Cyber Security Update - Secteur de la Santé

À USAGE INTERNE UNIQUEMENT

Date : 3 novembre 2021
Version : v1.0
Auteur : NCSC/GovCERT.ch
Contact : outreach@govcert.ch
Distribution : Secteur de la Santé MELANI, H+, HIN

Actualités (Octobre 2021)

En octobre 2021, diverses organisations en Suisse ont à nouveau été victimes de cyberattaques. Les données des entreprises victimes ont souvent été chiffrées par des rançongiciels. Le NCSC rappelle explicitement une fois de plus les recommandations en matière de cybersécurité préconisées depuis un certain temps déjà :

Attaques au rançongiciel réussies contre des entreprises suisses :
https://www.ncsc.admin.ch/ncsc/fr/home/aktuell/im-fokus/ransomware-8.html

Cette édition couvre les sujets suivants :

- Volume élevé de malspam "QuakBot".
- Qui est le "roi du ransomware" sur le dark web?
- Le président américain Joe Biden appelle à l'utilisation de l'authentification multifacteurs (MFA)
- Les attaques par rançongiciel contre les organismes de santé peuvent entraîner une augmentation du taux de mortalité
- Action en justice contre un hôpital américain à la suite d'une attaque par ransomware
- Les Pays-Bas pourraient faire appel aux services de renseignement ou à l'armée pour contrer les rançongiciels
- Cyberattaque contre plusieurs hôpitaux israéliens
- 2021 : 83% des victimes de ransomware ont payé

Volume élevé de malspam "QuakBot".

Nous avions déjà parlé du malware "QuakBot" (également connu sous les noms de "Qakbot" et "Qbot") dans notre précédente édition (numéro de septembre 2021). Ce dernier semble avoir pris la place du malware Emotet durant l'été, et est devenu encore plus actif au mois d'octobre. Ainsi, un grand nombre de cas de courriels malveillants ont été signalés au NCSC en octobre 2021, dans lesquels des criminels ont volé des conversations de courriel légitimes dans les boîtes aux lettres des ordinateurs infectés par "QuakBot". Ces conversations par email ont ensuite été utilisées par les auteurs pour tenter d'infecter d'autres ordinateurs (ce que l'on appelle également "email thread hijacking " ou "dynamite phishing").

"QuakBot" insère un lien vers un site web malveillant dans la conversation légitime. Ce lien pointe vers un fichier Excel malveillant à télécharger. Celui-ci contient à son tour une macro malveillante. Après avoir ouvert le fichier Excel, les criminels tentent de convaincre la victime, par le biais de l'ingénierie sociale, d'activer la macro contenue dans le fichier Excel. Si la victime l'active, la macro malveillante télécharge le maliciel "QuakBot" depuis un autre site web (piraté) et infecte le système.

