Classification : **PUBLIQUE**

TLP:CLEAR

Revue mensuelle des cybermenaces

Mars 2024

SOC – Centre opérationnel de sécurité

Version : 1.1

canton de vaud
LIBERTÉ ET PATRIE

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

Table des matières

Introduction

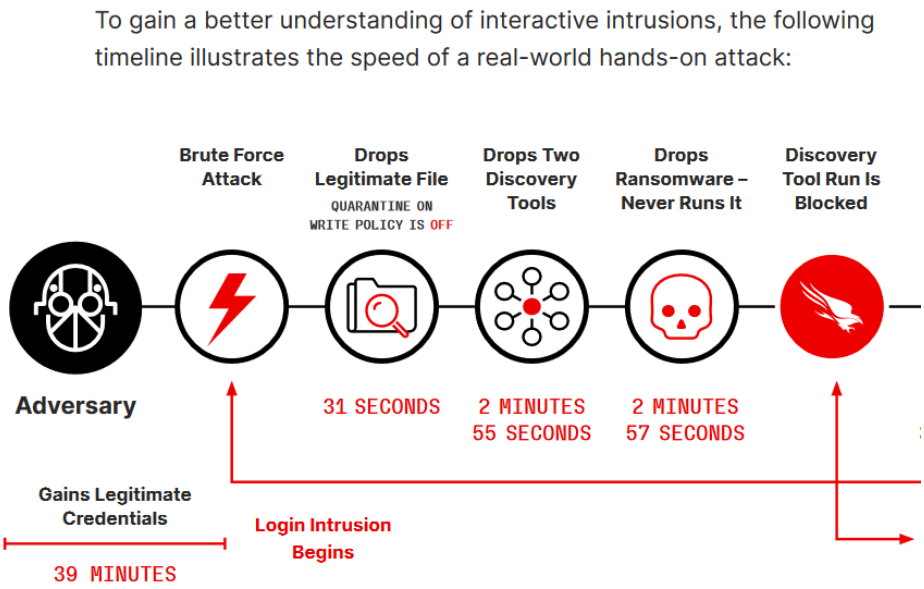
Ce rapport présente, de façon mensuelle, les actualités liées à la sécurité informatique que le Centre opérationnel de sécurité (SOC) de l'État de Vaud a estimé pertinentes. Il couvre à la fois des éléments internationaux et suisses, des incidents auxquels le SOC a dû répondre et des vulnérabilités qui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

