Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF
Centre national pour la cybersécurité NCSC
GovCERT.ch

Cyber Security Update - Secteur de la Santé

À USAGE INTERNE UNIQUEMENT

Date : 6 octobre 2021
Version : v1.0
Auteur : NCSC/GovCERT.ch
Contact : outreach@govcert.ch
Distribution : Secteur de la Santé MELANI, H+, HIN

Actualités (Juillet – Septembre 2021)

Au cours de l'été 2021, un certain nombre d'entreprises et d'organisations en Suisse ont à nouveau été attaquées et chiffrées par des rançongiciels. L'exposition au risque du secteur de la santé reste élevée.

- Les systèmes vulnérables exposés sur Internet favorisent les attaques de rançongiciels
- Les attaques de ransomware contre les hôpitaux se poursuivent
- Étude : la moitié des hôpitaux américains hors ligne en raison d'un ransomware
- Le ransomware "DoppelPaymer" est à nouveau actif sous le nom de "Grief"
- Une attaque par la chaîne d'approvisionnement ("Supply Chain Attack") touche plusieurs entreprises en Autriche
- Entretien avec l'auteur du ransomware "LockBit 2.0"

Nous avons également intensifié la protection afin de lutter contre le botnet "QakBot".

Les systèmes vulnérables exposés sur Internet favorisent les attaques de rançongiciels

Depuis des années, le NCSC (anciennement MELANI) ne cesse de mettre l'accent sur la gestion cohérente et complète des correctifs et du cycle de vie de tous les composants. Les vulnérabilités des systèmes internes permettent aux attaquants ayant un pied dans le réseau de la victime de s'y déplacer latéralement et de compromettre d'autres systèmes et services.

Plus fatales encore sont les vulnérabilités des systèmes qui sont exposés à Internet et qui peuvent facilement être exploités à distance pour exécuter un code malveillant sur le système vulnérable ("Remote Code Execution" - RCE). Ce type de vecteur est de plus en plus utilisé par les groupes de ransomware pour obtenir un accès initial aux réseaux d'entreprise.

Au cours de l'été 2021, plusieurs vulnérabilités sérieuses, permettant de telles attaques, ont été rendue publiques :

- Escalade locale de privilèges (CVE-2021-26084) dans Atlassian Confluence Server : https://confluence.atlassian.com/doc/confluence-security-advisory-2021-08-25-1077906215.html
- Téléchargement de fichier arbitraire (CVE-2021-22005) dans VMware vCenter : https://www.vmware.com/security/advisories/VMSA-2021-0020.html
- Diverses vulnérabilités dans Pulse Connect Secure (PCS) : https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44858/

En raison de l'augmentation des attaques par ransomware, le NCSC rappelle[1] l'importance de la mise en œuvre des meilleures pratiques en matière de cybersécurité et du fait que de nombreuses entreprises et organisations ne semblent toujours pas avoir mis en œuvre de telles mesures.

Protection contre le Botnet "QakBot"

"QakBot" s'est imposé, aux côtés de "TrickBot" et "Dridex", comme un vecteur d'infection populaire pour les attaques de type rançongiciels. QakBot utilise une approche qui était déjà utilisée par "Emotet", à savoir le "Email thread hijacking" (également appelé "dynamite phishing"[2]). Des courriels sont volés sur des ordinateurs déjà infectés. Ces messages sont ensuite renvoyés à l'expéditeur du courriel, accompagné d'un contenu malicieux. De cette façon, les criminels s'insèrent dans une conversation électronique légitime et existante, encourageant le destinataire à cliquer sur un lien dans l'e-mail ou à ouvrir un fichier malveillant joint. L'ouverture du document malicieux conduit immédiatement à une infection par un logiciel malveillant.

Afin de détecter et bloquer le trafic réseau vers les serveurs C&C connus du botnet QakBot, GovCERT alimente le service "MELANI BGP Feed" en adresses IP de serveurs C&C QakBot connus et actifs depuis septembre 2021. Les entreprises et organisations qui utilisent ce service bénéficient d'une protection supplémentaire contre Qakbot.

