou votre hébergeur, afin d'en atténuer l'impact. Pour les systèmes critiques, il peut être utile de faire appel à un service commercial de protection *DDoS* qui peut servir de bouclier.

En cas d'attaque *DDoS* liée à du chantage, l'OFCS recommande de ne pas entrer en matière avec les escrocs. Après un premier versement, ils seraient capables de réclamer davantage d'argent et de poursuivre leurs attaques. Il est donc préférable de signaler le cas à l'OFCS et de prendre contact avec la police en vue du dépôt d'une plainte pénale. Les recommandations d'usage figurent sous : [Attaque *DDoS* - que faire ? \(ncsc.admin.ch\)](#).

7 Gestion des données, fuites de données et chantage

Les fuites de données ou l'exposition de données par mégarde font régulièrement la une des journaux. C'est ainsi qu'en mai 2024, près de 500 Go de données biométriques et d'autres données sensibles de citoyens indiens, dont des militaires et des policiers, ont été mis en ligne en libre accès. La base de données concernée était mal configurée et aucun mot de passe

⁹⁰ [Mesures de cyberrésilience dans le contexte des grands événements et conférences internationales \(ncsc.admin.ch\)](#)

⁹¹ [Conférence de haut niveau sur la paix en Ukraine : premier bilan de l'OFCS sur les travaux du réseau de suivi de la cybersituation \(ncsc.admin.ch\)](#)

⁹² [Application layer DDoS attack \(cloudflare.com\)](#)

⁹³ [HTTP flood attack \(cloudflare.com\)](#)

n'en assurait la protection⁹⁴. Autrement dit, un accès protégé et une gestion efficace des données s'avèrent indispensables tant pour les entreprises que pour les autorités et les particuliers, afin de garantir la sécurité des données. Les fuites de données n'ont pas seulement des conséquences pour les organisations touchées, mais aussi pour d'autres qui se retrouvent à risque suite à l'incident. Quant aux informations sensibles de particuliers, elles aussi intéressent les acteurs malintentionnés. Après une fuite de données, le risque de subir une cyberattaque augmente pour les victimes, allant des usurpations de comptes, à l'hameçonnage (voir chap. 2), l'usurpation d'identité ou les fraudes financières (voir chap. 5). Selon les analyses actuelles de la situation en matière de cybermenace, les fuites de données proviennent essentiellement de groupes de rançongiciels, qui s'en servent comme arme à des fins de chantage (voir chap. 0). Il ne faut toutefois pas perdre de vue les autres causes de ce phénomène, comme une gestion déficiente des données au niveau de l'infrastructure interne ou des fournisseurs. Par ailleurs, des vulnérabilités existantes et des erreurs de configuration technique peuvent conduire à une exposition par mégarde de données, dont des acteurs mal intentionnés sont susceptibles de tirer parti.

7.1 Fuites de données au niveau des fournisseurs

Les fuites de données constituent un problème toujours plus important au niveau national comme à l'étranger, à plus forte raison quand des chaînes d'approvisionnement sont en cause. En Suisse, l'attaque par le rançongiciel *Play* subie en 2023 par l'entreprise de solutions informatiques *Xplain* a beaucoup fait parler d'elle. Les données de clients publiées par les criminels comprenaient notamment des données de l'Administration fédérale relevant de la sécurité intérieure. Début mars 2024, l'OFCS a publié un rapport qui décrivait la gestion de l'incident par l'Administration fédérale et qui analysait les données publiées pour en tirer les conclusions qui s'imposaient⁹⁵. Le tri effectué a révélé qu'environ 5 % du volume total de données publiées, soit 1,3 million d'éléments, concernaient l'administration fédérale. En outre, si la plupart de ces données appartenaient à *Xplain*, 9 040 éléments (près de 14 %) provenaient tout de même de l'Administration fédérale. Un peu plus de la moitié d'entre eux renfermaient un contenu sensible, comme des données personnelles et des informations techniques et/ou classifiées. Le tri et l'analyse effectués montrent qu'après une fuite de données, un lourd travail s'impose pour examiner en détail les documents concernés – notamment dans le cas des données non structurées⁹⁶. Le premier défi a consisté à trouver rapidement les instruments utiles au traitement et à l'analyse des données, ainsi que les ressources en personnel nécessaires pour en faire le tri et le classement manuellement. Une telle approche demande beaucoup de ressources et coûte d'autant plus cher que l'examen des données ne peut être entièrement automatisé.