Le paysage global des menaces

Actualités internationales

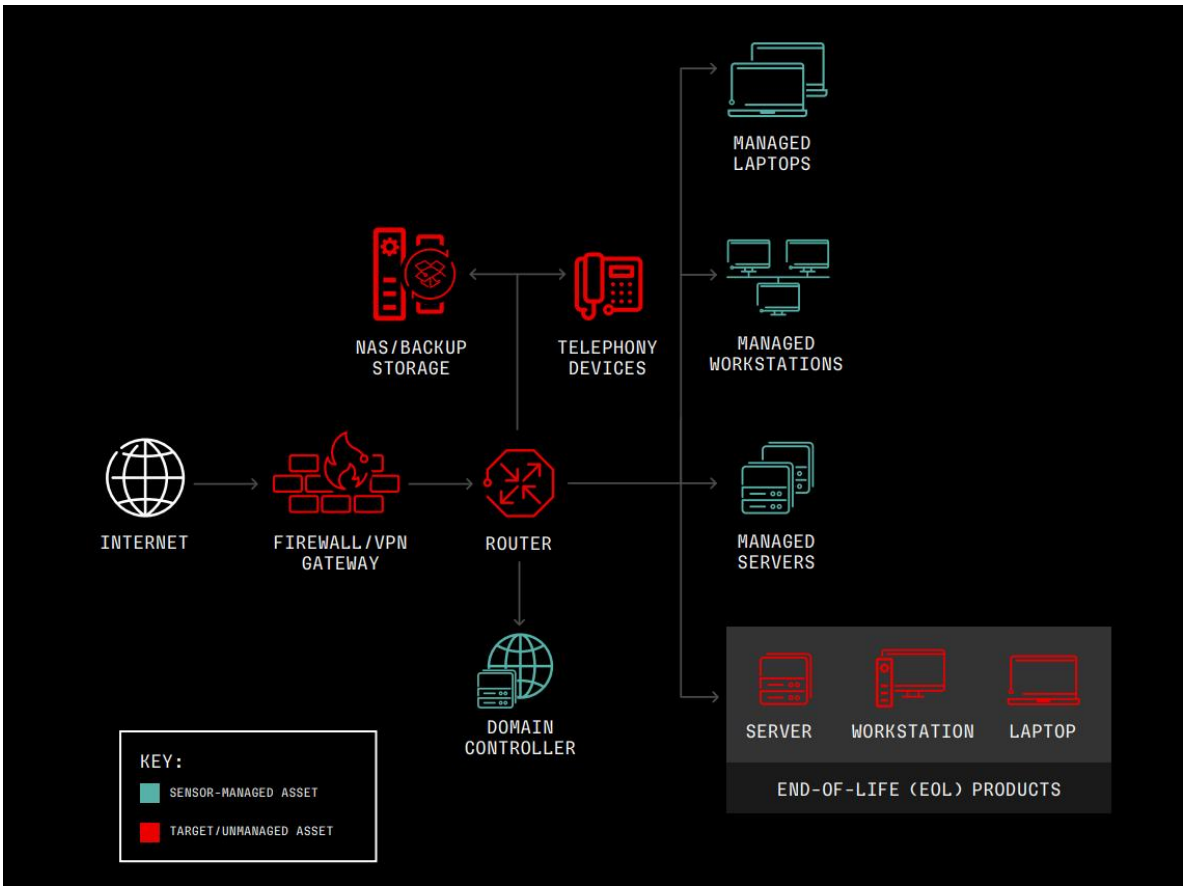
Rapport CrowdStrike 2023

La publication du rapport annuel "Global Threat Report" de la société CrowdStrike [1] à fin février 2024 vient illustrer les différentes tendances que nous avons observées au fil des derniers mois dans nos éditions. Cet éclairage sur les dynamiques de menaces met en exergue trois aspects importants : la vitalité croissante de l'écosystème criminel, la rapidité sans précédent des intrusions et la vulnérabilité croissante des environnements distribués ainsi que des chaînes d'approvisionnement informatique. En effet, avec l'introduction de 34 nouveaux acteurs de menaces relevés, le spectre des adversaires surveillés s'est considérablement élargi en 2023, atteignant un total de plus de 230 entités. Une des révélations les plus importante du rapport est la vitesse accrue à laquelle les adversaires peuvent désormais compromettre un système. Le temps moyen des intrusions interactives (typique des attaques de type ransomware) observé par les systèmes Crowdstrike est passé de 84 à 62 minutes entre 2022 et 2023. Le record d'incursion, fixé à 2 minutes et 7 secondes, illustre non seulement la rapidité d'action des cybercriminels, mais aussi le niveau de préparation et d'automatisation qu'ils ont atteint.



Le rapport met également en évidence une préoccupation grandissante autour de la sécurité de la chaîne d'approvisionnement. Les adversaires ciblent de plus en plus les fournisseurs tiers comme vecteurs d'attaque pour atteindre des réseaux d'entreprises bien protégés. En compromettant un seul fournisseur de services ou un élément de la chaîne d'approvisionnement logiciel, un attaquant peut potentiellement accéder à des centaines, voire des milliers, de cibles en aval. Ce dernier point est confirmé par les résultats de la société Wing Security spécialisée en sécurité de solution SaaS qui dans son dernier rapport sur l'état de la sécurité SaaS 2024 [2] révèle que 97% des 493 organisations sondées ont été exposées à des attaques via des applications compromises de la chaîne d'approvisionnement en 2023.

Autre information corroborant la tendance croissante observée les mois passés est l'augmentation importante des attaques sur les solutions en frontière des réseaux : les acteurs de la menace ont ajusté leurs stratégies en réponse à la visibilité accrue des capteurs EDR, en ciblant désormais la périphérie du réseau, où la visibilité du défenseur est généralement réduite.



En outre, une augmentation de 75 % des intrusions dans les environnements cloud a été enregistrée en 2023, mettant en lumière les défis de protection des données dans des environnements de plus en plus distribués.

