Rapport de renseignement

Revue mensuelle rétroactive des cybermenaces

SOC – Centre opérationnel de sécurité

Décembre 2023

Classification : TLP:CLEAR (https://www.first.org/tlp)

canton de vaud
LIBERTÉ ET PATRIE

Direction générale du numérique
et des systèmes d'information (DGNSI)

Décembre 2023, v1.0

Table des matières

Introduction

Ce rapport présente, de façon mensuelle, les actualités liées à la sécurité informatique que le Centre opérationnel de sécurité (SOC) de l'État de Vaud a estimé intéressantes. Il couvre à la fois des éléments internationaux et suisses, des incidents auxquels le SOC a dû répondre et les vulnérabilités qui ont été particulièrement médiatisées.

Le paysage global des menaces

Actualités internationales

Le mois de décembre s'est ouvert avec la publication d'une importante découverte en matière de sécurité informatique, nommée "LogoFAIL". LogoFAIL représente un ensemble de vulnérabilités de sécurité affectant diverses bibliothèques d'analyse d'images utilisées dans le firmware système par différents fournisseurs lors du processus de démarrage des appareils. Ces vulnérabilités présentes dans le code de référence des IBVs (Independent BIOS Vendor) ne concernent donc pas un seul fournisseur, mais impactent ainsi une multitude d'appareils basés sur l'architecture x86 et ARM. L'équipe de recherche de Binarly a découvert initialement LogoFAIL sur des appareils Lenovo avec des BIOS Insyde, AMI et Phoenix. Le danger de LogoFAIL réside dans le fait que les attaquants peuvent stocker des images de logo malveillantes soit sur la partition système EFI, soit dans des sections non signées d'une mise à jour du firmware. Lorsque ces images sont analysées au démarrage la vulnérabilité peut être déclenchée, permettant ainsi l'exécution d'une charge utile contrôlée par l'attaquant. Cela peut mener à une compromission profonde du système, rendant inefficaces les mesures de sécurité telles que le Secure Boot, y compris les mécanismes de démarrage vérifiés par le matériel comme Intel Boot Guard ou AMD Hardware-Validated Boot. Les détails techniques complets concernant les vulnérabilités LogoFAIL ont été présentés lors de la conférence Black Hat Europe le 6 décembre [1].

Dans son premier ensemble de mises à jour de sécurité pour le mois de décembre, Apple a corrigé deux vulnérabilités 0-day affectant WebKit (CVE-2023-42916 et CVE-2023-42917). La CVE-2023-42916 implique une lecture hors limites pouvant entraîner la divulgation d'informations sensibles, tandis que la CVE-2023-42917 permet l'exécution arbitraire de code via une corruption de mémoire. Ces failles, signalées par Clément Lecigne du Google TAG, affectent WebKit, le moteur de navigateur développé par Apple utilisé dans Safari ainsi que dans tous les navigateurs sur iOS et iPadOS. Bien que non confirmé par Apple, il est probable que ces vulnérabilités, comme pour les précédentes signalées par l'équipe TAG, aient été exploitées dans des logiciels d'espionnage (type Pegasus) pour des attaques ciblées [2]. Les correctifs pour ces vulnérabilités sont disponibles pour les utilisateurs d'iPhone, d'iPad et de Mac sous les versions récentes d'iOS, iPadOS et macOS [3], y compris un rétroportage des correctifs pour iOS et iPadOS 16.7.3, ainsi que pour tvOS 17.2 et watchOS 10.2.

Selon la plateforme de monitorage d'Internet Shadowservers [4] et la société Akamai [5], dans le courant de la troisième semaine du mois, des cybercriminels auraient commencé à exploiter activement une vulnérabilité critique récemment corrigée (CVE-2023-50164) dans Apache Struts, permettant l'exécution de code à distance en utilisant un code d'exploitation disponible publiquement [6]. Cette faille, touchant plusieurs versions de Struts, permet à un attaquant de téléverser des fichiers malveillants et d'accéder au serveur cible, ce qui peut entraîner des conséquences telles que l'accès non autorisé, le vol de données et la perturbation des services. Beaucoup de logiciels sont potentiellement impactés, et notamment Cisco qui enquête sur l'impact de cette vulnérabilité sur ses produits utilisant Apache Struts et devrait fournir des informations mises à jour sur les produits potentiellement affectés [7].

