Classification : **PUBLIQUE**

TLP:CLEAR

Revue mensuelle des cybermenaces

Février 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.

Le paysage global des menaces

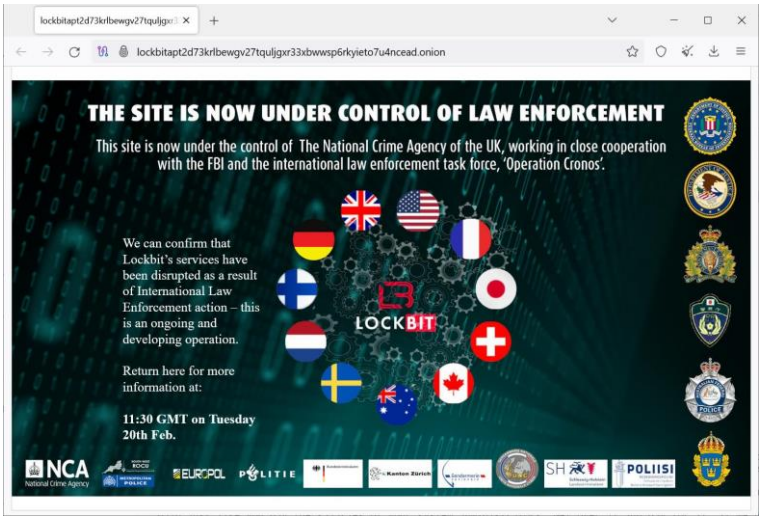
Actualités internationales

Les groupes d'attaquants évoluent

Le groupe de pirates informatiques TA577 est de retour. Ils utilisent désormais des e-mails de phishing pour s'emparer des informations d'authentification (hash NTLM). Bien que TA577 ait précédemment été associé à Qakbot et aux infections ransomwares de Black Basta, de nouvelles campagnes ont été observées les 26 et 27 février 2024. Ces campagnes utilisent des e-mails de phishing qui semblent être des réponses à des discussions antérieures, avec des pièces jointes ZIP uniques contenant des fichiers HTML malveillants. Un lien dans ces fichiers pointe sur un serveur SMB externe. Bien que ces attaques n'aient pas livré de charges utiles de logiciels malveillants, elles visent à capturer des hachages NTLM, qui peuvent être utilisés pour des attaques ultérieures telles que l'escalade de privilèges, le détournement de comptes, et la reconnaissance au sein d'un réseau compromis. [1]

Ce groupe est actif dans la récupération d'accès initiaux, qui peuvent ensuite être revendus à d'autres acteurs malicieux afin de déployer des attaques de plus grande envergure, telles que des rançongiciels. Il est particulièrement dangereux et surveillé par la communauté.

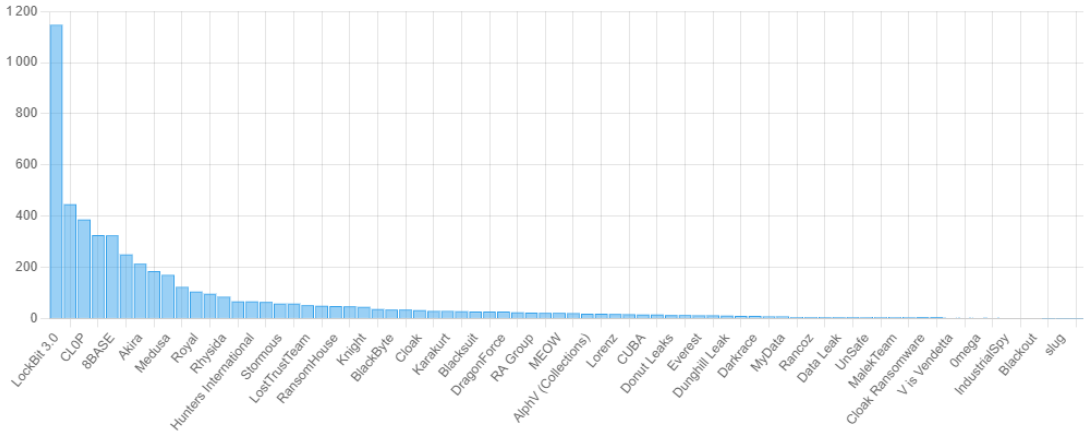
Un autre groupe de pirate, LockBit, actif dans les opérations de ransomware-as-a-service, a été perturbé par une opération de police de grande ampleur : le site d'annonce des victimes de LockBit a en particulier été saisi et affichait le message habituel dans ce genre de cas. [2]



Apparemment une vulnérabilité PHP aurait permis aux autorités de prendre le contrôle d'une partie de l'infrastructure de l'attaquant, de publier des clés de déchiffrement pour les victimes, et même d'arrêter deux opérateurs du gang en Pologne et en Ukraine.