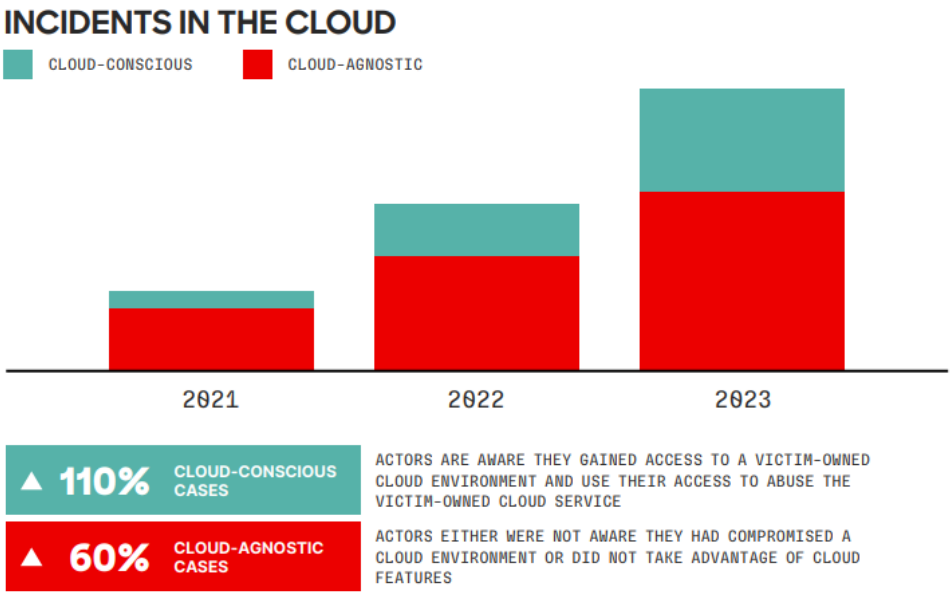


Figure 2. Increases in cloud cases

Microsoft dévoile l'ampleur de l'attaque par Midnight Blizzard

Exemplaire en matière, la publication par Microsoft de la suite de découvertes techniques sur l'attaque contre un compte d'un tenant cloud de test. Pour rappel, dans sa première déclaration du 19 janvier, Microsoft signalait que les comptes de

messagerie compromis incluaient « des comptes de messagerie d'entreprise de Microsoft, y compris des membres de notre équipe de direction et des employés de nos services de cybersécurité, juridique et autres », avec des courriels et documents joints exfiltrés. On apprend dans cette mise à jour publiée le 8 mars par l'équipe de Réponse aux cyberincidents de Microsoft [3] que Midnight Blizzard, un acteur soutenu par l'État russe également connu sous les noms d'APT29 ou Cozy Bear, a accédé au code source et aux systèmes internes de Microsoft. L'attaque, qui a débuté en novembre et a été détectée le 12 janvier, employait une technique de pulvérisation de mot de passe ("password spraying") visant un compte de test. Malgré une compromission initiale limitée à un faible pourcentage de comptes de messagerie, des investigations approfondies ont révélé un accès plus large aux systèmes internes et aux dépôts de code source, sans toutefois prouver la compromission des systèmes ou tenants cloud dédiés aux clients. Microsoft a identifié une utilisation par Midnight Blizzard de "secrets" exfiltrés, concernant des communications avec des clients, et a mis en garde contre la continuation d'activités malveillantes.

Failles Ivanti : Une centaine d'organisations françaises impactées

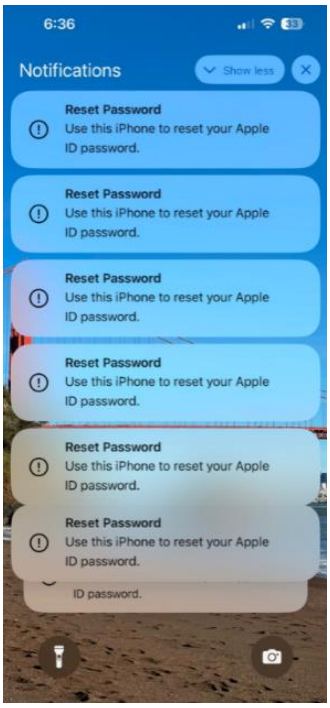
Concernant les attaques sur les passerelles de sécurité Ivanti relatées ces derniers mois, lors de la présentation du dernier panorama de la menace [4], l'Agence nationale française de la sécurité des systèmes d'information (ANSSI) a révélé qu'une centaine d'organisations en France ont été ciblées par des attaques exploitant des failles dans Ivanti Connect Secure et Policy Secure Gateways. Bien que ces vulnérabilités aient été rapidement utilisées avec succès par les attaquants, la plupart des intrusions n'ont pas mené à d'autres actions malveillantes visibles. L'ANSSI a également souligné la réactivité insuffisante des organisations françaises à mettre à jour leurs systèmes, rappelant l'importance de la gestion rapide des vulnérabilités pour contrer ces cyberattaques [5]. À noter que, dans ce contexte, la Cybersecurity and Infrastructure Security Agency (CISA) des États-Unis a confirmé avoir été confrontée à des compromissions réelles à la suite de ces attaques, ce qui l'a contrainte à déconnecter deux de ses systèmes Ivanti. Selon les informations fournies par Recorded Future [6], les services affectés incluraient l'Infrastructure Protection (IP) Gateway, contenant des données sur l'interdépendance des infrastructures américaines, ainsi que la passerelle pour le Chemical Security Assessment Tool (CSAT), qui stockait les plans de sécurité chimique pour le secteur privé. La CISA, cependant, n'a ni confirmé ni infirmé que ces systèmes spécifiques étaient ceux mis hors ligne.

