Rapport de renseignement

Revue mensuelle rétroactive des cybermenaces

SOC – Centre opérationnel de sécurité

canton de vaud
LIBERTÉ ET PATRIE

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

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

Du point de vue de l'état de la menace, le mois d'octobre a débuté avec une tendance déjà observée les mois précédents, caractérisée par l'exploitation rapide des failles par les cybercriminels, particulièrement dans le contexte des attaques par rançongiciel. En effet, le 2 octobre, une vulnérabilité affectant le logiciel WS_FTP a été remarquée pour son exploitation rapide sur Internet. Des alertes urgentes ont été lancées à de grandes entreprises, y compris des organisations gouvernementales et éducatives, pour mettre à jour immédiatement leur logiciel FTP, WS_FTP, en raison d'attaques actives. La firme australienne de cybersécurité Assetnote, qui a découvert cette faille, a noté que près de 2 900 hôtes utilisant WS_FTP étaient vulnérables sur Internet, appartenant principalement à de grandes entreprises et institutions. Progress Software a corrigé huit failles et recommande vivement la mise à jour. Le défaut de désérialisation .NET, particulièrement facile à exploiter, a été activement ciblé peu après la divulgation d'un code d'exploitation [1].

Il est à noter que l'exploitation massive du logiciel MOVEit, un outil de transfert de fichiers de la même société Progress Software, s'est établie comme le plus important piratage de l'année en cours. En effet, l'attaque sur MOVEit a dépassé le millier de victimes organisationnelles et affecté plus de 60 millions d'individus, se distinguant comme l'une des plus grandes failles sécuritaires récentes. Pour rappel, parmi les victimes du piratage MOVEit, on retrouve des entités majeures telles que le géant américain des services gouvernementaux Maximus, qui a confirmé l'accès non autorisé aux informations de santé protégées, y compris les numéros de sécurité sociale, de près de 11 millions d'individus. En France, Pôle emploi, l'agence nationale pour l'emploi, a été la deuxième plus grande victime identifiée, avec une violation de données personnelles touchant potentiellement jusqu'à 10 millions de personnes [2]. Progress Software, est depuis confrontée à de multiples poursuites judiciaires et une enquête de la SEC américaine, a révélé des coûts significatifs et des répercussions continues, avec des organisations signalant encore des brèches des mois après l'incident initial [3].

Les gangs de cybercriminalité déploient désormais des ransomwares dans les 24 heures suivant le piratage de leurs victimes, marquant une diminution significative par rapport au temps de préparation moyen de 4,5 jours observé l'année dernière. Selon un nouveau rapport de la société de cybersécurité Secureworks, l'année 2023 pourrait enregistrer un nombre record d'attaques par ransomware, avec trois fois plus de victimes répertoriées sur les sites de publication en mai que lors du même mois l'année précédente. Ces sites de publication des données exfiltrées, bien qu'imparfaits pour évaluer l'ampleur du problème des ransomwares, indiquent néanmoins que les extorsions de données et les ransomwares restent un modèle commercial criminel viable et une menace substantielle pour les entreprises. Secureworks révèle que dans plus de 50 % des cas traités par son service de réponse aux incidents, les attaquants ont réussi à exécuter leur malware en seulement 24 heures après avoir infiltré le réseau informatique de la victime. La durée médiane avant le déploiement du ransomware a chuté, et dans 10 % des cas, le ransomware a été déployé en seulement cinq heures après l'accès initial. Cette réduction du temps de préparation est probablement due à la volonté des cybercriminels de réduire les chances de détection, car l'industrie de la cybersécurité est devenue plus compétente pour détecter les activités précurseurs des ransomwares [4].