Les attaques de ransomware contre les hôpitaux se poursuivent

L'été n'a malheureusement pas été exempt d'attaques par ransomware. Des hôpitaux ont à nouveau été touchés par des attaques. En août 2021, par exemple, le système de santé américain a également été touché. À la suite d'une attaque par ransomware[3], le complexe hospitalier Memorial Health System (MHS) de Marietta, dans l'Ohio, a dû reporter ses opérations et refuser les patients dans la section d'urgence. En outre, MHS a dû recourir à des "procédures de secours" pour assurer un fonctionnement minimal.

[1] https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/ransomware-8.html

[2] https://www.heise.de/news/Ransomware-Qakbot-tritt-in-Emotets-Fussstapfen-6181387.html

[3] https://www.beckershospitalreview.com/cybersecurity/surgeries-canceled-ambulances-diverted-it-system-down-at-ohio-health-system-after-ransomware-attack.html

Selon plusieurs médias et déclarations du FBI[4], le ransomware "Hive" serait à l'origine de l'attaque contre MHS, utilisant des malspams et le protocole RDP (Remote Desktop Protocol) pour accéder aux réseaux d'entreprise. Il n'est pas connu si les attaquants ont demandé une rançon et si l'hôpital concerné y a donné suite. Toutefois, le magazine spécialisé Bleeping Computer[5] affirme avoir reçu des preuves que les attaquants ont volé des bases de données contenant des informations sur 200'000 patients.

En mai 2021, nous avions évoqué le prestataire de soins de santé américain "Scripps Health" qui avait été victime du ransomware "Conti". Ce prestataire de soins de santé gère 5 hôpitaux et 19 cliniques externes dans l'État américain de Californie. En août 2021, il a annoncé que la perte due à l'attaque de rançongiciel était estimée à 106.8 millions USD. La majeure partie de la perte de 91.6 millions USD est attribuée à l'arrêt des systèmes informatiques, qui, selon la société, a duré 4 semaines. Un montant supplémentaire de 21.1 millions de dollars a été consacré au processus de réponse à incidents et au redémarrage des systèmes[6]. Selon Scripps Health, seuls 5.9 millions de dollars ont été couverts par une police d'assurance.

Les attaques par ransomware de l'été dernier ne se sont pas limitées aux États-Unis. Des attaques par ransomware contre des hôpitaux en France sont également devenues publiques, comme celle contre l'hôpital de la ville d'Arles. Selon l'hôpital, ce dernier a été chiffré et complètement paralysé par un groupe appelé "Vice Society"[7]. Non seulement les postes clients et les serveurs ont été chiffrés par les attaquants, mais la sauvegarde a également été rendue inopérante. Le directeur de l'hôpital affecté a néanmoins fait une déclaration claire concernant le paiement éventuel d'une rançon : "[...] nous n'avons même pas lu la demande car nous ne paierons pas [...]". Certaines données volées lors de l'incident ont entretemps été publiées dans le dark web. "Vice Society" exploite, entre autres, la vulnérabilité "PrintNightmare" de Windows publiée à la mi-2021 (CVE-2021-36958) pour se déplacer latéralement dans le réseau de la victime.

[4] https://www.ic3.gov/Media/News/2021/210825.pdf

[5] https://www.bleepingcomputer.com/news/security/hive-ransomware-attacks-memorial-health-system-steals-patient-data/

[6] https://therecord.media/healthcare-provider-expected-to-lose-106-8-million-following-ransomware-attack/

[7] https://www.dna.fr/faits-divers-justice/2021/08/19/l-hopital-d-arles-pirate-les-hackers-demandent-une-rancon

Étude : la moitié des hôpitaux américains "hors ligne" en raison d'un rançongiciel

Une étude[8] réalisée par le spécialiste américain de la cybersécurité CyberMDX et Philips a conclu qu'au premier semestre 2021, près de la moitié (48%) des hôpitaux américains ont dû arrêter temporairement leurs systèmes en raison d'attaques par ransomware. Cela était dû à une attaque directe par ransomware ou à titre préventif en raison d'attaques ou d'indications provenant de l'extérieur. Les hôpitaux américains de taille moyenne ont également indiqué que les systèmes ont été affectés pendant 10 heures en moyenne, avec un coût horaire estimé à 45'700 USD.

