Classification : **PUBLIQUE**

TLP:CLEAR

Revue mensuelle des cybermenaces

Juin 2024

SOC – Centre opérationnel de sécurité

Version : 1.0

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.

Il est publié sous le sceau **TLP:CLEAR** (https://www.first.org/tlp), et peut ainsi être distribué largement. Les textes et illustrations sont la propriété exclusive de l'Etat de Vaud. Par conséquent, une autorisation spéciale et expresse est nécessaire pour toutes autres utilisations. Les règles usuelles de la bonne foi et de la citation seront respectées en cas d'utilisation ou reprise de tout ou partie par des tiers du présent rapport. Veuillez noter que ces informations sont publiées à titre informatif et n'engagent en aucun cas l'État de Vaud.

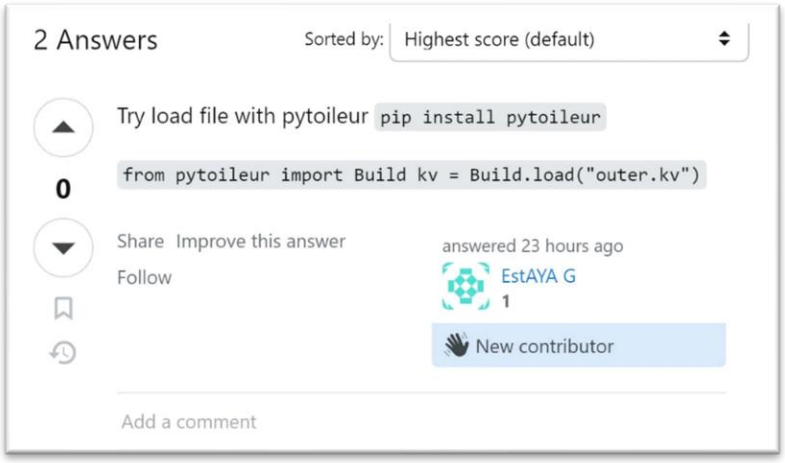
Le paysage global des menaces

Actualités internationales

Fuites de données massives : Ticketmaster et 361 millions d'e-mails exposés sur Telegram

Le mois de juin a débuté par l'annonce de fuites de données massives, dont certaines concernent également des informations suisses. Deux incidents majeurs se distinguent : la brèche chez Ticketmaster et la divulgation de 361 millions d'adresses e-mail sur Telegram. Ticketmaster, le géant de la billetterie en ligne, a confirmé une violation de grande ampleur après que des données volées ont été mises en vente [1]. Cette brèche a exposé des informations personnelles et financières de millions d'utilisateurs, augmentant les risques de fraude et d'usurpation d'identité. Les répercussions se font sentir mondialement, y compris en Suisse. Les experts en cybersécurité soulignent que la nature sensible des données compromises, telles que les numéros de cartes de crédit et les informations personnelles, pourrait entraîner des années de risques accrus d'attaques ciblées comme le spear-phishing. En parallèle, Troy Hunt, expert en cybersécurité et responsable du site "Have I Been Pwned", a révélé que 361 millions d'adresses e-mail, accompagnées de mots de passe, ont été publiées sur Telegram [2]. Ces données, regroupées en listes de combinaisons d'identifiants et mots de passe, proviennent de plusieurs milliers de canaux Telegram. Leur publication rend les utilisateurs vulnérables à des attaques de credential stuffing, où les attaquants essaient de se connecter à divers services en ligne en utilisant ces combinaisons. Les conséquences pour les victimes peuvent inclure des accès non autorisés à leurs comptes, la compromission de données supplémentaires et des pertes financières. Hunt souligne également que la facilité d'accès à ces informations via Telegram rend leur exploitation d'autant plus préoccupante, les rendant accessibles à une vaste audience de cybercriminels potentiels. Pour les utilisateurs concernés, il est recommandé de changer immédiatement leurs mots de passe et d'activer des mesures de sécurité supplémentaires comme l'authentification à deux facteurs. Par ailleurs, tout utilisateur peut vérifier la présence de son adresse e-mail parmi les données compromises en se rendant sur le site "Have I Been Pwned" (https://haveibeenpwned.com).

Attaque à la supply chain logicielle : nouvelle tactique d'attaque basée sur la confiance