Dans un tweet, l'équipe "Threat Intelligence" de Microsoft [8] a averti sur le retour du malware Qbot, ciblant désormais l'industrie hôtelière via des campagnes de phishing. Après une interruption due à une opération des forces de l'ordre [9], Qbot réapparaît avec une nouvelle campagne se faisant passer pour des employés de l'IRS (une agence du gouvernement fédéral des États-Unis). Ce malware, initialement un cheval de Troie bancaire en 2008, est devenu un vecteur pour diverses menaces cybernétiques, y compris les ransomwares.

L'opération internationale, baptisée HAECHI IV, a conduit à l'arrestation d'environ 3'500 suspects et à la saisie d'environ 300 millions de dollars d'actifs. Interpol a annoncé le 19 décembre [10] que cette opération, menée de juillet à décembre 2023, ciblait des organisations impliquées dans sept types d'arnaques en ligne : l'usurpation d'identité d'entreprise, la fraude en ligne, l'escroquerie à l'investissement, le hameçonnage vocal, le blanchiment d'argent lié aux jeux d'argent en ligne illégaux, les escroqueries aux sentiments et les chantages en ligne. Les enquêteurs ont utilisé le système

d'intervention rapide d'Interpol pour détecter les transactions frauduleuses en ligne, puis ont gelé les comptes bancaires et de fournisseurs de services d'actifs virtuels associés. L'opération a permis de bloquer 367 comptes d'actifs en cryptomonnaies liés à des réseaux de cybercriminels internationaux, avec la collaboration de plusieurs fournisseurs de services d'actifs virtuels. Selon Interpol, les autorités philippines et coréennes ont également saisi 199 millions de dollars en devises physiques et 101 millions de dollars en actifs lors d'une opération conjointe contre un important criminel du jeu en ligne à Manille. L'opération HAECHI IV a principalement ciblé la fraude à l'investissement, l'usurpation d'identité d'entreprise et la fraude en ligne. De plus, deux « Purple Notices » ont été émises pour avertir les pays de nouvelles techniques de fraude numérique, notamment la vente trompeuse de jetons non fongibles (NFT) et l'utilisation de l'intelligence artificielle et des « deepfakes » pour des escroqueries sophistiquées.

Le 19 décembre, le Département de la Justice des États-Unis a fait une annonce majeure [11]: le FBI a saisi le site Tor utilisé pour publier des données volées par AlphV/Blackcat, un groupe de rançongiciel notoire actif depuis novembre 2021. Ce groupe est connu pour ses attaques contre des entreprises de renom comme Swissport, NCR et Western Digital, exigeant des rançons allant de quelques dizaines de milliers à plusieurs millions de dollars. Cette saisie est le fruit d'une opération collaborative impliquant plusieurs agences internationales. Dans l'opération, le FBI a récupéré 946 paires de clés publiques/privées utilisées par AlphV/Blackcat, permettant ainsi à plus de 500 victimes de restaurer l'accès à leurs systèmes sans frais. Cette intervention a potentiellement épargné environ 68 millions de dollars en paiements de rançons. Cependant, le groupe a rapidement rebondi, établissant un nouveau site et clamant que les autorités n'avaient intercepté qu'une partie de leurs clés de déchiffrement. Ils ont également annoncé de nouvelles règles pour leurs affiliés, autorisant dorénavant les attaques contre toute infrastructure critique et les hôpitaux [12].