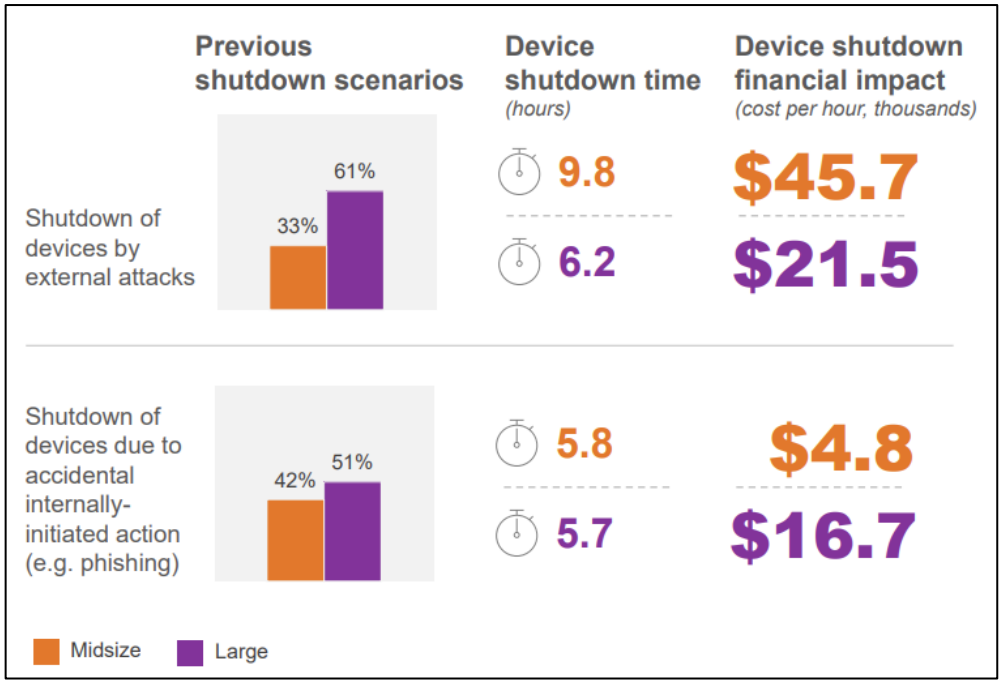

Figure 1 - Extrait de l'étude de CyberMDX

L'étude montre une fois de plus l'exposition aux risques élevés des organisations du secteur de la santé. Il est donc essentiel que des mesures visant à renforcer la sécurité informatique soient prises et mises en œuvre et qu'elles soient adaptées en permanence à l'évolution des menaces. Les recommandations correspondantes du NCSC se trouvent à la fin de ce document.

"DoppelPaymer" à nouveau actif sous le nom de "Grief"

Même les ransomwares ont besoin d'un rafraîchissement de leur "marque" de temps en temps, comme par exemple le ransomware "DoppelPaymer". Ce nom a acquis une grande notoriété en 2020 lorsqu'il a paralysé, suite à une attaque réussie, l'hôpital universitaire de Düsseldorf. Le groupe disparait des radars en mai 2021. A une exception près en septembre 2021, aucune nouvelle donnée provenant des victimes n'a été publiée sur leur "leak site" depuis, suggérant que le groupe à l'origine de "DoppelPaymer" fait soit une pause prolongée ou a complètement arrêté ses activités.

[8] https://www.cybermdx.com/press-releases/perspectives-in-healthcare-security-report/

Au début du mois de juillet 2021, un nouveau ransomware entre en scène : "Grief". Toutefois, les analyses techniques des échantillons de "Grief" ont rapidement indiqué que le ransomware était une nouvelle édition de "DoppelPaymer". Une différence importante avec DoppelPaymer est que la rançon pour Grief doit être payée à l'aide de la crypto-monnaie "Monero" (XMR) au lieu de Bitcoin (BTC). Malheureusement, la première victime suisse ne s'est pas fait attendre. Début juillet, le service de comparaison "Comparis" a été victime de "Grief" et, selon ses propres informations, a également payé une rançon d'un montant de 400'000 USD aux maîtres chanteurs.