L'incident a donné lieu à d'autres enquêtes au niveau fédéral : d'une part, le Ministère public de la Confédération (MPC) a ouvert deux procédures pénales liées à cette cyberattaque. D'autre part, le Préposé fédéral à la protection des données et à la transparence (PFPDT) a

⁹⁴ [Data Leak Exposes 500GB of Indian Police, Military Biometric Data \(hackread.com\)](#)

⁹⁵ [Cyberattaque contre l'entreprise Xplain : publication du rapport de l'Office fédéral de la cybersécurité sur l'analyse des données \(admin.ch\)](#)

⁹⁶ [Informations non structurées \(wikipedia.org\)](#)

mené sa propre enquête indépendante sur cette fuite de données⁹⁷. Elle a permis de constater que faute d'accords suffisants entre le fournisseur et deux offices fédéraux, les processus de support avaient transmis une quantité disproportionnée de données personnelles au fournisseur, qui les avait conservées sur son serveur. En outre, le Conseil fédéral a décidé à l'été 2023 de mettre sur pied un état-major de crise politico-stratégique « Fuite de données » (EMPS-F) ainsi que d'ordonner une enquête administrative⁹⁸. Sur la base des conclusions de cette enquête administrative⁹⁹, la Confédération a introduit différentes mesures en vue d'améliorer durablement et systématiquement la sécurité des données. La loi sur la sécurité de l'information (LSI), entrée en vigueur le 1^{er} janvier 2024, reflète et complète ces mesures¹⁰⁰.

Des incidents similaires sont également apparus au niveau international. Une campagne de grande envergure a ainsi pris pour cible la clientèle de *Snowflake*, entreprise implantée dans le monde entier et dont les comptes clients n'avaient pas toujours été suffisamment sécurisés. L'activité de base de *Snowflake* consiste à fournir une plateforme en nuage¹⁰¹ pour des données structurées ou non. La clientèle peut y stocker des données ainsi que les traiter en vue d'analyses approfondies fondées sur des méthodes d'apprentissage automatique. Cette plateforme comprend en outre un espace d'e-commerce (*marketplace*), où il est possible de vendre et d'échanger des données ainsi que d'utiliser gratuitement des données de tiers. Fin mai 2024, le groupe de pirates *ShinyHunters* a annoncé avoir exfiltré des données de l'entreprise *Ticketmaster* à l'aide d'un maliciel conçu pour voler des informations confidentielles (*infostealer*)¹⁰². 1,3 téraoctets (To) de données provenant de 560 millions d'utilisateurs de *Ticketmaster* ont été piratées sur la plateforme de *Snowflake*. L'auteur aux motifs pécuniaires a procédé ici comme les groupes de rançongiciels (voir chap. 0), sans toutefois chiffrer les données de ses victimes.

L'incident concernant *Ticketmaster* est loin d'être isolé. Beaucoup d'autres entreprises – dont *AT&T*¹⁰³ et *Santander*¹⁰⁴ – ont aussi fait les frais de la campagne d'extorsion due aux mêmes acteurs. Une enquête approfondie réalisée en collaboration avec l'entreprise de cybersécurité *Mandiant* a révélé que les premiers accès non autorisés aux bases de données remontaient à avril 2024. *Mandiant* n'a toutefois trouvé aucun indice suggérant que les exfiltrations de données stockées auprès de *Snowflake* aient pu provenir d'une erreur de configuration, d'une vulnérabilité ou d'un autre manquement qui serait imputable à l'infrastructure générale de *Snowflake*. A contrario, le vol de données aurait été rendu possible grâce à l'obtention de données d'accès de clients par des maliciels spécialisés¹⁰⁵. Les fuites de mots de passe

⁹⁷ Pour consulter le rapport contenant les résultats de l'enquête sur le traitement des données effectué par *Xplain* ainsi que des recommandations a été publié le 1^{er} mai 2024, voir [Le PFPDT clôt les enquêtes contre l'entreprise Xplain, ainsi que les offices fédéraux fedpol et OFDF \(edoeb.admin.ch\)](#).

⁹⁸ [Cyberattaque contre l'entreprise Xplain : le Conseil fédéral mandate un état-major de crise politico-stratégique «Fuite de données» \(admin.ch\)](#)

⁹⁹ Les résultats de l'enquête administrative ont été publiés le 1^{er} mai 2024, voir [Clôture de l'enquête administrative concernant la cyberattaque contre Xplain SA : le Conseil fédéral adopte des mesures \(admin.ch\)](#)

¹⁰⁰ [Le Conseil fédéral fixe l'entrée en vigueur de la loi sur la sécurité de l'information \(admin.ch\)](#).

¹⁰¹ [Cloud Computing \(wikipedia.org\)](#)

¹⁰² [Live Nation confirms Ticketmaster breach after hackers hawk stolen info of 560 million \(therecord.media\)](#)

¹⁰³ Voir [Toll of Snowflake Hack Widens With Theft of AT&T Text, Calling Data \(bloomberg.com\)](#), [AT&T Addresses Illegal Download of Customer Data \(att.com\)](#)

¹⁰⁴ [More than 12,000 Santander employees in US affected by Snowflake customer breach \(therecord.media\)](#)

¹⁰⁵ [Detecting and Preventing Unauthorized User Access \(snowflake.discourse.group\)](#)

RaidForums a pu être réactivée sous le nom de *BreachForums* et sous la direction du groupe *ShinyHunters*. La plateforme s'est imposée comme un des principaux forums pour la vente et le libre partage de données et d'informations d'accès volées. On y retrouve des données publiquement accessibles aussi bien que des contenus très sensibles. Par exemple, quelque cinq millions de photos passeport à haute résolution – avec mention du numéro d'identité – de citoyennes et citoyens du Salvador ont été mises sur le marché en avril 2024. L'acheteur recevait en prime un jeu de données renfermant des informations personnelles telles que nom, numéro d'identification, date de naissance et coordonnées. Tout indique que 80 % de la population salvadorienne figurait dans cette fuite de données¹¹³.

