30 mars 2026 | Office fédéral de la cybersécurité OFCS

Rapport semestriel 2025/II (juillet – décembre)

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 du sport DDPS
Office fédéral de la cybersécurité OFCS

Résumé

L'Office fédéral de la cybersécurité (OFCS) décrit dans le présent rapport semestriel les principaux cyberincidents survenus et l'évolution des cybermenaces tant en Suisse que sur la scène internationale. Au deuxième semestre 2025, l'OFCS a reçu 29 006 déclarations volontaires de cyberincidents et 145 déclarations obligatoires, le nombre total des notifications s'étant stabilisé à un niveau élevé. 52 % de ces annonces concernent encore le phénomène de la fraude, même si les appels de menace émanant prétendument des autorités [1], qui caracolent en tête de classement depuis le deuxième semestre 2023, se sont raréfiés ces derniers mois. Les principales menaces n'ont pas non plus changé en Suisse durant la période sous revue, malgré l'apparition ponctuelle de nouvelles variantes.

Variantes d'hameçonnage adaptées à la Suisse
Les cybercriminels ont continué à mener des campagnes d'hameçonnage par téléphone (*vishing*) et d'hameçonnage en temps réel[2] reposant sur des publicités frauduleuses diffusées à l'aide de moteurs de recherche. Des variantes d'attaques plus sophistiquées et mieux ciblées, intégrant des spécificités du marché suisse comme les programmes de fidélité, ont également été observées. En outre, les agresseurs ont parfois tiré parti d'un épisode d'hameçonnage qui venait d'aboutir pour duper une seconde fois leurs victimes par téléphone (double hameçonnage[3]). Dès l'été 2025, les criminels ont recouru à la technique du SMS Blaster pour diffuser en masse des SMS de phishing en contournant les méthodes de filtrage utilisées par les fournisseurs de services de communication.

Les rançongiciels, menace constante et sérieuse
Les rançongiciels[4] et le chantage aux données volées restent une menace permanente pour toutes sortes d'organisations suisses. 57 incidents liés à des rançongiciels ont été annoncés directement à l'OFCS, soit de manière volontaire, soit dans le cadre de l'obligation de signaler les cyberattaques. La variante Akira, déjà numéro un en Suisse au premier semestre 2025, a encore consolidé sa position. Une vulnérabilité découverte en 2024 dans les appareils SonicWall l'y a aidée, tous les utilisateurs concernés n'ayant pas pris la peine de suivre les instructions données par le fabricant pour se protéger.

Attaques contre des fournisseurs internationaux de la chaîne d'approvisionnement logicielle
Au deuxième semestre 2025, bien des organisations suisses ont subi des attaques tirant parti non seulement des vulnérabilités de produits logiciels courants, mais aussi de la compromission de logiciels à code source ouvert utilisés à grande échelle. Les campagnes Shai-Hulud de septembre et novembre 2025 ont ainsi infecté plus d'un millier de paquets npm (*node package manager*) téléchargés des centaines de millions de fois par mois. Le niveau de complexité

1 Appels au nom de fausses autorités (ncsc.admin.ch)
2 Hameçonnage (Phishing), Vishing, Smishing (ncsc.admin.ch)
3 Semaine 39 : Tentatives d'hameçonnage successives (ncsc.admin.ch)
4 Ransomware (ncsc.admin.ch)

des dépendances techniques actuelles donne des sueurs froides aux responsables informatiques : en cas de faille de sécurité d'une bibliothèque de logiciels utilisée, toutes les applications contenant un tel composant dans leur code sont potentiellement vulnérables.

Réseaux ORB en Suisse

Les réseaux ORB (*operational relay boxes*) deviennent toujours plus tentaculaires. Généralement constituées de routeurs et autres appareils connectés (IoT) ayant été préalablement infectés par un logiciel malveillant[5], ces infrastructures d'attaque exploitent sans scrupules les ressources piratées. Bien des appareils appartenant à des particuliers ou à des organisations suisses ont ainsi été impliqués dans des activités criminelles. D'où l'importance d'effectuer régulièrement les mises à jour de sécurité des appareils exposés à Internet pour lutter contre ce genre de réseaux. Il est de notoriété publique depuis 2024 que des acteurs étatiques utilisent également les réseaux ORB à des fins d'espionnage et de sabotage.

Les autres chapitres du présent rapport semestriel font état d'observations récentes et reviennent sur l'évolution des logiciels malveillants, des attaques affectant la disponibilité des sites web et autres services web, de la gestion des données, ainsi que du cyberespionnage et du cybersabotage. En dépit d'un environnement géopolitique toujours plus tendu, les effets de la cybermenace sont relativement stables et la Suisse fait preuve d'une grande robustesse en matière de cyberrésilience.

5 Logiciels malveillants (ncsc.admin.ch)

Table des matières

Editorial

Le niveau de cybermenaces persiste à un niveau élevé en Suisse. Dans leur grande majorité, les cyberincidents repérés sont liés à des activités criminelles. Les incertitudes économiques et le contexte géopolitique de plus en plus tendu sont favorables aux cyberattaques, qui se caractérisent aussi par une meilleure coordination ainsi qu'une efficacité et une précision en hausse. Au-delà de la menace persistante de la cybercriminalité, il faut également s'attendre à une recrudescence d'attaques plus sophistiquées, préparées de manière professionnelle par des acteurs soutenus au niveau étatique, dans un but stratégique.

Les attaques par rançongiciel restent l'un des grands défis des organisations en Suisse. La combinaison du chiffrement et de l'extorsion de données est un risque à prendre toujours au sérieux, tant par les milieux économiques que par l'administration. Le groupe de pirates informatiques *Akira*, par exemple, a considérablement étendu ses activités dans notre pays ces derniers mois. Parallèlement, les attaques tout au long des chaînes logistiques se multiplient, la publicité en ligne est de plus en plus souvent utilisée à des fins de tromperie et de fraude, et la digitalisation croissante entraîne une augmentation constante du nombre de vulnérabilités potentielles. Ces tendances élargissent la surface d'attaque en augmentant la complexité de la situation globale en matière de menaces.

Seuls un signalement et une évaluation systématiques des cyberincidents permettent d'obtenir une image réaliste et solide de la situation. Le présent rapport s'appuie ainsi sur les nombreux signalements spontanés de la population et des acteurs économiques. En effet, l'OFCS a reçu quelque 65 000 signalements en 2025, qui constituent une base indispensable pour dresser le tableau de la situation à l'échelle nationale. Autre étape importante pour renforcer la cyberrésilience du pays : l'introduction de l'obligation légale de signaler les cyberattaques contre les infrastructures critiques au 1er avril 2025. Pour la première fois, il est possible de procéder à une analyse structurée qui intègre les incidents faisant l'objet d'un signalement obligatoire.

Les signalements déjà reçus ont fourni de précieuses informations sur les types d'attaque, sur les secteurs touchés et sur les risques systémiques potentiels. Leur évaluation montre que la cybersécurité ne doit pas être une tâche isolée revenant à un petit nombre d'acteurs. Au contraire, elle concerne tout autant l'État que les milieux économiques et la société dans son ensemble. En effet, loin de s'arrêter à une organisation, une branche ou un pays, une cyberattaque provoque des dégâts au gré des nombreuses interdépendances numériques.

Dans ce contexte, les questions géopolitiques sont davantage discutées aux niveaux national et international. L'importance systémique croissante des dépendances numériques, l'influence des nouvelles technologies, à commencer par l'intelligence artificielle, et la nécessité d'une action coordonnée entre les États, les autorités de surveillance et les acteurs privés sont désormais au centre des débats.

Résultat : il est reconnu que la simple prévention ne suffit pas pour atteindre la cyberrésilience. La sécurité technique doit s'accompagner de structures de gouvernance claires, de bonnes capacités de réaction et de reprise, et d'une coopération étroite à l'échelle nationale comme internationale. C'est précisément dans ce domaine que nous voulons continuer d'investir, en simplifiant davantage la coopération et en nous unissant dans une action commune plus forte pour lutter contre les cybermenaces.

L’OFCS tient à remercier toutes les organisations et les personnes qui améliorent de manière significative la cyberrésilience du pays et contribuent à la cyberstratégie nationale (CSN) en signalant incidents et menaces, et en manifestant leur engagement et leur intérêt pour ce sujet. Cette unité d’action est essentielle pour continuer à affronter efficacement les défis dans le cyberespace.

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

1 Cybermenaces en Suisse – tour d'horizon

Une propriété centrale du cyberespace fait que les cyberattaques peuvent être menées à distance, de l'étranger. Les cyberpirates ont toutefois renoncé à l'impunité assurée par l'éloignement physique de leurs victimes pour venir déployer en Suisse, dès l'été 2025, des SMS Blaster[6]. En réponse au renforcement des mesures de filtrage déployées par les opérateurs de télécommunications pour lutter contre les attaques de phishing, les escrocs utilisent désormais dans les villes suisses des antennes de téléphonie mobile portables, de la taille d'un boîtier d'ordinateur, afin d'envoyer des SMS frauduleux aux téléphones mobiles situés dans un rayon d'un kilomètre (voir chap. 2). Les activités confirment d'abord que les cybercriminels sont à l'affût de nouveaux modes opératoires, quitte à devoir s'exposer dans l'espace public. Ensuite, que la cybermenace constitue un environnement dynamique, dans lequel les attaquants comme les défenseurs doivent constamment adapter leur approche à l'évolution de la situation.

Le rapport semestriel s'appuie avant tout, pour présenter la situation en matière de cybermenaces, sur les annonces volontaires effectuées à l'OFCS par la population et les entreprises. Ce rapport est le premier toutefois à faire la distinction entre les déclarations volontaires et obligatoires, les exploitants d'infrastructures critiques ayant depuis le 1er avril 2025 l'obligation de signaler certaines cyberattaques[7]. Au total, l'OFCS a traité durant la période sous revue 145 cyberincidents ayant fait l'objet d'une déclaration obligatoire. Le secteur public (25 %), l'informatique et les télécommunications (18 %), ainsi que la finance et les assurances (15,7 %) sont principalement concernés (voir fig. 1). Les types d'attaques les plus fréquents comprennent l'accès non autorisé à des systèmes (piratage), le vol de données d'accès et les attaques affectant la disponibilité (DDoS[8]). Des approches destructrices, reposant sur le chiffrement et le chantage (rançongiciels), ont servi dans 7 % des cas (voir fig. 2).

Le nombre de déclarations volontaires de cyberincidents a légèrement progressé en 2025, avec 64 733 annonces au total contre 62 954 en 2024. Au deuxième semestre 2025, l'OFCS a reçu 29 006 annonces à caractère volontaire (voir fig. 3). Les fraudes ont à nouveau été le phénomène le plus souvent signalé (15 090 annonces), devant l'hameçonnage (6 299 annonces) et les pourriels (4 284 annonces). Dans cette dernière catégorie, les arnaques à la publicité pour les investissements (catégorisées comme pourriels) ont connu une évolution frappante. La hausse dépasse 2 500 cas par rapport au deuxième semestre 2024, avec une brusque vague au premier semestre 2025, suivie d'un tassement durant la période sous revue. Les signalements concernant des boutiques en ligne frauduleuses, dont la marchandise est fictive ou falsifiée, ont également augmenté. Il est intéressant de noter que beaucoup de ces sites web mettent en avant le « facteur swissness » pour mieux gagner la confiance de la clientèle.