Intéressant dans ce contexte, l'étude réalisée à partir de centaines de conversations de négociation fuitées et rassemblées dans la base de données du projet Ransomchat [5], mis en place par le journaliste Valéry Rieß-Marchive, qui offre un aperçu des stratégies de négociation face à ces menaces. Analysées par l'équipe SEC4U, ces discussions révèlent l'existence de trois approches de négociations - compétitive, coopérative et intégrative - chacune avec ses tactiques [6]. L'importance est accordée à la gestion calme de la situation, à la communication professionnelle et sécurisée, et à l'évaluation des preuves de déchiffrement fournies par les cybercriminels, offrant ainsi des options stratégiques aux organisations pour répondre efficacement aux attaques sans céder aux demandes de rançon.

Concernant l'évolution des techniques d'attaque, il est important de souligner l'émergence en octobre de nouvelles méthodes exploitant les chatbots alimenté par l'intelligence artificielle, comme illustré par l'incident impliquant « Bing Chat » de Microsoft. Peu après son lancement en mars, des publicités ont été injectées dans les réponses de « Bing Chat », qui, selon Malwarebytes [7], sont utilisées pour du "malvertising", une méthode consistant à propager des logiciels

malveillants via des publicités en ligne. Les escrocs insèrent de fausses publicités plus visibles que les véritables annonces, redirigeant les victimes vers des sites frauduleux où elles sont encouragées à télécharger des logiciels malveillants [8].

La mise à jour de l'utilitaire en ligne de commande curl 8.4.0, publiée le 11 octobre, a suscité beaucoup d'attente ayant été annoncée à l'avance par le seul développeur [9] en charge de ce projet omniprésent [10] notamment dans les systèmes et objets connecté à base Unix/Linux. Cette annonce est, donc, considérée d'une importance majeure en raison de son impact sur de nombreuses applications libres et commerciales qui intègrent cette solution open source. Cette mise à jour corrige notamment la vulnérabilité critique CVE-2023-38545 liée au débordement de tampon avec SOCKS5 et la faille CVE-2023-38546 de moindre gravité, mais non négligeable liée à l'injection de cookies [11].

Une nouvelle technique de DDoS nommée "HTTP/2 Rapid Reset" a été exploitée, abusant d'une vulnérabilité zero-day dans le protocole HTTP/2, entraînant des attaques records. Les entreprises comme Amazon, Cloudflare et Google ont signalé avoir atténué des attaques massives, Google ayant fait face à une attaque de 398 millions de requêtes par seconde. La vulnérabilité "HTTP/2 Rapid Reset", identifiée sous le CVE-2023-44487, représente une nouvelle menace sérieuse pour la stabilité du Web en permettant des attaques DDoS d'une ampleur sans précédent [12]. Ce vecteur d'attaque exploite la fonctionnalité d'annulation de flux du protocole HTTP/2 pour envoyer et annuler continuellement des requêtes, submergeant les serveurs cibles. La correction de cette vulnérabilité nécessite donc la mise à jour de presque tous les serveurs web, un processus qui est complexe et peut laisser certains serveurs exposés sur le long terme [13].

Le 16 octobre, un bulletin de sécurité de la plus haute importance a été publié par Cisco [14], révélant l'existence d'une vulnérabilité critique au sein de leur système d'exploitation IOS X. Cette annonce intervient à la suite de plusieurs jours d'exploitation malveillante, qui a vu, jusqu'au 19 octobre, environ 36 541 appareils Cisco compromis, selon les données fournies par l'entreprise spécialisée en cybersécurité Censys [15]. La vulnérabilité en question est le produit d'une combinaison de deux failles distinctes, identifiées sous les noms de CVE-2023-20198 et CVE-2023-20273. La première a été utilisée pour obtenir un accès non autorisé aux systèmes tandis que la seconde a permis aux attaquants d'augmenter leurs privilèges et de prendre le contrôle complet des appareils affectés [16]. Cisco a réagi en affirmant avoir élaboré des correctifs pour ces vulnérabilités, avec une mise à disposition prévue pour le 22 octobre. En attendant, la firme conseille de désactiver le serveur HTTP sur les systèmes vulnérables ou, si cela n'est pas possible, de restreindre l'accès au serveur à des adresses de confiance uniquement. Il est important de noter que suivant la première annonce de Cisco, la mise à jour des systèmes n'était pas suffisante pour garantir la sécurité ; une vigilance accrue est nécessaire pour détecter toute activité suspecte telle que la création de nouveaux comptes administrateurs ou l'implantation de webshells, qui pourraient indiquer une compromission à la suite de cette série d'attaques.