Alerte sur une nouvelle campagne de cyber-espionnage visant les partis politiques occidentaux

Des experts en cybersécurité alertent sur une récente campagne d'espionnage orchestrée par APT29, un groupe associé au Service de renseignement extérieur russe (SVR), visant désormais les partis politiques occidentaux. Historiquement concentré sur des cibles diplomatiques et impliqué dans des attaques notables telles que celles contre les développeurs de vaccins COVID-19 et la campagne SolarWinds, APT29 a étendu ses activités en lançant, depuis février 2024, une offensive de phishing contre des partis politiques allemands. Les victimes étaient leurrées par des emails contrefaits, prétendument de l'Union chrétienne-démocrate (CDU), les dirigeant vers un fichier ZIP malicieux qui déployait un malware, Rootsaw, puis une nouvelle variante de backdoor, Wineloader. Mandiant, la firme de sécurité ayant révélé l'attaque [7], souligne que cette manœuvre signale un élargissement des opérations d'APT29 pour inclure l'espionnage politique, alignant ses actions avec les intérêts géopolitiques de Moscou, et met en garde contre la probabilité que d'autres partis et institutions occidentales soient dans le viseur de ces cyber-espions.

Attaques par "Fatigue MFA" : Les propriétaires d'iPhone visés

Des attaquants exploitent la lassitude humaine dans des attaques de phishing ciblant les utilisateurs d'iPhone, leur envoyant des demandes incessantes de réinitialisation de mot de passe via iCloud, parfois accompagné d'appels usurpés se faisant passer pour le support Apple. Ces attaques ont été repérées et détaillées par le chercheur en sécurité Brian Krebs en fin de mois [8].



Cette stratégie, connue sous le nom d'attaques par "fatigue MFA", inonde l'écran de l'appareil de notifications bloquant l'accès à d'autres fonctionnalités jusqu'à l'action de l'utilisateur, souvent pressé d'appuyer sur "Autoriser". Des groupes cybercriminels comme Fancy Bear et Lapsus$ ont réussi à exploiter cette technique par le passé.

Faille dans la conception architecturale affectant les puces Apple M1 et M2

Des chercheurs ont découvert une faille de sécurité, appelée GoFetch [9], dans les puces de la série M d'Apple, qui permet l'extraction des clés de chiffrement grâce à une attaque de canal latéral exploitant la fonction de prélecture dépendante de la mémoire des données (DMP). La vulnérabilité affecte les puces M1, M2 et potentiellement les futures puces de la série M en raison de leur microarchitecture similaire. Bien que la faille ne puisse pas être corrigée directement, elle peut être atténuée en intégrant des défenses dans des logiciels cryptographiques tiers, ce qui peut dégrader les performances des puces de la série M lors des opérations cryptographiques. Sur la nouvelle puce M3, il existe un bit spécial que les développeurs peuvent utiliser pour désactiver la fonction DMP, mais l'impact sur les performances cryptographiques n'est pas clair. La vulnérabilité met en lumière un problème de conception fondamental dans les puces de la série M qui ne peut pas être facilement résolu [10].

Révélation d'une brèche sophistiquée dans la chaîne d'approvisionnement Linux : la porte dérobée de XZ Utils

La découverte récente d'une porte dérobée dans la bibliothèque de compression de données XZ Utils, composante essentielle des principales distributions Linux, a généré une onde de choc à travers les communautés open-source et infosec. Cette porte dérobée méticuleusement conçue, suivie sous le nom de CVE-2024-3094, aurait pu déclencher des ravages généralisés si elle n'avait pas été repérée à temps. L'exploit, inséré par un mainteneur de confiance qui participait depuis 2 ans à ce projet, permettait l'exécution de code à distance sur les systèmes acceptant les connexions SSH. Bien qu'heureusement confiné aux dernières versions de la bibliothèque, la vulnérabilité a quand même réussi à infiltrer les canaux de distribution, constituant une menace pour les conteneurs, les machines virtuelles et même les systèmes de bureau des développeurs et des utilisateurs expérimentés.

L'incident souligne la vulnérabilité de l'écosystème open-source, où les projets s'appuient souvent sur de petites équipes ou des mainteneurs individuels avec des ressources limitées. XZ Utils, un exemple parfait, est devenu victime d'une attaque de la chaîne d'approvisionnement d'une sophistication sans précédent. Découvert presque par hasard par un ingénieur vigilant de Microsoft, le modus operandi de la vulnérabilité était aussi rusé qu'insidieux. En s'accrochant au démon du service SSH via la dépendance « liblzma », les attaquants pouvaient exécuter des commandes arbitraires avec précision et furtivité, en utilisant des techniques cryptographiques avancées pour échapper à la détection. Les répercussions de cette brèche dépassent largement les simples mises à jour logicielles. Avec de nombreux projets s'appuyant sur la bonne volonté et l'investissement personnel sur leur temps libre de petites équipes ou de mainteneurs individuels, la question de la confiance et de la sécurité dans la communauté open-source est remise en question.