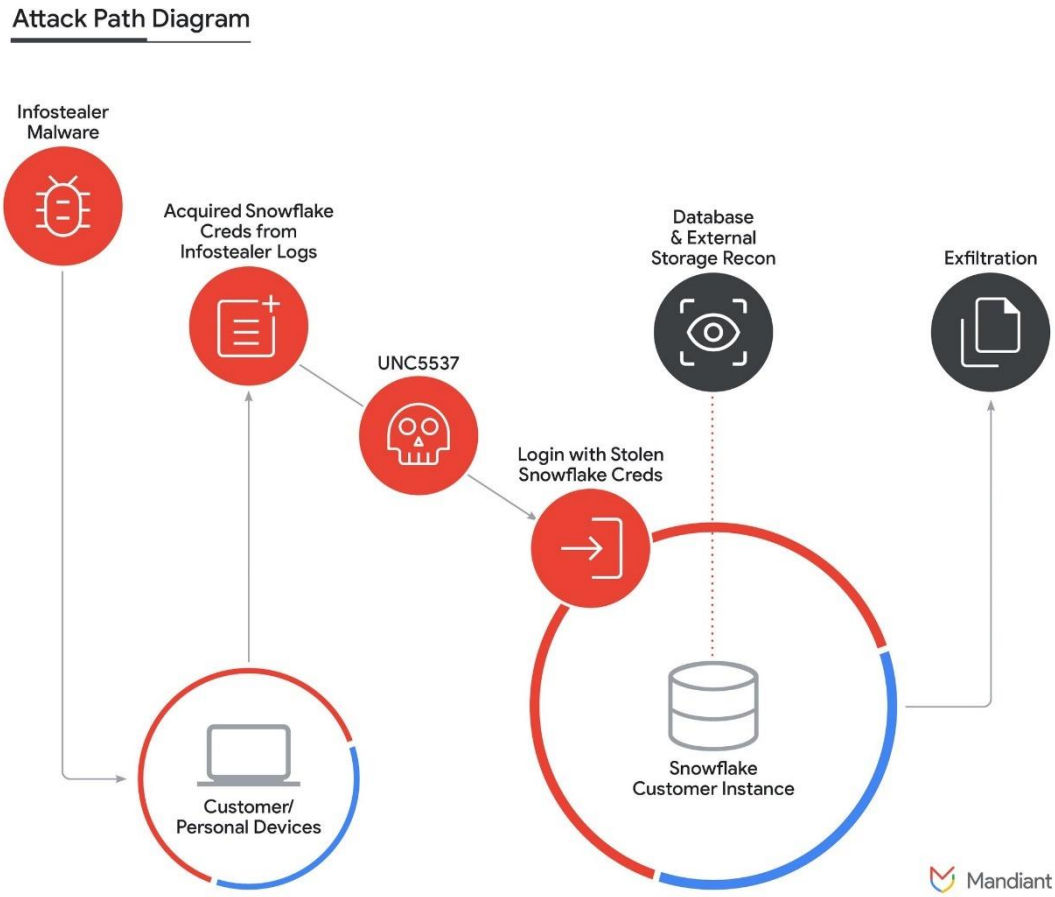
Les attaques sur la supply chain (chaîne d'approvisionnement) continuent d'évoluer et de représenter un défi majeur pour la cybersécurité. Ces attaques exploitent les vulnérabilités des chaînes d'approvisionnement logicielles pour infiltrer des systèmes en amont, pour pouvoir ainsi bénéficier d'une entrée dérobée en aval. Une nouvelle méthode, mise en lumière par BleepingComputer [3], montre que des cybercriminels se font passer pour des utilisateurs aidants sur des forums pour développeurs tels que Stack Overflow pour diffuser des malwares. En proposant des solutions apparemment utiles, mais contenant du code malveillant, ils parviennent à infecter les systèmes de développeurs en quête de réponses à leurs problèmes techniques. Un exemple cité dans l'article de BleepingComputer décrit comment un utilisateur, prétendant être un expert bien intentionné, propose une solution à un problème de codage. Cette solution inclut un lien vers un script ou une bibliothèque, qui, une fois téléchargé et exécuté, installe un malware sur le système de la victime. Ce type d'attaque peut entraîner des conséquences sérieuses pour les entreprises et les développeurs comme le vol de données sensibles ou l'accès non autorisé aux réseaux internes. Cet incident rappelle également une autre attaque récente sur la supply chain impliquant une porte dérobée dans la bibliothèque xz et liblzma (CVE-2024-3094) introduite par un développeur bénévole du projet. Pour se protéger contre ces attaques, il est important de vérifier la légitimité des sources et des intervenants avant de télécharger des scripts ou des bibliothèques, de faire de la sensibilisation auprès des développeurs, d'utiliser des outils de sécurité pour analyser les codes téléchargés, et de se tenir informé des vulnérabilités récentes.

Découverte d'extensions malveillantes sur le marketplace de Visual Studio Code

Un autre cas exemplaire dans ce contexte est le résultat d'une analyse sur le marketplace de l'éditeur de code développé par Microsoft, "Visual Studio Code". Des chercheurs israéliens y ont découvert des extensions malveillantes, y compris une copie trojanisée du thème populaire "Dracula Official" [4]. L'extension malveillante, nommée "Darcula", collecte des informations système et les envoie à un serveur distant. Une analyse plus approfondie a révélé des milliers d'extensions avec des millions d'installations potentiellement dangereuses. Ces extensions échappent souvent aux outils de détection traditionnels.

Incident de sécurité chez Snowflake : conséquences sur la chaîne d'approvisionnement

En parallèle à ces menaces, en avril 2024 le groupe de cybercriminels financièrement motivés UNC5537 a lancé une campagne de cyberattaques ciblant environ 165 instances de Snowflake, une plateforme de gestion et d'analyse de données en cloud largement utilisée par les entreprises. Les attaquants ont exploité des informations d'identification volées via des malwares de type infostealer, tels que Lumma, Meta et Redline Stealer, pour accéder aux comptes clients de Snowflake.