En mai de cette année, les autorités de poursuite pénale sont à nouveau intervenues contre *BreachForums*. Le FBI est certes parvenu à récupérer temporairement les domaines, avec l'aide de la police cantonale zurichoise¹¹⁴, mais les anciens administrateurs ont pu relancer le site sur le *darkweb* deux semaines plus tard. Il est même possible de retrouver l'accès à la page d'origine située dans le web visible¹¹⁵. Le bureau d'enregistrement de noms de domaine leur a visiblement rendu le site que venait de confisquer le FBI¹¹⁶. Les deux plateformes sont ainsi redevenues pleinement opérationnelles, comme l'a prouvé de manière spectaculaire la fuite de données de clients de *Snowflake* (voir chap. 7.1). Autrement dit, les autorités de poursuite pénale ont beau démanteler de tels réseaux ou plateformes de e-commerce et perturber les activités illégales s'y déroulant, la demande ne faiblit pas et l'infrastructure de sauvegarde est suffisamment robuste pour que de nouvelles plateformes soient créées.



Conclusion / Recommandations

Les données étant précieuses, il existe un grand intérêt criminel à se les procurer et à les revendre par des moyens déloyaux, ou à faire chanter les victimes en les menaçant de publier des données sensibles. En définitive, chacun devrait être conscient de la libre circulation des informations sur la toile, que ce soit intentionnel ou non. Des acteurs malveillants peuvent donc s'en servir pour des attaques d'ingénierie sociale. Par conséquent, le réel enjeu de la discussion sur la sécurité des données ne devrait plus être de savoir si une fuite de données peut se produire, mais plutôt quand elle aura lieu et comment rendre en pareil cas les données inutiles pour le pirate.

Les cinq **règles de base** de la conservation des données consistent à définir les **données** à enregistrer et traiter, la **forme**, la **responsabilité** et le **lieu** du stockage, ainsi que les personnes avec qui les données peuvent être **partagées**. Il est judicieux d'enregistrer les données avec précaution, de contrôler à des intervalles réguliers son stock de données et d'effacer les données superflues. Établissez des processus clairs et réalisables pour le traitement et la protection des données, et contrôlez-en la bonne mise en œuvre.

¹¹³ [Threat Actor Claims to Have Leaked Database Containing Personal Information of 5 Million Salvadoran Citizens \(dailydarkweb.net\)](#)

¹¹⁴ [Breachforum: FBI und Kapo Zürich gelingt Schlag gegen Hacker \(nzz.ch\)](#)

¹¹⁵ [BreachForums returns just weeks after FBI-led takedown \(theregister.com\)](#)

¹¹⁶ [Breach Forums Return to Clearnet and Dark Web Despite FBI Seizure \(hackread.com\)](#)

Les données issues d'anciennes fuites de données peuvent resservir pour de nouvelles attaques. Vérifiez donc périodiquement que vos données d'accès n'ont pas fuité, par exemple sur le site web [Have I Been Pwned \(haveibeenpwned.com\)](https://haveibeenpwned.com), ou sur [Identity Leak Checker des Hasso Plattner Instituts \(hpi.de\)](https://identityleakchecker.hpi.de).

Les données ne se négocient pas qu'au noir, mais aussi en toute légalité. Les courtiers¹¹⁷ et autres fournisseurs de données comme *Snowflake* permettent aux entreprises d'acheter commodément des données ou de les obtenir gratuitement. Le problème de ces plateformes légales tient au fait que des données collectées de manière illicite risquent d'y aboutir et que l'exploitant doit alors les retirer de la circulation¹¹⁸. En principe, le traitement des données personnelles par les entreprises est illégal du point de vue de la protection des données, si ces dernières ont été collectées sans le consentement explicite des personnes concernées et si elles sont traitées à des fins d'analyse en l'absence d'un intérêt public ou privé prépondérant¹¹⁹. Entre autres, il est assez simple pour les entreprises de collecter des données d'utilisateurs avec leur autorisation. Une telle pratique est très répandue, notamment dans le secteur de la publicité dont la collecte d'information constitue l'activité de base. Grâce à des identifiants publicitaires uniques, soit l'identifiant unique de chaque terminal mobile, les entreprises sont en mesure de collecter des données sur le comportement des utilisateurs, de les combiner et de les analyser afin de proposer des publicités personnalisées aux utilisateurs finaux. Ces identifiants publicitaires constituent une mine d'informations pour les entreprises, grâce à leur caractère permanent et à leur emploi possible sur différents appareils (interopérabilité)¹²⁰. Les *cookies* interviennent également dans l'analyse du comportement des utilisateurs. Mais contrairement aux identifiants publicitaires, les *cookies* sont des identifiants de visiteurs anonymes, qui ne sont collectés qu'une fois par appareil et ne permettent pas de créer un profil d'utilisateur complet. Ils enregistrent eux aussi les comportements de navigation et stockent les préférences et les caractéristiques des utilisateurs¹²¹. Outre les *cookies*, des méthodes comme le *fingerprinting* permettent d'enregistrer les utilisateurs et de les reconnaître à partir de métadonnées¹²². De même, le fait d'accepter les autorisations demandées par les applications d'appareils mobiles aboutit à transmettre à des entreprises des données personnelles, telles que des informations de localisation, comme le démontre une analyse de la SRF de juin 2024¹²³. Pour les besoins de ses recherches, la rédaction de SRF Data a reçu gratuitement en 2024, pendant une semaine, les données de localisation de 1,3 million d'appareils utilisés en Suisse qui, selon les dires du fournisseur, avaient été anonymisés. Il s'agissait sans doute d'informations collectées à des fins publicitaires par les capteurs de

