Rapport de renseignement cybermenaces

Août 2022

SOC – Centre opérationnel de sécurité

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

DGNSI

LIBERTÉ ET PATRIE

Direction générale du numérique
et des systèmes d'information

Système de Management Certifié SQS ISO 9001

ENSEMBLE POUR UNE SOCIÉTÉ NUMÉRIQUE RESPONSABLE

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.

Sommaire

Le paysage global des menaces

Actualités internationales

Les pirates responsables d'une série de cyberattaques récentes, y compris celles sur Twilio, MailChimp et Klaviyo, ont compromis plus de 130 organisations dans la même campagne de phishing. Cette campagne de phishing a utilisé un kit de phishing nommé « 0ktapus » pour voler 9 931 identifiants de connexion que les pirates ont ensuite utilisés pour accéder aux réseaux et systèmes de l'entreprise via des VPN et d'autres dispositifs d'accès à distance. La campagne 0ktapus est en cours depuis au moins mars 2022, visant à voler les identifiants d'identité Okta et les codes 2FA et à les utiliser pour mener des attaques ultérieures. Selonkta, l'acteur de la menace appelle les personnes ciblées et se fait passer pour l'assistance afin de comprendre le fonctionnement de l'authentification. Les cibles jusqu'à présent incluent les entreprises technologiques, les fournisseurs de télécommunications et les organisations ou les individus liés à la crypto-monnaie. [1], [2]

Cisco a annoncé le 10 août qu'à la fin du mois de mai dernier un groupe de ransomware nommé Yanluowang a réussi à s'introduire dans son réseau pour dérober des fichiers. Le gang a aussi tenté d'extorquer l'équipementier en le menaçant d'une publication des documents volés. Pour arriver à leur fin, les cybercriminels ont compromis le compte personnel Google d'un employé de Cisco associé avec un compte Box. L'attaquant a convaincu l'employé de Cisco d'accepter les notifications push d'authentification multifactorielle (MFA) par le biais de « la fatigue MFA et d'une série d'attaques sophistiquées de phishing vocal ». Une tactique payante, car le collaborateur accepte une de ses notifications et les cybecriminels peuvent ainsi accéder à son VPN et prendre pied dans le réseau de l'entreprise. Par la suite, le gang s'est déplacé latéralement pour compromettre des serveurs Citrix et obtenir des élévations de privilèges sur les contrôleurs de domaines. Disposant d'un pouvoir admin, ils ont utilisé des outils d'énumération comme ntdsutil, adfind et secretsdump pour collecter plus d'informations et ont installé une série de charges utiles sur les systèmes compromis, y compris une porte dérobée. [3]

Le département d'État américain a annoncé le 11 août une récompense de 10 millions de dollars pour des informations sur cinq membres de haut rang du rançongiciel Conti, notamment en montrant le visage de l'un des membres pour la première fois. Le programme Rewards of Justice est un programme du Département d'État américain dans le cadre duquel des récompenses monétaires sont offertes pour des informations relatives à des acteurs menaçants affectant la sécurité nationale des États-Unis. Lancé initialement pour recueillir des informations sur les terroristes ciblant les intérêts américains, le programme s'est étendu pour offrir des récompenses pour les informations sur les cybercriminels, tels que les pirates russes Sandworm , le rançongiciel REvil et le groupe de piratage Evil Corp. [4]

South Staffordshire Water, une compagnie qui fournit de l'eau potable à 1,6 million de Britanniques, a été la victime d'une cyber-attaque. L'approvisionnement en eau n'est en soi pas menacé, selon la compagnie, car il est en grande partie indépendant des systèmes IT internes qui ont été agressés. Le communiqué a été publié, après qu'un groupe exploitant un rançongiciel et appelé Clop ait indiqué sur un forum avoir attaqué les systèmes IT d'une autre compagnie des eaux. Clop y évoque cependant Thames Water, une compagnie nettement plus grande qui fournit elle de l'eau à 15 millions de Britanniques dans la région de Londres. Les attaquants se sont ainsi trompés de cibles et n'ont pas atteint la bonne société. [5]