Le 20 décembre Ivanti a publié des correctifs pour 13 vulnérabilités critiques dans sa solution de gestion des appareils Avalanche [13]. Ces failles, similaires à celles exploitées dans des attaques contre les systèmes informatiques de plusieurs ministères norvégiens et la police de Berne, permettaient des exécutions de code à distance sans interaction de l'utilisateur [14]. La mise à jour vers la version 6.4.2 d'Avalanche est recommandée pour sécuriser les systèmes.

L'attaque nommée "Terrapin", identifié sous le CVE-2023-48795 et publié en décembre, est une attaque sophistiquée qui cible le protocole SSH largement utilisé pour des communications sécurisées sur Internet. Découverte par des chercheurs de l'Université Ruhr de Bochum, cette attaque manipule les numéros de séquence pendant le processus initial de "handshake" du protocole SSH, compromettant ainsi l'intégrité du canal de communication. L'attaque est particulièrement efficace contre certaines configurations de chiffrement utilisées dans OpenSSH 9.5, ce qui permet aux attaquants de dégrader les algorithmes de clés publiques. Le principal mécanisme de l'attaque Terrapin implique l'exploitation de vulnérabilités dans le protocole de transport SSH. En manipulant les numéros de séquence pendant le processus de "handshake", les attaquants peuvent altérer les messages échangés, ce qui permet de tronquer des messages de négociation critiques sans n'être détecté ni par le client ni par le serveur. L'impact de l'attaque dépend de la nature des données échangées. L'attaque Terrapin a été identifiée sous trois vulnérabilités distinctes : CVE-2023-48795, CVE-2023-46445 et CVE-2023-46446. Ces identifiants aident à comprendre et à résoudre les vulnérabilités liées à l'attaque. L'équipe de recherche a également publié un scanner de vulnérabilité Terrapin sur GitHub [15], permettant aux administrateurs de détecter si un client ou un serveur SSH est vulnérable à cette attaque. Pour réussir, l'attaque nécessite que l'attaquant se positionne en tant qu'adversaire au milieu du réseau (adversary-in-the-middle, MiTM) pour intercepter et altérer l'échange de poignée de main. Malgré ces exigences spécifiques, l'attaque est réalisable dans des conditions réelles en raison du déploiement répandu des techniques de chiffrement concernées. Des solutions sont en cours d'élaboration pour atténuer les implications de sécurité de l'attaque Terrapin. Une solution proposée implique la mise en œuvre d'un échange de clés strict, rendant l'injection de paquets impossible. Cependant, il est important de noter que l'efficacité de cette contre-mesure dépend de sa mise en œuvre à la fois côté client et serveur. La recherche sur cette attaque a été publiée le 19 décembre 2023, et elle a suscité des discussions importantes dans la communauté sur son impact potentiel. Étant donné que le SSH est un protocole largement utilisé pour des communications sécurisées, cette vulnérabilité représente une menace significative pour de nombreux systèmes et réseaux à travers le monde.

Actualités suisses

La ville de Baden a récemment été victime d'une cyberattaque majeure, résultant en la fuite de données sensibles sur le Darknet. Un article de la NZZ publié le 4 décembre 2023 [16] décrit en détail l'ampleur de cet incident. Les cybercriminels ont mis en ligne 3 Go de données comprenant des adresses, des informations financières, des factures, et des listes de crémations, révélant ainsi une brèche de sécurité significative dans l'infrastructure informatique de la ville. Parmi les données divulguées, on trouve des tables comprenant plus de 24'000 noms et adresses d'habitants, des parties du budget municipal de 2013 à 2023, ainsi que d'autres informations sensibles. Bien que la base de données complète n'ait pas été récupérée, les fragments disponibles soulèvent des préoccupations quant à la sécurité des données personnelles des citoyens. La nature exacte et l'étendue des données détenues par les hackers restent incertaines. La ville a pris des mesures de sécurité renforcées, mais l'identité et les motivations des assaillants demeurent inconnues.

