18 novembre 2025 | Office fédéral de la cybersécurité OFCS

Rapport semestriel 2025/I (janvier – juin)

Cybersécurité

La situation en Suisse et sur le plan international

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de la défense,
de la protection de la population et 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 et l'évolution des cybermenaces tant en Suisse que sur la scène internationale. Au premier semestre 2025, l'OFCS a reçu 35 727 annonces de cyberincidents, nombre qui s'est stabilisé à un niveau élevé. 58 % de ces annonces concernent le phénomène de la fraude. Les principales menaces n'ont pas changé en Suisse, mais les malfaiteurs ont fait preuve d'innovation et développé des approches intéressantes.

Défi des rançongiciels et du chantage au vol de données
Les rançongiciels[1] et le chantage à la divulgation de données qui s'ensuit restent une menace bien réelle pour toute organisation active en Suisse. 57 incidents impliquant des rançongiciels ont été signalés à l'OFCS, la plupart par des entreprises ou des organisations, ce qui représente une légère augmentation par rapport aux 44 incidents notifiés à la même période de l'année précédente. La majorité des annonces indiquant la variante du rançongiciel concernaient le logiciel rançonneur *Akira*, talonné par *LockBit*. Les cyberattaques menées contre la chaîne d'approvisionnement sont un casse-tête pour les organisations touchées. En effet, en cas d'attaque contre leur prestataire informatique, la clientèle commerciale risque également d'en pâtir.

Publicités frauduleuses comme vecteur d'attaque
Les escrocs exploitent de plus en plus la publicité payante, dans les moteurs de recherche et les médias sociaux, pour propager leur hameçonnage en temps réel[2], leurs logiciels malveillants[3] et leurs investissements prétendument lucratifs. Dans le cas de la fraude à l'investissement en ligne[4] notamment, les victimes sont incitées par des annonces publicitaires à effectuer des investissements irréfléchis. Une variante faisant miroiter un remboursement des pertes subies après une fraude à l'investissement s'est entre-temps répandue en Suisse.

Phishing : clientèle bancaire visée
Au premier semestre 2025, diverses campagnes d'hameçonnage en temps réel et d'hameçonnage en deux étapes ont pris pour cible la clientèle des banques suisses en particulier. Des pages de publicité payante s'affichant avant les véritables pages de connexion dans les moteurs de recherche redirigeaient les victimes vers de faux sites d'e-banking. Les escrocs diffusaient également leurs sites d'hameçonnage par de petites annonces afin d'accéder aux données des cartes de crédit, aux accès à Twint et aux identifiants de connexion d'e-banking. Enfin, un nombre croissant de la méthode en deux étapes a été signalé, qui commence par demander à la clientèle bancaire de saisir des données moins sensibles sur une page d'hameçonnage, comme un numéro de téléphone, puis, dans un second temps, qui utilise les informations collectées pour tenter de convaincre leurs victimes, par téléphone, de donner l'accès à leur e-banking pour soi-disant vérifier des paiements potentiellement frauduleux.

---

1 Rançongiciels (ncsc.admin.ch)
2 Hameçonnage (*phishing*), *vishing*, *smishing* (ncsc.admin.ch)
3 Logiciels malveillants (ncsc.admin.ch)
4 Fraude à l'investissement (ncsc.admin.ch)

Hacktivisme : les attaques DDoS, instrument ayant fait ses preuves

Des attaques par saturation (DDoS)[5] sont également survenues en Suisse durant la période sous revue. Outre divers groupes d'hacktivistes propalestiniens, des groupes prorusses[6] ont lancé des attaques DDoS qui ont perturbé temporairement des services accessibles par Internet, à l'instar des sites web. Des mesures de prévention et de défense ciblées ont toutefois permis d'en atténuer l'effet pendant le Forum économique mondial et le Concours Eurovision de la chanson. Lors d'attaques DDoS, les pirates n'ont pas accès aux systèmes, mais surchargent de requêtes les services existants, provoquant des ralentissements ou des interruptions temporaires. Les hacktivistes voient dans les événements au centre de l'attention internationale une bonne plateforme pour faire parler de leur cause tout en déstabilisant l'opinion publique.

Autres phénomènes

Le secteur informatique suisse est soumis aux aléas internationaux. Les logiciels qu'il utilise couramment ne sont en effet pas à l'abri de vulnérabilités globales. Les cybercriminels en tirent parti pour accéder aux systèmes informatiques des entreprises et provoquer des fuites de données. Des acteurs étatiques peuvent en profiter à des fins d'espionnage ou de sabotage. La Suisse a connu jusqu'ici une situation relativement stable en matière de cybermenaces, mais le contexte international, en proie aux tensions géopolitiques et aux risques d'escalade, l'oblige à relever des défis de plus en plus complexes.

5 Attaque DDoS – que faire ? (ncsc.admin.ch)

6 Voir rapport semestriel 2023/1, chap. 2.

Table des matières

Editorial

Au premier semestre 2025, la Suisse a accueilli à deux reprises un événement international majeur, à savoir le Forum économique mondial en janvier à Davos, puis le Concours Eurovision de la chanson en mai à Bâle. Les manifestations couvertes par la presse mondiale sont souvent dans la ligne de mire des hacktivistes, qui paralysent temporairement ou contrefont les sites Internet officiels afin d'attirer l'attention des médias sur leur cause. Une prévention ciblée, des mesures de protection technique et une étroite collaboration avec les organisateurs et les autorités de sécurité ont toutefois permis de repousser avec succès en Suisse les attaques DDoS liées à ces deux événements. La collaboration a été d'autant plus fructueuse qu'elle était coordonnée et prospective. La Suisse est par conséquent sur la bonne voie pour renforcer sa cyberrésilience, comme le vise la cyberstratégie nationale.

Les auteurs, et il s'agit là d'une autre dimension préoccupante de la cybermenace, ne se contentent toutefois pas d'utiliser les grands événements comme tribune, mais détournent aussi l'image de personnalités connues en misant sur la confiance qu'elles inspirent. La population signale régulièrement à l'Office fédéral de la cybersécurité (OFCS) de fausses annonces publicitaires dans lesquelles, par exemple, la présidente de la Confédération Karin Keller-Sutter recommande soi-disant une plateforme d'investissement frauduleuse. Les escrocs tirent parti de la technologie *deepfake* pour imiter l'apparence et la voix de la Présidente de la Confédération. Ces manipulations, qui visent à endormir l'esprit critique des victimes, sont particulièrement perfides : la combinaison d'un visage familier, d'une voix contrefaite et d'une promesse de gain rend la supercherie plus crédible. L'OFCS explique régulièrement comment reconnaître les vidéos et publicités frauduleuses, rappelle les précautions à prendre et invite à la prudence.

La situation générale en matière de menace reste elle aussi tendue. Au premier semestre 2025, l'OFCS a reçu 36 000 signalements d'incidents, nombre qui s'est stabilisé à un niveau élevé. Plus de la moitié de ces annonces (58 %) concernaient des tentatives d'escroquerie. Les escrocs ne cessent de peaufiner leurs méthodes d'attaque : une technique en deux étapes a ainsi été observée. La victime est d'abord attirée sur un site d'hameçonnage, avant d'être contactée par téléphone. Les escrocs cherchent ainsi à obtenir d'elle, par manipulation psychologique, des données aussi sensibles que les identifiants de connexion à l'e-banking.

Dans le monde entrepreneurial, les attaques contre les prestataires informatiques ont redoublé. Ces incidents ne touchent pas que ces fournisseurs, mais également leurs clients, dont les données confidentielles risquent ainsi de se retrouver sur le *darknet*. La cybersécurité tout au long de la chaîne d'approvisionnement devient dès lors un enjeu majeur. L'OFCS aide les entreprises à mieux se protéger face aux attaques indirectes, en leur proposant des outils concrets et des recommandations pratiques.

Une autre étape importante visant à renforcer la cyberrésilience a été franchie avec l'introduction de l'obligation légale de signaler les cyberattaques contre les infrastructures critiques. Depuis le 1er avril 2025, il incombe aux exploitants de signaler les incidents graves à l'OFCS. Ce régime d'obligation garantit que les informations pertinentes circulent rapidement, que les risques soient détectés à un stade précoce et que les mesures coordonnées qui s'imposent puissent être adoptées.

Sur la scène politique, tout comme lors de grands événements ou dans la vie de tous les jours, la cybersécurité est un sujet omniprésent. Il est d'autant plus important que tous les protagonistes, au sein de l'administration comme dans les milieux économiques ou parmi la population, contribuent à la cybersécurité. Car la résilience résulte d'un mélange de coopération, de vigilance et de technologie.

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

1 Cybermenaces en Suisse – tour d'horizon

Dans le cyberespace, toute une série d'acteurs aux motivations et capacités variées détermine le paysage de la menace encourue par les entreprises, les organisations et les particuliers. Alors que dans d'autres pays occidentaux, les tensions géopolitiques et les escalades qui s'ensuivent ont abouti à des changements radicaux dans l'analyse des risques encourus par les infrastructures critiques, la Suisse doit également faire face à un environnement de menaces plus tendu. Malgré cette situation, la Suisse jouit jusqu'ici d'une situation relativement stable en termes d'incidents observés. Les experts en sécurité ont beau constater des changements et des évolutions difficiles à gérer, en raison des nouvelles techniques d'attaque, les principaux phénomènes observés et les conclusions en la matière sont restées relativement stables au fil du temps.
Afin d'obtenir à l'avenir une meilleure vue d'ensemble de la situation de la cybermenace et de pouvoir prévenir le plus tôt possible les exploitants d'infrastructures critiques, le Parlement a adopté une obligation de signaler les cyberattaques contre les infrastructures critiques[7]. Depuis le 1er avril 2025, l'OFCS recueille les déclarations sur le Cyber Security Hub (CSH), sa plateforme d'échange d'informations. Comme cette obligation de signaler a été introduite au milieu de la période sous revue, le recul manque encore. L'analyse systématique des incidents signalés ne sera possible qu'au deuxième semestre 2025. Le présent rapport repose essentiellement, comme jusque-là, sur les annonces volontaires de la population et des milieux économiques.