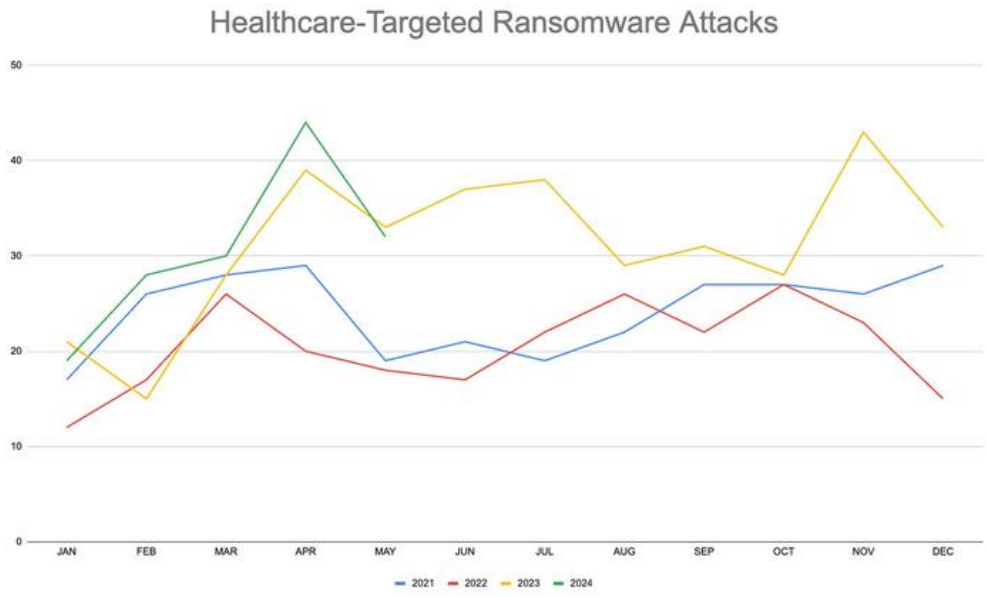
Ces informations, souvent datées de plusieurs années, ont permis aux cybercriminels d'exfiltrer des données importantes via des commandes SQL, qu'ils ont ensuite mises en vente sur des forums de cybercriminalité. Mandiant a confirmé que ces accès non autorisés étaient dus à des informations d'identification compromises et non à une faille de sécurité dans l'environnement de Snowflake [5]. Les répercussions de cet incident sont devenue évidente dans le courant du mois de juin, affectant des entreprises telles que Ticketmaster (relaté précédemment dans nos lignes), Santander Bank [6], Mitsubishi, Neiman Marcus [7], Allstate, Advance Auto Parts, Progressive, State Farm et Anheuser-Busch. Pure Storage [8] a également confirmé une violation de son espace de travail Snowflake. Cet incident démontre comment une faille dans une plateforme tierce peut avoir des répercussions en cascade sur de nombreuses organisations. Il souligne également l'importance de l'authentification multi-facteurs (MFA), la majorité des comptes compromis n'utilisant pas de MFA, ce qui a grandement facilité l'accès pour les attaquants.

Attaques sur les dispositifs FortiGate : une campagne d'espionnage de grande ampleur

Dans le contexte de cyberattaques croissantes sur les dispositifs FortiGate, le National Cyber Security Centre (NCSC) des Pays-Bas a publié des informations importantes [9] révélant une portée beaucoup plus vaste des attaques que ce qui était initialement connu [10]. Les services de renseignement néerlandais ont découvert une campagne de cyberespionnage chinoise exploitant une vulnérabilité dans les systèmes FortiGate (CVE-2022-42475). Cette vulnérabilité a été utilisée comme zero-day, c'est-à-dire qu'elle a été exploitée deux mois avant que Fortinet ne publie un correctif. Les attaquants ont accédé à au moins 20'000 dispositifs FortiGate dans le monde en l'espace de quelques mois en 2022 et 2023. Durant cette période, ils ont compromis environ 14'000 appareils avant que la vulnérabilité ne soit révélée publiquement. Les cibles comprenaient des gouvernements occidentaux, des institutions diplomatiques et des entreprises du secteur de la défense. Le malware nommé « Coathanger » a été conçu pour persister sur les dispositifs FortiGate, même après les redémarrages et les mises à jour du firmware. Il injecte une sauvegarde de lui-même dans le processus responsable du redémarrage, rendant son éradication extrêmement difficile sans un reformatage complet de l'appareil. Ce malware, attribué à un groupe de cyberespionnage soutenu par l'État chinois, a permis aux attaquants de maintenir un accès permanent aux systèmes infectés. L'intrusion a touché divers réseaux, y compris ceux du ministère néerlandais de la Défense. L'impact a été limité grâce à la segmentation des réseaux, ce qui a contenu l'attaque à un segment de recherche et développement non classifié, utilisé par moins de 50 utilisateurs.