Le 21 juillet 2023, le Centre national de cybersécurité (NCSC) avait révélé une faille de sécurité dans l'appliance MobileIron du développeur Ivanti, utilisée par la Police cantonale bernoise. Des mesures d'urgence ont été prises pour colmater la faille après la découverte d'une fuite de données touchant les utilisateurs du système. Dans le courant du mois de décembre, une enquête dirigée par le Ministère public bernois a permis d'identifier des individus ayant exploité la faille, conduisant à des perquisitions dans les cantons de Fribourg, Genève et Vaud, avec trois personnes appréhendées. Quatre autres personnes ont été identifiées et interrogées. Les autorités ont réussi à clarifier tous les accès non autorisés à la banque de données, et aucune transmission de données à des tiers n'a été constatée jusqu'à présent. Il est présumé que d'autres entreprises ont également été affectées par cette faille de sécurité [17], [18].

La décision du Conseil fédéral suisse de rattacher le nouvel Office fédéral de la cybersécurité (OFCS) au Département de la défense plutôt qu'au Département des finances suscite des tensions, selon un rapport de la télévision alémanique SRF. Depuis cette annonce, 10 collaborateurs du Centre national de cybersécurité (NCSC) ont démissionné, représentant 20% de l'effectif total, notamment au sein de l'équipe GovCERT intervenant en cas d'urgence informatique. Les départs sont attribués à des préoccupations liées à la proximité future avec le service de renseignement, créant un possible conflit d'intérêts. Le directeur du NCSC, Florian Schütz, assure que l'OFCS priorisera les intérêts de l'économie, de la société et des autorités, tout en soulignant la conformité avec la séparation légale des domaines de la cybersécurité. Malgré des tentatives de remplacement partiel, la perte de collaborateurs expérimentés a entamé la confiance envers la Confédération, soulignant la nécessité de la restaurer [19].

Le Gouvernement du Jura a validé sa nouvelle stratégie de cybersécurité. Le Canton souhaite impliquer dans la réflexion l'ensemble des institutions publiques, mais également les grands acteurs privés. Il s'agit de prendre en compte les menaces liées à la profonde et rapide mutation numérique, mais également celles qui concernent la protection des données sensibles. La stratégie vise à identifier les menaces et améliorer la maturité de l'ensemble des acteurs en matière de cybersécurité. Elle prévoit aussi la mise en œuvre de processus coordonnés sur le plan cantonal basés sur 5 piliers allant de la prévention à la restauration de données [20], [21].

Dans le contexte des cyberattaques ciblant le secteur financier suisse, un événement notable a eu lieu en décembre. Le Swiss Financial Sector Cyber Security Centre a annoncé un grand succès pour le premier exercice cyberopérationnel dans le secteur financier suisse [22]. Cet exercice a réuni environ 100 spécialistes en cybersécurité de banques et d'assurances ainsi que des partenaires. Il a été conçu pour simuler une panne majeure d'un fournisseur tiers, affectant de nombreux établissements financiers en Suisse. Les participants ont discuté des aspects opérationnels de la réaction à une cybercrise potentielle et la deuxième partie de l'exercice s'est concentrée sur le rôle opérationnel du Swiss FS-CSC, y compris ses procédures pour collecter, analyser et transmettre des informations aux membres. Ce cyberexercice a été perçu comme un pas important vers le renforcement de la cyberrésilience du secteur financier suisse.

Incidents et activités externes et/ou globaux

Abusix, une entreprise spécialisée en sécurité informatique, fournit des solutions de lutte contre le spam et de gestion des abus sur les réseaux, principalement destinées aux fournisseurs de services Internet, de télécommunications et d'hébergement. Depuis deux ans, Swisscom a confié à Abusix la responsabilité de gérer les signalements d'abus reçus [23]. Étant donné que les plages d'adresses publiques du Réseau Cantonal Vaudois dépendent de Swisscom, nos services sont fréquemment contactés pour traiter des signalements d'activité malveillante (« abuse report ») émanant de ces adresses. Ces dernières, utilisées par une multitude de directions et de services institutionnels, constituent les points de sortie pour la navigation internet et les courriels de milliers d'utilisateurs. Au cours du mois de décembre, nous avons examiné plusieurs de ces signalements. Parmi eux, l'un concernait des courriels non sollicités envoyés par une institution de santé, tandis qu'un autre impliquait une adresse émanant d'une institution éducative. Dans le premier cas, après vérification, il s'est avéré que le message incriminé était en réalité une communication d'information de masse légitime. Quant au second cas, il concernait une ancienne adresse, désormais supprimée, qui avait été piratée et utilisée à des fins de spam.

