Cyber Security Update - Secteur de la Santé

À USAGE INTERNE UNIQUEMENT

Date :	27 novembre 2020
Version :	v1.0
Auteur :	NCSC/GovCERT.ch
Contact :	outreach@govcert.ch
Distribution :	Secteur de la Santé MELANI, H+, HIN

Actualités (novembre 2020)

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, ainsi que du niveau toujours élevé des nouvelles infections liées au COVID19. Fin octobre, le FBI et l'autorité américaine CISA ont mis en garde contre les attaques de rançongiciels ciblant les organisations du secteur de la santé[1].

En Suisse, nous continuons à observer une forte activité de malspam, divers incidents de rançongiciels dans les petites organisations (PME et communes) et un nombre d'attaques par déni de service distribué (DDoS) supérieur à la moyenne.

Perturbation des accès réseaux dues à des attaques DDoS

Depuis début novembre, le NCSC a reçu plusieurs rapports d'attaques DDoS contre des ressources accessibles sur Internet (comme les sites de services en ligne). La majorité des entités touchées sont des entreprises du secteur financier. Cependant des entreprises d'autres secteurs ont également été attaquées[2].

Recommandation

Le NCSC recommande que toutes les organisations du secteur des soins de santé effectuent une analyse des risques d'exposition de leurs systèmes. Cette analyse devrait notamment répondre aux questions suivantes :

- Quels sont les systèmes accessibles depuis Internet ?
- De ces systèmes, lesquels sont essentiels aux processus opérationnels ?
- Existe-t-il des plans d'urgence au cas où ces systèmes seraient attaqués par une at-

[1] https://us-cert.cisa.gov/ncas/alerts/aa20-302a

[2] https://www.20min.ch/story/hacker-greifen-tx-group-an-119923568553

taque DDoS ? Les responsabilités des différents acteurs impliqués (réseaux, fournisseur de services Internet) ont-elles été établies et clarifiées ?
- Les systèmes accessibles depuis Internet partagent-ils des ressources avec des systèmes essentiels au fonctionnement de l'organisation (par exemple, même connexion Internet, même pare-feu) ? Existe-t-il un plan de basculement au cas où l'attaque de la ressource accessible au public affecterait d'autres systèmes internes ?

Pour les systèmes critiques des entreprises, le NCSC recommande de souscrire à une protection commerciale contre les DDoS (DDoS Mitigation Service). **De nombreux fournisseurs d'accès à Internet (FAI) proposent ce service moyennant un supplément. Prenez contact avec votre prestataire pour déterminer le coût et l'étendue d'un tel service.**

Données techniques de référence :
- Les attaquants se présentent sous des noms usurpés tels que "Fancy Bear" ou "Lazarus" mais ne sont pas liées à ces acteurs.
- La plupart des attaques sont volumétriques et basées sur l'utilisation de protocoles basés sur UDP avec un facteur d'amplification élevé. Les volumes de trafic maximum que nous avons observés se situaient entre 150 Gbps et 200 Gbps.
- Dans certains cas, les attaquants ont également utilisé des protocoles basés sur TCP et ont essayé de surcharger autant le réseau (par exemple à l'aide de TCP SYN flood) que la couche applicative (par exemple en envoyant des requêtes HTTP(S)).

Attaques de rançongiciels ciblant les réseaux d'entreprises

Comme mentionné en introduction, les ransomware continuent de représenter une menace majeure - même pour les organisations du secteur de la santé. De nombreux acteurs ne se contentent pas uniquement de chiffrer les informations, mais copient auparavant ces données afin de soumettre leur victime à du chantage. Les dommages causés peuvent être très importants, en particulier dans le cas des données de santé, mais aussi pour des données liées à des travaux de recherches. Vous trouverez ci-joint au présent document une liste des indicateurs de compromis actuels (IOC) qui sont associés à ces attaques. **Nous vous recommandons de vérifier les fichiers journaux de votre périmètre de sécurité (en particulier les journaux du proxy web, du DNS et du pare-feu) des 60 derniers jours.**

Nom du fichier	Description
cobalt_domains.txt	Cobalt Strike botnet C&C domains
cobalt_ips.txt	Cobalt Strike botnet C&Cs IPs
trickbot.txt	TrickBot C&C IPs (including port)
emotet.txt	Emotet C&C IPs (including port)
dridex.txt	Dridex C&C IPs (including port)

- Veuillez contacter GovCERT (incidents@govcert.ch) dès que possible si vous deviez détecter un flux réseau sortant vers l'un des domaines ou adresses IP mentionnés ci-dessus liés à Cobalt Strike (**quel que soit le port de destination**)
- Contactez également GovCERT (incidents@govcert.ch) si vous identifiez du trafic réseau sortant **correspondant à une adresse IP et au port de destination mentionnés** dans les listes liées à TrickBot, Emotet ou Dridex

Le risque d'infection par des logiciels malveillants peut être réduit en utilisant notre solution **MELANI BGP** combiné à notre Response Policy Zone (RPZ) ou notre **résolveur de DNS sécurisé**. Ces services sont offerts gratuitement. Pour de plus amples informations, veuillez contacter GovCERT : outreach@govcert.ch

Données techniques de référence :

- Le vecteur d'attaque initial des rançongiciels demeure souv**ent un courriel contenant une pièce jointe ou un lien malicieux** qui conduit au téléchargement d'un logiciel malveillant. Le risque de téléchargement de logiciels malveillants peut être réduit en utilisant par exemple URLhaus[3].
- Les accès à distance tels que **Citrix, RDP et VPN** restent des vecteurs d'attaque populaires. Ces derniers doivent être **maintenus à jour en permanence ; les connexions ne doivent être possibles que moyennant une authentification à deux facteurs**.
- Les agresseurs se déplacent latéralement dès qu'ils ont établi un premier accès dans le réseau de la victime. Cela signifie que les infections par Emotet, Trickbot ou autres logiciels malveillants doivent être immédiatement prises très au sérieux et, en cas d'infection éventuelle, une analyse doit être faite quant à une éventuelle propagation dans le réseau, notamment en direction de l'Active Directory.
- Les alertes des produits anti-virus en relation avec des outils d'attaque tels que Mimikatz, Metasploit ou Powershell Empire sont des indications d'une compromission plus profonde du réseau.

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.

[3] https://urlhaus.abuse.ch/api/