Quand les rançongiciels paralysent le secteur de la santé : deux incidents révélateurs

Les attaques par rançongiciels continuent de poser des défis importants dans le secteur de la santé, comme en témoignent les récents incidents impliquant Synnovis et Change Healthcare. À Londres, le groupe de cybercriminels Qilin a ciblé Synnovis, un fournisseur de services de pathologie, perturbant les services de santé et entraînant l'annulation d'opérations [11] ainsi que des pénuries de sang [12]. Le groupe a admis avoir sciemment provoqué cette crise, motivé par des objectifs politiques, bien que des experts mettent en doute cette justification [13]. De son côté, Change Healthcare, un fournisseur de technologies de santé, a dû payer une rançon de 22 millions de dollars à la suite d'une attaque par rançongiciel qui avait paralysé une partie du système sanitaire américain. Ce paiement illustre l'augmentation des rançons dans ce secteur, où les cybercriminels exploitent l'importance des services médicaux. En avril, la société de cybersécurité Recorded Future a suivi 44 cas de groupes criminels ciblant des organisations de santé avec des attaques par rançongiciels, volant leurs données, chiffrant leurs systèmes et exigeant des paiements tout en gardant leurs réseaux en otage. Cette augmentation des attaques, notamment en avril de cette année, montre une progression importante [14]. Ces incidents ont révélé de façon brutale les répercussions pour les patients et les institutions.

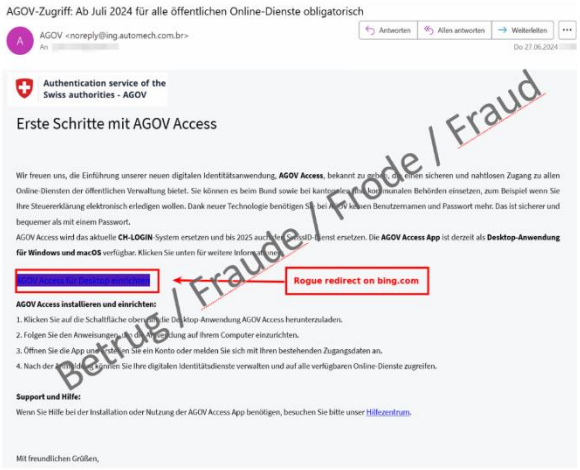


There were 44 ransomware attacks on health-care-related victims in April of this year, the most of any month on record, according to data collected by cybersecurity firm Recorded Future.

Actualités suisses

Poseidon : Une nouvelle menace pour les utilisateurs macOS en Suisse

Récemment, une campagne de cyberattaque ciblant spécifiquement les utilisateurs mac en Suisse a été détectée par l'Office fédéral de la communication suisse (OFCS) [15]. Cette campagne, menée par l'infostealer Poseidon, utilise des e-mails frauduleux prétendant provenir du service d'authentification des autorités suisses, AGOV. Un infostealer est un type de logiciel malveillant conçu pour voler des informations personnelles et sensibles telles que les mots de passe, les identifiants de connexion et les données bancaires. Ces e-mails malveillants invitent les destinataires à télécharger une fausse application sous prétexte de faciliter des démarches administratives électroniques, comme la déclaration d'impôts.



Contrairement à ce qui est annoncé, l'application « AGOV access » n'est disponible que sur smartphones, pas en tant qu'application de bureau. En téléchargeant ce faux logiciel, les victimes installent en réalité Poseidon sur leur système, un logiciel malveillant capable de voler des informations sensibles. Cette campagne suisse présente des similitudes et des différences notables par rapport à une autre campagne plus large interceptée par Malwarebytes [16], qui utilise également l'infostealer Poseidon. Dans la campagne générale, les cybercriminels ont recours à des publicités Google pour distribuer Poseidon, déguisé en fausses applications populaires. Ces publicités apparaissent dans les résultats de recherche et redirigent les utilisateurs vers des sites de téléchargement malveillants. Bien que les méthodes de distribution diffèrent, les deux campagnes exploitent des vecteurs de confiance (e-mails d'autorités suisses pour la campagne suisse et publicités Google pour la campagne générale) pour inciter les utilisateurs à télécharger le malware. Poseidon est une nouvelle variante de l'Atomic Stealer déjà connu pour ses attaques via des publicités Google. Ce logiciel malveillant utilise des scripts AppleScript encodés pour exfiltrer des données sensibles depuis les systèmes infectés. Ses capacités incluent la capture de mots de passe, la collecte d'informations système et l'enregistrement des frappes clavier. La spécificité du ciblage des utilisateurs macOS en Suisse via des courriels prétendument officiels constitue une anomalie notable dans un paysage de menaces généralement plus globalisé. Cette focalisation sur des institutions locales souligne l'importance pour les institutions et ses usagers de rester vigilants et de vérifier l'authenticité des communications électroniques, surtout celles impliquant des actions sensibles comme les téléchargements de logiciels.

Cyberattaque chez un prestataire de la ville d'Yverdon-les-Bains : 12'300 clients potentiellement exposés

Un prestataire externe du Service des énergies de la ville d'Yverdon-les-Bains a été victime d'une cyberattaque à la fin mai. Cet incident a potentiellement exposé les données de 12'300 particuliers et entreprises. Les informations compromises comprennent des données de contact et de facturation des abonnés du service. L'attaque a été rendue possible par une mauvaise manipulation du prestataire qui a rendu les informations accessibles depuis internet [17]. Les autorités cantonales et fédérales n'ont pas trouvé de traces de ces données sur le dark web jusqu'à présent.