¹¹⁷ Les courtiers en données (*data broker*) sont des personnes physiques ou morales qui collectent, compilent et revendent des informations personnelles.

¹¹⁸ Voir [Databroker: Belgian data marketplace publishes passport data of thousands of people \(netzpolitik.org\)](https://netzpolitik.org/en/databroker-belgian-data-marketplace-publishes-passport-data-of-thousands-of-people/), [European data broker: Sensitive passport data of Germans published online \(netzpolitik.org\)](https://netzpolitik.org/en/european-data-broker-sensitive-passport-data-of-germans-published-online/)

¹¹⁹ Voir les art. 30 et 31, al. 1 de la loi sur la protection des données (LPD ; RS 235.1) ; Sandra Husi/Stämpfli/Anne-Sophie Morand/Ursula Sury, *Datenschutzrecht*, Zürich 2023, p. 150 ss, N 277 ss.

¹²⁰ [Werbewelt ohne Cookies: Mit neuen ID-Technologien in die Zukunft \(traffactive.com\)](https://traffactive.com/fr/werbewelt-ohne-cookies-mit-neuen-id-technologien-in-die-zukunft/)

¹²¹ [DSGVO vs. ePrivacy: Datenschutz, einfach erklärt \(traffactive.com\)](https://traffactive.com/fr/dsgvo-vs-eprivacy-datenschutz-einfach-erklart/)

¹²² [Browser fingerprinting explained \(+7 top techniques\) \(fingerprint.com\)](https://fingerprint.com/fr/browser-fingerprinting-explained-7-top-techniques/)

¹²³ [Tracking mit Ortungsdiensten - Der Spion in unseren Handys \(srf.ch\)](https://srf.ch/fr/actualites/technologie/tracking-mit-ortungsdiensten-der-spion-in-unseren-handys)

localisation (*trackers*) d'applications et de sites web de différentes entreprises. Or contrairement aux promesses du fournisseur, SRF Data a pu rapidement attribuer les données à des personnes précises, ce qui porte de facto durablement atteinte à leur sphère privée.



Recommandations

Lors de l'utilisation quotidienne de votre appareil mobile, veillez à ne donner aux applications que vous utilisez que les **autorisations** que vous souhaitez réellement leur accorder. N'acceptez pas spontanément tous les **cookies**, dans la bannière des cookies des sites web et des applications. Quelques clics supplémentaires vous permettront de refuser les cookies allant au-delà de la fonctionnalité normale et d'empêcher ainsi l'enregistrement et la revente de vos données contre votre gré. Un [guide de la SRF](#)¹²⁴ explique comment mettre en œuvre ces divers points, avec les autres étapes entrant en ligne de compte.

8 Cyberespionnage et sabotage

Outre les acteurs non étatiques, la situation actuelle de l'ensemble des cybermenaces compte également des acteurs étatiques malintentionnés. On parle ici de menaces persistantes avancées (*advanced persistent threat, APT*)¹²⁵, eu égard à la patience dont de tels acteurs font preuve et à leurs importantes ressources temporelles, humaines, techniques et financières. Une *APT* a pour particularité de perfectionner ses méthodes quoi qu'il en coûte, afin de mener des attaques sur mesure, adaptées à ses objectifs. Une fois que des *APT* ont été détectées et éliminées d'un réseau, elles tenteront d'y revenir. Les *APT* évoluent souvent dans un contexte étatique et peuvent aussi s'allier avec des acteurs non-étatiques afin d'atteindre leurs buts. Leurs intérêts sont variés : Si certaines *APT* sont mues par l'appât du gain, la plupart se sont spécialisées dans le cyberespionnage ou le sabotage, voire les deux. Le présent chapitre traite de thèmes et développements du contexte international qu'il est indispensable de connaître pour se faire une idée de la position de la Suisse dans l'espace numérique.