Okta, la compagnie américaine spécialisée dans la gestion des identités et des accès, a révélé le 20 octobre un incident de sécurité critique [17]. Des acteurs malveillants ont exploité une vulnérabilité dans le système de gestion des cas de support, accédant ainsi aux fichiers de certains clients. Ce problème, affectant une minorité de clients (1% des 18 400 selon le communiqué officiel), a suscité une vive inquiétude, particulièrement à cause des fichiers HAR qui contiennent des informations sensibles telles que des cookies et des jetons de session. Bien que le service principal d'Okta soit resté sécurisé et fonctionnel, des entreprises telles que BeyondTrust, Cloudflare [18] et 1Password [19] ont été impactées. Cependant, les sociétés en question ont réagi promptement, détectant la menace et évitant tout dommage pour leurs clients selon leur communiqué respectif sur l'incident.

Deux bonnes nouvelles sur le front des cybermenaces sont tombées en fin de mois : les infrastructures de deux organisations criminelles spécialisées dans le ransomware ont été démantelées. D'abord, le groupe Trigona a subi une attaque majeure de la part de l'Ukrainian Cyber Alliance, perdant le contenu de leurs serveurs, leurs sauvegardes, et même leurs comptes en cryptomonnaies, à la suite d'une vulnérabilité exploitée dans le serveur Atlassian Confluence [20]. Ensuite, Europol a confirmé le 20 octobre le succès d'une opération conjointe entre plusieurs pays contre le groupe de cybercriminels Ragnar Locker [21]. Un membre russe du gang Ragnar Locker, responsable de multiples cyberattaques par ransomware, a été arrêté en France [22], marquant une victoire significative pour les autorités européennes et internationales dans la lutte contre la cybercriminalité.

Actualités suisses

Une note positive quant à la protection contre les menaces en Suisse : Trust Valley a récemment lancé un guide complet pour les PME [23], cherchant à renforcer leur résilience face aux cyberattaques. Dans un contexte où les PME suisses sont souvent ciblées par de telles attaques, ce guide représente une initiative opportune. Il offre un recueil de bonnes pratiques en cybersécurité et confiance numérique, structuré en huit sections et basé sur une collaboration étroite avec le Canton de Vaud et le soutien du Centre National pour la Cybersécurité. Ce programme, nommé Trust4SMEs, fournit des diagnostics, des formations et des conseils personnalisés pour améliorer la compréhension et la gestion des risques numériques [24].

Le projet de modernisation informatique des polices cantonale et municipales vaudoises, nommé «Odyssée», est actuellement en suspens en raison du retard causé par la cyberattaque subie par le prestataire Xplain, choisi pour remplacer trois applications obsolètes. Xplain avait remporté l'appel d'offres en 2018 avec sa solution «Polaris». Les données opérationnelles sensibles de Fedpol et des douanes suisses, dérobées lors de la récente attaque, ont été publiées sur le darknet. Les autorités vaudoises avaient alloué un budget de 21 millions de francs au projet, mais des inquiétudes concernant la faillite potentielle de Xplain et les risques financiers émergent parmi les élus du Grand Conseil. [25]

