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 : 1er juin 2021
Version : v1.0
Auteur : NCSC/GovCERT.ch
Contact : outreach@govcert.ch
Distribution : Secteur de la Santé MELANI, H+, HIN

Actualités (Mai 2021)

La situation dans le domaine de la cybersécurité reste tendue en raison des attaques actuelles contre les infrastructures critiques et en particulier contre les organisations du secteur de la santé.

- Les vagues de spam que nous avons détectées restent à un niveau élevé.
- L'activité des rançongiciels en Suisse continue de causer des dommages importants.
- Des attaques utilisant le rançongiciel "Conti" ont été menées entre autres contre le secteur de la santé aux États-Unis[1] et en Irlande.
- Cyberattaque contre des hôpitaux en Nouvelle-Zélande.
- Des cybercriminels attaquent des infrastructures critiques aux États-Unis.
- Nouvelle vulnérabilité critique dans Pulse Connect Secure.

Le ransomware "Conti" attaque le secteur de la santé

Le Health Service Executive (HSE) irlandais a été la cible d'une attaque réussie de rançongiciel en mai 2021. Des auteurs inconnus ont réussi à pénétrer dans le réseau de HSE et à chiffrer les systèmes avec un ransomware appelé "Conti". L'attaque a touché de nombreux systèmes, ce qui a poussé le HSE à désactiver temporairement tous les systèmes informatiques. Les tests COVID-19 n'ont par exemple plus pu être effectués. Les hôpitaux ont également dû passer au papier pour enregistrer et documenter les traitements. Le 28 mai 2021, le HSE a confirmé que des données concernant 520 patients avaient été volées et publiées sur Internet suite à l'attaque. Selon les médias[2], l'auteur inconnu a réussi à dérober 700 Go de

[1] https://www.aha.org/system/files/media/file/2021/05/fbi-tlp-white-report-conti-ransomware-attacks-impact-healthcare-and-first-responder-networks-5-20-21.pdf
[2] https://www.bleepingcomputer.com/news/security/irelands-health-services-hit-with-20-million-ransomware-demand/

données et réclame une rançon de 20 millions de dollars. Le 27 mai 2021, Paul Reid, directeur du HSE, a déclaré que le coût de la gestion de la cyberattaque s'élèverait probablement à plus de 100 millions USD[3].

En analysant les systèmes affectés, le Centre national de cybersécurité irlandais NCSC a pu trouver "Cobalt Strike". Il s'agit d'un outil commercial de test de pénétration qui est souvent utilisé par les cybercriminels pour pénétrer dans les réseaux d'entreprise. NCSC.ch a déjà eu connaissance de plusieurs cas en Suisse cette année, dans lesquels les ransomwares "Cobalt Strike" et "Conti" ont été utilisés pour chiffrer des données d'entreprise, les exfiltrer et faire chanter la victime.

Pratiquement au même moment que l'attaque contre HSE, Scripps Health, un service de santé à but non lucratif basé en Californie (États-Unis), a été la cible d'attaquant cherchant à déployer le rançongiciel "Conti"[4]. Selon ses propres déclarations, Scripps Health gère cinq hôpitaux et 19 établissements de soins ambulatoires et traite un demi-million de patients par an par l'intermédiaire de 2'600 médecins affiliés. Dans le cas de cette attaque, une grande partie des processus a dû passer du numérique au papier, car Scripps Health a mis hors ligne de nombreux systèmes afin de contenir l'attaque. Toutefois, selon les propres déclarations de l'entreprise, l'attaque a été détectée avant que le ransomware "Conti" ne procède à un quelconque chiffrement.

Cyberattaques contre des hôpitaux en Nouvelle-Zélande

À la mi-mai 2021, de nombreux hôpitaux du Waikato District Health Board en Nouvelle-Zélande ont été victimes de cyberattaques. Des inconnus ont apparemment réussi à voler des données, y compris des données de patients. Ils ont été divulgués à divers médias néozélandais à la fin du mois de mai 2021. Selon le ministre néo-zélandais de la santé, Andrew Little, les serveurs ont été chiffrés par le ransomware "Zeppelin" lors de la cyberattaque. Selon les médias[5], le traitement des patients et les salaires ont été affectés pendant plus d'une semaine. Plusieurs processus ont dû passer temporairement en mode manuel sans assistance électronique. Plus de 600 serveurs ont pu être remis en service entre-temps. Il n'y a actuellement aucune information publique concernant une demande de rançon.

"Zeppelin" est un "Ransomware-as-a-Service" (RaaS), proposé sur le dark web et qui a déjà été utilisé pour attaquer des organisations du secteur de la santé à plusieurs reprises. Le vecteur d'infection initial est souvent lié à une campagne de malspams.