6 Semaine 36 : Nouveau danger lié aux SMS Blaster

7 Information sur l'obligation de signaler (ncsc.admin.ch)

8 Attaque affectant la disponibilité (attaque DDoS) (ncsc.admin.ch)

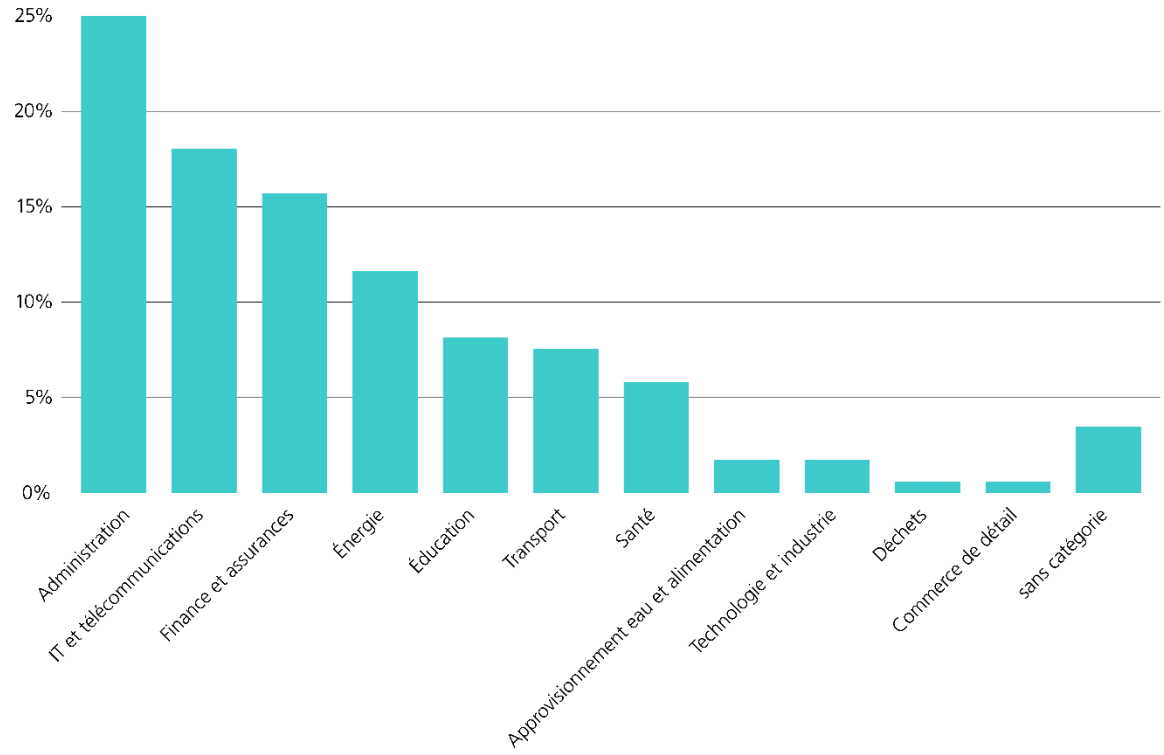

Fig. 1: répartition par secteur (en %) des déclarations obligatoires reçues par l'OFCS au deuxième semestre 2025

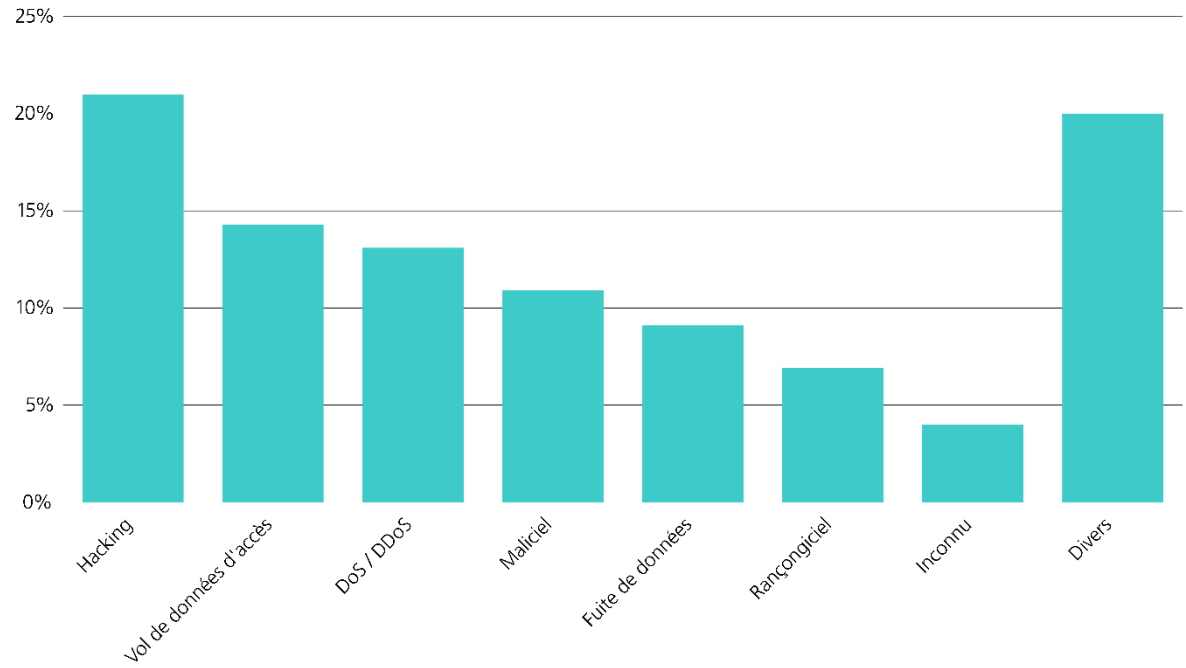

Fig. 2: répartition par type d'incident (en %) des déclarations obligatoires reçues par l'OFCS au deuxième semestre 2025

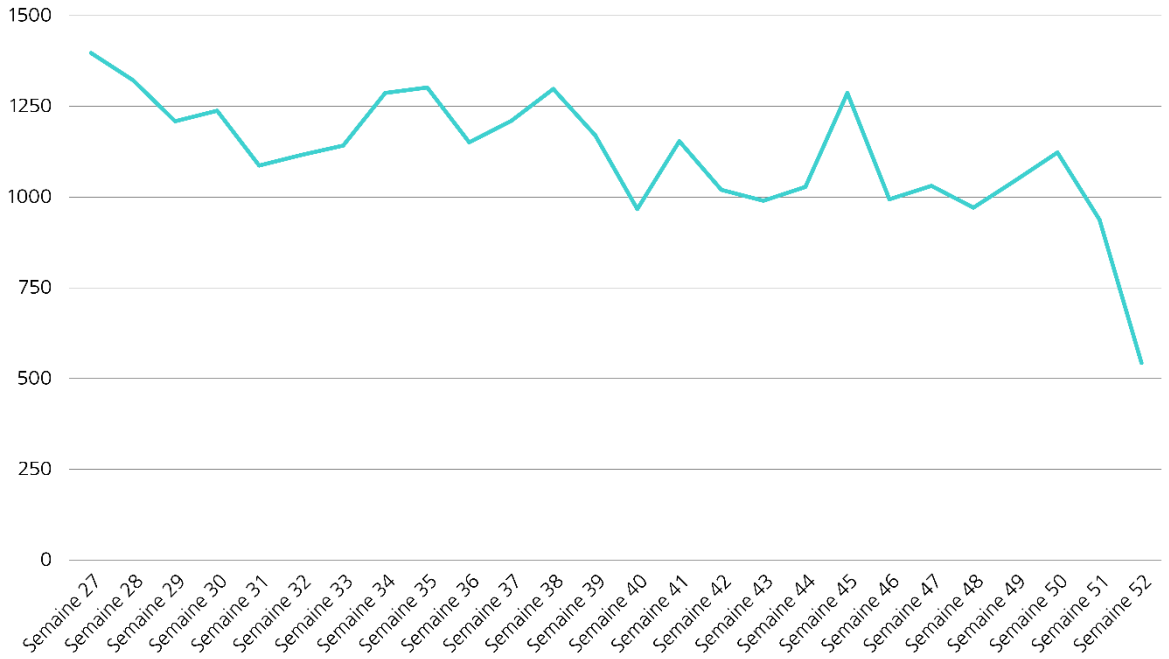

Fig. 3: annonces volontaires faites à l'OFCS (par semaine) au deuxième semestre 2025, voir Chiffres actuels (ncsc.admin.ch)

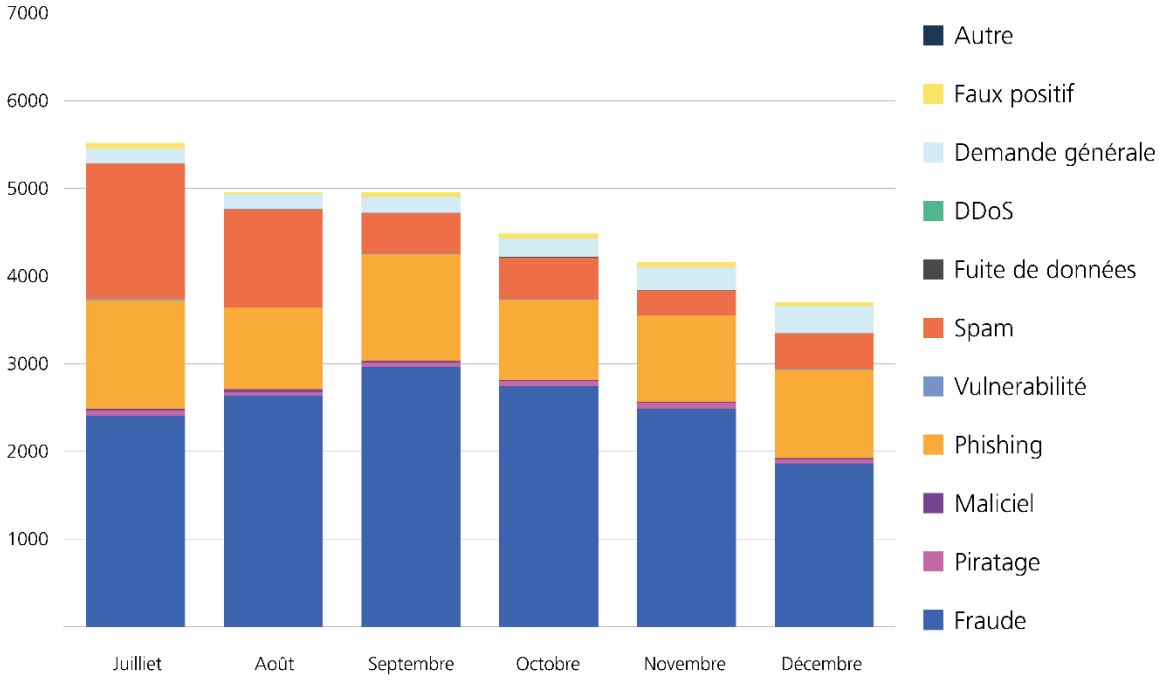

Fig. 4: annonces volontaires faites à l'OFCS au deuxième semestre 2025, par catégorie, voir Chiffres actuels (ncsc.admin.ch)

À l'opposé, le nombre d'appels de menace émanant prétendument des autorités[9] a chuté par rapport au deuxième semestre 2024, passant de 8 173 à 5 941 annonces. Il s'agit d'une première depuis l'apparition de ce phénomène au deuxième semestre 2023. Quant aux notifications de fraude à l'investissement en ligne[10], elles sont restées stables par rapport au semestre précédent, avec 430 cas signalés. À ceci près que dans un nombre croissant de cas, les victimes ont été relancées par les escrocs, sous prétexte que l'argent volé pouvait être récupéré moyennant un nouveau paiement.

Le rapport entre les annonces émanant de la population et celles effectuées par des entreprises, des associations ou des autorités est resté stable à raison de 90 % et 10 %. Si les appels de menace émanant prétendument des autorités et les tentatives d'hameçonnage concernent tant les entreprises que les particuliers, il ressort des annonces du deuxième semestre 2025 que 57 entreprises ont été prises pour cible par un rançongiciel. Les organisations restent typiquement exposées à la manipulation de factures à la suite d'un piratage de messagerie professionnelle (*Business E-Mail Compromise*, BEC[11]) ainsi qu'à l'arnaque au président[12]. Après avoir augmenté au cours du premier semestre 2025, les cas d'arnaque au président signalés ont diminué au cours du semestre sous revue ; en ce qui concerne le piratage de messagerie professionnelle, la tendance reste à la hausse : après les 59 annonces du premier semestre, pas moins de 73 cas ont été enregistrés au deuxième semestre 2025. Ce type de cyberattaque peut causer un grave préjudice financier, une victime ayant été délestée de 1,5 million de francs. En outre, comme les escrocs ont accès à des communications confidentielles, le risque de dommages collatéraux est bien réel pour tous les tiers concernés.

Données statistiques à l'appui, la cybersécurité et la protection de la Suisse face aux cyberrisques constituent un défi permanent pour les milieux économiques, l'État et la société. Aussi le rapport semestriel aborde-t-il un à un les principaux phénomènes caractérisant l'éventail des menaces dans le cyberespace suisse, à savoir l'hameçonnage, les maliciels, les vulnérabilités, les cas de fraude et d'ingénierie sociale[13], les attaques affectant la disponibilité des sites web et autres services Internet (DDoS), les fuites de données, le cyberespionnage et le cybersabotage. Le rapport se concentre sur les événements et développements apparus en Suisse. Les tendances internationales n'y apparaissent que dans la mesure où elles aident à comprendre notre environnement de menaces (voir chap. 8). Au fil des chapitres, les lecteurs pourront se faire une bonne idée des risques actuels, des incidents dignes d'attention et de l'évolution des principaux phénomènes. Selon le principe de responsabilité individuelle, voulant que chaque personne contribue à rendre la Suisse numérique plus sûre, le présent rapport formule également des recommandations au grand public sur la manière de relever ces divers défis.

---

9 Afin de mieux cerner le phénomène des appels de menace émanant prétendument des autorités, l'OFCS lui a consacré un rapport, publié en même temps que le rapport semestriel 2024/1.