Évaluation de l'efficacité des cantons dans la lutte contre la cybercriminalité : rapport du Conseil fédéral

Le Conseil fédéral suisse a publié un rapport en réponse aux postulats 22.3145 et 22.3017 visant à évaluer l'efficacité des cantons dans la lutte contre la cybercriminalité et à renforcer les autorités de poursuite pénale dans le domaine des cryptomonnaies [18]. Le rapport révèle que la cybercriminalité en Suisse est en constante augmentation, tant en termes de nombre de délits que de gravité des dommages causés. La majorité des cantons ont créé des unités dédiées à la lutte contre la cybercriminalité et des postes spécialisés pour les enquêteurs, les spécialistes forensiques et les analystes. Toutefois, il est largement admis que les ressources humaines et techniques actuelles sont insuffisantes pour traiter efficacement toutes les plaintes reçues. Le rapport recommande que chaque canton procède à une auto-évaluation pour s'assurer que les moyens investis sont adéquats par rapport à la situation actuelle. Le rapport souligne également deux obstacles majeurs à une amélioration de la lutte contre la cybercriminalité : l'absence de bases légales permettant l'échange automatique d'informations entre les cantons et avec la Confédération, et les lenteurs du régime de l'entraide internationale en matière pénale, inadapté aux preuves électroniques. Ces entraves compliquent la coordination entre les enquêtes menées dans différents cantons et diminuent les chances de succès des investigations. Le rapport propose plusieurs mesures pour pallier ces lacunes, notamment le développement d'une plateforme nationale de recherche (POLAP) et la création d'une convention intercantonale sur l'échange de données à des fins d'exploitation de systèmes de bases de données communs.

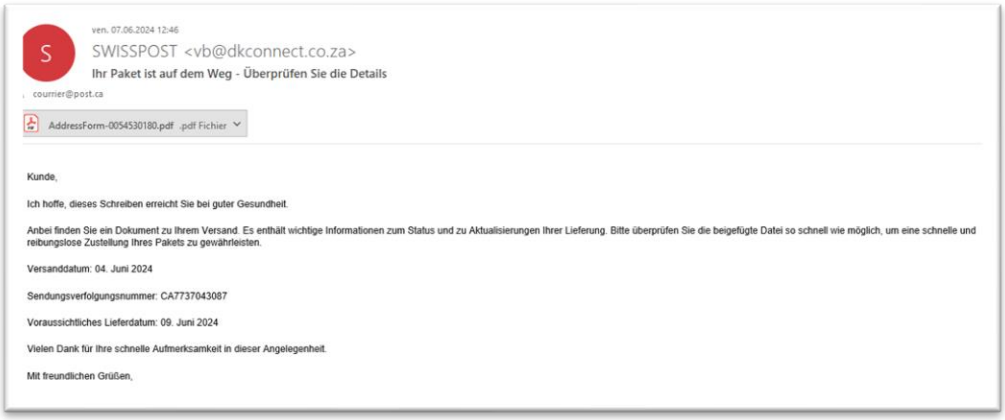
Premier bilan de l'OFCS sur la cybersécurité lors de la conférence de haut niveau sur la paix en Ukraine

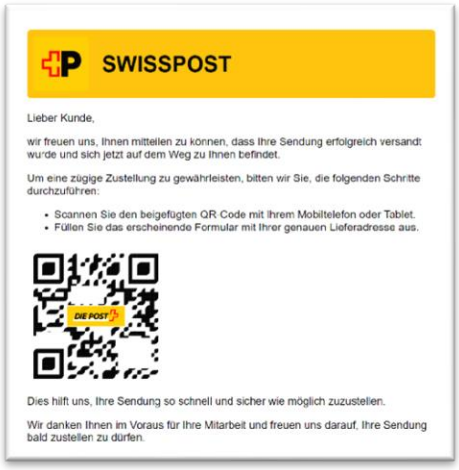
La conférence de haut niveau sur la paix en Ukraine, tenue les 15 et 16 juin 2024 au Bürgenstock, a rassemblé des délégations de près de cent États. Conformément aux attentes, plusieurs cyberattaques ont été détectées et neutralisées rapidement. L'Office fédéral de la cybersécurité (OFCS) a dressé un premier bilan de l'engagement du réseau de suivi de la cybersituation, composé d'une centaine de spécialistes issus des autorités nationales, cantonales et du secteur privé [19]. Les objectifs prioritaires de la cyberdéfense, qui incluaient la protection des moyens de communication et des ressources informatiques, ainsi que la coordination efficace entre les partenaires, ont été atteints grâce à une préparation minutieuse et une coopération sans faille. Pendant la conférence plusieurs incidents notables se sont produits dans le cyberespace. Des attaques par saturation (DDoS) menées par le groupe de hacktivistes pro-russes « NoName057(16) » ont visé les sites web de 22 autorités et organisations suisses, entraînant des perturbations mineures. Des tentatives d'intrusion dans les systèmes de messagerie des cantons de Nidwald et d'Obwald ont échoué, et une attaque de phishing contre la centrale d'appels sanitaires urgents de Lucerne a été rapidement contrée. Un incident technique lors d'une retransmission en direct a généré des rumeurs infondées de cyberattaques, tandis qu'une panne de courant à Berne a également alimenté les spéculations. Finalement, un acte de vandalisme numérique sur un portail public a été rapidement rectifié.