Des cybercriminels s'attaquent à des infrastructures critiques aux États-Unis

Colonial Pipeline, exploitant du plus grand réseau d'oléoducs de produits pétroliers raffinés des États-Unis, a été victime d'une cyberattaque début mai. Les circonstances exactes n'étaient pas claires au départ, mais l'entreprise a depuis annoncé qu'elle avait été victime du rançongiciel "DarkSide". La cyberattaque a eu des conséquences considérables : La société a dû interrompre temporairement l'exploitation de son pipeline. Cela a entraîné des goulots d'étranglement dans l'est des États-Unis. Dans une interview accordée au Wall

[3] https://www.irishtimes.com/news/health/cyberattack-hse-faces-final-bill-of-at-least-100m-1.4577076
[4] https://www.bleepingcomputer.com/news/security/health-care-giant-scripps-health-hit-by-ransomware-attack/
[5] https://www.reuters.com/article/us-newzealand-cyber-idCAKCN2D7024

Street Journal, Joseph Blount, responsable de Colonial Pipeline, a admis avoir payé une rançon de 4.5 millions de dollars. Il affirme que le paiement de la rançon était dans le meilleur intérêt du pays.

L'ampleur de la cyberattaque a suscité un débat aux États-Unis. À la mi-mai, les hackers à l'origine de "DarkSide" ont annoncé qu'ils se renonçaient à leur activité. Les pirates ont justifié cette démarche en disant qu'ils avaient perdu l'accès à leur infrastructure. On ignore si l'infrastructure a été mise hors ligne par les forces de l'ordre, si les auteurs inconnus de "DarkSide" ont décidé de mettre fin à leurs activités en raison de la pression exercée par les États-Unis ou s'il s'agit d'une pure tactique de diversion de la part des auteurs.

En analysant les comptes Bitcoin utilisés par "DarkSide", des chercheurs en sécurité[6] ont pu reconstituer les paiements de rançon de 47 victimes sur une période de 9 mois, pour un volume de plus de 90 millions USD.

Suite à la cyberattaque contre Colonial Pipeline, le président de l'Office fédéral allemand de la sécurité de l'information (BSI), Arne Schönbohm, s'est inquiété de la cybersécurité des infrastructures médicales allemandes. Dans une interview accordée à Zeit Online[7], il dit voir un plus grand danger dans les hôpitaux, faisant référence à plusieurs attaques de hackers contre eux ces dernières années.

Bien que la situation en matière de cybersécurité concernant les ransomwares soit actuellement tendue en Suisse, la NCSC n'a connaissance d'aucun cas de "DarkSide" en Suisse à ce jour. L'affaire Colonial Pipeline montre toutefois que même les infrastructures critiques ne sont pas épargnées par les cyberattaques.

Nouvelle vulnérabilité critique dans Pulse Connect Secure

En avril 2021, NCSC.ch a signalé plusieurs vulnérabilités critiques dans Pulse Connect Secure. Ce produit est utilisé par de nombreuses entreprises en Suisse pour permettre l'accès à distance au réseau d'entreprise (VPN). Surtout en période de COVID-19, ces accès à distance sont très demandés et constituent donc une cible populaire pour les cybercriminels. En mai 2021, une nouvelle vulnérabilité critique dans le produit susmentionné a été divulguée[8], permettant aux attaquants de visualiser les partages réseau SMB et d'exécuter du code arbitraire. Pour exploiter cette vulnérabilité, un attaquant doit d'abord réussir à s'authentifier auprès du système, en demandant des informations d'identification valides (nom d'utilisateur, mot de passe).

Les vulnérabilités de Pulse Connect Secure et de produits similaires tels que Citrix ont été utilisées à plusieurs reprises dans le passé par des cybercriminels pour s'introduire dans des réseaux d'entreprise, voler des données et se déplacer latéralement dans le réseau. Dans de nombreux cas, cela a conduit à la compromission de données d'entreprise et au chiffrement d'une grande partie des systèmes du réseau de la victime.

[6] https://www.elliptic.co/blog/darkside-ransomware-has-netted-over-90-million-in-bitcoin

[7] https://www.heise.de/news/BSI-Chef-sieht-Gefahr-von-Hackerangriffen-auf-Krankenhaeuser-6052664.html

[8] https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44800

Recommandations

Les deux attaques contre le secteur des soins de santé susmentionnées, ainsi que les cyberattaques contre des infrastructures critiques également observées, montrent clairement que l'exposition au risque est élevée. Ce risque peut cependant être considérablement réduit avec des mesures relativement faciles à mettre en œuvre, notamment par la sécurisation des systèmes de passerelle et une politique restrictive quant aux types de données qui peuvent être téléchargées et exécutées par courrier ou sur le web.

- 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 **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

- 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[9] pour **empêcher** le téléchargement de **malware**.

- **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.

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

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.