8.1 Cyberespionnage

8.1.1 Des institutions politiques sous pression

En début d'année, le *WEF* a qualifié 2024 d'année électorale record : des élections sont prévues dans plus de 50 pays¹²⁶. Or, expérience à l'appui, ces temps forts de la vie politique sont une aubaine pour des acteurs mal intentionnés. Tandis que les criminels y voient une bonne occasion de s'enrichir, les hacktivistes feront tout pour attirer l'attention sur leur cause. Quant aux acteurs étatiques, les élections leur servent tant à collecter des informations sur la

¹²⁴ [Anleitung gegen Tracking - So schützen Sie Ihr Handy vor Tracking \(srf.ch\)](#)

¹²⁵ [Advanced Persistent Threat \(wikipedia.org\)](#)

¹²⁶ [Why 2024 is a record year for elections around the world \(weforum.org\)](#)

population locale qu'à mener des opérations d'influence¹²⁷. Conformément à ces attentes, la cyberactivité malveillante a fortement augmenté dans ce contexte, comme le démontrent les élections européennes. Les cyberactivités dont les médias ont fait écho émanaient souvent d'hacktivistes et concernaient tantôt des menaces, tantôt des attaques réelles. C'est ainsi qu'au début des élections européennes, les sites web de partis néerlandais ont subi des attaques *DDoS*, dont le groupe prorusse *Hacknet* a revendiqué la responsabilité¹²⁸. L'impact direct de ces activités semble toutefois faible, les attaques *DDoS* ne restreignant que temporairement l'accès aux sites (voir chap. 6). Le groupe d'hacktivistes a toutefois atteint son objectif d'attirer l'attention sur lui et de gagner ainsi en visibilité.

Les élections parlementaires constituent également un contexte délicat à l'ère du cyberespionnage. Compte tenu de l'agenda très chargé et vu l'importance que revêt un processus électoral indépendant, l'Agence de l'Union européenne pour la cybersécurité (*ENISA*) avait actualisé en mars 2024 son recueil sur la sécurité et la résilience des élections¹²⁹. Malgré les mesures préventives, une semaine avant les élections européennes, l'Union chrétienne-démocrate d'Allemagne (*CDU*) fut victime d'une cyberattaque. Le Ministère allemand de l'intérieur a confirmé l'incident, mais sans publier d'informations détaillées¹³⁰. On sait seulement que les pirates ont pu accéder aux systèmes informatiques grâce à une vulnérabilité¹³¹. Tout indique qu'il s'agissait d'un acteur chevronné¹³².

À la différence des opérations de piratage menées pendant les élections européennes, il est très difficile de détecter les cyberattaques potentiellement lourdes de conséquences et elles sont plus rarement divulguées, en raison de leurs implications géopolitiques. La Suisse et ses institutions politiques ne font pas exception à la règle, comme le montrent les attaques rendues publiques en mai 2024, concernant 122 parlementaires qui avaient fait l'objet en 2021 d'attaques par hameçonnage ciblé (*spearphishing*), en Suisse et dans d'autres États européens¹³³. Ces attaques menées contre des élus fédéraux s'inscrivaient dans une plus vaste campagne dirigée contre des membres de l'Alliance interparlementaire sur la Chine (*IPAC*). Les autorités américaines et britanniques les ont publiquement attribuées au groupe étatique chinois *APT31*¹³⁴.

8.1.2 Développements internationaux dans le domaine du cyberespionnage

***ISoon* – une fuite de données riche en enseignements**

En février 2024, la plateforme de développement collaboratif *GitHub* a divulgué plus de 500 documents très vraisemblablement authentiques appartenant à la société chinoise *ISoon*. Il s'agissait de listes de cibles potentielles, de descriptions d'outils et de conversations entre collaborateurs. De nombreux experts ont jugé ces documents crédibles. Ils renseignent sur

¹²⁷ Pour une vue d'ensemble : [Poll Vaulting: Cyber Threats to Global Elections \(cloud.google.com\)](https://cloud.google.com/poll-vaulting)

¹²⁸ [Dutch political websites hit by cyber attacks as EU voting starts \(cloudflare.com\)](https://www.cloudflare.com/learning/ddos/what-is-ddos-attack/)

¹²⁹ [Safeguarding EU elections amidst cybersecurity challenges \(enisa.europa.eu\)](https://enisa.europa.eu/publications/safeguarding-eu-elections-amidst-cybersecurity-challenges)

¹³⁰ [CDU: Cyber-Angriff auf Parteizentrale – Verfassungsschutz eingeschaltet \(spiegel.de\)](https://www.spiegel.de/politik/deutschland/cdu-cyber-angriff-auf-partei-zentrale-verfassungsschutz-ingeschaltet-a-1234567)

¹³¹ [Hackerangriff auf CDU: Software wird auch in Mitteldeutschland genutzt \(mdr.de\)](https://www.mdr.de/news/hackerangriff-auf-cdu-software-wird-auch-in-mitteldeutschland-genutzt-100.html)

¹³² [Germany's Christian Democratic party hit by 'serious' cyberattack \(reuters.com\)](https://www.reuters.com/world/europe/germany-christian-democratic-party-hit-serious-cyberattack-2024-05-01/)