Moins d'une semaine après cette opération, une nouvelle infrastructure réapparaissait sur le Darknet et le groupe annonçait une reprise de ses activités, avec une meilleure sécurité, ressemblant une opération de communication pour rassurer ses affiliés, mais démontrant la complexité de démanteler complétement un groupe de cyber-pirates. [3]

Pour rappel, LockBit 3.0 est le ransomware le plus actif des 12 derniers mois, avec près de 1'150 victimes à travers le monde, dont un tiers aux Etats-Unis.



Les attaques et vols de données également

Un employé du service financier d'une multinationale hong-kongaise a été victime d'une escroquerie sophistiquée impliquant l'utilisation de deepfake. Un cyberpirate a invité la victime à une vidéoconférence comprenant de faux participants ressemblant à des collègues et au directeur financier. Sous l'influence de cette manipulation visuelle et auditive, la victime a effectué 15 transactions totalisant 24 millions d'Euros. L'escroquerie a été découverte plusieurs jours plus tard, soulignant la nécessité d'une vigilance constante. [4]

La prévention contre de telles attaques repose sur une sensibilisation accrue des employés aux risques du deepfake et de l'ingénierie sociale. Les entreprises doivent renforcer la formation de leurs employés et mettre en place des mesures de protection avancées. Il est crucial d'éduquer les employés sur la reconnaissance des signaux d'alerte, tels que des demandes de transactions secrètes, et de promouvoir une culture de cybersécurité solide.

Une cyberattaque d'ampleur historique a frappé Viamedis et Almerys, responsables de la gestion du tiers payant pour des assurances complémentaires en France, exposant les données de plus de 33 millions de personnes, représentant près de la moitié de la population française. Les informations compromises incluent des détails cruciaux tels que l'état civil, la date de naissance et les numéros de sécurité sociale. Bien que la CNIL rassure sur l'absence de données médicales et bancaires parmi les victimes, elle met en garde contre le risque d'hameçonnage. [5]

Les vulnérabilités critiques continuent

Les vulnérabilités critiques continuent en ce début d'année avec Fortinet qui a sorti un correctif pour son système d'exploitation FortiOS impactant en particulier sa solution VPN. Cette faille semblait déjà être exploitée avant sa publication, et a attiré l'attention de nombreux autres attaquants dès sa sortie. Ce n'est malheureusement ni la première ni la dernière vulnérabilité trouvée sur ces composants déployés très largement depuis la pandémie. [6]

Le Patch Tuesday, sortie mensuelle des correctifs pour les solutions Microsoft, a également compris son lot de vulnérabilités critiques [7]. En particulier deux peuvent être relevées. L'une dans Microsoft Office, qui permet à un attaquant d'automatiquement exécuter du code à partir du panneau de prévisualisation des courriels dans Outlook, en envoyant un document piégé [8]. Une autre dans Exchange, qui permet à un attaquant non authentifié d'élever ses privilèges en s'appuyant sur une attaque par relais NTLM ciblant un serveur Microsoft Exchange vulnérable. Cela signifie que l'attaquant va parvenir à s'authentifier auprès du serveur de messagerie en usurpant l'identité de l'utilisateur pris pour cible [9]. De précédentes vulnérabilités permettent justement de voler des identifiants NTLM, et les récentes activités du groupe TA557 (voir ci-dessus) justifie le niveau critique de cette vulnérabilité.

Actualités suisses

Concernant la vulnérabilité Microsoft Exchange corrigée dans le Patch Tuesday de février, il a été identifié 2'119 serveurs vulnérables en Suisse, parmi les 97'000 au niveau mondial. La majorité devrait être patchée dans les prochaines semaines mais il en restera malheureusement toujours quelques-uns avec cette vulnérabilité qui pourrait être exploitée dans le futur et potentiellement causer d'important dégâts ou vol de données. [10]

L'entreprise suisse Datasport a été victime d'une cyberattaque. Les données volées de près d'un million de sportifs amateurs contiennent des noms, des numéros de téléphone et des adresses e-mail. Elles ont été mises en vente sur une plateforme de pirates informatiques. Comme souvent, l'entreprise a d'abord cru que seules quelques jeux de données étaient concernés, avant de se rendre compte de l'ampleur du vol. [11]