10 Fraude à l'investissement en ligne (ncsc.admin.ch)

11 Piratage d'une messagerie professionnelle (ncsc.admin.ch)

12 Arnaque au président (ncsc.admin.ch)

13 Ingénierie sociale (Social Engineering) (ncsc.admin.ch)

2 Hameçonnage

L'hameçonnage permet aux cybercriminels de collecter les données d'accès, les informations financières et d'autres données confidentielles d'utilisateurs ne se doutant de rien. Il s'agit typiquement de persuader la personne ciblée d'agir d'une certaine façon (ingénierie sociale), sans distribuer de maliciel[14]. La méthode classique consiste à envoyer un message contenant un lien à un large groupe de destinataires. Ce lien conduit à une page imitant un site légitime. La victime jugeant le site crédible y introduira des données sensibles, comme les identifiants et les données de sa carte de crédit, qui parviennent ainsi aux escrocs. Tandis que l'hameçonnage par courriel reste une des méthodes les plus répandues, d'autres approches utilisent la voix (*voice phishing* ou *vishing*), le SMS (*smishing*) ou d'autres formes de messages mobiles encore pour accéder à des informations sensibles. Si l'hameçonnage vise une personne ou un groupe de personnes spécifique, il s'agit de harponnage (*spear phishing*). Contrairement à sa variante à large diffusion, ce type d'attaque conçu sur mesure pour la cible est très difficile à détecter.

En 2025, l'OFCS a reçu par son formulaire d'annonce public 12 280 signalements de tentatives d'hameçonnage, résultat quasiment identique à celui de l'année précédente. 6299 annonces concernent le deuxième semestre, soit 903 de plus qu'un an plus tôt à la même période.
Les statistiques de la plateforme antiphishing.ch[15] gérée par l'OFCS ont évolué différemment. Après avoir affiché une croissance continue jusqu'à la fin de l'année 2024, les cas annoncés ont entamé une décrue en 2025. Alors que 9355 adresses Internet (URL) d'hameçonnage étaient encore signalées au deuxième semestre 2024, leur nombre a diminué à 7969 en 2025 au cours de la même période. Afin de rendre leurs pages d'hameçonnage aussi crédibles que possible, les criminels usurpent régulièrement des noms de marques ou d'entreprises connues. Durant la période sous revue, les abus se sont concentrés sur les services postaux (24 %), les transports publics (20 %), le secteur financier (19 %), le secteur informatique (7 %) et le secteur des assurances (7 %) (voir fig. 5). Par ailleurs, les criminels sont toujours plus actifs dans le secteur des caisses-maladie[16] et le nombre d'URL d'hameçonnage signalées a augmenté dans le commerce de détail (5 %).

---

14 Au niveau international, le terme d'hameçonnage ne recouvre pas partout la même réalité. D'autres définitions incluent la diffusion de maliciels (voir Phishing (attack.mitre.org)). Mais l'OFCS exclut expressément cet aspect dans sa définition de l'hameçonnage.

15 Outre les cas d'hameçonnage qui lui sont directement signalés en tant qu'incidents, l'OFCS en reçoit d'autres par le biais de la plateforme antiphishing.ch, qui contient des sources supplémentaires. C'est pourquoi les chiffres indiqués ici peuvent différer du nombre d'annonces directes de cas d'hameçonnage.

16 Voir p. ex. Phishing-Mail richtet sich an Helsana-Kunden (cybercrimepolice.ch), Phishing-Mail – Rückerstattung CSS-Krankenkassengelder (cybercrimepolice.ch)

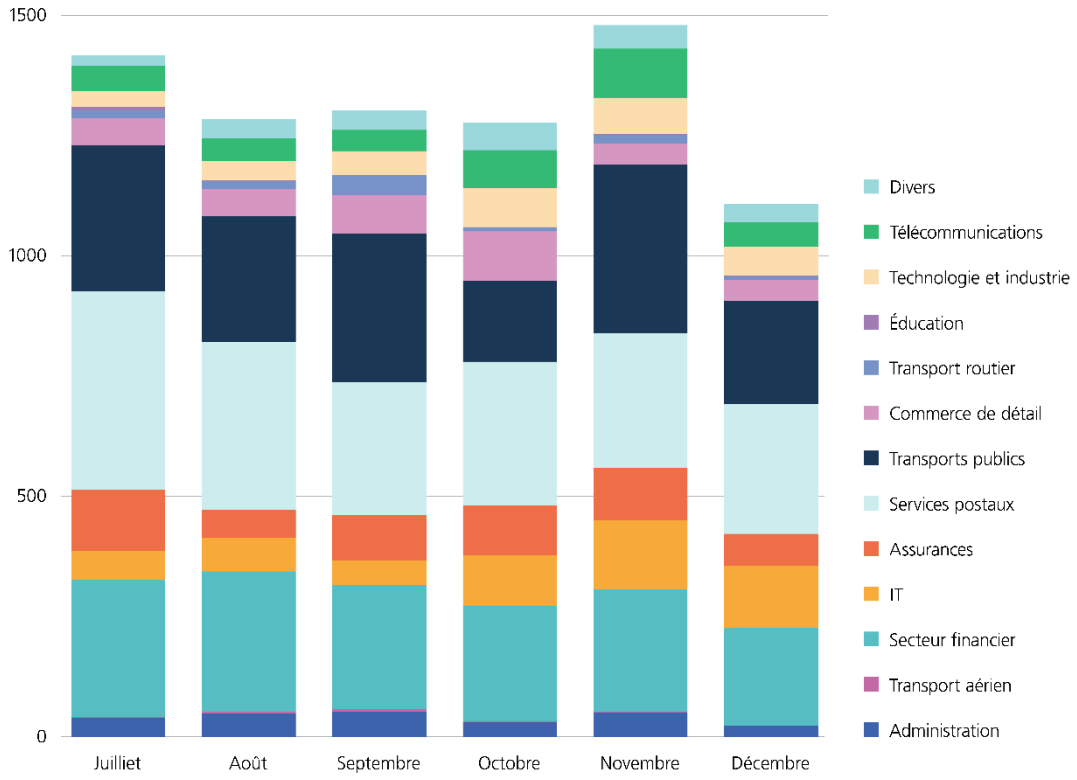

Fig. 5: nombre mensuel d'URL d'hameçonnage vérifiées et confirmées par l'OFCS au deuxième semestre 2025, ventilées par secteur ciblé

De manière générale, le deuxième semestre 2025 s'inscrit dans la continuité des tendances observées au premier semestre. Des messages d'hameçonnage aux formules passe-partout continuent d'être envoyés à grande échelle. Près de 40 % des URL d'hameçonnage signalées à l'OFCS se réfèrent encore à SwissPass ou à un service de livraison de colis. Mais des variantes de plus en plus sophistiquées et ciblées sont également diffusées, au prix d'un surcroît de travail pour leurs expéditeurs. D'une part, des cas d'hameçonnage bancaire en temps réel à partir de publicités malveillantes s'affichant dans les moteurs de recherche restent signalés[17]. Pour maximiser leurs chances de succès, les escrocs ne se contentent plus de diffuser des publicités malveillantes aboutissant à leurs sites d'hameçonnage, mais utilisent l'empoisonnement de l'optimisation pour les moteurs de recherche (*SEO poisoning*[18]) pour diffuser leurs sites. Dans une variante du *vishing (voice phishing)*, la victime est priée par courriel ou SMS non de cliquer sur un hyperlien, mais de rappeler un numéro de téléphone, sous prétexte d'une transaction d'e-banking suspecte.[19] D'autre part, face à la prise de conscience croissante de la population, les pirates cherchent à dissimuler leurs agissements en envoyant de prétendus courriels de vérification.[20] La victime y est invitée à confirmer son identité en saisissant ses

[17] Voir rapport semestriel 2025/1 ; chap. 2.

[18] Dans le cas du *SEO poisoning*, les agresseurs tentent de manipuler les moteurs de recherche afin que leurs sites web malveillants apparaissent en tête des résultats les plus pertinents (voir Empoisonnement de l'optimisation pour les moteurs de recherche (cyber.gc.ca)).

[19] Semaine 50 : un appel aux graves conséquences financières (ncsc.admin.ch)

[20] Voir p. ex. Semaine 48 : campagne d'hameçonnage au nom de SERAFE sous prétexte de vérification de la situation du ménage (ncsc.admin.ch)

données d'accès sur une page d'hameçonnage. Outre ces développements, les cyberincidents observés comprennent des cas de SMS Blaster[21] et de double hameçonnage[22], nouvelle méthode échelonnée en plusieurs étapes.

Recommandations

Signalez à l'OFCS les sites présentant un risque d'hameçonnage via reports@antiphishing.ch ou directement sur la plateforme antiphishing.ch. Pour obtenir un suivi de votre annonce, vous pouvez aussi signaler cet 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 bloqués.

Des campagnes adaptées à la Suisse

Au deuxième semestre 2025, les fraudeurs ont multiplié les attaques par hameçonnage ciblé, en optant pour des contenus typiquement suisses ou en s'adressant à des groupes de personnes spécifiques. Il s'agissait d'augmenter ainsi les chances de succès par rapport à l'hameçonnage de masse impersonnel. Dans ce contexte, un courriel d'hameçonnage signalait notamment aux personnes âgées qu'un avoir de caisse de pension oublié allait leur être crédité. Des variantes d'hameçonnage ont tiré parti d'anciennes fuites de données (voir chap. 7) pour rendre plus crédible la communication frauduleuse cherchant à soutirer des informations sensibles aux destinataires. Dans une autre tentative, les pirates s'adressaient directement à la clientèle de Swisscom. Au lieu des habituels courriels de remboursement, leur message faisait état de points de fidélité arrivant à expiration. Un site web sophistiqué et entièrement fonctionnel prétendait que le destinataire disposait de 8517 points de fidélité. Les victimes pouvaient ainsi ajouter des articles tels que des vélos ou des smartphones à un panier d'achat, jusqu'à épuisement de leurs points de fidélité. Il fallait toutefois s'acquitter de frais d'envoi et saisir des données sensibles en vue de l'expédition des marchandises convoitées.[23] Cette stratégie exploite la peur des destinataires de rater une bonne affaire. Des campagnes similaires ont été observées dans d'autres secteurs où les programmes de fidélisation sont répandus, comme les supermarchés suisses, les banques et les sociétés de cartes de crédit.

Collecte du profil de données complet

Outre les campagnes d'hameçonnage classiques visant les données de connexion ou les informations relatives aux cartes de crédit, l'OFCS a observé de nombreuses attaques où les renseignements demandés allaient bien au-delà des données d'accès. Les escrocs avaient créé à cet effet des pages web ressemblant à s'y méprendre à celles d'institutions dignes de confiance telles que des banques, des assurances, des caisses-maladie ou d'autres prestataires de services de paiement. Sous prétexte d'une vérification ou mise à jour de leurs données, les utilisateurs étaient invités à divulguer des informations personnelles détaillées. Dans un cas, les agresseurs sont allés jusqu'à exiger, en plus des informations personnelles, une signature numérique en vue d'un prétendu remboursement.

---

21 Semaine 46 : Comment les fraudeurs contournent les filtres SMS des fournisseurs d'accès (ncsc.admin.ch)

22 Semaine 39 : Tentatives d'hameçonnage successives (ncsc.admin.ch)

23 Phishing-SMS lockt mit angeblichen Cumulus-Punkten (cybercrimepolice.ch)

Lors de ces attaques, les fraudeurs cherchent à établir un profil de données aussi complet que possible de leurs victimes. De tels profils sont particulièrement précieux pour les activités criminelles, se prêtant aussi bien à l'usurpation d'identité qu'aux attaques d'ingénierie sociale ou à la revente au noir des données. Plus les profils sont complets, plus leur valeur commerciale est élevée. Ces cyberattaques confirment la constatation générale selon laquelle les attaques d'hameçonnage ciblé ont pris le relais des messages génériques envoyés en masse : le simple fait d'utiliser une formule de politesse ou une adresse correcte augmente la confiance du destinataire. Et si les malfaiteurs connaissent en plus leurs coordonnées bancaires ou d'autres informations personnelles, il est d'autant plus probable que les victimes leur communiquent d'autres données personnelles.