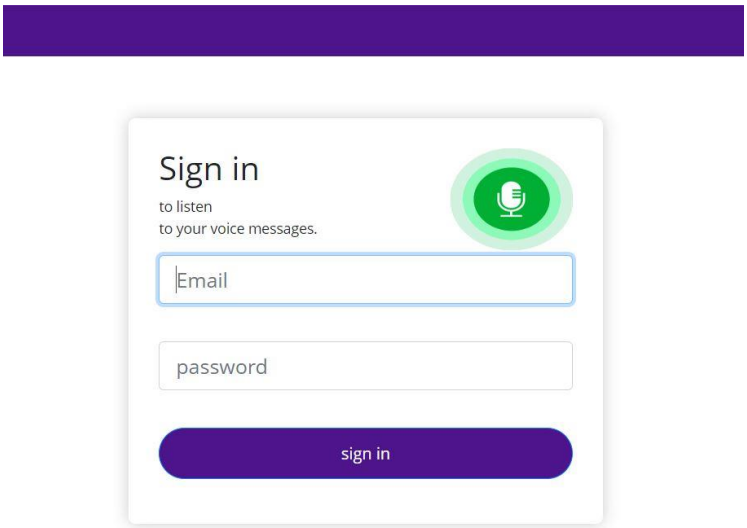
Le parlement fribourgeois a voté à l'unanimité en faveur d'une nouvelle Loi sur la protection des données, remplaçant un texte datant de 1994. Inspirée de la LPD fédérale en vigueur depuis septembre, la nouvelle loi conserve la couverture des personnes morales, contrairement à la loi fédérale. Elle renforce les droits individuels face à la multiplication des traitements, impose des obligations de transparence aux organismes publics, notamment en ce qui concerne les décisions basées sur des algorithmes, et propose des outils pour améliorer la sécurité des infrastructures et des processus liés aux données personnelles. Un délai d'adaptation de deux ans est prévu avec l'aide de l'Association des communes fribourgeoises. [26]

Principales observations et interventions du SOC

Au cours du mois d'octobre, de multiples tentatives d'hameçonnage imitant l'identité et le site de la police cantonale ont été signalées à nos services. Ces attaques ont été activement interceptées, mais leur nature persistante et leur simplicité délibérée représentent des défis pour les systèmes de filtrage. La campagne se distingue par l'utilisation massive d'adresses e-mails renouvelées fréquemment, notamment via les fournisseurs Bluewin et Gmail, ce qui entrave la mise en place de blocages préventifs efficaces. L'apparence de communication officielle par ces e-mails crée un faux sentiment d'autorité qui attire l'attention des destinataires.

La réactivité de nos utilisateurs est encourageante, avec de nombreux signalements effectués grâce au bouton de notification dédié. Ces actions permettent une identification et une neutralisation rapides de ces tentatives de fraude. Des mesures ont été prises pour informer les collègues de la Police ainsi que pour supprimer les diverses itérations de cette campagne malveillante.

Toujours dans le cadre de notre analyse des soumissions d'e-mails, en debout du mois, nous avons identifié et neutralisé une campagne de phishing qui usurpait le nom vd.ch. La particularité de cette campagne résidait dans la proposition aux destinataires de compléter un formulaire avec les informations de connexion professionnelles afin d'accéder à une prétendue messagerie vocale.



Note sympathique, cette campagne a été aussi remarquée par notre collègue François Nanchen, de la Division prévention criminalité de la Police, bien connu sous le nom d'eCop pour ses vidéos de sensibilisation fort amusantes. Après confirmation de notre part quant au caractère malveillant de cette campagne, il en a créé un sujet pour une de ses vidéos de sensibilisation publiée à cette adresse : https://www.youtube.com/shorts/4ehvKULOZ8Q

Depuis le 24 octobre et durant toute cette semaine, nous avons constaté dans nos signalements d'emails suspects, l'émergence de messages de phishing avec des caractéristiques particulières. Ces messages présentaient des similitudes avec les grandes campagnes de phishing actuelles, notamment l'utilisation de QR codes et des expéditeurs utilisant des adresses mail Office365 compromises. Ces messages présentaient toutefois la particularité de provenir depuis des adresses appartenant à des sociétés romandes. Au total, les adresses principales de sept entreprises vaudoises ont été interceptées par nos services.