DoppelPaymer n'est pas le premier ni le dernier groupe de rançongiciel à adopter une nouvelle identité. Le groupe à l'origine du ransomware "DarkSide" a également fait peau neuve après l'attaque contre l'entreprise américaine "Colonial Pipeline" et opère depuis l'été 2021 sous le nom de "BlackMatter". En septembre, "BlackMatter" a réussi un nouveau grand coup en attaquant le géant japonais de la technologie "Olympus".

Il existe plusieurs raisons possibles pour lesquelles ces groupes se réinventent régulièrement. Un facteur important est certainement les activités dans les forums fermés et les places de marché sur le dark web, où les acteurs et leurs "clients" ("affiliés") échangent des informations et proposent ou obtiennent des services. Si un acteur y tombe en disgrâce, enfreint les règles en vigueur ou est même exclu définitivement de la plateforme commerciale, il ne lui reste souvent que l'option d'un "rebranding" pour poursuivre ses activités illicites.

Une autre raison du changement de marque peut être la pression politique nationale ou internationale, comme les restrictions et les sanctions imposées par l'Office of Foreign Assets Control (une agence du département du Trésor américain) en lien avec les incidents de rançongiciels en 2020.

Une attaque par chaîne d'approvisionnement frappe plusieurs entreprises en Autriche

Une des plus graves cyberattaques l'histoire de l'Autriche s'est produite en septembre 2021. Des inconnus ont réussi à compromettre le dispositif d'un administrateur système d'un fournisseur de services informatiques[9]. Cela a permis aux criminels d'accéder à 34 entreprises qui étaient desservies par cette société. Les attaquants ont pu utiliser l'accès de l'administrateur pour chiffrer les réseaux des clients à l'aide d'un rançongiciel. On ignore quel était le montant de la demande de rançon et si les victimes ont payé. Cependant, après l'attaque, les attaquants ont publié les données des entreprises touchées sur le dark web, ce qui laisse penser que les victimes n'ont pas donné suite aux demandes de rançon. Selon les médias[10], le groupe de ransomware "BlackMatter" est à l'origine de cette cyberattaque.

L'approche de ces attaquants n'est pas nouvelle : comme nous l'avons déjà signalé dans un précédent numéro, les cybercriminels ont réussi à accéder à de multiples entreprises au printemps 2021 grâce à une "Supply Chain Attack" contre le fournisseur de services informatiques américain "Kaseya" et à les chiffrer à l'aide d'un ransomware.

[9] https://futurezone.at/digital-life/oesterreich-ransomware-angriff-unternehmen-hacker-angriff/401722305

[10] https://www.ots.at/presseaussendung/OTS_20210908_OTS0194/cyberangriff-auf-ooe-firmen-wichtige-daten-sichergestellt

Entretien avec les auteurs du ransomware LockBit 2.0

Le ransomware "LockBit" est probablement connu de nombreux lecteurs. Dans notre bulletin de février 2021, nous avions déjà fait état d'un entretien avec ces auteurs. Depuis juin 2021, ces criminels sont de retour avec une version révisée de leur rançongiciel "LockBit 2.0". Le ransomware continue d'être proposé en tant que "Ransomware-as-a-Service" (RaaS) sur le dark web. Dans une interview accordée à la chaîne YouTube russophone "Russian OSINT"[11], les auteurs ont une nouvelle fois fourni des informations sur leurs opérations. Les auteurs ont notamment fait les déclarations suivantes :

- Supply Chain Attacks : les auteurs partent du principe que les attaques par chaîne d'approvisionnement, comme celle dont a été victime le fournisseur de services informatiques américain Kaseya, vont se multiplier à l'avenir.
- La cybersécurité des entreprises reste faible : les auteurs estiment que les entreprises n'ont pas progressé dans la protection de leurs infrastructures. Et ce, malgré le fait que le nombre de cyberattaques par ransomware ait augmenté.
- La pandémie de COVID-19 : Les auteurs affirment qu'il est devenu plus facile de "contaminer des cibles" en raison de la pandémie.
- Ciblage de l'Europe et les États-Unis : l'auteur déclare que la fréquence des attaques (réussies) de ransomware contre des entreprises en Europe et aux États-Unis est due au fait qu'elles sont plus susceptibles d'avoir une cyber assurance.