Cet incident met en lumière l'importance d'une surveillance constante et d'une collaboration étroite au sein de la communauté open-source pour prévenir de telles attaques à l'avenir. Il souligne également le besoin de mécanismes de vérification robustes pour garantir l'intégrité des logiciels distribués.

Alors que les experts continuent d'analyser les détails de cette brèche et les réponses des différents acteurs, la question se pose naturellement si des vulnérabilités similaires auraient pu être installées dans d'autres composants sans être détectées à ce jour…

Actualités suisses

Dans un rapport approfondi publié par l'Office de la cybersécurité fédérale (OFCS) le 7 mars [11], un focus a été fait sur l'ampleur des répercussions de la cyberattaque orchestrée par le groupe de hackers Play contre l'entreprise Xplain en mai 2023. Cette offensive avait conduit à la divulgation de données sensibles et personnelles sur le darknet. Le rapport détaille l'examen de près de 1,3 million de données, soulignant l'impact majeur sur le Département fédéral de justice et police, sans pour autant aborder l'origine de la fuite, sujet d'une enquête administrative en cours.

Répartition et nature des données compromises :

Propriétaire des données	Nombre d'objets	Pourcentage
Xplain	47 413	73,03
Administration fédérale	9 040	13,92
Cantons	6 200	9,55
Organismes privés	955	1,47
Corps de police	944	1,45
Entreprises liées à la Confédération	355	0,55
Ministère public de la Confédération	16	0,02
Total	**64 923**	**100,00**

Tableau 2 Vue d'ensemble des propriétaires de données touchés

- Parmi les 64'923 objets analysés, une grande partie (plus de 70%) appartenait directement à Xplain, tandis que l'administration fédérale et les cantons étaient respectivement responsables d'environ 14% et 10% des données. Les entités privées et les corps de police représentaient moins de 2% chacun.
- Une attention particulière a été portée aux données provenant de l'administration fédérale, avec une majorité écrasante (plus de 95%) émanant des unités administratives du Département fédéral de justice et police, laissant un impact marginal sur les autres départements.
- Sur les 9'040 objets analysés appartenant à l'administration fédérale, 5'182 contenaient des données sensibles, incluant majoritairement des informations personnelles, techniques, des informations classifiées et quelques mots de passe.
- L'analyse a révélé que parmi les 121 objets classifiés examinés, la plupart étaient marqués comme INTERNE, et un tiers étaient CONFIDENTIELS, sans aucun document classé SECRET.

Fedpol a découvert que seulement 39% de ses données restaurées avaient été divulguées, notant des omissions spécifiques dans les documents mentionnant le terme "russisch". Armassuisse/PM a également identifié des documents non publiés, sans aucun schéma apparent dans les omissions. L'une des révélations les plus intrigantes du rapport

concerne la prudence des cybercriminels à l'égard des références à la Russie. La suppression délibérée des documents intitulés « InfoblattRussisch.docx » suggère une approche en ligne avec les pratiques d'autres groupes cybercriminels russes. Cette tactique indique également que l'analyse du stock de données par les criminels était superficielle, se focalisant sur des fichiers facilement identifiables. Le document en question est une fiche d'information en russe pour les personnes arrêtées (droits et obligations, procédure, etc.) sans contenu sensible. Il est présent dans différentes autres langues parmi les données publiées. Une analyse plus poussée a montré que le fichier « InfoblattRussisch.docx » n'a été retiré du stock de données que s'il n'était pas contenu dans une archive (p. ex. fichier .zip) et qu'il était donc facile à trouver. Cette manière de procéder indique que les criminels ont réalisé un examen superficiel du stock de données sans en parcourir le contenu selon l'*Office* fédéral de la *cybersécurité*.