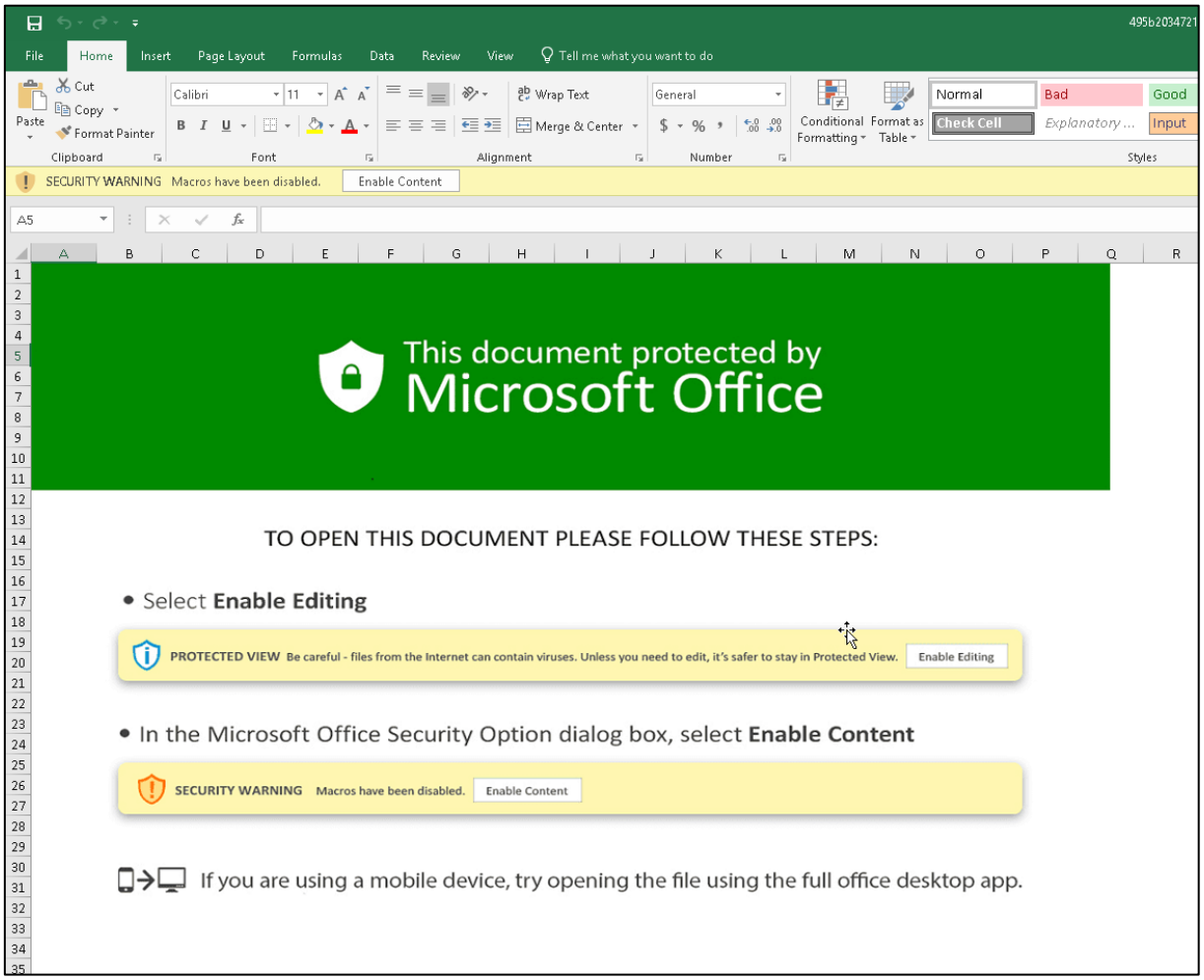

Figure 1: Exemple d'un fichier Excel malveillant (QuakBot)

Malgré l'usage d'une conversation légitime, ce type de courriel peut généralement être identifié comme un malspam relativement facilement en vérifiant l'adresse électronique de l'expéditeur. Les criminels utilisent actuellement une adresse d'expédition aléatoire au lieu de

l'adresse électronique de l'expéditeur original. Il vaut donc la peine de vérifier l'adresse électronique de l'expéditeur et d'examiner d'un œil critique tous les courriels apparemment légitimes si leur contenu contient des anomalies.

Qui est le "roi du ransomware" sur le dark web ?

Les chercheurs en sécurité informatique de la société "DarkTracer", spécialisée dans la surveillance des acteurs du dark web, ont mené une enquête sur les familles de ransomware les plus prolifiques dans le dark web. Le nombre d'entreprises victimes de ransomware a été additionné pour chaque famille de ransomware. Aucun détail quant à la durée de la collecte des données n'est disponible, mais les statistiques publiées par DarkTracer donnent un bon aperçu du paysage des familles de ransomware :