¹³³ [Schweizer Parlamentarier von chinesischen Staatshackern attackiert \(watson.ch\)](https://www.watson.ch/schweiz/parlament/schweizer-parlamentarier-von-chinesischen-staatshackern-attackiert)

¹³⁴ [Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians \(justice.gov\)](https://www.justice.gov/opa/pr/seven-hackers-associated-with-chinese-government-charged-with-computer-intrusions-targeting-perceived-critics-of-china-and-u-s-businesses-and-politicians), [UK holds China state-affiliated organisations and individuals responsible for malicious cyber activity \(gov.uk\)](https://www.gov.uk/government/news/uk-holds-china-state-affiliated-organisations-and-individuals-responsible-for-malicious-cyber-activity)

les activités d'un prestataire de services actif dans les domaines de la surveillance et des cyberattaques, et qui travaillerait notamment pour le Ministère de la sécurité publique, pour la sécurité de l'État ainsi que pour l'armée chinoise¹³⁵.

De tels documents sont révélateurs des pratiques d'externalisation chinoises dans le domaine des cyberopérations et du mode de fonctionnement de cet écosystème. Le risque de la sous-traitance repose sur le fait que le prestataire externe peut perdre le contrôle de certains maillons de la chaîne d'attaque (voir chap. 7.1). Mais cette approche a l'avantage de permettre à l'État concerné de nier toute implication, lorsqu'une opération est révélée au grand jour.

Essor des réseaux ORB

En janvier 2024, les autorités américaines ont signalé avoir démantelé un réseau d'attaque formé de routeurs compromis¹³⁶. Ce réseau aurait été développé par un groupe du nom de *Volt Typhoon*¹³⁷, que les autorités américaines lient à l'État chinois. Les États-Unis accusent ce groupe d'avoir pris pour cibles des infrastructures critiques situées sur son sol et ailleurs. Pour neutraliser ce réseau, les autorités américaines ont dû accéder à distance aux routeurs compromis. Ce n'est que dès lors qu'elles ont pu éradiquer le malicieux de ce réseau de machines zombies et empêcher toute nouvelle communication avec son infrastructure de commande et de contrôle.

Les réseaux composés de routeurs compromis ou d'autres objets en réseau, tels que les réseaux *ORB* (*operational relay boxes*) sont utilisés depuis longtemps par les *APT*. La nouveauté réside dans l'ampleur et la fréquence de leur usage, par des acteurs étatiques chinois notamment. Mais ce ne sont pas les seuls à le faire. *APT28* – aussi connue sous le nom de *Sofacy* – proche de l'agence de renseignement militaire russe (*GRU*) a recouru à des réseaux similaires, opérés par des criminels, pour ses cyberopérations¹³⁸. L'attaquant se sert de réseaux *ORB* et bénéficie ainsi de nombreux avantages : ils lui permettent de dissimuler son identité, de rendre la détection d'une attaque plus difficile, et si besoin de basculer rapidement vers une nouvelle infrastructure.

Cette évolution démontre que la tendance à la division du travail répandue parmi les cybercriminels influence également les méthodes employées par les acteurs étatiques. Des fournisseurs – aussi du milieu criminel – mettent à disposition des ressources d'infrastructure bénévolement au profit d'acteurs étatiques pour leurs opérations cyber. Cet exemple révèle encore à quel point les frontières entre les acteurs étatiques ou privés sont devenues perméables dans le cyberspace.

Conclusion / Recommandations

Outre les appareils de réseau proprement dits, comme les routeurs, d'autres appareils électroniques sont désormais constamment en ligne (comme par exemple les caméras, les téléviseurs et les appareils de stockage). Ces objets ne sont souvent peu voire pas du tout

¹³⁵ [iSoon leak sheds light on China's use of extensive hacker-for-hire ecosystem \(huntandhackett.com\)](https://www.huntandhackett.com/news/soon-leak-sheds-light-on-china-s-use-of-extensive-hacker-for-hire-ecosystem)

¹³⁶ [U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure \(justice.gov\)](https://www.justice.gov/opa/pr/2024/01/24-cyber-001)

¹³⁷ Voir [Rapport semestriel 2023/2](#) ; chap. 3.5.

¹³⁸ [Router Roulette: Cybercriminals and Nation-States Sharing Compromised Networks \(trendmicro.com\)](https://www.trendmicro.com/fr/fr/insights/cybercrime/router-roulette)

protégés, ce qui en fait une cible d'attaque. Ainsi ils risquent d'être détournés à l'insu de leurs propriétaires pour des activités malveillantes, par exemple au sein de réseaux *ORB*. De tels appareils doivent par conséquent eux aussi être protégés de manière adéquate et recevoir les mises à jour nécessaires, quand des vulnérabilités sont de notoriété publique. L'OFCS a publié diverses recommandations visant à garantir la sécurité de tels appareils, voir [Cyberconseil : précautions à prendre avec l'Internet des objets \(ncsc.admin.ch\)](#).