Le nombre de signalements n'a que faiblement progressé au premier semestre 2025, avec 35 727 annonces au total[8], ce qui représente une hausse de 938 par rapport au premier semestre de l'année précédente (voir fig. 1). Les fraudes ont à nouveau été le genre d'attaques le plus souvent signalées (voir fig. 2). Deux phénomènes en particulier ont connu une évolution dynamique : alors que les prétendus courriels de menace émanant des autorités[9] chutaient par rapport à l'année précédente de 13 730 à 10 578, les arnaques à la publicité pour les investissements se sont multipliées. Cet essor est surtout frappant en mars 2025, mois pendant lequel 851 signalements sont parvenus à l'OFCS, soit presque huit fois plus qu'à la même période l'année précédente (112 annonces). L'OFCS a également enregistré une hausse des incidents liés aux rançongiciels, qui sont passés de 44 incidents au printemps 2024 à 57 au premier semestre 2025, avec un pic en avril. Cette situation pourrait s'expliquer par l'attention médiatique accrue et les discussions liées à l'introduction de l'obligation de signaler les cyberincidents. À compter de mai 2025, le nombre d'annonces a de nouveau oscillé entre zéro et deux incidents par semaine.

---

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

8 L'OFCS publie dans ses statistiques toutes les notifications reçues, parmi lesquelles figurent aussi des questions générales, de simples informations ou des annonces impossibles à classer. C'est ainsi qu'au premier semestre 2025, 1430 annonces ne se rapportant à aucun phénomène ni incident spécifique lui sont parvenues.

9 Les appels de menace émanant prétendument d'autorités ont fait l'objet d'un rapport de l'OFCS publié en même temps que son rapport semestriel 2024/1.

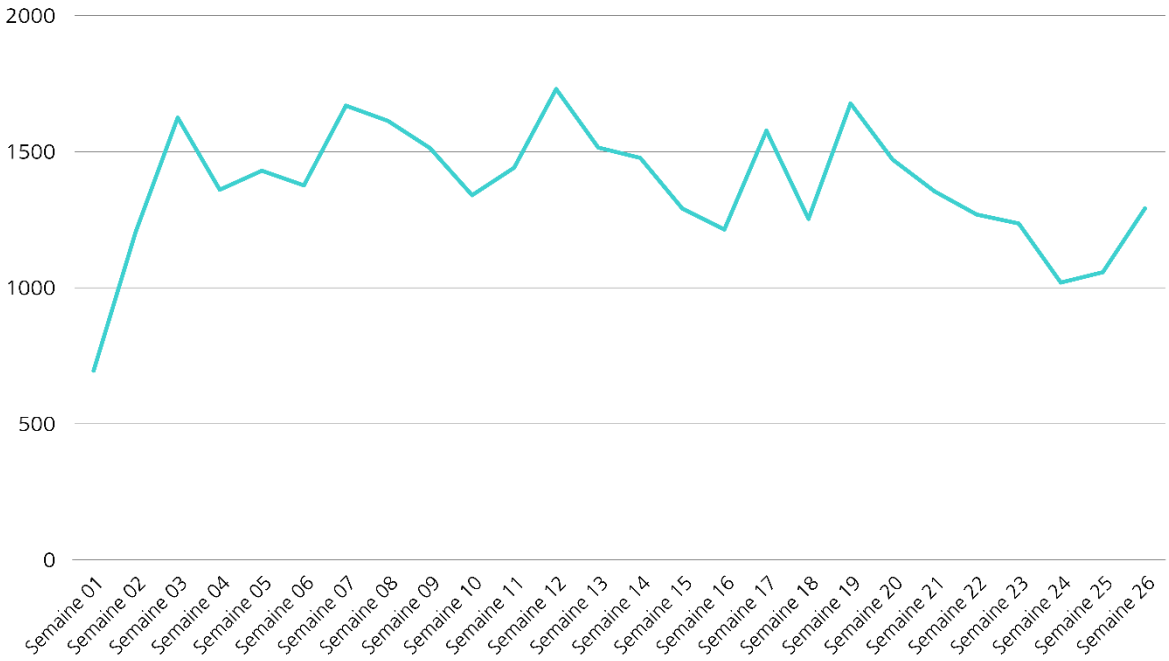

Fig. 1: nombre d'annonces par semaine parvenues à l'OFCS au premier semestre 2025, voir Chiffres actuels (ncsc.admin.ch)

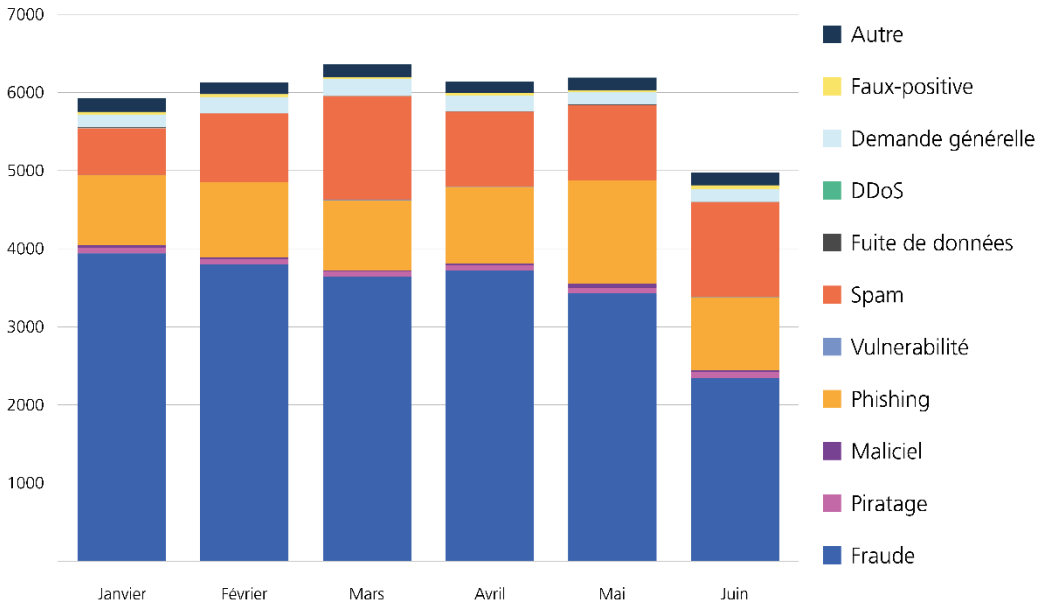

Fig. 2: annonces parvenues à l'OFCS au premier semestre 2025, selon la catégorie, voir Chiffres actuels (ncsc.admin.ch)

Le rapport entre les annonces émanant de la population (90 %) et celles qui proviennent des entreprises, associations et autorités (10 %) demeure stable. Comme les particuliers, les entreprises sont concernées par les prétendus courriels de menace émanant des autorités et par les tentatives d'hameçonnage. Deux genres d'attaques visent par contre typiquement les organisations, à savoir la fraude à la facturation[10] et l'arnaque au président[11] (voir chap. 5). L'essor du phénomène de l'arnaque au président constaté l'année dernière[12] s'est poursuivi. Les 605 tentatives d'arnaque au président signalées durant la période sous revue ont été presque aussi nombreuses que toutes les annonces de l'année 2024. Les communes, les écoles et les églises en ont à nouveau fait les frais.
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.

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

10 Piratage d'une messagerie professionnelle (ncsc.admin.ch)
11 Arnaque au président (ncsc.admin.ch)
12 Voir aussi le rapport semestriel 2024/2, chap. 5.3.
13 Ingénierie sociale (*social engineering*) (ncsc.admin.ch)
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.

sa variante à large diffusion, ce type d'attaque conçu sur mesure pour la cible est très difficile à détecter.

Au premier semestre 2025, l'OFCS a reçu via le formulaire d'annonce 5981 signalements de tentatives d'hameçonnage, soit 662 annonces de moins qu'un an plus tôt à la même période. Les annonces effectuées sur la plateforme antiphishing.ch[15] gérée par l'OFCS ont également reflué, après plusieurs semestres de croissance continue. Alors que 11 505 adresses Internet (URL) d'hameçonnage avaient été signalées au premier semestre 2024, leur nombre a diminué à 7412 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 et d'entreprises connues. Durant la période sous revue, les abus se sont concentrés sur les services postaux (23 %), le secteur financier (22 %), les transports publics (19 %), le secteur informatique (9 %) et les télécommunications (7 %). Depuis le début de l'année 2025, le nombre d'URL signalées imitant les sites web d'assureurs, par exemple de caisses-maladie, n'a cessé d'augmenter, passant à 6 % en moyenne. Par contre, toujours moins de pages d'hameçonnage en rapport avec le secteur informatique ont été signalées durant la période sous revue. Le nombre total d'annonces a connu un creux en mars et en avril, pendant lesquels les messages frauduleux usurpant l'identité d'organisations des transports publics ont été rares (voir fig. 3).