Vulnérabilités les plus médiatisées du mois

Ce tableau dresse une liste non exhaustive des failles fortement relayées par les médias durant le mois. L'application régulière des mises à jour en cas de composant vulnérable est l'une des protections les plus importantes contre les cyberattaques.

Identifiant	Informations
Terrapin CVE-2023-48795	La publication par des chercheurs universitaires de la vulnérabilité "Terrapin-Attack" [24] dans le protocole SSH, référencée sous le CVE-2023-48795, a suscité d'intenses débats dans la communauté de la cybersécurité sur ses implications théoriques et pratiques [25]. Cette faille permet à un attaquant, dans le rôle d'un intercepteur actif (Man-In-The-Middle, MITM), d'affaiblir le processus de sélection des algorithmes utilisés pendant l'authentification. En pratique, cela signifie que l'attaquant peut forcer l'utilisation d'un algorithme plus faible ou compromis, facilitant potentiellement le déchiffrement ou la manipulation des données transmises. Cependant, pour exploiter cette vulnérabilité, l'attaquant doit déjà être en position de pouvoir intercepter et modifier le trafic entre le client et le serveur SSH, ce qui limite son applicabilité à des scénarios où cette condition préalable est remplie. Néanmoins, cette vulnérabilité souligne l'importance de la vigilance et de la mise à jour régulière des systèmes pour protéger contre de telles faiblesses dans des protocoles de sécurité critiques comme SSH.
CVE-2023-45866	La vulnérabilité CVE-2023-45866 a fait l'objet d'une attention médiatique significative en raison de son large potentiel d'exploitation [26] et de son rôle dans de possibles scénarios d'attaques ciblées. Il s'agit d'une faille critique affectant les implémentations du protocole Bluetooth dans divers systèmes d'exploitation, notamment macOS, iOS, Android et Linux. Elle permet à un attaquant non authentifié d'injecter des frappes de clavier sur un appareil vulnérable, contournant ainsi la nécessité d'une confirmation de l'utilisateur pour se connecter à l'appareil. Cette vulnérabilité est préoccupante, car elle peut être exploitée sans matériel spécialisé, nécessitant seulement que l'attaquant soit à portée Bluetooth de l'appareil cible. Les systèmes affectés incluent macOS (versions Monterey 12.6.7 et Ventura 13.3.3), iOS (version 16.6), Android (versions 4.2.2, 6.0.1, 10, 11, 13, 14) et le noyau Linux avec BlueZ. Apple a publié des correctifs pour iOS, iPadOS et macOS [27], tandis que des correctifs pour Android sont disponibles pour les versions 11 à 14 et ont été envoyés aux fabricants de smartphones et de tablettes. Pour les dispositifs Linux utilisant la pile Bluetooth BlueZ, un correctif est également disponible [28].

Sources

Cette section fournit les sources d'informations utilisées pour la rédaction du contenu de ce rapport.

[1] « The Far-Reaching Consequences of LogoFAIL | Binarly – AI -Powered Firmware Supply Chain Security Platform », https://binarly.io/. Consulté le: 9 janvier 2024. [En ligne]. Disponible sur: https://binarly.io/

[2] Z. Zorz, « Apple patches two zero-days used to target iOS users (CVE-2023-42916 CVE-2023-42917) », Help Net Security. Consulté le: 9 janvier 2024. [En ligne]. Disponible sur: https://www.helpnetsecurity.com/2023/12/01/cve-2023-42916-cve-2023-42917/