Incidents et activités externes et/ou globaux

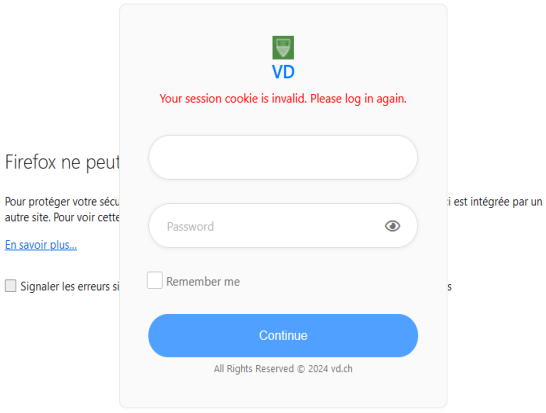
Analyse des menaces de phishing du mois

Au mois de juin, nos analyses de courriels ont révélé une recrudescence des campagnes de phishing utilisant des QR codes. Ce type de phishing se présente sous la forme d'un faux e-mail en allemand prétendant provenir de "SWISSPOST". L'e-mail informe la victime que son colis est en route et inclut une pièce jointe PDF contenant un QR code. Celui-ci redirige vers un site WordPress piraté, hébergeant un formulaire pour la saisie des informations personnelles. Nous avons également observé une variante de cette attaque durant la même période. Cette version redirige les victimes vers un formulaire de paiement sous prétexte de libérer le colis.





Ce mois, une autre campagne agressive de phishing a été détectée et bloquée par notre filtre de contenu. Cette attaque utilisait des techniques avancées de codage web pour adapter dynamiquement le logo et le nom de la société en fonction de l'adresse e-mail d'origine du clic. La page de phishing, hébergée sur un site compromis, affichait un message d'erreur "Your session cookie is invalid. Please log in again." et demandait aux utilisateurs de saisir leurs identifiants de connexion. Cette ruse ajoutait une couche de légitimité à l'attaque. L'utilisation d'une URL trompeuse comme "vd.ch" visait à convaincre les victimes qu'elles se trouvaient sur un site officiel. Dans la brève période d'environ une heure entre le signalement et la détection, nos systèmes n'ont relevé aucune interaction de nos utilisateurs sur la page, excluant ainsi la nécessité de prendre contact avec d'éventuelles victimes.



Fausses alertes antivirus affichées dans la barre de notifications

Les services de cybersécurité sont régulièrement sollicités, particulièrement ces derniers mois [20], pour des messages pop-up de prétendues alertes virus. Ces fausses alertes sont générées par des sites web malveillants qui utilisent une fonctionnalité des navigateurs permettant l'affichage de notifications. En général, ces sites obtiennent le consentement des utilisateurs en les incitant à accepter des notifications via des fenêtres contextuelles ou des messages trompeurs. Une fois ce consentement obtenu, ils peuvent envoyer des notifications alarmantes prétendant que l'ordinateur est infecté par des virus, incitant ainsi à cliquer sur des liens dangereux.

Bien que la fonctionnalité de notifications puisse être très utile pour des cas d'usage légitimes, comme l'arrivée de nouveaux e-mails, les rappels d'événements ou les notifications de réseaux sociaux, il est important de savoir comment gérer ces notifications pour éviter les abus. Il est en effet possible de contrôler quels sites peuvent utiliser la fonctionnalité de notification web dans les paramètres du navigateur et, dans certains cas, via des politiques de gestion en entreprise.

Récupération d'un domaine par un acteur malveillant

Le 25 juin 2024, une attaque de la chaîne d'approvisionnement a affecté plus de 100'000 sites via le domaine polyfill[.]io. Une entreprise chinoise, Funnull, a acquis le domaine polyfill[.]io à la suite de son abandon par la communauté open-source, et modifié des scripts pour rediriger les utilisateurs vers des sites malveillants. Ce service polyfill fournit du code JavaScript qui ajoute des fonctionnalités modernes à des navigateurs plus anciens (comme Internet Explorer). Sansec, une société de cybersécurité, a découvert cette intrusion et averti que le script injectait des logiciels malveillants sur des appareils mobiles. Cloudflare et Fastly ont créé des miroirs du service pour réduire les risques. Dans le cadre des fonctions du SOC et du CSIRT, une évaluation des sites cantonaux et communaux est en cours. Des premières prises de contact ont été opérées fin juin afin de supprimer les accès à ce domaine polyfill[.]io. [21]