Campagne *Coathanger* contre les appareils à la périphérie du réseau

Le NCSC néerlandais a constaté en juin 2024 une tendance relative aux attaques ciblées contre des appareils situés en périphérie, tels les pare-feux, les serveurs *VPN*, les routeurs et les serveurs relais de messagerie. Ces appareils sont directement reliés à Internet et sont donc exposés à des attaques. La campagne *Coathanger* a mis en lumière les risques inhérents à des appareils tels que les pare-feux ou les routeurs. Selon le NCSC néerlandais, un acteur étatique chinois a systématiquement exploité à des fins d'espionnage, en 2022 et en 2023, une faille de *FortiGate Firewall* qui lui a livré accès à au moins 20 000 appareils situés dans le monde entier. Avant la publication de cette vulnérabilité, il en a tiré parti pendant deux mois comme faille *zero day*¹³⁹. La campagne s'est attaquée au Ministère néerlandais de la défense et à d'autres gouvernements ou entités diplomatiques. Chaque fois qu'une cible lui paraissait intéressante, l'acteur de la menace y installait un maliciel afin d'obtenir un accès permanent aux systèmes infectés pour ses activités d'espionnage. Même lorsque le fabricant a découvert la faille de sécurité et a procédé à une mise à jour, l'acteur a pu maintenir son accès¹⁴⁰.

Activités liées à *APT29*

APT29 est un acteur connu de longue date pour ses cyberattaques sophistiquées menées à des fins d'espionnage. Les autorités de divers pays estiment qu'*APT29* opère pour le compte du Service de renseignements extérieurs de Russie (*SVR*)¹⁴¹. Comme toute *APT*, ce groupe ne cesse d'améliorer ses méthodes d'attaque, selon un rapport du groupe *Five Eyes*^{142 et 143}. *APT29* a ainsi directement attaqué des infrastructures en nuage pour accéder aux systèmes souhaités, au lieu de se concentrer sur les faiblesses logicielles de réseaux locaux. Au cours des six mois sous revue, il s'est montré particulièrement actif et a principalement attaqué des entreprises du secteur des technologies de l'information comme *HPE*¹⁴⁴, *Microsoft*¹⁴⁵ et plus récemment *Teamviewer*¹⁴⁶. *APT29* s'est en outre montré actif sur le terrain de l'espionnage politique, prenant pour cibles des entités diplomatiques et des gouvernements un peu partout dans le monde ainsi que des partis politiques. En France, l'Agence nationale de la sécurité

¹³⁹ [Vulnérabilité zero-day \(wikipedia.org\)](#)

¹⁴⁰ [Ongoing state-sponsored cyber espionage campaign via vulnerable edge devices \(ncsc.nl\)](#)

¹⁴¹ Voir [Rapport semestriel 2021/2](#) ; chap. 4.7.3.

¹⁴² *Five Eyes* désigne l'alliance des services du renseignement de l'Australie, du Canada, des États-Unis, de la Grande-Bretagne et de la Nouvelle-Zélande. Pour en savoir plus, voir [Five Eyes \(wikipedia.org\)](#) ou [Five Eyes Intelligence Oversight and Review Council \(FIORC\) \(dni.gov\)](#).

¹⁴³ [SVR cyber actors adapt tactics for initial cloud access \(ncsc.gov.uk\)](#)

¹⁴⁴ [Hewlett Packard Enterprise tells SEC it was breached by Russia's 'Cozy Bear' hackers \(therecord.media\)](#)

¹⁴⁵ [Update on Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard \(msrc.microsoft.com\)](#)

¹⁴⁶ [Teamviewer \(teamviewer.com\)](#)

des systèmes d'information (ANSSI) a signalé en juin 2024¹⁴⁷ que durant sa campagne baptisée *Diplomatic Orbiter*, *APT29* avait compromis des comptes de messagerie d'entités diplomatiques au moyen de courriels d'hameçonnage ciblé. Ce groupe s'en est également pris activement en 2024 à des partis politiques allemands¹⁴⁸.

8.2 Menaces subies par les systèmes de contrôle industriels et par la technologie opérationnelle

Loin de se limiter aux données et informations, les progrès de la transformation numérique s'étendent aux processus physiques et à leur pilotage, qui sont toujours plus souvent numérisés et mis en réseau par la même occasion avec les systèmes informatiques. Or, de tels systèmes ont de longs cycles de vie, ce qui complique souvent son intégration durable et sûre dans l'écosystème des technologies de l'information et de la communication. Qu'on le veuille ou non, toute négligence lors de l'adaptation de commandes industrielles peut être à l'origine de nouveaux risques, sur le plan de la sécurité. La prudence s'impose d'autant plus ici que les manipulations de processus cyber-physiques sont susceptibles d'avoir des répercussions sur les installations mécaniques, voire de menacer des vies humaines.

Des attaques ou tentatives de sabotage visant à perturber, voire détruire des équipements de production, ne s'observent généralement que lorsqu'un conflit a déjà dégénéré. Contrairement à ce que prétendent les hacktivistes, la Suisse est donc restée épargnée à ce jour, en dehors de retombées très ponctuelles de telles cyberattaques. Certains pirates affirment régulièrement avoir manipulé des systèmes de contrôle industriels (SCI) exposés sur Internet¹⁴⁹. Bien que des systèmes d'organisations suisses soient aussi cités dans ce contexte, aucun incident n'y a été signalé à ce jour.