[3] « À propos des correctifs de sécurité d'iOS 17.1.2 et d'iPadOS 17.1.2 », Apple Support. Consulté le: 9 janvier 2024. [En ligne]. Disponible sur: https://support.apple.com/fr-fr/HT214031

[4] « Shadowserver sur X : "We have started to see attempts to use PoC exploit code published for Apache Struts CVE-2023-50164 CVSS 9.8 RCE in our sensors (a few src IPs). Make sure to update your Struts installs ... Apache Security Bulletin: https://t.co/iVAinVdl7M NVD entry: https://t.co/oHoHGlcyu7" / X », X (formerly Twitter). Consulté le: 10 janvier 2024. [En ligne]. Disponible sur: https://twitter.com/Shadowserver/status/1734919288257974380

[5] « Observed Exploitation Attempts of Struts 2 S2-066 Vulnerability (CVE-2023-50164) », Akamai. Consulté le: 9 janvier 2024. [En ligne]. Disponible sur: https://www.akamai.com/blog/security-research/apache-struts-cve-exploitation-attempts

[6] D. Siswanto, « dwisiswant0/cve-2023-50164-poc ». 4 janvier 2024. Consulté le: 10 janvier 2024. [En ligne]. Disponible sur: https://github.com/dwisiswant0/cve-2023-50164-poc

[7] « Hackers are exploiting critical Apache Struts flaw using public PoC », BleepingComputer. Consulté le: 10 janvier 2024. [En ligne]. Disponible sur: https://www.bleepingcomputer.com/news/security/hackers-are-exploiting-critical-apache-struts-flaw-using-public-poc/

[8] « Microsoft Threat Intelligence sur X : "Microsoft has identified new Qakbot phishing campaigns following the August 2023 law enforcement disruption operation. The campaign began on December 11, was low in volume, and targeted the hospitality industry. Targets received a PDF from a user masquerading as an IRS employee. https://t.co/oYTq9kjrrq" / X », X (formerly Twitter). Consulté le: 10 janvier 2024. [En ligne]. Disponible sur: https://twitter.com/MsftSecIntel/status/1735856754427047985

[9] « Qbot malware returns in campaign targeting hospitality industry », BleepingComputer. Consulté le: 10 janvier 2024. [En ligne]. Disponible sur: https://www.bleepingcomputer.com/news/security/qbot-malware-returns-in-campaign-targeting-hospitality-industry/

[10] « USD 300 million seized and 3,500 suspects arrested in international financial crime operation ». Consulté le: 10 janvier 2024. [En ligne]. Disponible sur: https://www.interpol.int/News-and-Events/News/2023/USD-300-million-seized-and-3-500-suspects-arrested-in-international-financial-crime-operation

[11] « Office of Public Affairs | Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant | United States Department of Justice ». Consulté le: 9 janvier 2024. [En ligne]. Disponible sur: https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant

[12] P. Paganini, « FBI claims to have dismantled AlphV/Blackcat ransomware operation, but the group denies it », Security Affairs. Consulté le: 9 janvier 2024. [En ligne]. Disponible sur: https://securityaffairs.com/156124/breaking-news/alphv-blackcat-ransomware-group-seizure.html

[13] « New Ivanti Avalanche Vulnerabilities | Ivanti ». Consulté le: 10 janvier 2024. [En ligne]. Disponible sur: https://www.ivanti.com/blog/new-ivanti-avalanche-vulnerabilities

[14] « Ivanti releases patches for 13 critical Avalanche RCE flaws », BleepingComputer. Consulté le: 10 janvier 2024. [En ligne]. Disponible sur: https://www.bleepingcomputer.com/news/security/ivanti-releases-patches-for-13-critical-avalanche-rce-flaws/

[15] « Release v1.1.2 · RUB-NDS/Terrapin-Scanner », GitHub. Consulté le: 10 janvier 2024. [En ligne]. Disponible sur: https://github.com/RUB-NDS/Terrapin-Scanner/releases/tag/v1.1.2