Incidents et activités externes et/ou globaux

Quand un problème de sécurité est identifié sur une des adresse IP public du canton par des société externes, c'est la DGNSI qui est contactée, car le canton est le propriétaire de ces adresses. Certains partenaires utilisent notre infrastructure réseau, ce qui peut nous amener à devoir relayer l'information au client final utilisant l'adresse IP identifié. Durant le mois d'octobre nous avons été contactés par une entreprise qui recherche de composant vulnérable sur internet au sujet de la présence d'un IP, dédié à un partenaire, vulnérable aux dernière faille critiques Citrix. C'est, donc, en qualité de CSIRT pour le réseau cantonal que nous avons pris contact avec l'établissement concerné pour information et suivi de résolution.

Une commune vaudoise a également subi un phishing et une compromission de la boite email d'un collaborateur, simplement protégée par un login et mot de passe. L'attaquant a utilisé ce compte pour relayer d'autres courriels malicieux au nom de la personne lésée. La commune a procédé à la réinitialisation de l'ensemble des mots de passe des collaborateurs, avec l'aide de son prestataire informatique. L'ajout d'une authentification forte (MFA) pour cet accès sera étudié très prochainement par la commune.

Lors d'une opération de recherche de vulnérabilités, un collaborateur de la DGNSI a remonté au SOC un soucis sur un espace de stockage appartenant à une école d'ingénierie vaudoise. Ce site internet, normalement utilisé pour partager des documents avec l'extérieur, était utilisé pour échanger des morceaux de musique MP3. Le contenu du site avait été modifié par une personne externe pour monétiser cet accès. Un contact entre le SOC et le correspondant informatique de l'école a rapidement permis de supprimer le contenu illégitime.

Le SOC a été contacté par l'entité cybercrime de la Police Cantonale Vaudoise, concernant un accès d'une école de santé à une adresse IP appartement au groupe Vice Society. L'école a immédiatement démarrée une réponse à incident avec un partenaire spécialisé qui a permis d'identifier la présence de l'attaquant dans l'infrastructure informatique. Celui-ci était

toujours dans une phase de reconnaissance et n'avait pas encore procédé au chiffrement des données. Le signalement précoce de cet accès a réellement permis d'éviter une attaque qui aurait certainement démarrée quelques heures plus tard durant le week end.

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
Citrix Bleed CVE-2023-4966	Des acteurs malveillants exploitent une vulnérabilité critique nommée 'Citrix Bleed', identifiée comme CVE-2023-4966, pour cibler des réseaux gouvernementaux, techniques et juridiques sur Internet. Découverte en octobre et exploitée activement depuis fin août 2023, cette faille affecte les appareils Citrix NetScaler ADC et Gateway, permettant aux attaquants d'accéder à des informations sensibles. Les attaques sont difficiles à détecter en raison de la faible quantité de preuves numériques laissées, rendant les mouvements latéraux et le vol de données d'identification particulièrement furtifs. Citrix a publié des correctifs et a alerté les administrateurs pour renforcer leurs systèmes contre ces attaques qui ne nécessitent aucune interaction de l'utilisateur pour être menées à bien [27].
F5 BIG-IP CVE-2023-46747	La vulnérabilité CVE-2023-46747 a capté l'attention de la communauté de la cybersécurité en raison de sa sévérité élevée (score CVSS de 9.8), de son exploitation active dans des attaques sophistiquées, et de son large impact sur les infrastructures réseau utilisant les équipements F5 BIG-IP. Les chercheurs en sécurité ont souligné le danger en raison de la capacité des attaquants à exécuter du code à distance sans authentification [28]. De plus, la publication de scripts de preuve de concept sur des plateformes publiques comme GitHub [29] a mis en évidence l'accessibilité de cette vulnérabilité aux acteurs malveillants, augmentant l'urgence pour les organisations d'appliquer des correctifs ou des mesures d'atténuation.