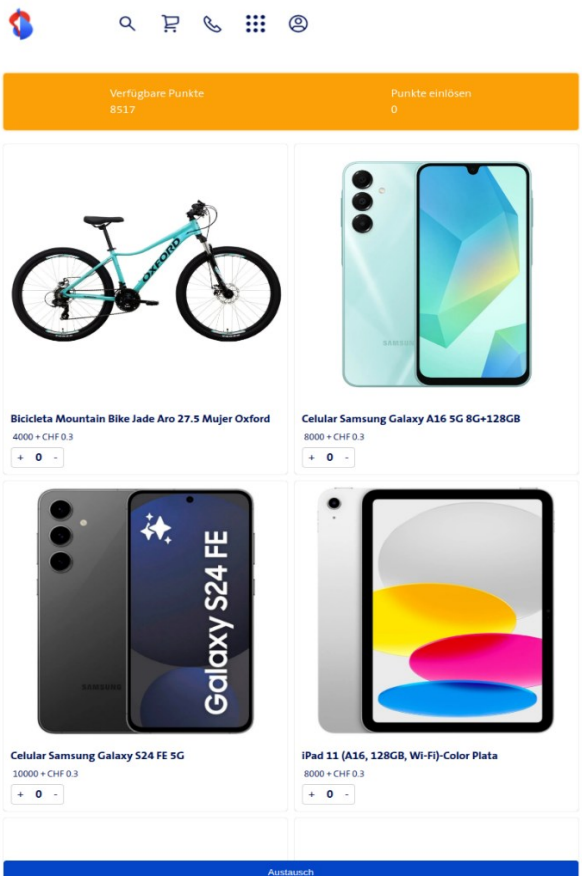

Fig. 6: site web frauduleux d'utilisation de points de fidélité géré au nom de Swisscom

Double hameçonnage

Durant la période sous revue, l'OFCS a également reçu des annonces concernant de nouvelles variantes d'hameçonnage sophistiquées, ce qui corrobore la tendance à l'usage de méthodes toujours plus ciblées et raffinées. Dans le double hameçonnage (*double phishing*), les escrocs procèdent par étapes, en réutilisant aussitôt pour une seconde attaque, menée par téléphone, les données recueillies lors de la première : les victimes recevaient d'abord un message d'hameçonnage classique, muni d'un lien vers un site frauduleux, au sujet par exemple d'un prétendu remboursement d'impôt ou d'une amende de stationnement. Outre les données de sa carte de crédit, il fallait indiquer le nom de sa banque et son propre numéro de téléphone. Quelques minutes plus tard, les escrocs appelaient le numéro fraîchement obtenu, en se faisant passer pour le service de sécurité de l'établissement financier en question. Ils

prétendaient que le compte venait d'être piraté, ou que de l'argent avait été détourné. Afin de protéger le compte, la victime devait leur donner immédiatement accès à son ordinateur, via un outil d'accès à distance. En réalité, les pirates profitaient de cet accès pour effectuer des transactions sur le compte e-banking de la victime.
Grâce au renforcement des mesures de sécurité adoptées par les banques, les attaques directes lancées contre les comptes d'e-banking sont devenues rares. Les malfaiteurs incitent à la place leurs victimes à leur céder d'elles-mêmes le contrôle de leur e-banking, afin de contourner ainsi les mesures de sécurité habituelles. Leur appel semble plausible aux victimes, un incident de sécurité s'étant bel et bien produit lors du premier hameçonnage. Cette variante montre que les escrocs savent combiner les attaques par écrit et par téléphone, afin de paraître plus crédibles et de maximiser leurs profits. Des agissements similaires ont été observés à propos de prétendues amendes de stationnement ou de petites annonces frauduleuses. La langue reste toutefois un obstacle majeur dans ce type d'attaques téléphoniques. Dans un cas concret, les attaquants ne pouvaient communiquer qu'en français. Mais il est vrai que grâce à l'utilisation de l'intelligence artificielle (IA), les compétences linguistiques sont susceptibles un jour de passer à l'arrière-plan pour les appels téléphoniques, qu'il sera possible d'effectuer à l'aide d'outils de traduction simultanée.

SMS Blaster

À la fin de l'été 2025, une nouvelle forme de diffusion de l'hameçonnage et de la fraude en ligne a été observée pour la première fois en Suisse, avec le SMS Blaster.[24] Bien que cette méthode soit déjà connue dans certaines régions d'Europe et d'Asie, elle constitue un nouveau vecteur de diffusion en Suisse et son éradication requiert une étroite coopération entre les autorités et les opérateurs de télécommunications. Techniquement parlant, le SMS Blaster est un appareil portable de la taille d'un boîtier d'ordinateur qui se fait passer pour une antenne de téléphonie mobile et incite les téléphones portables situés à proximité à se connecter à lui. Une fois la connexion établie, l'appareil pris pour cible est rétrogradé au protocole 2G obsolète. En mode 2G, les pirates exploitent à partir de là une vulnérabilité connue sous le nom de *NULL cipher*, afin d'envoyer des SMS sans les contrôles habituels ni l'intervention de l'opérateur mobile légitime. Des messages d'hameçonnage par SMS (*smishing*) parviennent ainsi aux appareils mobiles situés dans un rayon d'un kilomètre, en contournant les filtres et mécanismes de blocage standard mis en place par l'opérateur réseau concerné. Le contenu des SMS transmis et les sites web utilisés dans ce contexte correspondent aux modèles d'hameçonnage déjà connus de l'OFCS, entre les notifications de colis ou d'amendes impayées ou les offres alléchantes basées sur des points de fidélité, qui toutes visent à récupérer des données d'accès ou des informations de carte de crédit.

Recommandations

Activez autant que possible l'authentification multifactorielle (AMF) pour renforcer la sécurité de vos comptes. Cette méthode, qui réduit significativement le risque de violation de données, peut cependant tour de même être déjouée par des techniques d'ingénierie sociale[25]. Méfiez-

[24] Semaine 46 : Comment les fraudeurs contournent les filtres SMS des fournisseurs d'accès (ncsc.admin.ch)
[25] Ingénierie sociale (Social Engineering) (ncsc.admin.ch)

vous donc des demandes frauduleuses, transmises par courriel ou par SMS, vous invitant à confirmer des accès ou à divulguer votre code. N'oubliez pas non plus qu'il est facile de falsifier une adresse électronique ou un numéro de téléphone afin de rendre un message plus crédible. N'inscrivez jamais de données de votre carte de crédit ou d'autres données sensibles sur une page que vous avez ouverte à partir d'un lien reçu par courriel ou sms.

3 Maliciels

Les logiciels malveillants (*malware* ou maliciels) sont un des principaux outils dont disposent les cybercriminels pour s'introduire dans un appareil ou un réseau. En règle générale, ces programmes déploient une activité indésirable et nuisible sur les systèmes informatiques à l'insu de leurs utilisateurs[26], par exemple en leur dérobant des données, en les manipulant ou en les supprimant. Il existe différentes méthodes d'infection par maliciel, à travers toutes sortes de canaux et sur tous types d'appareils et d'infrastructures.

3.1 Accès initial au moyen de maliciels

Par accès initial, on entend toutes les activités qu'un attaquant déploie pour compromettre un système externe. L'intrusion peut s'effectuer, par exemple, au moyen des données d'accès (p. ex. nom d'utilisateur et mot de passe) obtenues par ingénierie sociale et par hameçonnage (voir chap. 2), en tirant parti de vulnérabilités (voir chap. 4) ou à l'aide d'un maliciel, comme un cheval de Troie. Cette dernière approche, qui exige en général une action de la part des utilisateurs, recourt à différents mécanismes de tromperie (ingénierie sociale) pour persuader la victime d'installer le maliciel. Le logiciel malveillant peut ainsi être dissimulé dans un autre programme ou une pièce jointe ou un lien reçu par courriel et qui semble inoffensif à première vue.

Durant la période sous revue, l'OFCS n'a observé aucun nouveau mode de propagation des logiciels malveillants. La plupart des campagnes signalées correspondaient aux tendances internationales et ne présentaient aucune caractéristique spécifique à la Suisse. Les cybercriminels continuent de recourir massivement à la méthode *ClickFix*[27] décrite dans les précédents rapports, qui consiste à amener la victime à installer elle-même le maliciel. Il en ressort que ce mode opératoire a conservé un rapport coût/bénéfice intéressant. Par pur opportunisme, les pirates cherchent toujours à infecter les appareils d'un maximum d'utilisateurs, sans cibler un quelconque groupe de population ou secteur d'activité. On observe tout au plus des adaptations ponctuelles, destinées à renforcer la crédibilité de leurs scénarios auprès de leurs destinataires suisses.

---

26 Logiciels malveillants (ncsc.admin.ch)

27 Voir rapport semestriel 2024/2, chap. 3.1 et rapport semestriel 2025/1, chap. 3.1.

Plusieurs notifications reçues concernent l'envoi de factures, censées provenir d'une société de recouvrement active en Suisse. Les courriels se réfèrent à une prétendue facture QR envoyée en pièce jointe pour paiement. En réalité, la pièce jointe est un fichier HTML. Lors de son ouverture, le destinataire reçoit un message signalant que le PDF ne peut être affiché, car JavaScript est désactivé. Il lui faut donc appuyer sur les combinaisons de touches *Windows* + *R*, suivies de *Ctrl* + *V*. Selon la méthode ClickFix, l'opération aboutit à l'exécution d'un script malveillant préalablement copié dans le presse-papiers et à l'installation du maliciel.[28] L'OFCS a également reçu plusieurs signalements liés à des portails de petites annonces. Les criminels se faisaient passer pour des acheteurs pressés. Ils prétendaient avoir déjà effectué un paiement et avaient joint à leur courriel un fichier nommé *twint-rechnung.zip*. Or ce fichier contenait un logiciel malveillant spécialisé dans le vol de données personnelles ou financières (*infostealer*), qui collecte principalement les données d'accès enregistrées dans le navigateur.[29] Plusieurs cyberattaques ont également été menées à l'aide de fausses offres d'emploi, principalement sur la plateforme LinkedIn.[30] Dans un cas, les escrocs simulaient un problème technique lors du téléchargement d'une vidéo de présentation, en priant le candidat d'exécuter une commande copiée dans son presse-papier. Là encore, il s'agissait d'une variante de ClickFix. Dans un autre cas, un candidat a dû télécharger des fichiers pour une tâche de programmation, dans le cadre d'un prétendu processus de recrutement. Les fichiers en question contenaient un code malveillant qui dérobait des données confidentielles sur l'ordinateur de la victime. Ces deux derniers modes opératoires ont fréquemment été observés à l'échelon international et passent pour être typiques des groupes nord-coréens contrôlés par l'État (voir chap. 8). De telles attaques visent en particulier les collaborateurs d'entreprises actives dans le domaine des cryptomonnaies ou de la blockchain, y compris en Suisse.[31]

Parallèlement à ces attaques ciblées, de nombreux incidents observés s'inscrivent dans des campagnes internationales ne visant pas spécifiquement la Suisse. L'OFCS a de nouveau constaté la présence de publicités malveillantes parmi les résultats des moteurs de recherche (*malvertising*)[32]. Dans un cas concret, ce vecteur d'attaque aboutissait à une infection, suivie d'une attaque de rançongiciel.[33] D'autres campagnes proposaient des logiciels d'édition PDF gratuits afin de mieux diffuser leurs maliciels. Le code malveillant ne se téléchargeait que plusieurs mois après l'installation d'un produit au fonctionnement irréprochable jusque-là, avec pour effet que l'application paraissait légitime.[34]

En outre, plusieurs attaques ont pris pour cible la chaîne d'approvisionnement logicielle. Après avoir compromis les comptes de gestionnaires de paquets sur des plateformes de développement à code source ouvert (p. ex. GitHub et npm), les pirates ont pu injecter du code malveillant dans des composants très utilisés. Entre autres incidents, la compromission du compte

---

28 Semaine 33 : Les cybercriminels misent sur l'ingénierie sociale pour diffuser des logiciels malveillants (ncsc.admin.ch)

29 Semaine 40 : Hameçonnage par petites annonces – les pirates informatiques diffusent désormais des logiciels malveillants au lieu de simples liens d'hameçonnage (ncsc.admin.ch)

30 Semaine 49 : Arnaque à l'emploi – Comment les personnes en recherche d'emploi tombent dans le piège de logiciels malveillants (ncsc.admin.ch)

31 Analysis of Contagious Interview Campaigns by North Korean Threat Actors (sentinelone.com)

32 Voir rapport semestriel 2025/1, chap. 3.3.

33 From Bing Search to Ransomware: Bumblebee and AdaptixC2 Deliver Akira (thedfirreport.com)

34 TamperedChef: Malvertising to Credential Theft (labs.withsecure.com)

appartenant au développeur Qix a abouti à la publication de versions manipulées de dizaines de bibliothèques courantes.[35] Les agresseurs ont par ailleurs modifié, lors de la campagne *Shai-Hulud 2.0*, des centaines de composants de projets à code source ouvert afin qu'ils exécutent automatiquement du code malveillant lors de leur installation.[36] Cette campagne menée à grande échelle a permis aux escrocs de dérober des données sensibles et de se déplacer d'un compte de développeur à l'autre à l'aide d'identifiants compromis.

Recommandations

Ne cliquez pas sur des liens suspects, n'ouvrez aucun fichier joint et abstenez-vous de scanner les codes QR. En cas de doute, demandez à l'expéditeur supposé, par d'autres canaux, si le courriel en question émane bien de lui. Faites preuve de prudence dès qu'une fenêtre de téléchargement s'ouvre.

Lorsque vous recherchez un logiciel sur Internet, vérifiez avant de le télécharger que vous vous trouvez bien sur le site officiel du fabricant ou sur un autre site de confiance. Lorsque vous utilisez un moteur de recherche, vérifiez si le site Internet affiché apparaît avec la mention « annonce ». Dans ce cas, il s'agit de référencement payant, et la prudence est de mise, car les pirates optent souvent pour cette méthode de publicité en ligne afin de figurer en haut des résultats de recherche.

Installez régulièrement les mises à jour sur vos systèmes et limitez autant que possible les accès autorisés. Si vous pensez que votre ordinateur a été infecté, faites-le immédiatement analyser et, le cas échéant, nettoyer par un spécialiste. Le plus sûr reste de faire réinitialiser l'ordinateur. Dans ce cas, n'oubliez pas de sauvegarder préalablement toutes vos données personnelles.