Des attaques à caractère de sabotage ont par contre eu lieu dans le cadre des conflits actuels en Ukraine et à Gaza¹⁵⁰. En mars 2024, divers fournisseurs Internet ukrainiens ont été victimes de cyberattaques destructives¹⁵¹, tandis que des organisations d'approvisionnement énergétique ont subi à la fois une pluie de missiles et des attaques cybernétiques¹⁵². De nouveaux outils de piratage sont régulièrement déployés dans ce genre d'attaques, à l'instar du nouveau malicieux destructeur de données (*wiper*) nommé *AcidPour*¹⁵³, découvert durant ces campagnes de sabotage. En outre, une variante de *Kapeka*¹⁵⁴, malicieux créant des portes dérobées, a permis les perturbations du système d'approvisionnement énergétique. Les autorités ukrainiennes ont attribué ces activités de sabotage à l'*APT Sandworm*¹⁵⁵, rattachée à l'agence de renseignement militaire russe (*GRU*).

La Russie a elle aussi subi plusieurs actes de cybersabotage. À Moscou, le réseau de capteurs industriels *Moscollector* a par exemple été pris pour cible. Le groupe *Blackjack* s'est servi du

¹⁴⁷ [Malicious activities linked to the Nobelium intrusion set \(cert.ssi.gouv.fr\)](https://cert.ssi.gouv.fr)

¹⁴⁸ [APT29 Uses WINELOADER to Target German Political Parties \(cloud.google.com\)](https://cloud.google.com)

¹⁴⁹ [Dark Web Profile: Hunt3r Kill3rs \(socradar.io\)](https://socradar.io)

¹⁵⁰ [Bad Karma, No Justice: Void Manticore Destructive Activities in Israel \(research.checkpoint.com\)](https://research.checkpoint.com)

¹⁵¹ [Russian military intelligence may have deployed wiper against multiple Ukrainian ISPs \(cyberScoop.com\)](https://cyberScoop.com)

¹⁵² [Russian hackers target 20 energy facilities in Ukraine amid intense missile strikes \(therecord.media\)](https://therecord.media)

¹⁵³ [AcidPour | New Embedded Wiper Variant of AcidRain Appears in Ukraine \(sentinelone.com\)](https://sentinelone.com)

¹⁵⁴ [Kapeka: A novel backdoor spotted in Eastern Europe \(labs.withsecure.com\)](https://labs.withsecure.com)

¹⁵⁵ [APT44: Unearthing Sandworm \(services.google.com\)](https://services.google.com)

maliciel *Fuxnet*¹⁵⁶ pour rendre inutilisable l'équipement réseau des capteurs liés aux numéros d'urgence, aux aéroports ou aux gazoducs.

Le risque que de telles actions de sabotage aient des conséquences néfastes, venant notamment de prétendus hacktivistes gravitant autour des parties belligérantes, n'a pas disparu. Au-delà des dommages collatéraux ponctuels, des infrastructures européennes pourraient ainsi être prises pour cibles, si des acteurs malintentionnés devaient estimer avoir affaire à un pays adverse. Les autorités norvégiennes¹⁵⁷ et tchèques¹⁵⁸ ont déjà mis en garde contre le risque accru de sabotage en Europe. Un autre indice révélateur d'une telle évolution tient aux avertissements des fabricants¹⁵⁹ de systèmes de contrôle industriels signalant que les appareils exposés sur Internet sont spécialement menacés¹⁶⁰. Il est vrai que les attaques par rançongiciel ont des effets similaires au sabotage dans l'environnement des systèmes industriels, raison pour laquelle la protection contre de telles formes d'attaque s'impose.



Conclusion / Recommandations

Sécurisez vos systèmes industriels, afin d'empêcher les attaques décrites dans le présent chapitre. L'OFCS propose à cet effet une série de [mesures de protection pour les systèmes de contrôle industriels \(SCI\)](#).

Les [normes minimales par secteur](#) élaborées par l'Office fédéral pour l'approvisionnement économique du pays (OFAE) en collaboration avec les organisations sectorielles concernées proposent des solutions quant à elles un peu plus complètes.

Plusieurs partenaires internationaux ont publié une [fiche d'information](#) commune visant à déjouer les attaques lancées par les groupes hacktivistes lors de conflits.

¹⁵⁶ [Unpacking the Blackjack Group's Fuxnet Malware \(claroty.com\)](#)

¹⁵⁷ [Alarm over Russian-directed sabotage operations growing across Europe \(therecord.media\)](#)

¹⁵⁸ [Russia is trying to sabotage European railways, Czech minister said \(securityaffairs.com\)](#)

¹⁵⁹ [Security Advisory \(rockwellautomation.com\)](#)

¹⁶⁰ [It appears that the number of industrial devices accessible from the internet has risen by 30 thousand over the past three years \(isc.sans.edu\)](#)