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
Microsoft Message Queuing (MSMQ) CVE-2024-30080	Une vulnérabilité critique a été identifiée dans le composant MSMQ de Microsoft, permettant l'exécution de code à distance (RCE) [22]. En envoyant des paquets spécialement conçus, un attaquant non authentifié peut exploiter cette faille pour compromettre totalement le système cible. Les impacts potentiels incluent l'exfiltration de données, l'accès non autorisé aux systèmes et la possibilité d'exécuter du code malveillant. Pour mitiger cette menace, il est recommandé de désactiver le service MSMQ si non nécessaire et de déployer les correctifs fournis par Microsoft.
Microsoft Outlook CVE-2024-30103	Cette vulnérabilité permet une exécution de code à distance sans interaction de l'utilisateur via l'aperçu des e-mails dans Microsoft Outlook [23]. Un attaquant peut exploiter cette faille pour créer des fichiers DLL malveillants, pouvant conduire à une compromission totale du système. Découverte par Morphisec, [24] cette vulnérabilité n'a pas encore été divulguée, mais la présentation du PoC lors de la conférence DEFCON en août pourrait faciliter son exploitation. Elle a été corrigée dans le cadre des mises à jour de sécurité du Patch Tuesday de juin 2024. Les impacts potentiels incluent l'exfiltration de données, l'accès non autorisé aux systèmes et la possibilité d'exécuter du code malveillant. Les mesures de mitigation incluent la mise à jour rapide des clients Outlook vers les versions corrigées. Dans l'impossibilité de patcher rapidement, la désactivation de la fonctionnalité d'aperçu automatique des e-mails est particulièrement recommandée, en particulier après la divulgation du PoC.
Veeam Backup Enterprise Manager CVE-2024-29849	Une vulnérabilité critique a été découverte dans Veeam Backup Enterprise Manager [25], permettant à un attaquant non authentifié de se connecter à l'interface web de gestion en tant que n'importe quel utilisateur. Cette faille a attiré l'attention car elle permettait à un attaquant de s'authentifier en tant qu'utilisateur légitime sans aucune vérification, menaçant la sécurité des données critiques sauvegardées par de nombreuses entreprises et institutions.
Phoenix SecureCore UEFI CVE-2024-0762	Une vulnérabilité a été découverte dans le firmware Phoenix SecureCore UEFI, affectant de nombreux modèles de PC équipés de processeurs Intel. Cette faille, surnommée "UEFICanHazBufferOverflow," [26], peut potentiellement permettre à un attaquant de prendre le contrôle de la machine au niveau du firmware, échappant ainsi aux contrôles de sécurité du système d'exploitation. Les entreprises utilisant massivement des PC équipés de ces microsystèmes, sont particulièrement concernées. Il est conseillé d'appliquer les mises à jour fournies par les fabricants, comme Lenovo [27], dès que possible.

Sources

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

[1] « Ticketmaster confirms massive breach after stolen data for sale online », BleepingComputer. Consulté le: 3 juillet 2024. [En ligne]. Disponible sur: https://www.bleepingcomputer.com/news/security/ticketmaster-confirms-massive-breach-after-stolen-data-for-sale-online/
[2] « Telegram Combolists and 361M Email Addresses », Troy Hunt. Consulté le: 3 juillet 2024. [En ligne]. Disponible sur: https://www.troyhunt.com/telegram-combolists-and-361m-email-addresses/
[3] « Cybercriminals pose as "helpful" Stack Overflow users to push malware », BleepingComputer. Consulté le: 3 juillet 2024. [En ligne]. Disponible sur: https://www.bleepingcomputer.com/news/security/cybercriminals-pose-as-helpful-stack-overflow-users-to-push-malware/
[4] « Malicious VSCode extensions with millions of installs discovered », BleepingComputer. Consulté le: 3 juillet 2024. [En ligne]. Disponible sur: https://www.bleepingcomputer.com/news/security/malicious-vscode-extensions-with-millions-of-installs-discovered/
[5] « UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion », Google Cloud Blog. Consulté le: 3 juillet 2024. [En ligne]. Disponible sur: https://cloud.google.com/blog/topics/threat-intelligence/unc5537-snowflake-data-theft-extortion
[6] « More than 12,000 Santander employees in US affected by Snowflake customer breach ». Consulté le: 3 juillet 2024. [En ligne]. Disponible sur: https://therecord.media/santander-employees-bank-breach-affected
[7] « Neiman Marcus says 64,000 affected by breach of Snowflake customer account ». Consulté le: 3 juillet 2024. [En ligne]. Disponible sur: https://therecord.media/neiman-marcus-snowflake-breach-thousands
[8] « Pure Storage confirms data breach after Snowflake account hack », BleepingComputer. Consulté le: 3 juillet 2024. [En ligne]. Disponible sur: https://www.bleepingcomputer.com/news/security/pure-storage-confirms-data-breach-after-snowflake-account-hack/
[9] N. C. S. Centrum, « Aanhoudende statelijke cyberspionagecampagne via kwetsbare edge devices - Nieuwsbericht - Nationaal Cyber Security Centrum ». Consulté le: 4 juillet 2024. [En ligne]. Disponible sur: https://www.ncsc.nl/actueel/nieuws/2024/juni/10/aanhoudende-statelijke-cyberspionagecampagne-via-kwetsbare-edge-devices
[10] Z. Zorz, « 20,000 FortiGate appliances compromised by Chinese hackers », Help Net Security. Consulté le: 4 juillet 2024. [En ligne]. Disponible sur: https://www.helpnetsecurity.com/2024/06/12/coathanger-fortigate/
[11] « Des hôpitaux londoniens doivent annuler des opérations à cause d'une cyberattaque », rts.ch. Consulté le: 4 juillet 2024. [En ligne]. Disponible sur: https://www.rts.ch/info/monde/2024/article/des-hopitaux-londoniens-doivent-annuler-des-operations-a-cause-d-une-cyberattaque-28527005.html
[12] « Blood Shortages Hit London Hospitals After Ransomware Attack ». Consulté le: 4 juillet 2024. [En ligne]. Disponible sur: https://www.darkreading.com/cyberattacks-data-breaches/blood-shortages-hit-london-hospitals-after-ransomeware-attack
[13] C. Jones, « Qilin has 'no regrets' over the healthcare crisis it caused ». Consulté le: 4 juillet 2024. [En ligne]. Disponible sur: https://www.theregister.com/2024/06/20/qilin_our_plan_was_to/
[14] « Medical-Targeted Ransomware Is Breaking Records After Change Healthcare's $22M Payout | WIRED ». Consulté le: 4 juillet 2024. [En ligne]. Disponible sur: https://www.wired.com/story/change-healthcare-22-million-payment-ransomware-spike/
[15] D. fédéral de la défense DDPS de la protection de la population et des sports, « Des cybercriminels diffusent des maliciels pour macOS au nom d'AGOV ». Consulté le: 3 juillet 2024. [En ligne]. Disponible sur: https://www.ncsc.admin.ch/ncsc/fr/home/aktuell/im-fokus/2024/poseidon.html
[16] « "Poseidon" Mac stealer distributed via Google ads | Malwarebytes ». Consulté le: 3 juillet 2024. [En ligne]. Disponible sur: https://www.malwarebytes.com/blog/news/2024/06/poseidon-mac-stealer-distributed-via-google-ads
[17] W. agence digitale, « Informations sur une cyberattaque ayant visé un fournisseur de services informatiques de la Ville ». Consulté le: 3 juillet 2024. [En ligne]. Disponible sur: https://www.yverdon-les-bains.ch/medias/actualites/detail/annonce-dune-fuite-de-donnees-par-un-fournisseur-externe-du-service-des-energies-de-la-ville-dyverdon-les-bains