[16] S. Huwiler, « Adressen und Finanzdaten – Baden ist von Hackern angegriffen worden », *Neue Zürcher Zeitung*, 4 décembre 2023. Consulté le: 9 janvier 2024. [En ligne]. Disponible sur: https://www.nzz.ch/zuerich/hackerangriff-auf-baden-sensitive-daten-von-buergerinnen-und-buerger-sind-im-darkweb-zu-finden-ld.1768723

[17] « Canton de Berne: Suite à une faille de sécurité dans un système informatique: plusieurs personnes prévenues identifiées et perquisitions effectuées », q. Consulté le: 5 janvier 2024. [En ligne]. Disponible sur: https://www.police.be.ch/fr/start/themen/news/medienmitteilungen.html
[18] www rjb ch Bernois RJB, Radio Jura, « La police bernoise arrête sept personnes dans l'affaire de vol de données ». Consulté le: 5 janvier 2024. [En ligne]. Disponible sur: https://www.rjb.ch/rjb/Actualite/Region/20231206-La-police-bernoise-arrete-sept-personnes-dans-l-affaire-de-vol-de-donnees.html
[19] « Un employé du NCSC sur cinq a démissionné en 2023 ». Consulté le: 5 janvier 2024. [En ligne]. Disponible sur: https://www.ictjournal.ch/news/2023-12-07/un-employe-du-ncsc-sur-cinq-a-demissionne-en-2023
[20] www jura ch Jura République et Canton du, « Stratégie cantonale de cybersécurité ». Consulté le: 5 janvier 2024. [En ligne]. Disponible sur: https://www.jura.ch/CHA/SIC/Centre-medias/Communiques-2023/Strategie-cantonale-de-cybersecurite.html
[21] M. Barbezat, « Le canton du Jura a validé sa première stratégie de cybersécurité • Cybersécurité OSINT », Cybersécurité OSINT. Consulté le: 5 janvier 2024. [En ligne]. Disponible sur: https://www.ledecodeur.ch/2023/12/27/le-canton-du-jura-a-valide-sa-premiere-strategie-de-cybersecurite/
[22] « Premier exercice cyber opérationnel sur la place financière suisse - Swiss Financial Sector Cyber Security Centre ». Consulté le: 9 janvier 2024. [En ligne]. Disponible sur: https://fscsc.ch/fr/news/premier-exercice-cyber-operationnel-sur-la-place-financiere-suisse/
[23] T. Hurtmann, « Swisscom Uses Abusix To Protect Their Network Against Email-Borne Threats », Abusix. Consulté le: 9 janvier 2024. [En ligne]. Disponible sur: https://abusix.com/swisscom-uses-abusixs-full-suite-of-products-for-protection-against-email-borne-threats-and-full-visibility-within-its-network/
[24] « Terrapin Attack ». Consulté le: 9 janvier 2024. [En ligne]. Disponible sur: https://terrapin-attack.com/
[25] D. Goodin, « SSH protects the world's most sensitive networks. It just got a lot weaker », Ars Technica. Consulté le: 9 janvier 2024. [En ligne]. Disponible sur: https://arstechnica.com/security/2023/12/hackers-can-break-ssh-channel-integrity-using-novel-data-corruption-attack/
[26] « Une faille bluetooth expose des millons de systèmes Android, Linux et MacOS/iOS - Le Monde Informatique », LeMondeInformatique. Consulté le: 9 janvier 2024. [En ligne]. Disponible sur: https://www.lemondeinformatique.fr/actualites/lire-une-faille-bluetooth-expose-des-millons-de-systemes-android-linux-et-macos-ios-92384.html
[27] « À propos des correctifs de sécurité d'iOS 17.2 et d'iPadOS 17.2 », Apple Support. Consulté le: 9 janvier 2024. [En ligne]. Disponible sur: https://support.apple.com/fr-ch/HT214035
[28] « CVE-2023-45866- Red Hat Customer Portal ». Consulté le: 9 janvier 2024. [En ligne]. Disponible sur: https://access.redhat.com/security/cve/cve-2023-45866