La société Bâloise de placement de personnel « Le Team », possédant 25 succursales en Suisse a été victime du rançongiciel Black Basta, qui a pu voler 200 gigaoctets en décembre 2023. Ce n'est finalement que le 21 février que l'entreprise s'est rendu compte de l'ampleur de la fuite et a communiqué sur l'incident. Il s'agit notamment de données pertinentes pour l'entreprise, de contrats signés avec les clients, d'informations d'ordre financier et d'autres informations internes, mais également des données personnelles des clients, comme des copies de cartes d'identité ou des dossiers médicaux. [12]

Incidents et activités externes et/ou globaux

Certains utilisateurs ont besoin de transformer des fichiers Microsoft Office en PDF. Souvent leur premier réflexe est de télécharger le premier utilitaire gratuit proposé par le moteur de recherche et qui souvent peut être exécuté sans installation. Malheureusement ces outils sont souvent accompagnés d'un Adware (petit logiciel se chargeant d'injecter de la publicité) qui s'installe dans le profil de l'utilisateur. Même si ces Adware ne se chargent que d'ajouter un système de publicités (non désirées), ils peuvent évoluer une fois installés et proposer d'autres services comme la collecte d'information ou dans de récents cas (malware AdLoad [13]), être utilisé comme proxy. Ces applications souvent utilisées une seule fois restent présentes sur les postes de travail et peuvent rester une menace bien après leur utilisation.

L'augmentation du cours des crypto monnaies ses dernières semaines ne passe pas inaperçue pour les spammeurs qui profitent de la situation en envoyant de nombreux messages non sollicités à nos collaborateurs. Ces e-mails promettent des gains importants en bitcoin ou ethereum sur des plateformes fictives crées pour l'occasion.

A la suite de la divulgation par l'éditeur Fortinet de deux vulnérabilités affectant leurs équipements firewalls (CVE-2024-21762 et CVE-2024-23113), une communication spécifique a été entreprise via l'application mobile Cybersécurité proposée par la DGNSI. Des partenaires IT des communes ont été avertis spécifiquement de l'importance du patching rapide de ces vulnérabilités, de même que des partenaires locaux du canton.

La fondation Shadowserver, effectuant des scans d'Internet à la recherche de vulnérabilités, est désormais utilisée régulièrement par le SOC en cas de vulnérabilité critique. Plusieurs communes ont ainsi été contactées spécifiquement afin de demander un patching prioritaire contre ces deux vulnérabilités Fortinet. D'autres vulnérabilités touchant les infrastructures Microsoft Exchange ont également été remontées par la solution Shadowserver. Un contact a été pris par le service CSIRT avec les communes concernées, et un suivi sera effectué afin de s'assurer de la correction de ces failles, qui, rappelons-le, sont le plus souvent utilisées comme porte d'entrée lors d'attaques par rançongiciel.

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
Fortinet CVE -2024-21762 CVE-2024-23313	Il s'agit d'une vulnérabilité d'écriture hors limites dans FortiOS, qui permet à un attaquant distant non authentifié d'exécuter du code arbitraire ou des commandes via des requêtes HTTP spécialement conçues. Cette vulnérabilité peut être exploitée pour prendre le contrôle d'un système affecté. Versions affectées : Diverses versions de FortiOS, FortiProxy, FortiPAM et FortiSwitchManager sont touchées par l'une ou l'autre de ces vulnérabilités, et des versions corrigées ont été fournies. Cependant, certaines anciennes versions ne recevront pas de correctif, donc les utilisateurs sont invités à migrer vers une version corrigée. Pour les versions vulnérables, il est recommandé de télécharger les mises à jour manuellement depuis le site de Fortinet ou de désactiver SSL VPN (pour CVE-2024-21762) ou de supprimer l'accès fgfm pour chaque interface (pour CVE-2024-23313)1234. Il est important de noter que les vulnérabilités dans les Fortinet SSL VPN ont été ciblées par des acteurs de la menace hautement motivés, et certaines ont été exploitées en tant que zero-day ou après leur divulgation publique [14]
Microsoft CVE-2024-21412	La CVE-2024-21412 est une vulnérabilité qui découle d'un défaut d'application de la fonctionnalité de " Mark-of-the-Web " (MotW), utilisée par Windows pour identifier les fichiers provenant de sources potentiellement non fiables, telles que les téléchargements Internet, WebDAV et les partages SMB. En temps normal, les fichiers téléchargés depuis le Web sont marqués avec la MotW, ce qui incite Windows Defender SmartScreen à émettre des alertes lorsque ces fichiers tentent de s'exécuter ou lorsque l'utilisateur essaie de les exécuter directement. Ce mécanisme constitue une défense essentielle, empêchant l'exécution de code non autorisé ou malveillant sans la connaissance ou le consentement de l'utilisateur. Cependant, la CVE-2024-21412 a permis aux attaquants de contourner ces protections en exploitant une faille dans la gestion des raccourcis Internet (fichiers .URL) et d'autres mécanismes. Grâce à des campagnes de spear-phishing soigneusement conçues et à l'utilisation de sites Web compromis, les attaquants ont distribué ces fichiers .URL malveillants. Lorsqu'ils sont exécutés, ces fichiers ne portaient pas la balise MotW, aveuglant ainsi SmartScreen quant à leur intention malveillante. Cette négligence a permis l'exécution du malware DarkMe