Sources

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

[1] M. J. S. October 2 et 2023, « Alert: Attackers Actively Exploiting WS_FTP Vulnerabilities ». Consulté le: 8 novembre 2023. [En ligne]. Disponible sur: https://www.databreachtoday.eu/alert-attackers-actively-exploiting-wsftp-vulnerabilities-a-23200

[2] « MOVEit, the biggest hack of the year, by the numbers | TechCrunch ». Consulté le: 8 novembre 2023. [En ligne]. Disponible sur: https://techcrunch.com/2023/08/25/moveit-mass-hack-by-the-numbers/

[3] « MOVEit fallout continues as National Student Clearinghouse says nearly 900 schools affected ». Consulté le: 8 novembre 2023. [En ligne]. Disponible sur: https://therecord.media/progress-facing-lawsuits-sec-action

[4] « Cybercrime gangs now deploying ransomware within 24 hours of hacking victims ». Consulté le: 8 novembre 2023. [En ligne]. Disponible sur: https://therecord.media/ransomware-deployment-dwell-time-decreasing

[5] V. Marchive, « Ransomchats ». 3 novembre 2023. Consulté le: 8 novembre 2023. [En ligne]. Disponible sur: https://github.com/Casualtek/Ransomchats

[6] « Ransomware Negotiation: Dos and Don'ts! | www.neteye-blog.com ». Consulté le: 8 novembre 2023. [En ligne]. Disponible sur: https://www.neteye-blog.com/2023/09/ransomware-negotiation-dos-and-donts/

[7] J. Segura, « Malicious ad served inside Bing's AI chatbot », Malwarebytes. Consulté le: 8 novembre 2023. [En ligne]. Disponible sur: https://www.malwarebytes.com/blog/threat-intelligence/2023/09/malicious-ad-served-inside-bing-ai-chatbot

[8] Email et Print, « Bing Chat : attention, des liens malveillants peuvent se cacher dans les réponses », ZDNet France. Consulté le: 8 novembre 2023. [En ligne]. Disponible sur: https://www.zdnet.fr/actualites/bing-chat-attention-des-liens-malveillants-peuvent-se-cacher-dans-les-reponses-39961596.htm

[9] « How I made a heap overflow in curl | daniel.haxx.se ». Consulté le: 8 novembre 2023. [En ligne]. Disponible sur: https://daniel.haxx.se/blog/2023/10/11/how-i-made-a-heap-overflow-in-curl/

[10] Z. Zorz, « Curl project squashes high-severity bug in omnipresent libcurl library (CVE-2023-38545) », Help Net Security. Consulté le: 8 novembre 2023. [En ligne]. Disponible sur: https://www.helpnetsecurity.com/2023/10/11/cve-2023-38545-socks5/

[11] « CVE-2023-38545, CVE-2023-38546: Frequently Asked Questions for New Vulnerabilities in curl », Tenable®. Consulté le: 8 novembre 2023. [En ligne]. Disponible sur: https://www.tenable.com/blog/cve-2023-38545-cve-2023-38546-frequently-asked-questions-for-new-vulnerabilities-in-curl

[12] « New "HTTP/2 Rapid Reset" zero-day attack breaks DDoS records », BleepingComputer. Consulté le: 8 novembre 2023. [En ligne]. Disponible sur: https://www.bleepingcomputer.com/news/security/new-http-2-rapid-reset-zero-day-attack-breaks-ddos-records/

[13] « HTTP/2 Rapid Reset: A New Protocol Vulnerability Will Haunt the Web for Years | WIRED ». Consulté le: 8 novembre 2023. [En ligne]. Disponible sur: https://www.wired.com/story/http-2-rapid-reset-flaw/

[14] « Cisco Security Advisory: Multiple Vulnerabilities in Cisco IOS XE Software Web UI Feature », Cisco. Consulté le: 8 novembre 2023. [En ligne]. Disponible sur: https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-iosxe-webui-privesc-j22SaA4z

[15] B. Vigliarolo, « Cisco finally patches IOS XE after six days of zero day hits ». Consulté le: 8 novembre 2023. [En ligne]. Disponible sur: https://www.theregister.com/2023/10/22/in_brief_security/