3.2 Rançongiciels

Lors d'une attaque par rançongiciel, les pirates utilisent un logiciel malveillant pour verrouiller les données du système informatique de leur victime, qui deviennent ainsi inutilisables.[37] En règle générale, ils font d'abord une copie des données, puis les chiffrent et exigent une rançon. Ils promettent un outil de déchiffrement (clé de décryptage) à la victime si elle paie et la menacent de publier les données volées si elle s'y refuse. Dans ce cas, les groupes de rançongiciels accentuent souvent la pression pour la convaincre de payer, par exemple en prenant contact avec certains de ses clients ou fournisseurs pour les faire chanter eux aussi, en les menaçant de publier les données dérobées.

35 Dev snared in crypto phishing net, 18 npm packages compromised (theregister.com)
36 Shai-Hulud 2.0 Supply Chain Attack (wiz.io)
37 Rançongiciels (ncsc.admin.ch)

Au deuxième semestre 2025, l'OFCS a enregistré 79 incidents causés par des rançongiciels dans des organisations suisses (voir fig. 7). Cette forte hausse par rapport aux 57 annonces du premier semestre 2025 ou aux 47 cas du deuxième semestre 2024 tient à la méthode de recensement utilisée par l'OFCS. En effet, le présent rapport ne tient plus seulement compte des incidents signalés volontairement au guichet national pour les cyberrisques de l'OFCS (47 cas), mais aussi des cas signalés en vertu de l'obligation d'annoncer les cyberattaques contre des infrastructures critiques (10 cas), ou des incidents dont l'OFCS a eu vent par ses partenaires nationaux (22). Le nombre d'incidents signalés volontairement au guichet national pour les cyberrisques de l'OFCS est toutefois resté constant. Quant au nombre réel d'incidents liés à des rançongiciels en Suisse, il est sans doute supérieur aux 79 incidents observés au total par l'OFCS, toutes les organisations concernées ne signalant pas les incidents ni ne portant plainte, par crainte pour leur réputation.

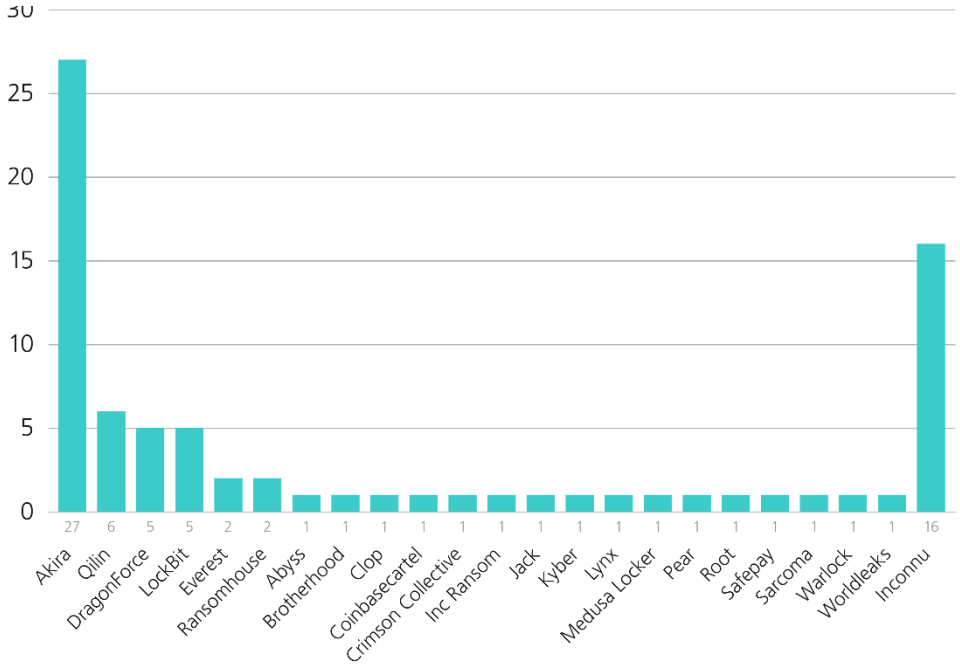

Fig. 7: nombre d'incidents signalés à l'OFCS et observés par ses soins, en rapport avec les groupes de rançongiciels en activité au deuxième semestre 2025

Akira a été en 2025 le groupe de rançongiciels le plus présent en Suisse. Déjà numéro un au premier semestre, il a intensifié ses activités, passant de 7 à 26 attaques connues de l'OFCS.[38] Akira fait partie des rançongiciels les plus actifs au niveau international, piratant des organisations de toutes tailles et dans tous les secteurs d'activité. Durant la période sous revue, les attaques de ce groupe ont surtout touché des organisations utilisant des appareils SonicWall, ce qui a d'abord fait croire à l'exploitation d'une faille du jour zéro (voir chap. 4). Or les agresseurs tiraient parti d'une vulnérabilité plus ancienne, découverte en août 2024 et pour laquelle une mise à jour de sécurité était disponible. De nombreuses organisations n'avaient toutefois pas suivi les instructions du fabricant, omettant de modifier les données de connexion de leur

38 Cybercriminalité : Le groupe AKIRA intensifie ses activités (admin.ch)

pare-feu. Akira a ainsi obtenu un accès avec des droits étendus aux systèmes de ses victimes, ce qui a grandement facilité la propagation de son rançongiciel.[39]
Qilin, *DragonForce* et *LockBit* se sont également distingués en Suisse, avec chacun cinq ou six attaques réussies à leur actif. En septembre 2025, *DragonForce* a annoncé que les trois groupes allaient s'allier. Or trois mois plus tard, cette alliance s'apparente davantage à une stratégie visant à recruter de nouveaux participants (affiliés) qu'à une véritable collaboration opérationnelle.[40] Avec plus de 700 victimes recensées dans le monde durant la période sous revue, Qilin s'avère être le groupe le plus redoutable à l'heure actuelle. Son niveau d'activité élevé est lié au modèle d'affaires RaaS (*Ransomware as a Service*). Les développeurs du rançongiciel proposent une plateforme prête à l'emploi. Les participants peuvent ainsi déployer des attaques par rançongiciel, récupérer et publier des données et mener des négociations, en échange d'une partie de la rançon versée. Le nombre particulièrement élevé de victimes du groupe Qilin suggère que son modèle RaaS compte une importante clientèle d'affiliés.[41] Ce groupe a par exemple créé un service juridique qui analyse les données volées dans le contexte du droit en vigueur. Les partenaires de Qilin peuvent ainsi faire pression lors des négociations, en soulignant les risques liés au non-respect des prescriptions légales et aux éventuelles poursuites pénales à craindre. L'activité du groupe LockBit a chuté en 2025, en raison tant de la répression internationale que de fuites de données internes.[42] Au mois de septembre, ce groupe annonçait toutefois le lancement d'une nouvelle version baptisée *LockBit 5.*0. Pour le seul mois de décembre 2025, cette version s'est vu attribuer plus de 100 victimes, dont une signalée en Suisse. Ce qui donne à penser que le groupe a su recruter de nouveaux membres et reprendre ses opérations.

Au cours de la période sous revue, plusieurs incidents majeurs à l'échelle internationale ont révélé l'ampleur potentielle des attaques par rançongiciel. Au Royaume-Uni, un incident survenu chez Jaguar Land Rover a entraîné un arrêt de la production pendant plusieurs semaines et affecté plus de 5000 entreprises de la chaîne d'approvisionnement de ce constructeur automobile. Le gouvernement britannique a même dû directement intervenir en lui accordant une garantie de crédit de 1,5 milliard de livres sterling, et le préjudice économique total a été estimé à 1,9 milliard de livres sterling.[43] D'autres organisations ont été victimes d'un rançongiciel, comme la société Collins Aerospace : l'incident a affecté plusieurs grands aéroports européens et perturbé le trafic aérien. Suite à cette cyberattaque, un système d'enregistrement utilisé par de nombreuses compagnies aériennes est resté indisponible pendant plusieurs jours.[44]

En Suisse, aucun incident de cette ampleur n'a été observé pendant le semestre écoulé. La menace que font peser les rançongiciels reste toutefois d'autant plus élevée que les groupes criminels sont en mesure d'exploiter très vite les vulnérabilités ou les accès compromis. Même

39 Akira Ransomware Group Utilizing SonicWall Devices for Initial Access (rapid7.com)
40 In depth analysis of the alleged Qilin, DragonForce and LockBit alliance (yarix.com)
41 The Evolution of Qilin RaaS (sans.org)
42 Voir rapport semestriel 2025/1, chap. 3.2.
43 Jaguar Land Rover cyberattack cost $2.5 billion, says monitoring group (therecord.media)
44 Ransomware behind global airport outage, says ENISA (theregister.com)

si à ce jour aucun des groupes connus ne s'en prend spécifiquement à la Suisse, les attaques opportunistes constituent la norme et touchent donc également les organisations suisses.

Recommandations

Le site de l'OFCS renferme une liste de mesures préventives pour faire face aux rançongiciels, et une marche à suivre en cas d'incident. Il est indispensable de former et d'entraîner le personnel à la gestion des pannes informatiques, pour garantir une réaction rapide et efficace de sa part en cas d'urgence. De façon générale, l'OFCS et ses partenaires internationaux[45] déconseillent aux victimes de payer une rançon. D'abord, il n'y a aucune garantie que les cybercriminels tiennent parole. Ensuite, l'argent des rançons apporte une aide financière aux cybercriminels pour continuer à développer leurs structures et mener d'autres attaques.

3.3 Réseaux ORB clandestins en Suisse

La menace croissante due aux réseaux proxy ORB (*operational relay boxes*)[46] agissant dans l'ombre n'épargne pas la Suisse. Le nombre d'appareils compromis faisant partie de ces réseaux ne cesse d'augmenter. Plusieurs activités malveillantes imputables à ces infrastructures avaient pour cibles des systèmes ou organisations suisses. En outre, les pirates parviennent à s'immiscer sans être repérés dans la vie privée des propriétaires d'appareils infectés.
Un réseau ORB se compose de routeurs et d'autres objets connectés préalablement compromis. Ce sont souvent, par exemple, des serveurs et des routeurs appartenant à des particuliers ou à de petites entreprises, ainsi que des appareils de l'Internet des objets (IoT). Les réseaux qui, dans le passé, se composaient essentiellement d'une infrastructure de serveurs loués se font rares. Entre-temps, les réseaux ORB reposant sur un vaste parc de terminaux compromis, accessibles et pilotables à partir d'un petit nombre de serveurs virtuels loués, se sont imposés un peu partout.
La plupart du temps, ces réseaux sont créés et exploités par des organisations spécialisées agissant sur mandat de tiers. Ces derniers disposent ainsi, moyennant rémunération, d'infrastructures prêtes à l'usage (*proxy-network-as-a-service*). Cette solution permet aux acteurs malveillants de dissimuler efficacement l'origine de leurs activités, de contourner les mécanismes de détection et de faire évoluer leurs opérations avec un risque opérationnel minime. Car à la différence des réseaux de zombies déployés par les groupes cybercriminels, les réseaux ORB misent sur le camouflage, sur la résilience et l'évolutivité, et par là satisfont aux exigences d'acteurs malveillants sophistiqués, parfois parrainés par des États.[47]

---

45 Guidance for organisations considering payment in ransomware incidents (ncsc.gov.uk)

46 Voir rapport semestriel 2025/1, chap. 8.1 et rapport semestriel 2024/2, chap. 8.1, ainsi que IOC Extinction? China-Nexus Cyber Espionage Actors Use ORB Networks to Raise Cost on Defenders (cloud.google.com).

47 Voir p. ex. rapport semestriel 2024/2, chap. 8.1.

Recommandations

Les réseaux ORB ont besoin d'un maximum d'appareils infectés. Il est donc essentiel de prendre toutes les mesures utiles pour réduire le risque de compromission et empêcher ainsi que vos systèmes ne soient involontairement intégrés à des infrastructures criminelles. Les mesures de sécurité suivantes vous sont fortement recommandées.

- Installez régulièrement les mises à jour de sécurité des appareils reliés à Internet ;
- Activez les mises à jour automatiques ;
- Utilisez des mots de passe forts et si possible un deuxième facteur d'authentification (authentification multifactorielle, MFA) ;
- Limitez au strict minimum l'accès depuis Internet à vos services et à vos ports ouverts ;
- Si vous n'en avez pas besoin, désactivez la fonction UPnP (*universal plug and play*).

La mise en œuvre systématique de ces mesures réduira considérablement votre surface d'attaque et contribuera ainsi à freiner l'essor et le pouvoir de nuisance des réseaux proxy ORB opérant dans le plus grand secret.

4 Vulnérabilités

Une vulnérabilité désigne une faille présentant un risque pour la sécurité d'un système informatique. Il peut s'agir d'une vulnérabilité logicielle, d'une erreur de conception ou de configuration, comme l'utilisation d'un identifiant par défaut.[48] Les failles du jour zéro (*zero-day vulnerability*) constituent un défi particulier, car bien que déjà connues et donc susceptibles d'être exploitées par des malfaiteurs, elles n'ont pas encore de correctif de sécurité. Avec l'essor de la numérisation et la mise en réseau des appareils, l'exploitation de vulnérabilités, isolées ou interdépendantes, peut causer de graves dommages aux données comme aux systèmes.