Sources

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

[1] « TA577's Unusual Attack Chain Leads to NTLM Data Theft | Proofpoint US », Proofpoint. Consulté le: 8 mars 2024. [En ligne]. Disponible sur: https://www.proofpoint.com/us/blog/threat-insight/ta577s-unusual-attack-chain-leads-ntlm-data-theft
[2] « LockBit ransomware disrupted by global police operation ». Consulté le: 5 mars 2024. [En ligne]. Disponible sur: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-disrupted-by-global-police-operation/
[3] « LockBit ransomware returns, restores servers after police disruption ». Consulté le: 5 mars 2024. [En ligne]. Disponible sur: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-returns-restores-servers-after-police-disruption/
[4] « Piégé par un deepfake en visio, un employé transfère 24 M€ à des escrocs - Le Monde Informatique », LeMondeInformatique. Consulté le: 5 mars 2024. [En ligne]. Disponible sur: https://www.lemondeinformatique.fr/actualites/lire-piege-par-un-deepfake-en-visio-un-employe-transfere-24-meteuro-a-des-escrocs-92875.html
[5] « Un vol massif de données touche la moitié de la population française ». Consulté le: 5 mars 2024. [En ligne]. Disponible sur: https://www.ictjournal.ch/news/2024-02-13/un-vol-massif-de-donnees-touche-la-moitie-de-la-population-francaise
[6] Z. Zorz, « Critical Fortinet FortiOS flaw exploited in the wild (CVE-2024-21762) », Help Net Security. Consulté le: 5 mars 2024. [En ligne]. Disponible sur: https://www.helpnetsecurity.com/2024/02/12/critical-fortinet-fortios-flaw-exploited-in-the-wild-cve-2024-21762/
[7] « Patch Tuesday - February 2024 | Rapid7 Blog », Rapid7. Consulté le: 5 mars 2024. [En ligne]. Disponible sur: https://www.rapid7.com/blog/post/2024/02/13/patch-tuesday-february-2024/
[8] « CVE-2024-21413 - Security Update Guide - Microsoft - Microsoft Outlook Remote Code Execution Vulnerability ». Consulté le: 6 mars 2024. [En ligne]. Disponible sur: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-21413
[9] « CVE-2024-21410 - Security Update Guide - Microsoft - Microsoft Exchange Server Elevation of Privilege Vulnerability ». Consulté le: 6 mars 2024. [En ligne]. Disponible sur: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2024-21410
[10] « Plus de 2000 serveurs Exchange suisses vulnérables à une faille | ICTjournal ». Consulté le: 5 mars 2024. [En ligne]. Disponible sur: https://www.ictjournal.ch/news/2024-02-20/plus-de-2000-serveurs-exchange-suisses-vulnerables-a-une-faille
[11] « Datasport subit un vol de données: 900'000 Suisses concernés ». Consulté le: 6 mars 2024. [En ligne]. Disponible sur: https://www.ictjournal.ch/news/2024-02-05/datasport-subit-un-vol-de-donnees-900000-suisses-concernes
[12] « Une société suisse a été hackée et des données très sensibles volées », watson.ch/fr. Consulté le: 5 mars 2024. [En ligne]. Disponible sur: https://www.watson.ch/fr/!414451442
[13] P. Paganini, « A massive campaign delivered a proxy server application to 400,000 Windows systems », Security Affairs. Consulté le: 8 mars 2024. [En ligne]. Disponible sur: https://securityaffairs.com/149592/cyber-crime/rise-proxy-server-application.html
[14] « PSIRT Advisories | FortiGuard ». Consulté le: 2 mars 2023. [En ligne]. Disponible sur: https://www.fortiguard.com/psirt/FG-IR-22-300