Une grande partie des annonces d'hameçonnage étaient des cas classiques de fraude à la carte de crédit. Or, là aussi, les criminels ont tenté d'améliorer leurs chances de succès, par exemple en limitant l'accès à leurs pages d'hameçonnage aux utilisateurs d'appareils mobiles. Car comme les autorités travaillent principalement avec des ordinateurs de bureau, la probabilité d'une découverte rapide diminue ainsi. Les tentatives d'hameçonnage en chaîne[16] aux dépens de comptes Microsoft 365 sont également restées nombreuses. Des méthodes de contournement de l'authentification multifactorielle (AMF) ont également servi. En outre, l'OFCS a enregistré des tentatives d'hameçonnage plus sophistiquées, visant Twint ou l'e-banking. À cet effet, les escrocs ont par exemple utilisé des plateformes de petites annonces comme prétexte pour entrer en contact, ou suivi une procédure en deux étapes, utilisant l'hameçonnage par téléphone. Ces méthodes sont certes plus complexes à mettre en place que les courriels d'hameçonnage classiques, mais elles inspirent davantage confiance et accroissent les chances de succès des malfaiteurs. Grâce à des contacts personnels établis parfois sur plusieurs jours, ils paraissent crédibles, veillant notamment à rassurer leurs victimes au cas où elles deviendraient méfiantes.

---

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 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.

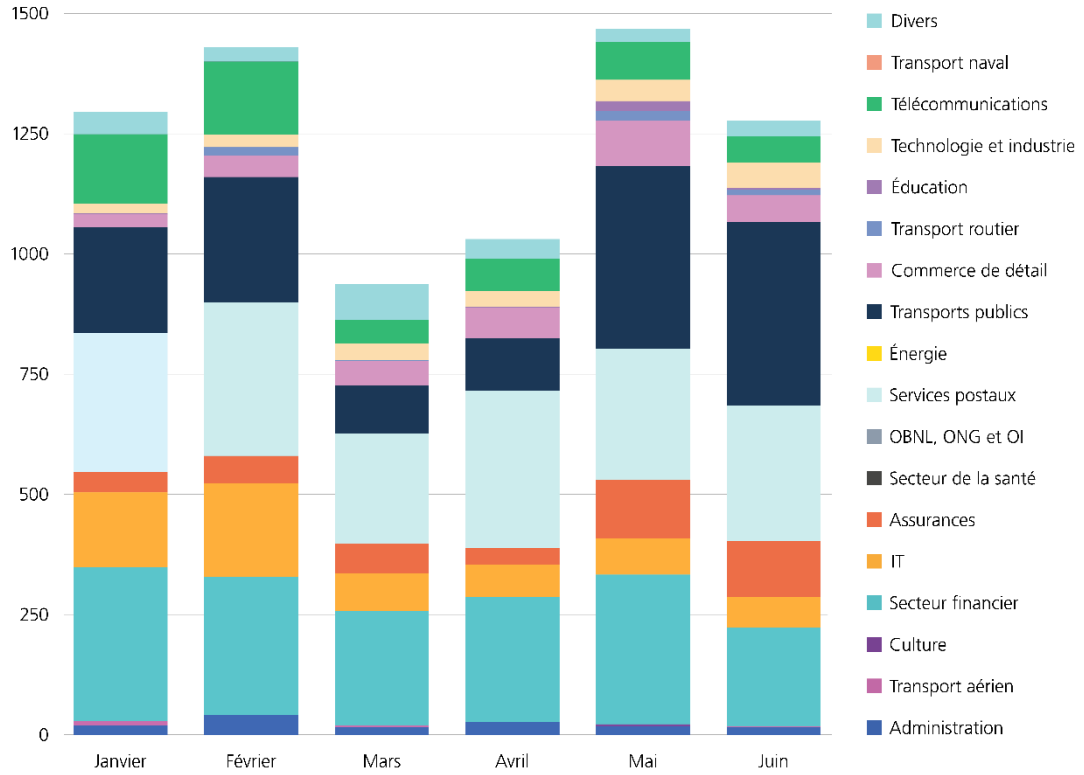

Fig. 3: nombre mensuel d'URL d'hameçonnage vérifiées et confirmées par l'OFCS au premier semestre 2025, ventilées par secteur sur la base des noms de marques usurpés.

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.

Hameçonnage en temps réel : applications bancaires prises pour cibles

Les banques suisses misent généralement sur l'authentification multifactorielle (AMF) pour renforcer la sécurité d'accès à leurs services bancaires en ligne et aux autorisations de paiement, exigeant de leurs clients qu'ils inscrivent un code SMS ou confirment une notification Push. Cette précaution permet d'éviter toute intrusion dans les applications bancaires à l'aide de données volées. Il y a dix ans encore, les escrocs utilisaient principalement des maliciels, comme *Retefe*, tel que publié dans le rapport *Opération Emmental*[17], afin de contourner les mécanismes de protection des applications bancaires. Entre-temps, les maliciels d'e-banking

[17] Voir Retefe – Attaque contre des clients de banques suisses : précisions de MELANI (ncsc.admin.ch)

ont quasiment disparu en Suisse. La plupart des attaques visant les comptes d'e-banking relèvent de l'ingénierie sociale et de l'hameçonnage en temps réel, particulièrement présent à la fin du mois de juin 2025. À la différence de l'hameçonnage classique et comme son nom l'indique, les malfaiteurs dérobent en temps réel des données d'accès, qu'ils s'empressent d'utiliser avant qu'elles ne deviennent invalides.
Les victimes sont redirigées vers de fausses pages d'e-banking via des annonces publicitaires payantes qui s'affichent dans les moteurs de recherche avant les véritables pages de connexion. Ces campagnes d'hameçonnage, imitant surtout des sites de banques cantonales, provenaient souvent de domaines[18] portant l'extension « .app », « .digital » ou « .help ».[19] Dès qu'une personne saisit ses données d'accès sur la fausse page, les escrocs se connectent en parallèle sur le véritable site d'e-banking. Pour faire patienter leur victime, ils simulent par exemple une lenteur de connexion en affichant un sablier. Et quand le site authentique leur demande le deuxième facteur, les pirates transmettent la demande sur l'écran de leur victime. Une fois en possession du deuxième facteur, ils pillent le compte e-banking de leur victime. Bien souvent, les escrocs prennent la précaution d'envoyer un message d'erreur à la victime, l'informant qu'il lui faut se reconnecter, afin qu'elle ne se doute de rien.

Prise de contrôle du compte Twint à l'aide de petites annonces

L'hameçonnage en temps réel tire aussi souvent parti de petites annonces. Ce genre de tentatives d'attaques a quintuplé depuis août 2024 (voir fig. 4). Les attaques passent d'abord inaperçues : un prétendu acquéreur s'annonce peu après la publication d'une annonce et propose d'organiser la livraison et le paiement anticipé, par exemple via la Poste suisse. La victime reçoit alors un lien pour récupérer l'argent censé lui avoir été transféré. La page frauduleuse qui s'ouvre lui demande les données de sa carte de crédit, ses identifiants d'utilisateur de Twint ou ceux d'e-banking. En correspondant à l'offre concrète, en indiquant le prix correct et en affichant même parfois une photo de l'objet vendu, ces pages inspirent confiance.

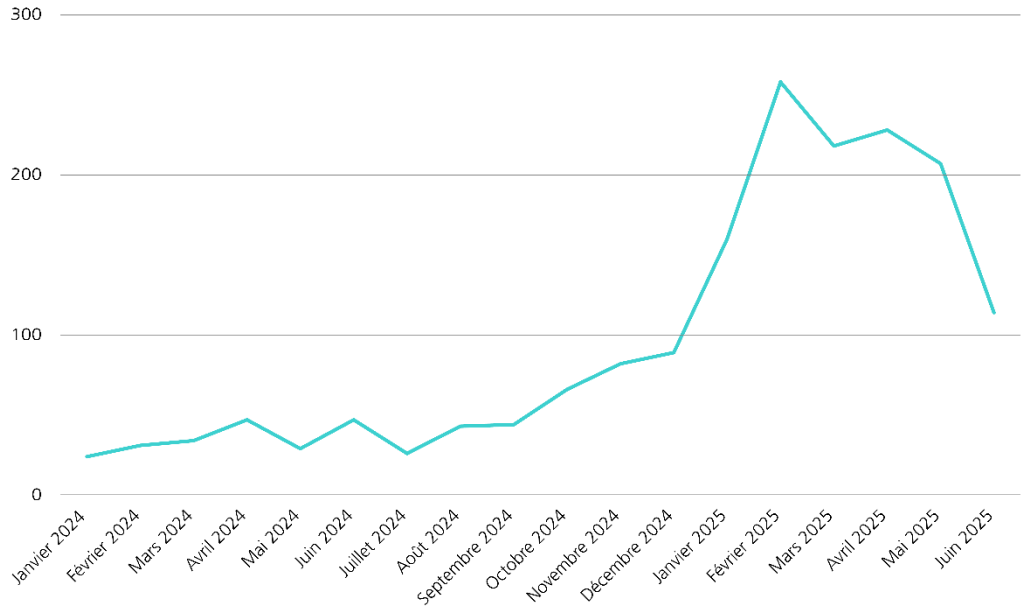

Fig. 4: hausse des cas d'hameçonnage par petites annonces à partir de janvier 2024

[18] Voir Glossaire (ncsc.admin.ch), terme Domaines.

[19] Voir Attention : Hameçonnage en temps réel au nom de banques cantonales (ncsc.admin.ch)

Une fois les données en leur possession, les escrocs font patienter la victime pendant qu'ils se connectent en arrière-plan à son compte. Ils s'intéressent apparemment moins aux comptes d'e-banking qu'aux comptes Twint y étant liés. Au lieu d'effectuer un paiement frauduleux dans le système d'e-banking, ils associent un de leurs appareils au compte Twint de la victime, ce qui leur permet d'effectuer immédiatement des transactions irrévocables. Bien souvent, les cybercriminels ont le temps de faire plusieurs opérations avant que la fraude ne soit découverte par la banque. Ils veillent d'ailleurs à brouiller les pistes en transférant de l'argent sur plusieurs comptes, dont certains piratés.

Attaques en deux étapes avec hameçonnage par téléphone

L'hameçonnage par téléphone est une sous-variante de l'hameçonnage en temps réel. Il comporte fréquemment deux étapes, ce qui constitue sa nouveauté. Dans un premier temps, les escrocs utilisent des sites d'hameçonnage pour obtenir de leurs victimes des informations moins sensibles, par exemple, au lieu des données d'accès à l'e-banking, le numéro de téléphone et la relation bancaire.