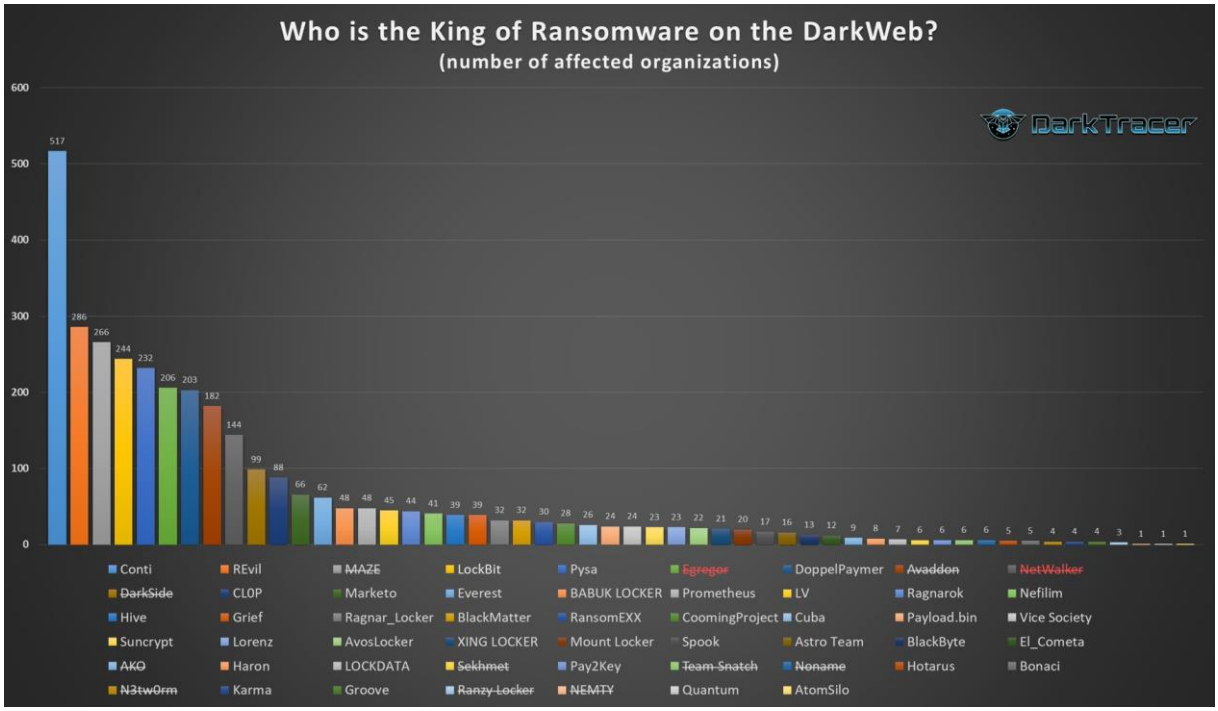

Figure 2: Nombre de victimes (entreprises) par famille de ransomware

Selon l'évaluation, le ransomware "Conti" est la famille de ransomware la plus dangereuse en nombre de victimes. Le ransomware "REvil" (également connu sous le nom de "Sodinokibi") est loin derrière en deuxième position. Ces dernières années, les deux familles de rançongiciels ont malheureusement également attaqué et chiffré des entreprises en Suisse.

Le président américain Joe Biden appelle à l'utilisation de l'authentification multifacteurs (MFA)

Dans une déclaration publiée par la Maison Blanche[1], le président américain Joe Biden appelle, entre autres, à l'utilisation de l'authentification multifacteurs (Multi-Factor Authentication - MFA) pour contrer la menace représentée par les ransomwares. C'est la première fois qu'un président préconise publiquement l'utilisation de l'MFA.

[1] https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/01/statement-by-president-joe-biden-on-cybersecurity-awareness-month/

Le NCSC appelle depuis des années à la généralisation de l'authentification à deux facteurs (2FA), qui fait partie des solutions MFA. Malgré ces recommandations, des entreprises suisses sont régulièrement victimes de ransomware par le biais de données d'accès volées pour les accès à distance (tels que VPN ou RDP) non protégé par un second facteur d'authentification. Malheureusement, le mois dernier n'a pas fait exception à la règle : un grand nombre de cas de ransomware en Suisse ces derniers mois ont été rendus possibles par l'absence d'authentification à deux facteurs.

Les attaques de rançongiciels contre les organismes de santé peuvent entraîner une augmentation du taux de mortalité

Les résultats d'une étude[2] publiée en octobre par l'institut américain "Ponemon"[3] montrent que les attaques par ransomware contre les organismes de santé pendant la pandémie de COVID-19 peuvent entraîner une augmentation du taux de mortalité. Les chercheurs ont interrogé 597 experts en informatique. Les résultats de l'enquête montrent que près d'une entreprise sur quatre du secteur de la santé a connu une augmentation du taux de mortalité en raison d'attaques par rançongiciel.