Le gang de rançongiciels LockBit - une opération de rançongiciel active depuis près de trois ans répertoriant plus de 700 victimes - a annoncé qu'il travaillait à renforcer ses défenses contre les attaques par déni de service distribué et qu'il allait intensifier l'activité pour tripler l'extorsion. Ce sont là les effets d'une attaque DDoS subie ces derniers temps dans le but présumé d'empêcher le groupe de publier des données d'entreprise volées au géant de la sécurité Entrust. Les données ont été saisies le 18 juin et devaient être rendues publiques le 19 août car la société Entrust a refusé de payer la rançon. L'attaque DDoS n'a mis qu'un arrêt temporaire aux fuites de données Entrust. LockBit est maintenant opérationnel et était

prêt à partager la fuite de données Entrust avec tous ceux qui s'y intéressent. Après cela, le 27 août, LockBit a publié un torrent avec 343 Go de données appelé "entrust.com", comme promis précédemment. [6], [7]

Le 21 aout, un Centre Hospitalier en France à Corbeil-Essonnes a été victime d'une attaque informatique. L'activité de l'établissement est sérieusement perturbée. Une demande de rançon de 10 millions de dollars a été exigée par les hackers, a indiqué une source policière. L'attaque a rendu inaccessible tous les logiciels métiers de l'hôpital, les systèmes de stockage notamment d'imagerie médicale et le système d'information ayant trait aux admissions des patients. Le journaliste français en cybersécurité Valéry Riess-Marchive a identifié des signes d'une infection LockBit 3.0. Si LockBit 3.0 est responsable de l'attaque contre l'hopital, il violera les règles du programme RaaS, qui interdisent aux affiliés de chiffrer les systèmes des prestataires de soins de santé. [8], [9]

A la fin du mois d'août, l'éditeur de sécurité McAfee a découvert 5 extensions Google Chrome permettant de suivre les activités de surf des utilisateurs. Celles-ci ont été téléchargées plus de 1.4 millions de fois au total. Celles-ci ont été depuis désactivées par Google : Netflix Party, Full Page Screenshot Capture, FlipShope – Price Tracker Extension… [10]

Actualités suisses

Dans le contexte de la numérisation croissante du secteur de la santé, le Centre national pour la cybersécurité (NCSC) a émis une série de recommandations à l'intention des hôpitaux et autres établissements de santé. La liste des recommandations comprend des mesures techniques ainsi qu'organisationnelles, considérées comme des « exigences minimales » en matière de cybersécurité. [11]

La Poste franchit une nouvelle étape en permettant aux chasseurs de bugs (bug bounty) de tester pour la première fois l'infrastructure de vote électronique proprement dite. Durant 4 semaines, des hackeurs étiques pourront remporter jusqu'à CHF 30'000.- s'ils trouvent une faille critique. [12]

Une faille critique dans un système des CFF a été corrigée trois ans après son signalement par des spécialistes en sécurité. Une enquête interne a été ouverte pour déterminer la cause de l'erreur et de ce délai, et des processus ont été améliorés pour réagir plus rapidement dans ce genre de situation. [13]

Principales observations et interventions du SOC

L'Administration Cantonale Vaudoise a reçu quelques courriels de type « arnaque au président » se faisant passer pour une société active sur le canton de Vaud. Un nom de domaine similaire à celui de l'entreprise a été créé pour l'occasion afin de tromper les utilisateurs. Ces e-mails ont été interceptés et bloqués. Cette société a été contactée pour qu'elle puisse prendre les mesures nécessaires.

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
Atlassian CVE-2022-36804	Atlassian a publié un avis de sécurité avertissant les utilisateurs de Bitbucket Server et de Data Center d'une faille de sécurité critique que les attaquants pourraient exploiter pour exécuter du code arbitraire sur des instances vulnérables. La dernière faille est une injection de commande dans plusieurs points de terminaison API du produit logiciel. Il a reçu un score de gravité CVSS de 9,9 sur un maximum de 10,0, ce qui en fait une vulnérabilité critique qui doit être corrigée immédiatement. [14]
Apple CVE-2022-32893 CVE-2022-32894	Apple a publié une mise à jour Safari pour macOS Big Sur et Catalina afin de corriger une vulnérabilité zero-day exploitée à l'état sauvage pour pirater des Mac. Le correctif zero-day est un problème d'écriture hors limites dans WebKit qui pourrait permettre à un pirate d'exécuter du code à distance sur un appareil vulnérable. [15]
Palo Alto CVE-2022-0028	Palo Alto Networks a émis un avertissement de sécurité concernant une vulnérabilité activement exploitée affectant PAN-OS, le système d'exploitation utilisé par les produits matériels de mise en réseau de l'entreprise. Le problème est une mauvaise configuration de la politique de filtrage d'URL qui pourrait permettre à un attaquant distant non authentifié de mener des attaques par déni de service (DoS) TCP amplifiées. [16]

Sources

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

[1] « Okta entangled by Twilio phishing attack », *Cybersecurity Dive*. https://www.cybersecuritydive.com/news/okta-twilio-phishing-attack/630820/ (consulté le 6 septembre 2022).