Dans un second temps, les escrocs suivent un schéma classique : ils appellent la victime en se faisant passer par exemple pour un certain Monsieur Fischer du service de sécurité de la banque dont ils ont obtenu le nom lors de la première étape. Le plus souvent, le numéro de téléphone qui s'affiche correspond au numéro officiel de ladite banque. Les escrocs utilisent des techniques d'usurpation d'identité[20] pour falsifier les numéros de téléphone et les adresses électroniques. Au téléphone, ils expliquent aux victimes vouloir empêcher l'exécution d'un paiement frauduleux qui, dans bien des cas, se monte à 800 francs. Afin d'annuler cette opération, la victime est priée d'installer sur son ordinateur un logiciel d'accès à distance et de leur donner les autorisations d'accès nécessaires à son ordinateur et à son compte bancaire. Les escrocs pourront ainsi effectuer en arrière-plan des transactions dans l'e-banking de leur victime. Face à ces risques, il est essentiel que le personnel bancaire en contact avec la clientèle soit bien formé et au point sur ces questions. Il sera ainsi à même d'alerter rapidement les clients sceptiques sur une fraude potentielle, au nom de l'établissement bancaire.

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[21]. Méfiez-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.

20 Usurpation d'identité (*spoofing*) (ncsc.admin.ch)

21 Ingénierie sociale (*social engineering*) (ncsc.admin.ch)

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[22], 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.

Au premier semestre 2025, l'OFCS a de nouveau identifié des campagnes malveillantes cherchant à infecter des systèmes informatiques. Outre l'utilisation abusive de fichiers image avec l'extension « .svg », les pirates ont aussi, par exemple, envoyé de fausses factures pour installer leurs maliciels sur les systèmes pris pour cible. La plupart de ces campagnes ne présentaient pas de caractéristique propre à la Suisse et leur mode opératoire ne différait guère de ce qui s'observe sur la scène internationale.
Selon les données dont dispose l'OFCS, la diffusion de maliciels par courriel (*malspam*) ne joue qu'un rôle secondaire dans les infections de réseaux d'entreprises. En revanche, les cybercriminels recourent de plus en plus à des sites web compromis[23] ou publient des publicités malveillantes (*malvertising*) sur les moteurs de recherche[24] pour parvenir à leurs fins (voir chap. 3.3).

La méthode *ClickFix*[25] a gagné du terrain dans ce contexte. Les sites web imitant les portails de réservation d'hôtel en sont un bon exemple. Concrètement, un script est copié dans le presse-papier lors de la visite d'une page web malveillante ou d'un site authentique, mais compromis. Il est ensuite demandé à l'utilisateur d'appuyer sur les combinaisons de touches

22 Logiciels malveillants (ncsc.admin.ch)
23 ClearFake's New Widespread Variant: Increased Web3 Exploitation for Malware Delivery (sekoia.io)
24 University site cloned to evade ad detection distributes fake Cisco installer (malwarebytes.com)
25 Voir rapport semestriel 2024/2, chap. 3.1.

Windows + *R*, *Windows* + *X* ou encore *CTRL* + *V* pour exécuter une tâche prétendument nécessaire. Les escrocs prétextent la nécessité de résoudre un captcha[26] ou d'accepter des cookies[27]. Cette action aboutit en réalité à l'exécution du script malveillant en attente dans le presse-papier, et donc à l'installation du maliciel, par exemple dans l'interface *PowerShell*[28].

Le maliciel *Lumma Stealer*, dont l'action malveillante repose sur la technique *ClickFix*, est fréquemment déployé et documenté de longue date, au point qu'il semble avoir les faveurs des cybercriminels[29]. En mai 2025, une opération conjointe d'entreprises informatiques et d'autorités de poursuite pénale a permis de démanteler l'infrastructure de *Lumma Stealer* et de freiner tout au moins temporairement sa propagation[30]. Le même mois, un autre coup de filet concerté au niveau international sous le nom d'*Operation Endgame* frappait au cœur l'infrastructure de sept variantes de maliciels[31]. Ces mesures déstabilisent les courtiers d'accès initial (*initial access broker*), et donc l'économie cybercriminelle. Tout indique cependant qu'ils cherchent aussitôt à se doter d'une nouvelle infrastructure. D'autres criminels qui ne sont pas touchés directement par les opérations policières ne manquent pas d'ailleurs de profiter du vide laissé pour tenter de répondre à la demande avec leurs propres produits, à l'instar du maliciel *Rhadamanthys*, utilisant lui aussi *ClickFix* et ayant fait l'objet de campagnes de distribution par courriel en Suisse et ailleurs en Europe. Dans leurs courriels, les escrocs se font passer pour des cabinets d'avocats et menacent leurs victimes de conséquences juridiques pour violation des droits de la propriété intellectuelle. Des précisions sur l'infraction commise sont censées figurer dans un fichier PDF à télécharger. Or, cette annexe est un fichier exécutable malveillant, qui entraîne une infection de l'ordinateur par *Rhadamanthys*[32].

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

26 Semaine 9: Les hôtels et leur clientèle, des cibles de choix pour les cybercriminels (ncsc.admin.ch)
27 Abuse.ch: Booking themed ClickFix campaign using a fake cookie banner (linkedin.com)
28 Voir rapport semestriel 2024/2, chap. 3.1.
29 Voir rapport semestriel 2024/2, chap. 3.1.
30 Démantèlement de Lumma Stealer : Microsoft conduit une action mondiale contre un outil prisé du cybercrime (microsoft.com)
31 Operation ENDGAME strikes again: the ransomware kill chain broken at its source (europol.europa.eu)
32 Copyright Phishing Lures Leading to Rhadamanthys Stealer Now Targeting Europe (cybereason.com)

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[33]. 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.

Au premier semestre 2025, le guichet national pour les cyberrisques de l'OFCS a reçu 57 signalements d'incidents liés à des rançongiciels, émanant principalement d'entreprises (voir fig. 5). Ce chiffre représente une légère augmentation par rapport aux 44 incidents du premier semestre 2024. Le nombre réel d'incidents de ce genre survenus en Suisse est probablement un peu plus élevé, faute de signalement systématique par les organisations lésées. Les groupes de rançongiciels les plus présents en Suisse au premier semestre 2025 sont les mêmes qu'un an plus tôt : il s'agit d'*Akira*, avec huit attaques réussies et *LockBit* avec sept[34]. Depuis mars 2023, *Akira* compte parmi les groupes les plus actifs au niveau international, s'attaquant à des organisations de toutes tailles et dans tous les secteurs. *LockBit* était jusqu'en février 2024 l'un des groupes les plus nuisibles et redoutés. Bien qu'il ait encore développé au début de 2025 sa nouvelle variante intitulée *LockBit 4.0*, son activité a chuté en raison de diverses opérations policières et de la répression internationale, mais aussi de fuites de données internes[35]. Dans un nombre relativement élevé d'incidents (27), la variante de maliciel n'est pas précisée, de sorte que ces cas ont été regroupés sous « inconnu » dans le graphique.

33 Rançongiciels (ncsc.admin.ch)

34 Voir rapport semestriel 2024/1 et 2024/2, chap. 3.2 sur les variantes de rançongiciels.

35 What the LockBit 4.0 Leak Reveals About RaaS Groups (darkreadings.com)

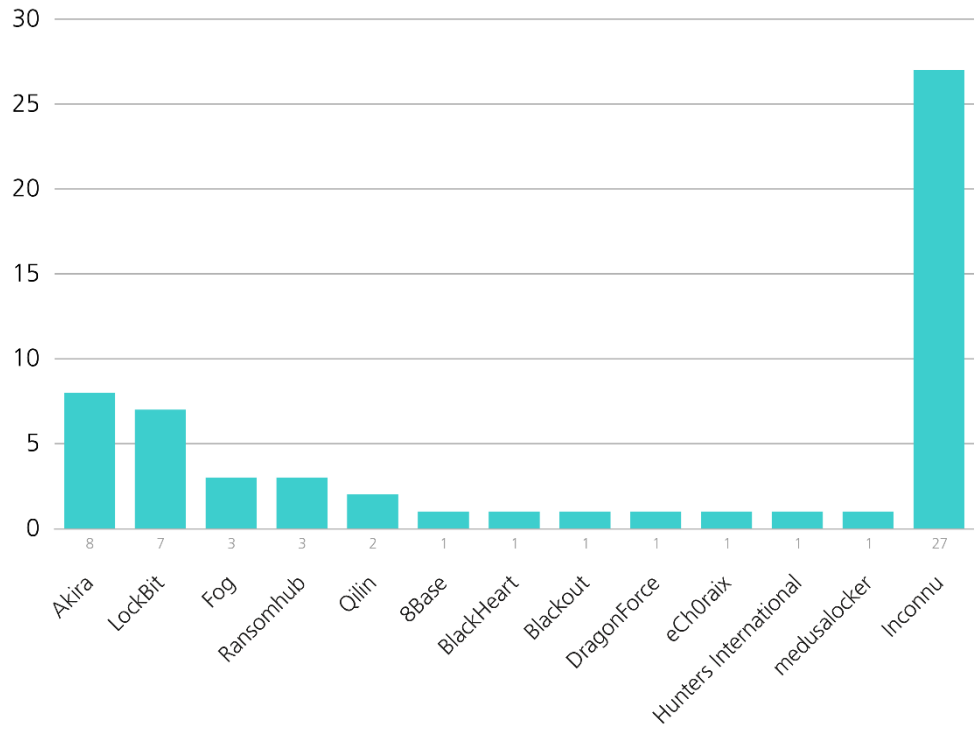

Fig. 5: nombre d'incidents dus à des groupes de rançongiciels ayant été signalés à l'OFCS au premier semestre 2025