Action en justice contre un hôpital américain suite à une attaque par ransomware

Comme le rapportait en octobre le magazine américain consacré aux technologies de l'information "TechRepublic", une patiente a intenté une action en justice contre un hôpital de l'État américain de l'Alabama suite à la naissance avec des lésions cérébrales de son bébé[4]. La patiente accuse l'hôpital d'avoir été frappé par une attaque de ransomware lors de l'accouchement de son enfant en juillet 2019. Cette attaque aurait provoqué le dysfonctionnement de divers systèmes informatiques. Selon l'acte d'accusation, cela a entraîné un dysfonctionnement de la "technologie de surveillance" de la maternité, qui était utilisée pour surveiller le rythme cardiaque du bébé, provoquant des lésions cérébrales irréversibles chez le bébé. Le bébé est décédé à l'âge de 9 mois. L'obstétricien a déclaré par la suite qu'un accouchement par césarienne aurait été effectué si la surveillance du rythme cardiaque avait fonctionné.

Les Pays-Bas pourraient faire appel aux services de renseignement ou à l'armée pour contrer les rançongiciels

Le ministre néerlandais des affaires étrangères, Ben Knapen, a répondu à une question parlementaire sur les ransomwares en déclarant que le gouvernement pourrait faire appel aux services de renseignement ou à l'armée pour contrer ces attaques si la sécurité nationale était menacée[5]. L'infrastructure informatique des attaquants pourrait par exemple être mise

[2] https://www.businesswire.com/news/home/20210922005436/en/New-Ponemon-Institute-Research-Shows-Ransomware-Attacks-on-Healthcare-Delivery-Organizations-Can-Lead-to-Increased-Mortality-Rate

[3] https://www.ponemon.org/

[4] https://www.techrepublic.com/article/lawsuit-claims-ransomware-attack-caused-fatal-injury-to-infant-at-alabama-hospital/

[5] https://therecord.media/netherlands-can-use-intelligence-or-armed-forces-to-respond-to-ransomware-attacks/

hors ligne. Outre les services de renseignement, le cyber commandement de l'armée néerlandaise pourrait également mener des contre-attaques.

Cyberattaque contre plusieurs hôpitaux israéliens

En octobre, le ministère israélien de la santé a annoncé que plusieurs hôpitaux israéliens avaient été la cible de cyberattaques[6]. La plupart des attaques ont cependant été repoussées. Malgré tout, l'hôpital "Hillel Jaffe" de la ville côtière de Chadera a lutté pendant plusieurs jours contre les conséquences d'une attaque par ransomware. Selon les médias, le personnel a dû passer temporairement à des systèmes alternatifs et procéder à l'admission des patients sans support informatique. Des informations quant au vecteur d'infection, la famille de ransomware utilisée et le paiement éventuel d'une rançon ne sont pas connues.

2021 : 83% des victimes de ransomware ont payé

En octobre 2021, la société de sécurité informatique ThycoticCentrify a publié une étude sur les ransomwares. Elle conclut que 83% des 300 entreprises informatiques américaines interrogées qui ont été victimes de ransomware en 2021 ont payé une rançon[7]. Le Financial Crimes Enforcement Network américain indique également[8] que 590 millions de dollars américains en rançon ont été extorqués à l'aide de ransomwares au cours du premier semestre de l'année[9].

Recommandations

- Les systèmes exposés sur 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.

---

[6] https://www.gov.il/he/departments/news/17102021-01

[7] https://www.darkreading.com/attacks-breaches/2021-state-of-ransomware-report-reveals-83-of-victims-paid-to-get-data-restored

[8] https://www.heise.de/news/Ransomware-Im-ersten-Halbjahr-allein-in-den-USA-590-Millionen-US-Dollar-gezahlt-6220438.html

[9] https://www.fincen.gov/sites/default/files/2021-10/Financial%20Trend%20Analysis_Ransomware%20508%20FINAL.pdf

- 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[10] 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.

[10] 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.