L'évolution dans le domaine des vulnérabilités s'est précipitée au deuxième semestre 2025. Cela s'est traduit par des incidents dus à des cyberattaques contre la chaîne d'approvisionnement logicielle (*supply chain*). Les produits logiciels modernes reposent en bonne partie sur des bibliothèques de programmes externes et incluent des composants prêts à l'emploi. Cette approche permet certes un développement efficace, chaque fonction n'ayant plus besoin d'être programmée à partir de zéro. Mais elle est à l'origine de dépendances techniques complexes. Car si l'une des bibliothèques intégrées au code présente une faille de sécurité, toutes les applications utilisant ce composant sont potentiellement vulnérables.
Les incidents survenus dans le contexte de la plateforme de développement npm (*node package manager*), lors desquels les agresseurs ont exploité cet effet de levier dans les deux campagnes *Shai-Hulud* de septembre et novembre 2025, en constituent un bon exemple (voir chap. 3.1). Durant la seconde attaque, plusieurs centaines de paquets npm téléchargés des centaines de millions de fois par mois ont été infectés. Le logiciel malveillant recherche notamment les données d'accès dans les référentiels pris en charge et les publie avec le compte

48 Faille de sécurité (ncsc.admin.ch)

de la victime.[49] Les responsables informatiques sont confrontés à un défi de taille : les systèmes d'inventaire ou les solutions de gestion des actifs n'enregistrent traditionnellement que les applications finales installées et ne répertorient pas individuellement les composants tiers qu'elles renferment. Autrement dit, le risque réel reste souvent invisible et l'utilisateur n'est pas en mesure de le gérer directement.

Une dépendance s'installe ainsi vis-à-vis de la diligence des éditeurs de logiciels. Ces derniers ont certes l'obligation de documenter de manière transparente les composants qu'ils utilisent et d'en traquer en permanence les vulnérabilités. Or la sécurité des clients finaux ne peut être garantie que si les développeurs connaissent bien leurs dépendances et fournissent des mises à jour corrigées dès qu'une faille est découverte. Sans gestion proactive de la chaîne d'approvisionnement, le risque pour les utilisateurs reste difficilement contrôlable. Même les vulnérabilités courantes peuvent s'avérer problématiques. L'OFCS a ainsi été prévenu, dans la deuxième quinzaine de juillet, de l'exploitation massive d'une vulnérabilité affectant la plateforme de gestion de données SharePoint, aux dépens notamment d'organisations suisses. Comme l'a montré une analyse ultérieure du fabricant[50], tant les acteurs étatiques que les milieux criminels tiraient parti de cette vulnérabilité pour s'introduire au sein d'organisations aux systèmes vulnérables (voir chap. 8.1).

Recommandations

Dans la mesure du possible, laissez 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.
Il est important d'établir une gestion efficace des correctifs pour remédier en temps utile aux vulnérabilités, surtout dans les entreprises. Pour ce faire, il faut tenir un inventaire à jour de l'infrastructure et des produits utilisés (SBOM[51]). Donnez particulièrement la priorité aux failles de sécurité des parties de votre infrastructure accessibles depuis Internet. Effectuez régulièrement des tests de pénétration et des analyses des vulnérabilités, afin d'identifier de manière proactive les failles de sécurité potentielle. Quant aux logiciels ou aux systèmes dont le fabricant n'assure plus le support (*end of life,* EOL), il convient de les désactiver, ou si possible de les reléguer dans une zone cloisonnée, séparée physiquement du réseau. Mettez en place un monitoring et tirez parti du renseignement sur les cybermenaces (*threat intelligence*) afin de pouvoir réagir rapidement aux développements qui l'exigent. La surveillance en temps réel de votre infrastructure, avec les avantages offerts par l'automatisation, vous aidera à identifier les tentatives d'attaques et les anomalies dans un délai très proche. En outre, diverses mesures comme les tests d'intrusion (*red teaming*[52]), les audits de sécurité réguliers ou le lancement

[49] Shai-Hulud 2.0 Aftermath: Trends, Victimology and Impact (wiz.io)

[50] Disrupting active exploitation of on-premises SharePoint vulnerabilities (microsoft.com)

[51] Nomenclature logicielle (wikipedia.org)

[52] Une *red team* ou équipe rouge est un groupe indépendant mandaté par une organisation afin d'analyser son infrastructure et ses processus dans des conditions réelles, comme le ferait un attaquant potentiel, le but étant d'identifier et de combler les lacunes de sécurité avant toute cyberattaque réelle (voir Équipe rouge (wikipedia.org)).

d'un programme de primes aux bogues (*bug bounty program*) sont utiles pour vérifier régulièrement et améliorer l'efficacité des processus de sécurité.

5 Escroquerie et ingénierie sociale

L'escroquerie consiste à tromper intentionnellement une personne afin de s'enrichir ou d'enrichir quelqu'un d'autre illégalement, en causant à la victime un dommage matériel.[53] Dans l'espace numérique, le principal défi réside dans le fait que les escrocs peuvent opérer à distance. Les cybercriminels sévissent souvent depuis des pays où les poursuites pénales sont plus compliquées. Ils ne recourent généralement pas à des techniques sophistiquées pour mener leurs cyberattaques, et préfèrent manipuler leurs victimes potentielles (par l'ingénierie sociale[54]) en leur faisant exécuter elles-mêmes certaines étapes nécessaires pour que la fraude aboutisse.

Au deuxième semestre 2025, l'escroquerie (ou fraude) est restée le phénomène le plus fréquemment signalé de manière volontaire à l'OFCS, malgré un recul à 15 090 annonces par rapport aux 18 269 du deuxième semestre 2024. Cette évolution tient surtout à la chute du nombre d'appels de menace émanant prétendument des autorités, qui constituent depuis la mi-2023 une part essentielle des fraudes notifiées. Les signalements ont reflué de 8 173 au premier semestre à 5 941 durant la période sous revue. Or bien qu'après deux semestres d'affilée on puisse parler ici de tendance baissière durable[55], les appels frauduleux demeurent la forme d'escroquerie la plus répandue, avec 39,4 % des cas annoncés.
Les jeux-concours frauduleux impliquant des entreprises réputées conservent la deuxième place du classement (1 698 annonces, 11 % du total). Il s'agit de messages contenant de fausses promesses de gain, par exemple d'appareils techniques, d'outils ou de bons d'achat. Les envois sont souvent effectués au nom d'enseignes du secteur alimentaire ou du commerce de détail. Les prétendus gagnants sont redirigés vers un site web, où il leur faut saisir les données de leur carte de crédit et souscrire à leur insu à un abonnement-piège. Le phénomène des faux courriels de menace envoyés au nom d'autorités (1 436 cas) arrive en troisième position, suivi de la fraude au paiement anticipé (1 243 cas). Les annonces de *fake-sextortion* sont en baisse, passant de 1 209 courriels signalés au deuxième semestre 2024 à 837 durant la période sous revue. Il ne faut pas pour autant s'attendre à une atténuation durable du phénomène, les courriels de *fake-sextortion* étant envoyés par vagues. Le nombre de boutiques en ligne frauduleuses est par ailleurs en hausse : 824 signalements ont été enregistrés au deuxième semestre, soit 266 de plus qu'au premier. Ce phénomène est lié à une concentration des annonces entre novembre et janvier, les fraudeurs cherchant à profiter des ventes de Noël. Le nombre de signalements de fraudes aux petites annonces a quant à lui diminué, passant de 553 au deuxième semestre 2024 à 462 durant la période considérée, tout en restant assez stable d'une année à l'autre.

---

53 Voir l'art. 146 du code pénal suisse pour une définition juridique.

54 Ingénierie sociale (*Social Engineering*) (ncsc.admin.ch)

55 Voir rapport semestriel 2025/1 ; chap. 5.

En termes de préjudice financier, le phénomène de la fraude à l'investissement en ligne reste le plus dommageable. Le nombre d'annonces a progressé d'une centaine de cas par rapport au deuxième semestre 2024. Les cas signalés restent toutefois stables sur l'ensemble de l'année 2025, avec 418 annonces au premier semestre et 430 au deuxième. En revanche, la tendance est à la hausse en ce qui concerne les arnaques à la récupération, où les malfaiteurs cherchent à faire croire aux victimes de fraudes à l'investissement en ligne qu'elles pourront récupérer l'argent volé. Tandis qu'au premier semestre 2025, 145 cas de « fraude au remboursement » avaient été signalés[56], leur nombre a largement doublé durant la période sous revue, avec 325 cas signalés.

Fraudes aux dépens des entreprises

Au deuxième semestre, les entreprises suisses ont signalé nettement moins de cas d'arnaque au président que six mois plus tôt. Après un nombre record de 605 annonces au cours des six premiers mois de 2025, seuls 366 cas ont été enregistrés. La baisse par rapport au deuxième semestre 2024 atteint 68 cas. Ce recul significatif s'explique par l'absence de vagues de fraudes visant les écoles, les communes et les églises, pratique encore courante au premier semestre. En revanche, les signalements de manipulation de factures à la suite du piratage d'une messagerie professionnelle (*business email compromise*, BEC)[57] ont continué d'augmenter, passant de 49 cas au deuxième semestre 2024 à 73 au deuxième semestre 2025. À la différence des cas d'arnaque au président, les données utilisées pour ce type de fraude ne proviennent pas de sources publiques, mais de comptes de messagerie piratés (BEC). De tels incidents sont généralement liés à des activités d'hameçonnage antérieures contre des employés de l'entreprise, comme l'hameçonnage en chaîne[58] (voir chap. 2). Lorsqu'un nouveau compte de messagerie électronique a été piraté, les agresseurs l'analysent à la recherche de contenus exploitables. S'ils y découvrent par exemple des commandes ou des factures, ils manipuleront la communication avec ce client professionnel afin de l'amener à virer le montant dû sur un numéro de compte IBAN leur appartenant.

Vols d'identité au sein d'entreprises

Les particuliers ne sont pas les seuls concernés par l'usurpation d'identité, qui touche un nombre croissant d'entreprises. En pareil cas, les fraudeurs cherchent à tirer parti de la confiance qu'inspire un nom établi. Les entreprises qui ne disposent pas de leur propre site web sont particulièrement menacées. Les cybercriminels procèdent de manière systématique : ils recherchent des entreprises appropriées dans le registre du commerce, enregistrent des noms de domaines et créent un site web en leur nom. Pour paraître sérieux, ils reprennent les informations officielles, comme l'adresse et le numéro d'enregistrement au registre du commerce de la véritable entreprise. Sur cette base, ils mettent en place diverses escroqueries, allant des fausses boutiques en ligne aux plateformes de fraude à l'investissement en ligne. Un exemple récent concerne une société fiduciaire établie depuis plus de dix ans sur le marché.

---

56 Voir rapport semestriel 2025/1 ; chap. 5, alinéa sur la fraude au remboursement.

57 Au niveau international, la définition du *Business Email Compromise* (BEC) n'est pas utilisé de manière uniforme, d'autres définitions considérant par exemple la fraude au président comme une sous-variante du BEC (voir Business Email Compromise (fbi.gov)). L'OFCS distingue toutefois explicitement ces phénomènes et suit la définition de l'Office fédéral de la police (fedpol).

58 L'hameçonnage en chaîne s'apparente à un système boule de neige : dès qu'un compte est compromis, des courriels d'hameçonnage sont expédiés à tous les contacts de son carnet d'adresses.

Les malfaiteurs ont utilisé les données du registre du commerce afin de créer un site web et de s'y présenter à la clientèle comme la véritable entreprise. Ils ont notamment exigé des paiements anticipés pour de prétendus services fiduciaires, sans jamais fournir la moindre prestation. Alors que les victimes perdaient leur l'argent, la véritable société a vu sa réputation ternie, dans la mesure où des tiers lésés l'ont associée à tort à ces pratiques frauduleuses.

Offres d'emploi frauduleuses

Les escrocs créent aussi parfois des sites web au nom d'entreprises existantes, dans le but de diffuser de fausses offres d'emploi. Depuis sa création, l'OFCS reçoit régulièrement des signalements concernant de telles offres accrocheuses, diffusées sur divers portails. Les personnes en quête d'un travail dans le secteur de la restauration, souvent originaires de l'étranger, risquent tout particulièrement de se faire piéger. En cas d'envoi d'une pièce d'identité ou d'un CV, la réponse positive ne se fait pas attendre. Or peu après, les escrocs demandent de l'argent, par exemple pour les frais d'assurance-maladie ou d'enregistrement, souvent en se servant de fausses adresses électroniques du Secrétariat d'État aux migrations. Faute d'être au courant des formalités administratives de la Suisse, bien des demandeurs d'emploi s'empressent de payer les frais frauduleux.