D'un point de vue statistique, la menace liée aux rançongiciels est toujours d'actualité. Alors que de nouveaux groupes continuent d'apparaître, d'autres disparaissent ou se transforment, en raison notamment de restructurations internes[36], de fuites de données[37] ou d'opérations menées par les autorités de poursuite pénale[38]. Aucun des groupes connus ne s'en prend spécifiquement aux organisations suisses, mais leurs attaques, relevant le plus souvent de l'opportunisme, n'épargnent pas la Suisse. L'accès initial provient généralement de maliciels, de vulnérabilités non corrigées ou de données d'accès dérobées au cours de campagnes d'hameçonnage et de vol d'informations[39]. Cette évolution reflète la division du travail et la spécialisation au sein de l'économie criminelle : tandis que certains acteurs se concentrent sur le vol des données d'accès, d'autres développent par exemple de nouveaux rançongiciels. D'où le succès des modèles d'affaires qui, à l'instar de *RaaS* (*Ransomware-as-a-Service*), permettent de lancer des attaques même avec des connaissances techniques rudimentaires. Les développeurs proposent ainsi et entretiennent, sur des plateformes prêtes à l'emploi, les instruments nécessaires aux différentes étapes d'une attaque par rançongiciel (p. ex. exfiltration des données, chiffrement, communication et paiement). Le groupe *DragonForce*, qui sévit aussi en Suisse, en est une bonne illustration : déjà à l'œuvre en 2023[40], il met à disposition,

---

36 Lynx Ransomware: A Rebranding of INC Ransomware (paloaltonetworks.com)

37 LockBit Ransomware Gang Hacked, Operations Data Leaked (darkreading.com)

38 Key figures behind Phobos and 8Base ransomware arrested in international cybercrime crackdown (europol.europa.eu)

39 Un *infostealer* (voleur d'informations) désigne un logiciel malveillant qui, une fois installé sur un système, collecte des informations sensibles (p. ex. données d'accès) pour les envoyer aux pirates.

40 Voir rapport semestriel 2023/2, chap. 3.4.2.

depuis le début de 2025, une plateforme complète, que ses partenaires peuvent exploiter en leur propre nom. En contrepartie, les développeurs perçoivent un pourcentage fixe des rançons payées[41].

Outre l'infrastructure utilisée, les groupes les plus compétents ne cessent d'affiner leurs techniques d'attaque, afin de contourner les mesures de défense en constante amélioration. Certains gangs utilisent désormais des outils *EDR Killer*, qui peuvent être des maliciels ou des logiciels légitimes utilisés à mauvais escient[42]. Les groupes de rançongiciels parviennent ainsi à modifier, voire à désactiver les produits de sécurité en place, afin d'éviter toute détection précoce. Ils ont ainsi le temps d'identifier les données sensibles avant leur exfiltration et leur chiffrement. Afin d'obtenir un impact maximal, ils opèrent d'ordinaire durant les heures creuses, soit de nuit, les jours fériés ou en fin de semaine.

Au printemps 2025, plusieurs incidents survenus en Suisse ont mis en évidence le risque que les attaques de rançongiciels peuvent représenter pour les organisations tierces. Après la compromission d'un fournisseur, les données d'accès potentiellement piratées sont susceptibles de servir de vecteurs d'attaque. L'attaque par rançongiciel menée contre *Cistec*, fabricant suisse de systèmes d'information hospitalière, en est un bon exemple : les accès à distance aux systèmes hospitaliers accordés à *Cistec* en vue de la maintenance de ses logiciels auraient pu servir au lancement d'attaques malveillantes contre des hôpitaux[43]. D'autres cas impliquant des prestataires informatiques rappellent que si une organisation est prise pour cible, sa clientèle risque d'en subir les conséquences directes. Quand une filiale du groupe *Ilem* a été piratée, près de 15 % de ses clients ont été temporairement privés d'accès aux services proposés dans le nuage[44]. La société *2sic* a bien su repousser une attaque, en déconnectant ses systèmes du réseau, avec pour revers de la médaille une panne de deux à trois jours durant laquelle la clientèle n'a pu utiliser ses systèmes[45]. Enfin, certains incidents soulignent le risque de fuite des données, si la victime directe dispose d'informations provenant de clients commerciaux et de tiers (voir chap. 7). Après la cyberattaque dont la Fondation suisse pour la santé RADIX a été victime, des données dérobées ont été publiées. Parmi ses clients figuraient plusieurs services fédéraux. Même si RADIX n'avait pas directement accès aux systèmes de l'administration fédérale, des informations issues de l'administration fédérale figuraient parmi les données compromises[46].

41 DragonForce expands ransomware model with white-label branding scheme (bleepingcomputer.com)

42 Ransomware crews add EDR killers to their arsenal – and some aren't even malware (theregister.com)

43 Ransomware-Angriff auf KIS-Anbieter Cistec (inside-it.ch); « On est passé à côté d'une catastrophe nationale » (medinside.ch)

44 Ransomware-Angriff auf Genfer IT-Gruppe Ilem (inside-it.ch)

45 Ransomware Angriff auf 2sic Hosting abgewehrt (2sic.com)

46 Cyberattaque contre la Fondation Radix : Des données de l'administration fédérale aussi concernées (ncsc.admin.ch)

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[47] 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 *Malvertising* : usage abusif d'annonces publicitaires dans les moteurs de recherche

L'OFCS a observé en 2025 différents cas d'usage abusif d'annonces publicitaires, qui s'affichaient dans les moteurs de recherche à des fins d'hameçonnage (voir chap. 2) ou pour diffuser des maliciels (*malvertising*). À cet effet, les cybercriminels font usage de publicité payante, imitant des pages web légitimes ou des marques connues. Le référencement les place bien en vue, au-dessus des résultats de recherche ordinaires, accroissant les risques pour les victimes potentielles de cliquer dessus. Les utilisateurs ayant cru à tort avoir affaire à un lien fiable sont alors redirigés vers un site web frauduleux qui installe directement le code malveillant[48], ou qui les invite à télécharger un fichier d'installation infecté. Bien souvent, ces campagnes misent sur des termes de recherche populaires comme *Download*, *Update* ou *Support*, et sur des logiciels connus comme Chrome. Les pirates peuvent ainsi diffuser une annonce vantant un logiciel apparemment officiel, derrière lequel se cache en réalité un cheval de Troie ou un rançongiciel.
Ce genre de pratique abusive est susceptible de porter ses fruits même avec des moteurs de recherche aussi connus que Google ou Bing. Car les annonces publicitaires sont commandées et publiées en temps réel, ce qui permet aux cybercriminels d'adapter rapidement leurs campagnes pour contourner les mesures de précaution introduites.

Recommandations

Il importe de télécharger des logiciels uniquement dans les magasins d'applications officiels ou sur des portails dignes de confiance, sans se fier aux annonces affichées dans le moteur de recherche, même si celles-ci semblent correspondre à nos besoins. Il faut aussi vérifier dans les résultats de recherche si le référencement est normal, ou s'il s'agit d'une entrée publicitaire (*sponsored*). En outre, des bloqueurs de publicité, des correctifs de sécurité récents et des solutions de protection des terminaux permettent de réduire sensiblement les risques d'infection. Il peut être judicieux pour les entreprises de n'autoriser le téléchargement de logiciels, et donc de maliciels potentiels, qu'après consultation du service informatique.

47 Guidance for organisations considering payment in ransomware incidents (ncsc.gov.uk)
48 What Is a Drive by Download Attack? (kaspersky.com)

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[49]. 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.

Du fait de sa forte imbrication internationale, le paysage informatique suisse est directement exposé aux vulnérabilités planétaires. Comme les milieux économiques, l'administration et les exploitants d'infrastructures critiques font majoritairement appel aux produits de fournisseurs internationaux de premier plan, les failles de sécurité de fabricants établis dans le monde entier comme Fortinet, Microsoft ou Ivanti ont des répercussions en Suisse aussi. Les enjeux du cyberespace et les menaces qu'il comporte ne s'arrêtent pas aux frontières politiques. En d'autres termes, un problème au niveau mondial risque bien d'affecter la Suisse aussi.

Il est connu et établi que la plupart des vulnérabilités critiques appartiennent à quelques grandes catégories. Les pirates informatiques comme les chercheurs en sécurité font ainsi la distinction entre, d'une part, les terminaux des utilisateurs, comme les ordinateurs portables, les postes de travail et les appareils mobiles et, d'autre part, l'infrastructure exposée à Internet. Des composants comme les pares-feux ou les accès VPN forment la première ligne de défense tout en constituant aussi un risque de compromission. Si les malfaiteurs parviennent à y ouvrir une brèche en tirant parti d'une vulnérabilité périphérique, ils obtiendront ainsi l'accès initial nécessaire pour s'établir dans le système et y poursuivre leurs activités.
Cette dynamique oblige les entreprises et les autorités suisses à gérer en permanence un volume élevé de mises à jour de sécurité pour ces composants essentiels. Une gestion rapide et complète des correctifs s'avère indispensable afin de protéger les actifs numériques et de garantir la résilience face aux cyberattaques.

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. Donnez particulièrement la priorité aux failles de sécurité des parties de votre infrastructure accessibles depuis Internet. Effectuez régulièrement

49 Faille de sécurité (ncsc.admin.ch)

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*)[50], les audits de sécurité réguliers ou le lancement 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[51]. 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[52]) en leur faisant exécuter elles-mêmes certaines étapes nécessaires pour que la fraude aboutisse.