[18] « Le Conseil fédéral publie un rapport sur la lutte contre la cybercriminalité en Suisse ». Consulté le: 4 juillet 2024. [En ligne]. Disponible sur: https://www.admin.ch/gov/fr/accueil/documentation/communiques.msg-id-101469.html
[19] D. fédéral de la défense DDPS de la protection de la population et des sports, « Conférence de haut niveau sur la paix en Ukraine : premier bilan de l'OFCS sur les travaux du réseau de suivi de la cybersituation ». Consulté le: 4 juillet 2024. [En ligne]. Disponible sur: https://www.ncsc.admin.ch/ncsc/fr/home/aktuell/im-fokus/2024/kfu-erste-bilanz.html
[20] « Think twice before accepting notifications on Chrome: threats on the rise », Cybernews. Consulté le: 3 juillet 2024. [En ligne]. Disponible sur: https://cybernews.com/security/chrome-notifications-lurking-dangers/
[21] « Polyfill.io JavaScript supply chain attack impacts over 100K sites », BleepingComputer. Consulté le: 5 juillet 2024. [En ligne]. Disponible sur: https://www.bleepingcomputer.com/news/security/polyfillio-javascript-supply-chain-attack-impacts-over-100k-sites/
[22] « CVE-2024-30080 - Security Update Guide - Microsoft - Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability ». Consulté le: 2 juillet 2024. [En ligne]. Disponible sur: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-30080
[23] « CVE-2024-30103 - Security Update Guide - Microsoft - Microsoft Outlook Remote Code Execution Vulnerability ». Consulté le: 2 juillet 2024. [En ligne]. Disponible sur: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2024-30103
[24] « You've Got Mail: Critical Microsoft Outlook Vulnerability Executes as Email is Opened ». Consulté le: 2 juillet 2024. [En ligne]. Disponible sur: https://blog.morphisec.com/cve-2024-30103-microsoft-outlook-vulnerability
[25] « KB4581: Veeam Backup Enterprise Manager Vulnerabilities (CVE-2024-29849, CVE-2024-29850, CVE-2024-29851, CVE-2024-29852) », Veeam Software. Consulté le: 2 juillet 2024. [En ligne]. Disponible sur: https://www.veeam.com/kb4581?ck=1700057206377
[26] C. Garland, « UEFIcanhazbufferoverflow: Widespread Impact from Vulnerability in Popular PC and Server Firmware », Eclypsium | Supply Chain Security for the Modern Enterprise. Consulté le: 2 juillet 2024. [En ligne]. Disponible sur: https://eclypsium.com/blog/ueficanhazbufferoverflow-widespread-impact-from-vulnerability-in-popular-pc-and-server-firmware/
[27] « Multi-vendor BIOS Security Vulnerabilities (May, 2024) - Lenovo Support HK ». Consulté le: 2 juillet 2024. [En ligne]. Disponible sur: https://support.lenovo.com/hk/en/product_security/ps500621-multi-vendor-bios-security-vulnerabilities-may-2024