Recommandations

- Les systèmes exposés à Internet tels que RDP, les services VPN, etc. doivent toujours être maintenus au dernier niveau de patch. **Les mises à jour de sécurité doivent être appliquées rapidement.**

- **Les interfaces d'administration ne doivent jamais être exposées sur Internet**, mais uniquement accessible via une zone de réseau séparée, typiquement une zone de gestion / d'administration. L'accès à une telle zone doit se faire exclusivement à l'aide d'une authentification forte (authentification à deux facteurs - 2FA) et tous les accès doivent être protocolés. Les appareils utilisés pour l'administration des systèmes ne doivent pas être utilisés à d'autres fins, en particulier pas pour la navigation sur Internet ou la consultation des emails.

- Les **accès à distance** tels que VPN et RDP ainsi que tous les autres accès aux ressources internes (par exemple webmail, Sharepoint, etc.) doivent être sécurisés par un second facteur (**authentification à deux facteurs** - 2FA). Assurez-vous que vous disposez des logs journalisant les tentatives d'accès réussies et échouées sur une période suffisamment longue. Stockez ces données de manière centralisée et évaluez-les régulièrement.

- Bloquer les adresses IP connues des serveurs de commande et contrôle (C&C) des botnets en mettant en œuvre le **flux MELANI BGP** (contact : outreach@govcert.ch). Vous pouvez vérifier si vous ou votre fournisseur mettez déjà en œuvre cette protection en tentant d'accéder aux adresses de test suivantes dans votre navigateur web. Si la connexion échoue, vous êtes déjà protégé :
  - http://ip-protection.govcert.ch
  - http://melbl-protection.govcert.ch

[11] https://ke-la.com/lockbit-2-0-interview-with-russian-osint/

- Bloquer les noms de domaine connus des serveurs de commande et de contrôle (C&C) des botnets en mettant en œuvre la **RPZ MELANI** ou le **résolveur DNS sécurisé** (contact : outreach@govcert.ch)

- Bloquer la réception de **pièces jointes dangereuses** sur votre passerelle de messagerie, y compris les **documents Office contenant des macros**. Une recommandation des extensions de fichiers à bloquer se trouve ici :
  - https://www.govcert.ch/downloads/blocked-filetypes.txt

- Créer **régulièrement des sauvegardes de vos données**. Utilisez le principe de génération (quotidien, hebdomadaire, mensuel - au moins 2 générations de chaque). Assurez-vous que vous **déconnectez physiquement** le support sur lequel vous avez créé la copie de sauvegarde de l'ordinateur ou du réseau après le processus de sauvegarde.

- Utilisez une liste telle que URLHaus[12] pour **empêcher** le téléchargement de **malware**.

- **Protégez et surveillez les ressources centrales** telles qu'un Active Directory et préparez des plans d'urgence en cas de compromission éventuelle.

- **Prenez au sérieux les notifications** des autorités concernant un problème de sécurité dans votre entreprise. En cas de doute sur l'authenticité d'un rapport, appelez l'autorité qui l'a envoyé.

- Veillez à ce que les **mises à jour de sécurité soient appliquées rapidement**. Les mises à jour de sécurité hautement critiques doivent être appliquées immédiatement et ne doivent pas être reportées à la prochaine fenêtre de maintenance.

- **Choisissez soigneusement vos fournisseurs**, notamment ceux **de services informatiques**, et assurez-vous que votre prestataire de services a également mis en œuvre les meilleures pratiques en matière de cybersécurité. Assurez-vous contractuellement que votre fournisseur vous informe rapidement des incidents pertinents dans son entreprise ou en cas de vol éventuel de données de clients (data breach). N'accordez pas aux fournisseurs de services un accès à distance illimité à votre réseau et sécurisez-les autant que possible.

Contact GovCERT

GovCERT est en tout temps à votre disposition, que ce soit en cas d'incident de sécurité avéré mais également en cas de soupçons (par exemple pour l'analyse d'emails suspects) :

Adresse email: incidents@govcert.ch
Permanence téléphonique : +41 79 152 20 80 (**uniquement en cas d'urgence !**)

Contactez outreach@govcert.ch en cas de questions techniques ou d'intérêt pour l'implémentation de services offerts par NCSC.

[12] https://urlhaus.abuse.ch/