Comme les années précédentes, l'escroquerie (ou fraude) a été durant le semestre écoulé le phénomène le plus souvent signalé à l'OFCS (20 878 annonces, soit 58 % du total). La baisse d'environ 2000 signalements de cyberincidents enregistrée par rapport au premier semestre 2024 tient surtout au moins grand nombre d'appels de menace émanant prétendument des autorités (voir fig. 6). Ils ont reflué au deuxième trimestre 2025, quand douze mois plus tôt ils enregistraient des pics d'un millier d'annonces par semaine. Les données à disposition de l'OFCS ne permettent toutefois pas de dire si cette évolution va être durable ni si elle s'explique par les mesures adoptées par les opérateurs télécom.

---

50 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)).

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

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

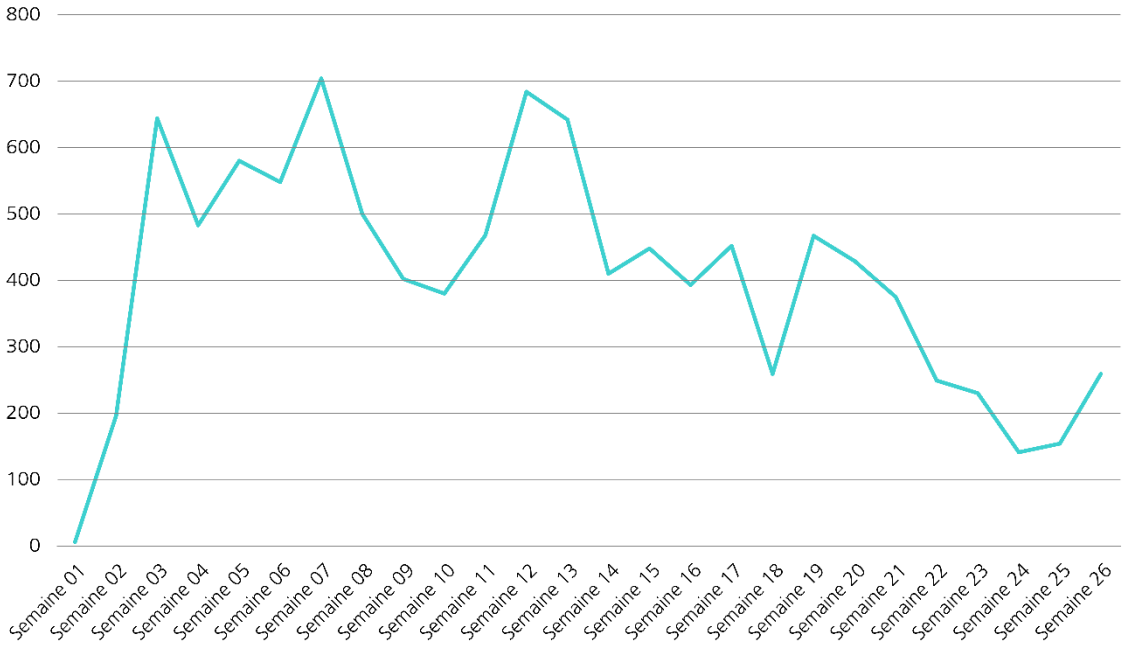

Fig. 6: diminution des signalements d'appels de menace émanant prétendument des autorités, au deuxième trimestre 2025

Le phénomène des faux courriels de menace envoyés au nom d'autorités et accusant leurs destinataires d'un acte pénalement répréhensible a connu une évolution similaire à celle des appels téléphoniques frauduleux : avec 1487 annonces, il est en repli au niveau suisse par rapport à la même période de l'année précédente (2252). Les jeux-concours frauduleux, aboutissant d'ordinaire à un abonnement-piège ou à un site d'hameçonnage, sont eux aussi en perte de vitesse. Après un pic de 2398 annonces au deuxième semestre 2024, ils ont reflué à 1916 cas. Des noms d'entreprises connues, actives dans le secteur alimentaire ou le commerce de détail, dans la distribution de matériel électronique ou le secteur des transports, sont souvent usurpés dans ce contexte. Les signalements de *fake sextortion* (1136) demeurent quant à eux stables[53].

La forte croissance des arnaques au président survenue au deuxième semestre 2024[54] s'est poursuivie. Tandis que l'OFCS avait reçu au total 719 annonces durant l'année 2024, 605 signalements lui étaient déjà parvenus cette année à la fin du mois de juin. Les organisations les plus touchées par cette fraude sont celles qui cultivent la transparence sur leur structure organisationnelle et indiquent des possibilités de contact : communes, écoles et églises. La variante techniquement plus complexe à base de manipulations de factures à la suite du piratage d'une messagerie professionnelle[55] (*Business E-Mail Compromise* ou BEC) a enregistré une légère baisse de 65 à 59 incidents par rapport à la même période de l'année précédente.

---

53 Voir rapport semestriel 2024/2, chap. 5.2.

54 Voir rapport semestriel 2024/2, chap. 5.3.

55 Au niveau international, le phénomène du *Business Email Compromise* (BEC) n'est pas utilisé de manière uniforme, c'est pourquoi d'autres définitions considèrent par exemple la fraude au président comme une sous-forme du BEC (cf. Business Email Compromise (fbi.gov)). Le BACS distingue toutefois explicitement ces phénomènes et suit la définition de l'Office fédéral de la police (fedpol).

La fraude à l'investissement cause souvent elle aussi un grave préjudice financier. Les publicités trompeuses renvoyant vers ces sites ont connu un essor marqué. Alors que 729 cas avaient été signalés durant la même période de l'année précédente, on en dénombrait déjà 3485 au premier semestre 2025. Toujours dans le cadre de la fraude à l'investissement en ligne, une variante faisant miroiter un remboursement des pertes subies s'est entre-temps répandue en Suisse, avec 145 cas signalés. Les escrocs prennent contact avec les victimes de fraude à l'investissement, en affirmant pouvoir les aider à récupérer l'argent volé, à la condition, naturellement, que de nouveaux paiements soient effectués en avance, en échange de ce prétendu service. Les publicités trompeuses en rapport avec la fraude à l'investissement en ligne, la fraude au remboursement, et les spécificités de l'arnaque au président et de l'escroquerie par piratage de messagerie professionnelle (BEC) sont expliquées plus en détail ci-après.

Publicités trompeuses en amont de la fraude à l'investissement
Des sites web douteux sont régulièrement diffusés à travers des petites annonces et des liens dans les médias sociaux, sur des portails de *streaming* ou dans des bannières publicitaires payantes. Le nombre de cas signalés à l'OFCS a été multiplié par cinq au printemps 2025. Les escrocs imitent des portails d'information et publient de fausses interviews dans lesquelles des personnalités connues dont ils ont usurpé l'identité vantent des offres d'investissement censées être peu risquées et générer des rendements mirobolants, moyennant un apport modeste de 250 francs/euros par exemple (voir fig. 7). Ces portails imitent ceux de médias suisses connus comme le *Blick*, *20 Minutes*, la *SRF* ou la *RTS*. Les personnalités utilisées sont issues du monde du sport, des médias ou de la politique[56]. Désormais, les escrocs complètent aussi leurs articles par des vidéos falsifiées (*deepfake*)[57] s'inspirant par exemple de journaux télévisés. Dès qu'une personne a fait un premier versement, un portail créé sur mesure lui annonce que l'argent qu'elle a investi va rapidement travailler et se multiplier. Les pirates visent ainsi à inciter leurs victimes à transférer davantage d'argent. Ils sont à même de publier de manière automatisée, en très peu de temps, de nombreux contenus frauduleux sur des sites web sans être soumis au moindre contrôle de la part de leur hébergeur. Et comme il est forcément bien plus long d'identifier, de signaler et de désactiver ce type de pages que de les créer, les autorités ont souvent un temps de retard.

Fraude au remboursement après une fraude à l'investissement en ligne
Les annonces de fraudes liées à de fausses promesses d'aide pour récupérer l'argent perdu ont augmenté en Suisse, passant de 31 signalements au premier semestre 2024 à 145 en 2025. Les victimes d'une perte financière espèrent toujours récupérer leur argent. Les escrocs en profitent pour prétendre, au nom d'une autorité de poursuite pénale ou d'une entreprise sérieuse, avoir localisé la somme perdue. Mais, pour récupérer l'argent « retrouvé », la personne est priée de s'acquitter à l'avance d'un émolument, d'une taxe ou d'autres frais. Afin de rehausser leur crédibilité, les malfaiteurs joignent à leur proposition des documents d'apparence officielle, souvent établis au nom d'autorités britanniques ou chypriotes.

---

56 Semaine 35 : Fraude impliquant des personnalités connues – La face cachée de l'intelligence artificielle (ncsc.admin.ch)

57 *Deepfake* (wikipedia.org)

Arnaque au président et escroquerie par piratage de messagerie professionnelle

Au cours de la période sous revue, le nombre d'arnaques au président a fortement augmenté, tandis que l'escroquerie par piratage de messagerie professionnelle (*Business E-Mail Compromise* ou BEC) ne refluait que légèrement. Les scénarios typiques de ces deux variantes très similaires incluent de faux courriels adressés par un partenaire commercial à la comptabilité d'une entreprise avec demande de versement, fausses factures de fournisseurs ou lettres censées émaner de cabinets d'avocats ayant pour objet une prétendue acquisition secrète. Alors que dans l'arnaque au président les informations utilisées proviennent de sources publiques, il s'agit dans le cas du BEC, d'informations internes préalablement obtenues par piratage de comptes de messagerie professionnelle. Les criminels peuvent ainsi formuler des demandes plus crédibles, expressément adaptées à leurs victimes. Au lieu de s'en tenir à une requête générale, ils précisent par exemple les coordonnées bancaires ou les numéros de factures et s'inspirent du style de l'entreprise imitée. Les attaques ciblées sont techniquement plus sophistiquées et plus longues à préparer – les pirates doivent par exemple espionner les usages de communication ou les processus internes – mais ces efforts paient puisque, en fin de compte, le dommage financier infligé aux victimes est généralement plus élevé.