[16] « Active exploitation of Cisco IOS XE Software Web Management User Interface vulnerabilities », Cisco Talos Blog. Consulté le: 8 novembre 2023. [En ligne]. Disponible sur: https://blog.talosintelligence.com/active-exploitation-of-cisco-ios-xe-software/

[17] « Unauthorized Access to Okta's Support Case Management System: Root Cause and Remediation », Okta Security. Consulté le: 8 novembre 2023. [En ligne]. Disponible sur: https://cms.oktaweb.dev/harfiles

[18] « How Cloudflare mitigated yet another Okta compromise », The Cloudflare Blog. Consulté le: 8 novembre 2023. [En ligne]. Disponible sur: http://blog.cloudflare.com/how-cloudflare-mitigated-yet-another-okta-compromise/

[19] « Okta Support System incident and 1Password | 1Password », 1Password Blog. Consulté le: 8 novembre 2023. [En ligne]. Disponible sur: https://blog.1password.com/okta-incident/

[20] Email et Print, « Les pirates du rançongiciel Trigona à leur tour hackés », ZDNet France. Consulté le: 8 novembre 2023. [En ligne]. Disponible sur: https://www.zdnet.fr/actualites/les-pirates-du-rancongiciel-trigona-a-leur-tour-hackes-39961946.htm
[21] « Ragnar Locker ransomware gang taken down by international police swoop », Europol. Consulté le: 8 novembre 2023. [En ligne]. Disponible sur: https://www.europol.europa.eu/media-press/newsroom/news/ragnar-locker-ransomware-gang-taken-down-international-police-swoop
[22] B. Bodnar, « Un cybercriminel russe membre du gang Ragnar Locker arrêté en France », Numerama. Consulté le: 8 novembre 2023. [En ligne]. Disponible sur: https://www.numerama.com/cyberguerre/1538912-un-cybercriminel-russe-membre-du-gang-ragnar-locker-arrete-en-france.html
[23] « Cyber Guide – Cyber Guide for SME ». Consulté le: 8 novembre 2023. [En ligne]. Disponible sur: https://guide.trustvalley.swiss/
[24] M. Barbezat, « La TrustValley publie un guide contre les cyberattaques pour aider les PME », OSINT Cybersécurité. Consulté le: 8 novembre 2023. [En ligne]. Disponible sur: https://www.ledecodeur.ch/2023/10/09/la-trustvalley-publie-un-guide-contre-les-cyberattaques-pour-aider-les-pme/
[25] « L'attaque contre Xplain bloque la modernisation de l'IT de la police vaudoise ». Consulté le: 10 novembre 2023. [En ligne]. Disponible sur: https://www.ictjournal.ch/news/2023-10-16/lattaque-contre-xplain-bloque-la-modernisation-de-lit-de-la-police-vaudoise
[26] « Fribourg a sa nouvelle Loi sur la protection des données ». Consulté le: 10 novembre 2023. [En ligne]. Disponible sur: https://www.ictjournal.ch/news/2023-10-13/fribourg-a-sa-nouvelle-loi-sur-la-protection-des-donnees
[27] « Hackers use Citrix Bleed flaw in attacks on govt networks worldwide », BleepingComputer. Consulté le: 7 novembre 2023. [En ligne]. Disponible sur: https://www.bleepingcomputer.com/news/security/hackers-use-citrix-bleed-flaw-in-attacks-on-govt-networks-worldwide/
[28] H. Labus, « F5 fixes critical BIG-IP vulnerability, PoC is public (CVE-2023-46747) », Help Net Security. Consulté le: 7 novembre 2023. [En ligne]. Disponible sur: https://www.helpnetsecurity.com/2023/10/30/cve-2023-46747/
[29] W01fh4cker, « Vulnerability details ». 7 novembre 2023. Consulté le: 7 novembre 2023. [En ligne]. Disponible sur: https://github.com/W01fh4cker/CVE-2023-46747-RCE