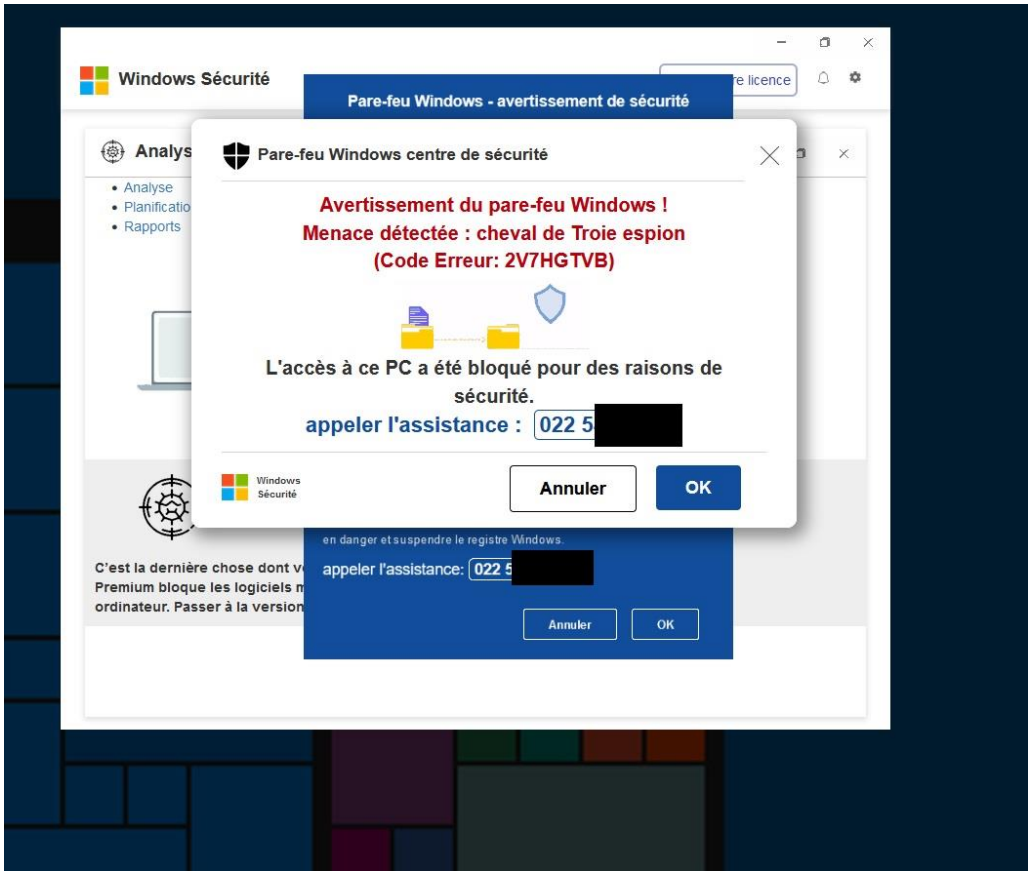
Bilan vaudois 2023 : Augmentation marquée de la cybercriminalité

Le Bilan 2023 sur la criminalité numérique dans le canton de Vaud, présenté le 25 mars [12], montre une hausse significative de 36,8% des activités cybercriminelles par rapport à l'année précédente. Les pertes financières engendrées par ces fraudes sont importantes, avec notamment 12,6 millions de francs dus à la fraude à l'investissement en ligne (199 cas), 4,6 millions à l'arnaque aux sentiments (67 cas), 3,1 millions aux fausses assistances techniques (461 cas) et 1,7 million au phishing (498 cas). Parmi ces infractions, les plus courantes incluent les arnaques via petites annonces (+32,4%), les abus d'identité (+44,6%), les fraudes au support technique (+65,9%) et le phishing (+212%).

Incidents et activités externes et/ou globaux

Recrudescence des arnaques au support technique : la variante suisse romande

Au cours du mois dernier, nous avons observé une recrudescence des arnaques au support technique, qui suivent les modalités habituelles.



Un constat intéressant a été mis en avant dans la page dédiée aux "variantes d'arnaque au faux support technique" [13] publiée par l'Office Fédéral de la Sécurité Cyber (OFSC), soulignant la particularité régionale de cette campagne. Selon leurs observations basées sur les statistiques nationales, ces arnaques semblent prédominantes en Suisse romande, donnant lieu à ce qu'ils ont désigné sous le nom de "variante suisse romande". Cette spécificité régionale suggère que les attaques sont soit exclusivement déployées dans cette région, soit activées uniquement pour les navigateurs réglés en français. Cette focalisation géographique et linguistique des attaques peut en grande partie être expliquée par l'utilisation stratégique des publicités Google, comme observé lors de l'analyse de nos alertes pour ce cas particuliers. En effet, les cybercriminels détournent les fonctionnalités de ciblage de la plateforme pour diriger les utilisateurs vers des sites frauduleux, souvent déguisés en publicités pour des logiciels légitimes. Les options de ciblage avancées disponibles dans les campagnes publicitaires permettent ainsi de viser spécifiquement une population donnée, exploitant les configurations linguistiques et régionales pour optimiser l'efficacité de leurs ciblages.

Force d'intervention cybersécurité cantonale (CSIRT)

Depuis son entrée en fonction le 1er janvier 2024, l'équipe de la force d'intervention cybersécurité cantonale (CSIRT) fraîchement mise en place dans le cadre de la convention avec les communes n'a heureusement pas été mobilisée pour soutenir une des communes ou associations intercommunales du canton lors d'un cyber incident. Afin d'être préparés au mieux à ce scénario, des réunions ont été organisées avec l'unité cybercrime de la police cantonale et avec nos partenaires de réponse à incident pour s'assurer d'être alignés sur les procédures de gestion de crise.