L'arnaque ne touche d'ailleurs pas que les demandeurs d'emploi étrangers et fait également des victimes en Suisse. L'OFCS reçoit ainsi souvent des annonces concernant des pages web qui imitent des sites d'entreprises connues et usurpent des noms aussi établis que Manor ou Zalando. Les personnes ayant manifesté leur intérêt reçoivent les données d'accès aux plateformes de ces entreprises fictives, sur lesquelles il leur est demandé d'accomplir des tâches simples contre rémunération. De telles missions consistent par exemple à évaluer des produits ou à tester des applications et des jeux. Les rétributions obtenues apparaissent en continu sur la plateforme fictive. Les demandeurs d'emploi reçoivent souvent au début un petit montant destiné à les mettre en confiance. Les victimes sont par la suite poussées à payer des frais pour libérer des gains d'un montant plus élevé, qui ne se concrétisent jamais. Il leur faut également utiliser leur compte bancaire personnel ou leur portefeuille de cryptomonnaies pour des transactions servant par exemple à blanchir de l'argent. Dans un cas signalé à l'OFCS, une victime a perdu près de 80 000 francs.

Recommandations

L'OFCS s'efforce de faire immédiatement retirer du réseau les sites frauduleux. Mais comme ces sites sont généralement hébergés sur des serveurs étrangers, l'OFCS est tributaire ici de la bonne volonté des opérateurs des pays concernés. Il est donc recommandé aux entreprises de signaler en toute transparence sur leurs sites web les tentatives de fraude survenues. D'habitude, les demandeurs d'emploi consultent au préalable le site web légitime des entreprises. S'ils y trouvent un avertissement, ils reconnaîtront d'emblée la fraude.

Nouvelle augmentation des cas d'arnaque à la récupération

Les cas de fraude à l'investissement en ligne signalés en Suisse sont aujourd'hui les incidents les plus coûteux. Or bien souvent, les escrocs ne s'arrêtent pas une fois la supercherie découverte, et enfoncent le clou avec une arnaque à la récupération (*recovery scam*). Ils contactent à diverses reprises leurs victimes, en prétendant que le butin de la fraude initiale a été retrouvé et qu'elles pourront ainsi récupérer leur argent. Les annonces reçues à ce sujet ont largement

doublé pendant la période sous revue, passant de 145 au premier semestre 2025 à 325 au second.
Comme au premier semestre 2025[59], les escrocs se font généralement passer pour un cabinet d'avocats ou une autorité telle qu'Europol, Interpol ou l'agence de régulation financière de Chypre. Un collaborateur fictif de l'OFCS a même sévi.[60] Les malfaiteurs enregistrent des adresses électroniques à l'apparence authentique, qui imitent celles de personnes réelles appartenant aux organisations précitées. Ils se présentent en outre avec des documents officiels falsifiés, afin d'accroître leur crédibilité aux yeux des victimes ou parfois de faire valoir des créances fictives. En plus d'envoyer des courriels, les escrocs contactent leurs victimes par téléphone, afin de savoir plus précisément à qui ils ont affaire. La plupart de ces appels sont passés en anglais.
L'effet insidieux de l'arnaque à la récupération tient à ce que la perte ainsi occasionnée dépasse parfois celle subie lors de la fraude initiale. Par exemple, une victime avait perdu 10 000 francs en 2023 lors d'une fraude à l'investissement en ligne. Deux ans plus tard, les escrocs se sont à nouveau manifestés et lui ont proposé leur aide pour récupérer la somme perdue, moyennant des frais de 22 000 francs. Les victimes consentent parfois à payer des frais aussi exorbitants, car les escrocs leur font miroiter un gain d'investissement. En l'occurrence, le gain était censé atteindre 600 000 francs.

Recommandations

Soyez sceptique si vous recevez des courriels, des messages ou des appels vous menaçant de graves conséquences (perte d'argent, plainte pénale, blocage du compte ou de la carte) en cas d'inaction, pour vous mettre sous pression. N'oubliez pas que les escrocs peuvent aisément falsifier leur adresse électronique[61]. Ne donnez jamais suite à une demande de paiement inhabituelle et méfiez-vous des promesses de gains. Dans les entreprises, tous les processus liés au trafic des paiements devraient faire l'objet de règles internes précises. Gardez bien à l'esprit qu'aucune banque ou société de cartes de crédit ne vous priera par courrier électronique de changer de mot de passe ou de vérifier les données de votre carte de crédit. De même, des employés de banque ne vous demanderont jamais lors d'un appel téléphonique vos jetons de sécurité ou d'autres données personnelles d'accès à vos comptes d'e-banking ou Twint afin de vérifier votre identité.

59 Voir rapport semestriel 2025/1 ; chap. 5, alinéa concernant la fraude au remboursement.
60 Semaine 38 : Attention à Daniel Bruno, prétendu collaborateur du NCSC
61 Usurpation d'identité (spoofing) (ncsc.admin.ch)

6 Attaques affectant la disponibilité de sites et de services Internet

Lors d'attaques affectant la disponibilité de sites et de services Internet (*Distributed Denial of Service*, attaque par déni de service distribué, *DDoS*), les escrocs cherchent à rendre temporairement inaccessible un service en ligne, en le saturant de requêtes. De fait, les attaques DDoS ne sont pas directement à l'origine d'accès non autorisés ou de fuites de données, ni ne causent de dommage permanent aux systèmes. Très prisées pour attirer l'attention des médias et du grand public (hacktivisme), elles permettent aussi souvent aux criminels de dissimuler une autre activité ou de faire chanter leurs victimes.

Au cours de la période sous revue, aucune attaque DDoS liée au hacktivisme n'a fait les gros titres en Suisse. L'OFCS n'a pas non plus été prévenu d'activités d'extorsion s'appuyant sur des attaques DDoS dues aux milieux criminels. Ce calme contraste avec les turbulences du semestre précédent[62], où plusieurs organisations basées en Suisse avaient subi de telles attaques, dans le cadre de grandes manifestations comme le World Economic Forum (WEF) ou le Concours Eurovision de la chanson. Au deuxième semestre 2025, l'OFCS a bien reçu quelques annonces à propos de tentatives d'attaques d'origine inconnue, principalement dans les secteurs de la finance, de l'informatique et de l'administration publique. Elles n'ont toutefois entraîné que des pannes de courte durée, qu'il a été possible de résoudre grâce aux mesures déjà en place.

L'opération *Eastwood*[63] déployée à la mi-juillet 2025 par les autorités de poursuite pénale a temporairement freiné le zèle des hacktivistes prorusses. Des enquêteurs suisses ont également pris part aux arrestations, aux saisies et à la neutralisation de l'infrastructure malveillante. Le collectif *NoName057(16)* a toutefois renouvelé ses outils et repris ses actions de perturbation après quelques semaines. Il a ainsi revendiqué des attaques contre la Poste française, qui ont retardé la distribution des colis peu avant Noël. La victime n'a toutefois confirmé aucune revendication ni attribution de cette cyberattaque.[64] Début décembre 2025, la justice américaine avait déjà engagé des poursuites contre ce groupe, en soulignant ses liens avec des institutions publiques russes.[65] D'où la nécessité d'un dispositif de défense approprié pour les grands événements[66] à venir en Suisse et dans ses environs, afin de maintenir la disponibilité des services en ligne même durant les périodes de forte attention internationale.

Quant à l'infrastructure d'attaque utilisée, il convient de mentionner le réseau de zombies *Aisuru*, qui s'est signalé à l'échelle mondiale par des attaques DDoS générant un trafic réseau

---

62 Rapport semestriel 2025/1 (ncsc.admin.ch)

63 Global operation targets NoName057(16) pro-Russian cybercrime network – The offenders targeted Ukraine and supporting countries, including many EU Member States (europol.europa.eu)

64 Pro-Russian hacking group claims cyberattack on France's postal service (apnews.com)

65 Office of Public Affairs | Justice Department Announces Actions to Combat Two Russian State-Sponsored Cyber Criminal Hacking Groups (justice.gov)

66 Voir Cyberrésilience : un enjeu clé pour les grands événements et conférences internationales (ncsc.admin.ch)

pouvant atteindre 30 Tb/s. Avec de telles bandes passantes, les attaques ne font pas que pousser à leurs limites techniques les organisations prises pour cibles, mais risquent de causer de nombreuses victimes collatérales sur Internet.[67]

Recommandations

Le site Internet de l'OFCS propose dans sa rubrique Attaque affectant la disponibilité (attaque DDoS) diverses mesures de prévention et de défense contre ce type d'attaque. 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 doublée de chantage, l'OFCS recommande de ne pas entrer en matière. Après un premier versement, les escrocs pourraient augmenter la mise et poursuivre leurs attaques. Il est donc préférable de signaler le cas à l'OFCS et de s'adresser à la police pour déposer une plainte pénale. Les recommandations d'usage figurent sous : Attaque DDoS – que faire ?

7 Gestion des données, fuites de données et chantage

Les fuites de données ou l'exposition des données par mégarde font régulièrement parler d'elles, en Suisse comme à l'étranger. En plus de constituer une violation de la sécurité des données, ces incidents peuvent causer des dommages supplémentaires, notamment en faisant courir un risque en aval à d'autres organisations ou particuliers. Car en cas de fuite de données chez un fournisseur, il ne suffit pas aux entreprises de surveiller tous les accès à leur propre infrastructure, des tentatives de fraude sont également à craindre (voir chap. 5). Quant aux particuliers, ils risquent de voir leurs informations sensibles être exploitées à des fins d'usurpation de compte, d'hameçonnage (voir chap. 2), de vol d'identité ou de fraude financière. Les fuites de données jouent ainsi un rôle de premier plan dans les attaques au chantage menées à l'aide de rançongiciels. Faute de paiement de la rançon demandée, elles sont généralement publiées ou mises en vente (voir chap. 3.2). D'autres causes peuvent aussi conduire à exposer des données par inadvertance, comme une gestion inadéquate des données d'une infrastructure ou des vulnérabilités existantes (voir chap. 4), de même que des erreurs de configuration technique.

La liste des fuites de données subies par la population et les organisations suisses s'est encore allongée au deuxième semestre 2025. Il s'agit d'une véritable bombe à retardement. Même des années plus tard, les données publiées peuvent aider les pirates à lancer de nouvelles attaques. On a ainsi observé que les cybercriminels réutilisaient systématiquement les données fuitées, y compris en Suisse. Car en mentionnant dans leurs courriels des informations

67 Cloudflare's 2025 Q3 DDoS threat report -- including Aisuru, the apex of botnets (cloudflare.com)

telles que le nom, la date de naissance ou le numéro de téléphone, ils rendent leurs campagnes d'hameçonnage ou de *fake sextortion* d'autant plus crédibles auprès des victimes potentielles.

Des organisations suisses ont également fait les frais de vastes campagnes internationales d'exfiltration de données et de chantage menées par des acteurs criminels. L'incident survenu chez Logitech en est un bon exemple.[68] À l'instar de beaucoup d'autres multinationales, Logitech a été victime d'une campagne de chantage due au groupe Clop, qui lui a dérobé des données en tirant parti d'une vulnérabilité du jour zéro du logiciel Oracle E-Business Suite (EBS).[69] L'intrusion n'a certes mis en péril ni les produits, ni l'activité commerciale de Logitech, mais a néanmoins provoqué une fuite de données non sensibles de clients et de collaborateurs. Après avoir suivi à ses débuts en 2019 l'approche classique des rançongiciels basée sur le chiffrement (voir chap. 3.2), le groupe de hackers Clop a peu à peu changé de mode opératoire : il commence par compromettre systématiquement, à grande échelle, des produits servant au transfert des données, avant d'en venir au chantage à la publication des données auprès de ses différentes victimes.[70] C'est ce qui s'est passé dans l'incident actuel basé sur Oracle EBS : alors que leurs agissements ont pu être retracés à partir du 10 juillet 2025, les agresseurs ont attendu le 29 septembre pour signaler à la direction des organisations piratées les fuites survenues et la rançon à verser afin d'empêcher la publication de données compromises. À la différence des opérations de chantage classiques basées sur le chiffrement, les agresseurs peuvent ainsi opérer plus longtemps dans l'ombre, puisqu'ils ne rendent publiques les diverses attaques menées qu'à la date prévue à cet effet dans leur campagne. Dès le moment où quelques victimes ont payé la somme demandée, l'opération devient rentable et les pirates bénéficient d'économies d'échelle. Car en exploitant à plusieurs reprises la même faille (encore inconnue) sans se faire remarquer, ils peuvent maximiser le nombre de victimes au prix d'un minimum d'efforts.

Recommandations

Il est bien connu que les informations publiées sur Internet laissent des traces indélébiles. Quelques règles générales s'appliquent dans ce contexte. Déterminez conformément au principe fondamental de la conservation des données qui enregistre et traite quelles données, sous quelle forme, dans quel lieu du stockage, et les partage avec qui. Il est judicieux d'enregistrer les données avec précaution, de contrôler à intervalles réguliers son stock de données et d'effacer les données superflues. Chiffrez autant que possible vos données sensibles. Archivez hors ligne celles qui sont dignes d'être conservées, mais que vous n'utilisez plus activement. Établissez des processus structurés et efficaces pour le traitement et la protection des données, et contrôlez-en la bonne mise en œuvre.

---

68 Logitech Cybersecurity Disclosure (ir.logitech.com)

69 Oracle E-Business Suite Zero-Day Exploited in Widespread Extortion Campaign (cloud.google.com)

70 Le rapport semestriel 2023/1 décrit à son chap. 4.4.1 une telle campagne (*MOVEit*) et donne au chap. 4.5.1 des informations détaillées sur son auteur. D'autres campagnes du même genre ont été identifiées. Voir Accellion FTA, GoAnywhere MFT et Cleo.