L'accès au compte de la victime est indispensable pour qu'une telle attaque soit fructueuse. Aussi les comptes Microsoft 365 suisses font-ils fréquemment l'objet d'attaques d'hameçonnage (voir chap. 2). En plus d'écrire à tous les contacts du carnet d'adresses lors de nouvelles attaques (par hameçonnage en chaîne notamment), les escrocs passent au crible les comptes piratés à la recherche de contenus pouvant leur rapporter de l'argent. S'ils y découvrent par exemple une facture encore ouverte, ils s'immiscent dans la conversation. Bien que l'arnaque soit directement possible à partir du compte de messagerie compromis, les escrocs préfèrent souvent enregistrer un nom de domaine similaire. Cette précaution leur permet de créer d'autres adresses électroniques pour mieux duper leurs victimes, soit la clientèle professionnelle de la société infiltrée. Ils demandent ensuite aux clients ayant des factures impayées de verser le montant sur un autre compte. Les destinataires pensent avoir affaire à la même personne, puisque le style adopté et les détails de la facture correspondent à l'historique de la conversation. Au-delà des pertes financières subies, un piratage peut ternir une réputation. Car les partenaires risquent de ne plus faire confiance à une organisation qui s'est fait dérober des informations aussi confidentielles que des données de clients (voir chap. 7).

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[58]. 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

58 Usurpation d'identité (spoofing) (ncsc.admin.ch)

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.

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.

Le début de l'année 2025 a été mouvementé. Le 10 janvier, une attaque DDoS perturbait pendant près de 45 minutes la téléphonie, Outlook, différents sites Internet de la Confédération et des applications spécialisées. Les contre-mesures adoptées ont toutefois permis de stabiliser rapidement la situation[59]. Quelques jours plus tôt, les services en ligne de plusieurs banques suisses avaient déjà subi des pannes temporaires[60]. Le groupe hacktiviste propalestinien *RooTDoS* a revendiqué les attaques, en invoquant pour se justifier l'entrée en vigueur de l'interdiction de se dissimuler le visage[61].
Vers la fin janvier, comme on pouvait s'y attendre, des attaques DDoS ont été lancées contre plusieurs sites web suisses, à l'occasion du Forum économique mondial. Ces opérations, qui n'ont pas affecté les activités[62], ont été revendiquées par *NoName057(16)*, groupe hacktiviste prorusse ayant déjà fait parler de lui lors d'autres grandes manifestations tant suisses qu'internationales[63]. Son but premier est d'instaurer un climat de menace, qui ne repose que dans une moindre mesure sur une réelle menace.
Le 19 mars 2025, divers services informatiques de l'administration fédérale ont été temporairement perturbés à la suite d'attaques DDoS massives[64]. Il n'a été possible d'élucider ni l'origine des attaques ni les motifs des pirates. À la mi-mai enfin, comme déjà lors du Forum économique mondial, des attaques DDoS ont visé divers sites Internet lors du Concours Eurovision de la chanson organisé à Bâle[65]. Ces attaques n'ont toutefois eu aucune influence sur

59 Panne des systèmes informatiques de la Confédération, en raison d'une attaque DDoS (ncsc.admin.ch)
60 Les services de la Banque Migros ont été fortement perturbés (watson.ch)
61 CyberKnow: "Pro-palestine hacktivists, RootDos are targeting Migros bank in Europe (x.com)
62 Les attaques DDoS attendues ont commencé (ncsc.admin.ch)
63 Plusieurs sites web suisses touchés par une cyberattaque (swissinfo.ch)
64 Panne des systèmes informatiques de la Confédération, en raison d'une attaque DDoS (ncsc.admin.ch)
65 Les attaques DDoS attendues dans le cadre de l'ESC ont commencé (ncsc.admin.ch)

le déroulement des épreuves, grâce notamment aux mesures préventives prises par les organisateurs[66].

En dehors des pratiques hacktivistes, des attaques DDoS accompagnées de chantage ont été observées ponctuellement. Après une première brève attaque de démonstration, les maîtres chanteurs menaçaient d'en déployer une seconde à grande échelle, au nom du fameux groupe *NoName057(16)*. Ces menaces n'ont toutefois jamais été mises à exécution[67]. Et comme le chantage DDoS ne fait pas partie des modes opératoires de ce collectif de hackers, tout indique que les attaques signalées étaient dues à de simples imitateurs.
Expérience à l'appui, les attaquants et leurs motifs restent inconnus dans la plupart des attaques DDoS. Quantité d'acteurs malveillants sont en effet susceptibles de faire appel, souvent contre rémunération, à l'infrastructure toujours plus performante des groupes de cyberpirates, pour s'en prendre aux cibles de leur choix[68]. Selon une analyse spécifique au secteur financier, la menace pesant sur les services accessibles par Internet est devenue un défi stratégique majeur[69]. Le savoir-faire croissant des attaquants exige une gestion avisée des risques pour bien protéger les fonctions critiques.

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

66 Cyberrésilience : un enjeu clé pour les grands événements et conférences internationales (ncsc.admin.ch)
67 Voir rapport semestriel 2024/1, chap. 6 décrivant une campagne analogue.
68 Défendre Internet : comment Cloudflare a bloqué une gigantesque attaque DDoS de 7,3 Tb/s (cloudflare.com)
69 From Nuisance to Strategic Threat: DDoS Attacks Against the Financial Sector (fsisac.com)

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. **Fehler! Verweisquelle konnte nicht gefunden werden.**). 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.

Un incident de sécurité survenu chez un fournisseur de services en nuage a affecté sa nombreuse clientèle professionnelle internationale, dont celle basée en Suisse. Le 20 mars 2025, un acteur malveillant connu sous le pseudonyme *rose87168* publiait un post sur le site de revente de données piratées *BreachForums*[70]. Il prétendait avoir piraté des serveurs d'Oracle et dérobé six millions d'enregistrements de données d'utilisateurs[71]. Ce pirate avait notamment proposé aux entreprises concernées d'effacer les données en sa possession en échange du versement d'une rançon. La situation était d'autant plus gênante pour la clientèle d'Oracle que ce fournisseur se montrait hésitant et réservé dans sa communication. Dans ces conditions, ni les entreprises ni les autorités ne pouvaient se faire une idée de la gravité de la fuite de données[72]. Ce n'est que le 16 avril 2025 que l'agence de cybersécurité américaine a fait toute la lumière sur l'incident. Apparemment, le système cloud obsolète *Oracle Classic* avait fait les frais d'un accès non autorisé[73]. Cette intrusion et les données d'accès dérobées ont principalement mis en danger les entreprises et les utilisateurs individuels ayant négligé de changer de mot de passe et d'identifiant après la migration du système vers *Oracle Cloud*.

Contrairement à l'incident susmentionné, le prestataire de services suisse *Chain IQ* a été visé directement par un chantage à la divulgation de données du groupe *World Leaks*. Le 12 juin 2025, ce dernier publiait près de 900 GB de données de *Chain IQ*, parmi lesquelles figuraient des données d'autres entreprises suisses du secteur financier, du commerce de détail et du secteur de la construction[74]. Le butin comprenait par exemple les numéros de téléphone internes de contacts professionnels et des informations sur des projets d'acquisition[75]. *Chain IQ* a communiqué que la cyberattaque était due à un maliciel jusque-là inconnu, qui avait permis de se déplacer dans son système sans se faire repérer[76]. Près d'un mois s'était écoulé entre l'intrusion initiale et l'envoi du message de chantage. Les criminels ont sans doute utilisé ce temps pour compliquer l'analyse technique de l'attaque après sa détection.

---

70 Voir rapport semestriel 2024/1, chap. 7.2 pour en savoir plus sur BreachForums et le commerce des données.

71 Oracle denies breach after hacker claims theft of 6 million data records (bleepingcomputer.com)

72 Oracle attempt to hide serious cybersecurity incident from customers in Oracle SaaS service (doublepulsar.com)

73 CISA Releases Guidance on Credential Risks Associated with Potential Legacy Oracle Cloud Compromise (cisa.gov)

74 Plus de 100 000 employés d'UBS touchés par un vol massif de données sensibles, affectant aussi Pictet (letemps.ch)

75 Cyber-Attack Chain IQ Group AG (chainiq.com)

76 Cyberattacks pose security risks for all companies (chain iq.com)

World Leaks est un nouveau projet d'extorsion lancé par les opérateurs du groupe de rançongiciels *Hunters International*[77]. Contrairement à leur activité antérieure de rançongiciel, exercée en Suisse aussi[78], les escrocs prétendent exfiltrer avec *World Leaks* des données à des fins de chantage, renonçant à tout verrouillage des systèmes. Or, malgré ces allégations, la presse internationale s'est fait l'écho de victimes de *World Leaks* dont les données avaient été chiffrées avec un logiciel[79].

Les fuites de données peuvent également toucher des particuliers, dont les informations personnelles se retrouveront ensuite sur le *dark web*[80] ou le web profond[81]. Ces informations sont susceptibles d'aboutir à des réseaux criminels, si, par exemple, après un cyberincident ou une exposition par mégarde, les données de clients font l'objet d'une fuite, comme le montrent les deux incidents survenus au premier semestre 2025.

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.

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[82] ou sur Identity Leak Checker de l'Institut Hasso Plattner[83].