[2] « Twilio hackers hit over 130 orgs in massive Okta phishing attack », *BleepingComputer*. https://www.bleepingcomputer.com/news/security/twilio-hackers-hit-over-130-orgs-in-massive-okta-phishing-attack/ (consulté le 6 septembre 2022).

[3] « Cisco hacked by Yanluowang ransomware gang, 2.8GB allegedly stolen », *BleepingComputer*. https://www.bleepingcomputer.com/news/security/cisco-hacked-by-yanluowang-ransomware-gang-28gb-allegedly-stolen/ (consulté le 6 septembre 2022).

[4] « US govt will pay you $10 million for info on Conti ransomware members », *BleepingComputer*. https://www.bleepingcomputer.com/news/security/us-govt-will-pay-you-10-million-for-info-on-conti-ransomware-members/ (consulté le 6 septembre 2022).

[5] « Hackers attack UK water supplier but extort wrong company », *BleepingComputer*. https://www.bleepingcomputer.com/news/security/hackers-attack-uk-water-supplier-but-extort-wrong-company/ (consulté le 6 septembre 2022).

[6] « LockBit ransomware gang gets aggressive with triple-extortion tactic », *BleepingComputer*. https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-gets-aggressive-with-triple-extortion-tactic/ (consulté le 6 septembre 2022).

[7] « LockBit claims ransomware attack on security giant Entrust, leaks data », *BleepingComputer*. https://www.bleepingcomputer.com/news/security/lockbit-claims-ransomware-attack-on-security-giant-entrust-leaks-data/ (consulté le 6 septembre 2022).

[8] « Dans l'Essonne, le centre hospitalier Sud-Francilien victime d'une cyberattaque, son activité fortement perturbée », *Le Monde.fr*, 22 août 2022. Consulté le: 6 septembre 2022. [En ligne]. Disponible sur: https://www.lemonde.fr/pixels/article/2022/08/22/un-hopital-de-l-essonne-victime-d-une-cyberattaque-son-activite-fortement-perturbee_6138677_4408996.html

[9] « French hospital hit by $10M ransomware attack, sends patients elsewhere », *BleepingComputer*. https://www.bleepingcomputer.com/news/security/french-hospital-hit-by-10m-ransomware-attack-sends-patients-elsewhere/ (consulté le 6 septembre 2022).

[10] « Chrome extensions with 1.4 million installs steal browsing data », *BleepingComputer*. https://www.bleepingcomputer.com/news/security/chrome-extensions-with-14-million-installs-steal-browsing-data/ (consulté le 6 septembre 2022).

[11] « Des exigences de cybersécurité minimales pour les acteurs de la santé ». https://www.ictjournal.ch/news/2022-08-02/des-exigences-de-cybersecurite-minimales-pour-les-acteurs-de-la-sante (consulté le 2 septembre 2022).

[12] « La Poste convie les hackers éthiques sur son infrastructure de vote électronique ». https://www.ictjournal.ch/news/2022-08-09/la-poste-convie-les-hackers-ethiques-sur-son-infrastructure-de-vote-electronique (consulté le 2 septembre 2022).

[13] « Mise à jour: les CFF mettent trois ans à colmater la fuite de données ». https://www.ictjournal.ch/news/2022-08-19/mise-a-jour-les-cff-mettent-trois-ans-a-colmater-la-fuite-de-donnees (consulté le 2 septembre 2022).

[14] « Atlassian Bitbucket Server vulnerable to critical RCE vulnerability », *BleepingComputer*. https://www.bleepingcomputer.com/news/security/atlassian-bitbucket-server-vulnerable-to-critical-rce-vulnerability/ (consulté le 6 septembre 2022).

[15] « Apple releases Safari 15.6.1 to fix zero-day bug used in attacks », *BleepingComputer*. https://www.bleepingcomputer.com/news/security/apple-releases-safari-1561-to-fix-zero-day-bug-used-in-attacks/ (consulté le 6 septembre 2022).

[16] « Palo Alto Networks: New PAN-OS DDoS flaw exploited in attacks », *BleepingComputer*. https://www.bleepingcomputer.com/news/security/palo-alto-networks-new-pan-os-ddos-flaw-exploited-in-attacks/ (consulté le 6 septembre 2022).