Les données issues d'anciennes fuites peuvent servir 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[71] ou sur Identity Leak Checker de l'Institut Hasso Plattner[72].

8 Cyberespionnage et cybersabotage

Les acteurs étatiques ou dirigés par l'État représentent un type particulier de menace dans le cyberespace. Des groupes souvent désignés comme menaces persistantes avancées (*advanced persistent threat*, APT)[73] se livrent à des activités d'espionnage et plus rarement de sabotage, quand c'est dans leur intérêt. Alors que le cyberespionnage représente un défi permanent pour les services suisses de contre-espionnage, les attaques de cybersabotage ciblées ne s'observent généralement que dans le contexte de conflits et autres situations géopolitiques tendues.[74] À la différence des cybercriminels mus par l'appât du gain, les APT choisissent leurs cibles selon des critères précis, puis déploient des efforts considérables pour accéder aux informations souhaitées ou pour obtenir l'effet escompté. Les organisations potentiellement concernées doivent par conséquent se doter d'un dispositif de défense robuste contre ce type de menace. Sans perdre de vue que les APT peuvent se permettre de peaufiner leurs attaques pendant des années, tant elles disposent d'importantes ressources humaines, techniques et financières.

8.1 Cyberespionnage

Comme dans le passé, il est apparu au deuxième semestre 2025 que les APT (*advanced persistent threat*) tirent activement parti des vulnérabilités des produits couramment utilisés dans les entreprises, qu'il s'agisse de failles du jour zéro ou d'autres erreurs pour lesquelles les mises à jour de sécurité n'ont pas été installées à temps. En juillet 2025, Microsoft a publié coup sur coup les correctifs de quatre vulnérabilités affectant différentes versions de son logiciel SharePoint destiné aux serveurs locaux. Le géant de la tech a également signalé que divers acteurs basés selon lui en Chine avaient exploité ces vulnérabilités à des fins d'espionnage, mais aussi pour diffuser des rançongiciels.[75] Microsoft a par ailleurs détecté diverses activités qui, moyennant l'installation d'un code malveillant supplémentaire, garantissaient un accès permanent et vraisemblablement exclusif au serveur piraté. L'affaire a connu un retentissement planétaire, car des infrastructures critiques figuraient parmi les victimes.[76] Dans ce cas comme dans beaucoup d'autres, les APT ont perdu leur privilège d'exclusivité, une fois la

[71] Voir Have I Been Pwned (haveibeenpwned.com)
[72] Voir Identity Leak Checker (sec.hpi.de)
[73] APT – Glossary (csrc.nist.gov)
[74] Voir aussi le communiqué de presse consacré au rapport sur la situation « La sécurité de la Suisse 2025 » : la confrontation mondiale a des répercussions directes sur la Suisse (vbs.admin.ch)
[75] Disrupting active exploitation of on-premises SharePoint vulnerabilities (microsoft.com)
[76] ToolShell Attacks Hit 400+ SharePoint Servers, US Government Victims Named (securityweek.com)

vulnérabilité rendue publique. Les criminels en particulier sont à l'affût des vulnérabilités récentes, comme on a pu le constater à propos d'une faille de sécurité de la bibliothèque JavaScript React.[77]

Les appareils périphériques (*edge device*) continuent de représenter pour les pirates informatiques un moyen efficace de pénétrer dans un système, en tirant parti d'une faille existante ou d'un contrôle d'accès mal protégé. Par conséquent, les appareils en fin de vie et ne recevant plus de mises à jour encourent un risque accru d'attaques malveillantes. L'APT *Static Tundra*, suspecté d'agir pour le compte des services secrets militaires russes, s'est en particulier servie d'appareils Cisco obsolètes et n'étant plus pris en charge pour compromettre des organisations actives dans les télécommunications, dans le secteur de l'enseignement supérieur ou dans l'industrie manufacturière.[78]
La division du travail et la spécialisation, pratiquées de longue date dans le secteur de la cybercriminalité, ont fait tache d'huile dans le cyberespionnage. Il est notamment facile pour les acteurs étatiques de sous-traiter les activités décrites ci-dessus, nécessaires à l'obtention d'un accès initial. C'est en particulier l'hypothèse avancée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI) lors de son enquête sur les attaques menées via des appareils réseau de la société Ivanti, qui avaient touché des organisations des secteurs de l'administration, des télécommunications, des médias, de la finance et des transports. L'agence française établit des liens entre l'activité de l'acteur malveillant *Houken* et la Chine et soupçonne ce dernier d'avoir vendu des accès initiaux à des acteurs étatiques.[79].
Alors que l'exploitation des failles de sécurité ou celle de configurations non sécurisées d'appareils réseau est une méthode privilégiée, les attaquants envoient également des courriels d'hameçonnage ciblé (voir chap. 2) ou mènent des attaques dites du point d'eau (*watering hole attack*). Ce dernier type d'attaque a probablement été utilisé par le groupe de hackers APT29, soupçonné d'opérer pour le compte des services de renseignement russes, dans le but de rediriger 10 % des visiteurs de sites web légitimes mais infectés vers un site web qu'il contrôlait.[80]

Afin d'accéder durablement aux systèmes compromis, après l'obtention d'un accès initial, et pour mieux atteindre l'objectif principal d'exfiltration des données à l'insu de leurs propriétaires, les pirates exploitent la technique de la porte dérobée (*backdoor*). Dans ce contexte, l'affaire *Brickstorm* a fait grand bruit dans la période sous revue. Selon les autorités américaines et canadiennes, des acteurs étatiques chinois utilisent cette porte dérobée, afin notamment d'attaquer des environnements réseau virtuels. Leurs cibles comprendraient les infrastructures gouvernementales et les services administratifs, ainsi que des organisations du secteur informatique.[81] Dans un premier rapport paru en septembre, Google a également cité les secteurs

---

77 Multiple Threat Actors Exploit React2Shell (CVE-2025-55182) (cloud.google.com)

78 Russian state-sponsored espionage group Static Tundra compromises unpatched end-of-life network devices (blog.talosintelligence.com)

79 Voir Rapport menaces et incidents du CERT-FR (cert.ssi.gouv.fr)

80 Amazon disrupts watering hole campaign by Russia's APT29 (aws.amazon.com)

81 BRICKSTORM Backdoor (cisa.gov)

juridiques parmi les cibles potentielles d'attaques, en soulignant qu'une fois compromis ils peuvent servir de point de départ en vue de l'infiltration d'autres organisations.[82]

Recommandations

Pour se prémunir contre ce type de menace, il faut agir à plusieurs niveaux, selon une stratégie de défense en profondeur[83]. Comme les malfaiteurs sont prêts à investir beaucoup de temps et de ressources dans leurs outils d'attaque, ils parviennent à identifier et à exploiter de nouvelles vulnérabilités dans la plupart des cas. Par conséquent, une stratégie de défense fructueuse se doit de prendre en compte tous les éléments fondamentaux de l'infrastructure informatique : par exemple le périmètre, le réseau, les terminaux, mais aussi le facteur humain et l'organisation proprement dite. Il est également important de savoir qu'une intrusion par une APT ne peut jamais être entièrement exclue, tant les ressources et le savoir-faire des cybercriminels sont étendus, et ce même dans les organisations s'étant dotées d'un concept de sécurité structuré par couches et appliqué scrupuleusement. Une segmentation du réseau, conçue pour isoler par exemple les systèmes critiques ou les données sensibles, peut toutefois plus facilement empêcher que l'infection ne compromette l'ensemble. D'autres recommandations figurent dans la norme minimale pour les TIC.

8.2 Menaces contre les systèmes de contrôle industriels et la technologie opérationnelle

La digitalisation n'entraîne pas seulement une utilisation croissante des technologies de l'information dans le cyberespace et dans l'espace de l'information, mais comprend aussi, voire pilote, un nombre croissant de processus physiques. Ainsi, la technologie opérationnelle, longtemps isolée, court les mêmes risques que l'environnement système auquel elle est de plus en plus connectée, à commencer par les systèmes de contrôle industriels. Les personnes ne travaillant pas dans le secteur industriel sont susceptibles de prendre conscience de cette évolution au travers des progrès de la domotique et des projets de maisons intelligentes.

À la connaissance de l'OFCS, aucune attaque de cybersabotage n'a été commise au deuxième semestre 2025 contre des systèmes industriels suisses. Le contexte international reste cependant marqué par des activités destructrices[84], dans le contexte de la guerre en Ukraine et du conflit au Proche-Orient. En dehors de ces zones de conflit, les hacktivistes tentent de faire parler d'eux en manipulant des systèmes OT exposés et insuffisamment protégés sur

82 Another BRICKSTORM : Stealthy Backdoor Enabling Espionage into Tech and Legal Sectors (cloud.google.com)

83 Voir Normes minimales pour les TIC (ncsc.admin.ch), al. 1.6 Éléments d'une stratégie de défense en profondeur.

84 Sandworm hackers use data wipers to disrupt Ukraine's grain sector (bleepingcomputer.com), Iran-linked cyberattack reportedly disrupts public services in Albania's capital (therecord.media)

Internet. Les autorités américaines[85], norvégiennes[86], danoises[87] et canadiennes[88] prêtent à ces hacktivistes des liens avec l'État russe. Mais à l'heure actuelle, ces agresseurs n'ont pas su dépasser le stade des tentatives de manipulation, et les mesures de sécurité conventionnelles ont suffi pour en venir à bout.[89]

Les tentatives de sabotage observées ne visaient d'ailleurs pas seulement les systèmes industriels, mais également les systèmes d'information et de communication. Le gouvernement luxembourgeois a dénoncé comme acte de sabotage délibéré le *black-out* survenu le 23 juillet 2025, où le réseau mobile national 4G et 5G a été paralysé trois heures entières, impactant toute la société luxembourgeoise. Les services des urgences, le réseau Internet et les opérations bancaires en ligne sont restés presque partout inaccessibles.[90] Il s'agirait d'une perturbation intentionnelle, et donc d'une tentative couronnée de succès d'infiltrer par exemple de manière ciblée un réseau mobile. Les agresseurs auraient exploité des vulnérabilités des routeurs du fabricant Huawei, provoquant une panne à grande échelle du réseau.[91]

La menace qui pèse sur les systèmes OT tient en partie aux vulnérabilités d'appareils industriels qui, dans le cas des systèmes intégrés, ne peuvent souvent être corrigées qu'au prix d'efforts considérables. Des chercheurs en sécurité ont ainsi constaté, à l'aide de la technique du pot de miel (*honeypot*) que les agresseurs ne se limitaient pas à des opérations destructrices, mais tiraient aussi parti d'anciennes failles de sécurité.[92] L'Agence américaine pour la cybersécurité et la sécurité des infrastructures (CISA) a confirmé que plusieurs vulnérabilités avaient également été exploitées dans des systèmes de contrôle des processus de fabrication.[93] Et ce n'est pas tout : outre la mise en réseau croissante de ces systèmes, l'intégration de l'IA dans les processus industriels représente un défi supplémentaire pour la cybersécurité. Car si cette nouvelle technologie offre de nombreux avantages et permet des gains d'efficacité, elle augmente au passage la surface d'attaque. Aussi l'intégration de l'IA doit être accompagnée de mesures de sécurité appropriées.[94]

---

85 Actions to Combat Two Russian State-Sponsored Cyber Criminal Hacking Groups (justice.gov)

86 Norwegian Police Say Pro-Russian Hackers Were Likely Behind Suspected Sabotage at a Dam (securityweek.com)

87 Denmark summons Russian ambassador over alleged cyberattacks on water utility (therecord.media)

88 AL25-016 Abus de systèmes de contrôle industriels (SCI) accessibles depuis Internet par des hacktivistes (cyber.gc.ca)

89 Pro-Russia Hacktivists Conduct Opportunistic Attacks Against US and Global Critical Infrastructure (cisa.gov)

90 Luxembourg probes reported attack on Huawei tech that caused telecoms outage (therecord.media)

91 Huawei, at the heart of the Post outage (paperjam.lu)

92 Anatomy of a Hacktivist Attack: Russia-Aligned Group Targets OT/ICS (forescout.com)

93 CISA CVE-2025-5086 to Catalog (cisa.gov), CISA Adds two Vulnerabilities to Catalog (cisa.gov)

94 Principles for the secure integration of Artificial Intelligence in Operational Technology (cyber.gov.au)

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 pour les TIC élaborées par l'Office fédéral pour l'approvisionnement économique du pays (OFAE), en collaboration avec les organisations sectorielles concernées, sont un peu plus complètes. Les recommandations relatives à l'OT[95] de l'Information Security Society Switzerland (ISSS) fournissent une aide supplémentaire à cet égard. La CISA a fourni une base[96] pour une utilisation sécurisée de l'intelligence artificielle dans l'environnement OT.

95 ISSS Operational Technology (OT) Empfehlungen (cybernavi.ch)

96 Joint Guidance on Deploying AI Systems Securely (cisa.gov)