77 The beginning of the end: the story of Hunters International (group-ib.com)

78 Voir Cyberattaque contre la Caisse de compensation Swissmem: incident maîtrisé, conséquences tirées, parée pour l'avenir (ak-swissmem.ch)

79 World Leaks: An Extortion Platform (blog.lexfo.blog.fr)

80 *Web profond* (wikipedia.org), *dark web* (wikipedia.org)

81 Leaked: Politicians' emails and passwords on the dark web (proton.me) ; voir Quarante-quatre élus fédéraux victimes d'une fuite de données confidentielles (rts.ch)

82 Voir Have I Been Pwned (haveibeenpwned.com)

83 Voir Identity Leak Checker (sec.hpi.de)

8 Cyberespionnage et cybersabotage

Les acteurs étatiques ou proches de l'État représentent un type particulier de menace dans le cyberespace. Des groupes souvent désignés comme menaces persistantes avancées (*advanced persistent threat*, APT)[84] 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[85]. 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

Au deuxième semestre 2024, il avait déjà été question des attaques menées par l'APT chinoise présumée *Salt Typhoon* contre des opérateurs de télécommunication américains et européens[86]. En février 2025, une entreprise de sécurité a fait état des récentes activités déployées par cet acteur contre des appareils réseau de CISCO présentant des vulnérabilités[87]. Le mois suivant, des activités d'un autre groupe de cyberespionnage, suspecté lui aussi d'opérer pour le compte de la Chine, étaient détectées. Cette APT baptisée, elle, *Silk Typhoon* a été associée à plusieurs opérations internationales menées dans différents secteurs, à l'aide de méthodes aussi raffinées que les failles du jour zéro (*zero-day vulnerability*). Autre particularité, ce groupe s'en prend aux chaînes d'approvisionnement (*supply chain attack*) : *Silk Typhoon* a ainsi tenté de s'introduire dans des environnements clients en compromettant au préalable leurs prestataires informatiques[88].
Comme beaucoup d'APT, *Silk Typhoon* opère à l'aide de réseaux d'attaque constitués d'appareils soumis à son contrôle, soit les réseaux *ORB* (*operational relay boxes*)[89], dans lesquels la compromission d'appareils périphériques (*edge device*) exposés joue un rôle majeur. Ceux-ci sont par ailleurs des points d'entrée dans les réseaux des entreprises. Les exemples actuels

---

84 APT – Glossary (csrc.nist.gov)

85 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)

86 Voir rapport semestriel 2024/2, chap. 8.1.

87 RedMike (Salt Typhoon) Exploits Vulnerable Cisco Devices of Global Telecommunications Providers (recordedfuture.com)

88 Suspected China-Nexus Threat Actor Actively Exploiting Critical Ivanti Connect Secure Vulnerability (CVE-2025-22457) (cloud.google.com)

89 Voir rapport semestriel 2024/1, chap 8.1.2.

de compromissions concernent les pare-feu[90], les solutions d'accès à distance par VPN[91] et les routeurs[92].

L'APT appelée *Laundry Bear* est venue allonger la liste des groupes d'espionnage suspectés d'opérer pour la Russie. Les autorités néerlandaises[93] lui attribuent différentes cyberattaques contre diverses organisations basées dans le pays, dont la police nationale. Selon Microsoft, qui l'appelle *Void Blizzard*, ce groupe est actif depuis avril 2024 au moins et s'intéresse principalement à des cibles liées à l'OTAN et à l'Ukraine. D'autres groupes déjà établis et soupçonnés d'espionnage au profit de la Russie avaient déjà sévi en début d'année 2025. En mai par exemple, les autorités américaines ont accusé *APT28* de s'en prendre aux entreprises occidentales actives dans la logistique et les technologies, notamment à celles apportant leur soutien à l'Ukraine[94]. Les autorités françaises ont également attribué à cette APT les cyberattaques subies par plusieurs organisations[95]. Ces récents événements montrent que les pays occidentaux en particulier hésitent de moins en moins à désigner publiquement les États à l'origine de cyberattaques contre leurs intérêts nationaux. À la fin du mois de mai 2025, la République tchèque a ainsi attribué officiellement à la Chine une cyberattaque lancée contre son ministère des Affaires étrangères[96].

Contrairement à leurs homologues étrangers, les cyberacteurs soupçonnés de travailler au profit du régime nord-coréen ne se contentent pas d'espionnage, mais se consacreraient aussi à d'autres occupations lucratives, comme le vol de cryptomonnaies[97]. Dans le cadre de l'opération *Contagious Interview*, des acteurs probablement nord-coréens se sont à nouveau fait passer pour des recruteurs sur LinkedIn. Les candidats à leurs prétendus postes de développeurs de logiciels recevaient les tâches à accomplir sur leur propre ordinateur, dans un environnement non protégé. Or le code fourni renfermait des paquets malveillants, qui installaient un maliciel[98]. Une autre variante liée à *ClickFix* (voir chap. 3.1) faisait croire aux candidats qu'un logiciel ne fonctionnait pas, et donc qu'il leur fallait le télécharger[99]. Les collaborateurs informatiques suspectés d'opérer clandestinement pour le régime nord-coréen constituent un autre exemple typique. En plus de générer des devises pour financer leur gouvernement, ils soustraient des données à l'entreprise infiltrée à des fins d'espionnage, avant de lui réclamer

90 Console Chaos: A Campaign Targeting Publicly Exposed Management Interfaces on Fortinet FortiGate Firewalls (arcticwolf.com)

91 Ivanti Connect Secure VPN Targeted in New Zero-Day Exploitation (cloud.google.com), Suspected China-Nexus Threat Actor Actively Exploiting Critical Ivanti Connect Secure Vulnerability (CVE-2025-22457) (cloud.google.com)

92 Tracking AyySSHush: a Newly Discovered ASUS Router Botnet Campaign (censys.com)

93 Dutch intelligence unmasks previously unknown Russian hacking group 'Laundry Bear' (therecord.media)

94 Russian GRU Targeting Western Logistics Entities and Technology Companies (cisa.gov)

95 Russie – Attribution de cyberattaques contre la France au service de renseignement militaire russe (APT28) (29 avril 2025) (diplomatie.gouv.fr)

96 Czech Republic says China behind cyberattack on ministry, embassy rejects accusations (reuters.com)

97 Bybit loses nearly $1.5 billion in crypto hack – What we know so far (economictimes.indiatimes.com)

98 Another Wave: North Korean Contagious Interview Campaign Drops 35 New Malicious npm Packages (socket.dev)

99 Lazarus ClickFake Interview Campaign: From Contagious to ClickFix Malware Tactics (blog.sekoia.io)

une rançon[100]. Ces cas sont en augmentation en Europe, et sont aussi observés en Suisse[101]. Pour parvenir à leurs fins sans se faire repérer, les escrocs ont souvent besoin de l'aide sur place de personnes n'ayant pas pleinement conscience du rôle qu'on leur fait jouer. Ce phénomène, qui sévissait déjà aux États-Unis, tend à se déplacer vers les entreprises européennes, sans doute en raison de la vigilance accrue des autorités américaines et des mesures répressives adoptées contre ces campagnes d'espionnage.

Recommandations

Pour se prémunir contre ce type de menace, il faut agir à plusieurs niveaux, selon une stratégie de défense en profondeur[102]. 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 chaque cible. 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.

Les attaques de systèmes de contrôle industriel à des fins de sabotage interviennent surtout dans le contexte d'une escalade géopolitique, comme la guerre en Ukraine ou le conflit au Proche-Orient entre Israël et l'Iran à la mi-juin 2025. Outre les manipulations des systèmes,

[100] Voir rapport semestriel 2024/2, chap. 8.1.

[101] DPRK IT Workers Expanding in Scope and Scale (cloud.gloogle.com)

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

des maliciels destructeurs de données (*wiper*) sont désormais déployés pour rendre tous les fichiers inutilisables et empêcher ainsi le fonctionnement des systèmes d'approvisionnement ou de production. La campagne *PathWiper* lancée en juin 2025 contre les infrastructures critiques en Ukraine en est une illustration frappante[103]. En Suisse, aucun acte de sabotage impliquant des cyberacteurs étatiques n'a été observé à ce jour et un tel acte est considéré comme extrêmement improbable. Par contre, une attaque à l'étranger peut en tout temps engendrer des dégâts collatéraux dans notre pays[104].

Les tentatives de manipuler par opportunisme des systèmes de contrôle industriels insuffisamment protégés et exposés sur Internet sont toutefois bien plus fréquentes que ce genre d'attaques ciblées. Des groupes d'hacktivistes cherchent ainsi à attirer l'attention sur leur cause. Certains agissent pour des organismes d'État. Les pirates, dépourvus de solides compétences, se contentent d'intervenir dans le premier circuit auquel ils obtiennent l'accès. Leurs cibles ne sont donc généralement pas stratégiques, à l'instar du barrage régulateur d'une pisciculture[105] ou encore de microcentrales électriques de moulins[106].
Outre ces différents types d'attaques contre des systèmes, la surface d'attaque du paysage système ne cesse de s'étendre avec l'arrivée d'un grand nombre de nouveaux opérateurs, privés pour la plupart. L'essor de l'énergie solaire, et avec elle quantité de nouvelles installations solaires raccordées au réseau électrique, ont fait augmenter le nombre de systèmes pilotables. Or, bien des onduleurs, dispositifs-clés pour la connexion au réseau d'alimentation, présentent des vulnérabilités et donc des risques d'accès non autorisé[107]. Il faudra par conséquent accorder à la cybersécurité toute l'importance nécessaire afin de réduire l'exposition de ces nouveaux acteurs du réseau aux manipulations abusives.

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[108] de l'Information Security Society Switzerland (ISSS) fournissent une aide supplémentaire à cet égard.

103 Newly identified wiper malware "PathWiper" targets critical infrastructure in Ukraine (blog.talosintelligence.com)
104 « La sécurité de la Suisse 2025 » : la confrontation mondiale a des répercussions directes sur la Suisse (vbs.admin.ch)
105 Cyberattack on Norwegian Dam Highlights Password Exposure Risks (claroty.com)
106 Hacktivists Target France Over Diplomatic Moves (cyble.com)
107 SUNDOWN A Dark Side to Solar Energy Grids (forescout.com)
108 ISSS Operational Technology (OT) Empfehlungen (cybernavi.ch)