Le mois de mars a été un mois de lancement des présentations du service à l'extérieur. Le CSIRT a rencontré l'AVRiC (Association Vaudoise des Responsables informatiques Communaux) représentant les plus grandes communes ainsi que les syndics des districts de Nyon et du Gros-de-Vaud afin de présenter les activités prévues dans le cadre de ce nouveau service. Dans le même registre, des échanges ont eu lieu avec des professeurs et doctorants de l'Université de Lausanne pour recueillir leurs idées sur la manière de développer et mettre à disposition des standards minimaux en matière de sécurité des systèmes d'information.

Dans le but de réduire le risque de survenance d'une cyberattaque, des communes faisant partie du réseau cantonal vaudois (RCV) ont été notifiées personnellement de vulnérabilités critiques identifiées chez elles et détectées par un service externe. Notamment sur Microsoft Exchange et FortiOS. Grâce à un travail de suivi, toutes les communes ont patché les vulnérabilités annoncées.

Le 15 mars, une première séance de synchronisation avec les membres du comité de pilotage (COPIL) a eu lieu afin de faire état des premiers mois d'activités du service et des travaux en cours pour la suite.

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
Windows CVE-2024-21412	Le chercheur de Trend Micro ont démontré dans le courant du mois [14] comme cette vulnérabilité dans Microsoft Windows corrigée en février a été exploitée dans une campagne zero-day par les opérateurs de DarkGate pour contourner les protections de Windows Defender SmartScreen. Cette faille a été exploitée en utilisant des redirections ouvertes dans les technologies Google DoubleClick Digital Marketing (DDM), démontrant une sophistication accrue dans les méthodes d'attaque. Les attaquants ont intégré une redirection ouverte à partir du domaine doubleclick[.]net dans un fichier PDF diffusé via une campagne de phishing, redirigeant la victime vers un serveur web compromis pour initier la chaîne d'infection. L'exploitation de cette CVE, combinée à l'abus de la confiance accordée aux domaines liés à Google, a permis de contourner les protections de Microsoft Defender SmartScreen, conduisant à l'infection par des logiciels malveillants sans que les victimes ne reçoivent d'avertissement. Cette capacité à dépasser des mécanismes de sécurité critiques dans Windows, associée à l'utilisation créative de services publicitaires légitimes pour propager des menaces, explique pourquoi la CVE-2024-21412 a été particulièrement médiatisée.
XZ Utils (SSH) CVE-2024-3094	Une porte dérobée a été découverte dans le logiciel populaire de compression de données xz Utils, largement utilisé sur les systèmes Linux et de type Unix. La porte dérobée, probablement mise en place sur plusieurs années, permettait aux attaquants d'exécuter à distance un code arbitraire sur les systèmes utilisant les versions compromises de xz Utils notamment dans le service d'administration à distance SSH. La porte dérobée a été introduite à travers une série de modifications de code suspectes et des efforts d'ingénierie sociale pour faire intégrer les mises à jour dans les principales distributions Linux telles que Debian et Red Hat. La vulnérabilité dans ce composant a été particulièrement médiatisée en raison de sa liaison avec les attaques de la chaîne d'approvisionnement, soulignant la sophistication des menaces pesant sur les composants open source largement répandus. Les chercheurs ont mis en évidence la nature complexe et la durée temporelle de l'attaque orchestrée par un individu identifié sous le nom de Jia Tan. Cet incident a mis en lumière les risques associés aux attaques ciblant la chaîne d'approvisionnement, où des composants logiciels tiers peuvent être exploités comme vecteurs pour compromettre de vastes systèmes [15].
JetBrains TeamCity CVE-2024-27198 CVE-2024-27199	Les CVE-2024-27198 et CVE-2024-27199 ont révélé des vulnérabilités de contournement d'authentification dans JetBrains TeamCity, mettant en lumière les risques de sécurité pour les services d'intégration et de déploiement continus sur Internet. La rapidité avec laquelle les chercheurs de Rapid7 ont divulgué les détails techniques de ces vulnérabilités, seulement quelques heures après la publication des correctifs par JetBrains [16], a suscité un débat important sur les pratiques de divulgation responsable et le "patching silencieux". JetBrains a plaidé pour une approche de divulgation progressive, visant à fournir aux clients le temps nécessaire pour appliquer les correctifs avant la publication des détails exploitables, tandis que Rapid7 a défendu la nécessité d'une transparence immédiate pour prévenir les abus par les acteurs malveillants [17]. Cette situation a illustré les défis éthiques et pratiques auxquels sont confrontés les chercheurs en sécurité et les fournisseurs de logiciels dans la gestion des divulgations de vulnérabilités.

Sources

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

[1] « CrowdStrike 2024 Global Threat Report », crowdstrike.com. Consulté le: 4 avril 2024. [En ligne]. Disponible sur: https://www.crowdstrike.com/resources/reports/crowdstrike-2024-global-threat-report/

[2] « The 2024 State of SaaS Report », Wing Security. Consulté le: 5 avril 2024. [En ligne]. Disponible sur: https://wing.security/resources/report/the-2024-state-of-saas-security/

[3] « Update on Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard | MSRC Blog | Microsoft Security Response Center ». Consulté le: 5 avril 2024. [En ligne]. Disponible sur: https://msrc.microsoft.com/blog/2024/03/update-on-microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/

[4] « Panorama de la cybermenace 2023 – CERT-FR ». Consulté le: 5 avril 2024. [En ligne]. Disponible sur: https://cert.ssi.gouv.fr/cti/CERTFR-2024-CTI-001/

[5] E. ZDNet, « Failles d'Ivanti : une centaine d'organisations victimes en France », ZDNET. Consulté le: 5 avril 2024. [En ligne]. Disponible sur: https://www.zdnet.fr/actualites/failles-d-ivanti-une-centaine-d-organisations-victimes-en-france-39964604.htm

[6] « CISA forced to take two systems offline last month after Ivanti compromise ». Consulté le: 5 avril 2024. [En ligne]. Disponible sur: https://therecord.media/cisa-takes-two-systems-offline-following-ivanti-compromise

[7] « APT29 Uses WINELOADER to Target German Political Parties », Mandiant. Consulté le: 5 avril 2024. [En ligne]. Disponible sur: https://www.mandiant.com/resources/blog/apt29-wineloader-german-political-parties

[8] « Recent 'MFA Bombing' Attacks Targeting Apple Users – Krebs on Security ». Consulté le: 5 avril 2024. [En ligne]. Disponible sur: https://krebsonsecurity.com/2024/03/recent-mfa-bombing-attacks-targeting-apple-users/

[9] « GoFetch: Breaking Constant-Time Cryptographic Implementations Using Data Memory-Dependent Prefetchers ». Consulté le: 5 avril 2024. [En ligne]. Disponible sur: https://gofetch.fail

[10] D. Goodin, « Unpatchable vulnerability in Apple chip leaks secret encryption keys », Ars Technica. Consulté le: 5 avril 2024. [En ligne]. Disponible sur: https://arstechnica.com/security/2024/03/hackers-can-extract-secret-encryption-keys-from-apples-mac-chips/

[11] « Cyberattaque contre l'entreprise Xplain : publication du rapport de l'Office fédéral de la cybersécurité sur l'analyse des données ». Consulté le: 5 avril 2024. [En ligne]. Disponible sur: https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-100315.html

[12] « Bilan 2023 de la criminalité dans le canton de Vaud », État de Vaud. Consulté le: 5 avril 2024. [En ligne]. Disponible sur: https://www.vd.ch/toutes-les-actualites/actualite/news/i-bilan-2023-de-la-criminalite-dans-le-canton-de-vaud-1

[13] D. fédéral de la défense DDPS de la protection de la population et des sports, « Semaine 1 : Variantes d'arnaque au faux support technique ». Consulté le: 5 avril 2024. [En ligne]. Disponible sur: https://www.ncsc.admin.ch/ncsc/fr/home/aktuell/im-fokus/2024/wochenrueckblick_1.html

[14] « CVE-2024-21412: DarkGate Operators Exploit Microsoft Windows SmartScreen Bypass in Zero-Day Campaign », Trend Micro. Consulté le: 4 avril 2024. [En ligne]. Disponible sur: https://www.trendmicro.com/en_us/research/24/c/cve-2024-21412--darkgate-operators-exploit-microsoft-windows-sma.html

[15] « The Mystery of 'Jia Tan,' the XZ Backdoor Mastermind | WIRED ». Consulté le: 4 avril 2024. [En ligne]. Disponible sur: https://www.wired.com/story/jia-tan-xz-backdoor/

[16] C. Jones, « Rapid7 flames JetBrains over vulnerability disclosure ». Consulté le: 4 avril 2024. [En ligne]. Disponible sur: https://www.theregister.com/2024/03/05/rapid7_jetbrains_vuln_disclosure_dispute/

[17] « JetBrains vulnerability exploitation highlights debate over "silent patching" ». Consulté le: 4 avril 2024. [En ligne]. Disponible sur: https://therecord.media/jetbrains-rapid7-silent-patching-dispute