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

Actualités (janvier 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 malspam que nous avons détectées restent à un niveau élevé.
- Une activité soutenue du virus "Emotet" a été constatée durant les premières semaines de janvier 2021.
- Le 27 janvier, un effort coordonné au niveau mondial a permis de démanteler le botnet "Emotet" et d'arrêter des suspects.
- Nous avons observé des attaques DDoS isolées, sans ciblage d'un secteur d'activité spécifique.
- De nombreuses attaques contre les comptes en nuage tels que Office 365 sont constatées. Dans ce contexte, nous recommandons l'utilisation généralisée de l'authentification à 2 facteurs, en particulier pour ces services exposés, et l'intégration de ces services dans la surveillance de la sécurité.
- À la mi-janvier, un hôpital européen a été victime d'une cyberattaque majeure.

Démantèlement du botnet "Emotet"

Le logiciel malveillant "Emotet" a été actif pendant plus de 2 ans et a été utilisé, entre autres, pour pénétrer les réseaux d'entreprises et d'autres institutions dans le monde entier pour ensuite les chiffrer à l'aide de rançongiciels. Selon les estimations des experts en sécurité et du NCSC, "Emotet" était le logiciel malveillant le plus dangereux au monde en 2019 et 2020. Plusieurs hôpitaux ont été touchés par ces attaques au cours des 12 derniers mois. Les dommages causés par "Emotet" sont estimés en centaines de millions.

Depuis un certain temps, nous poursuivons une stratégie proactive pour réduire la menace posée par "Emotet" aux citoyens, mais aussi aux entreprises et en particulier aux établissements de santé en Suisse à l'aide de mesures techniques. Nous sommes convaincus que

ces mesures ont fait leurs preuves et que le nombre d'incidents majeurs de cybersécurité en Suisse a ainsi pu être réduit de manière significative.

Le 27 janvier 2021, EUROPOL a mené une opération contre "Emotet" en coopération avec les forces de l'ordre de différents pays, dont les Pays-Bas, l'Allemagne, la France et le Royaume-Uni[1]. L'infrastructure de botnet utilisée par les auteurs pour contrôler et gérer les ordinateurs infectés par "Emotet" ont été démontées ("takedown") ou saisies par les autorités. La statistique suivante illustre le nombre de serveurs Command & Control (C&C) actifs du botnet "Emotet" qui ont été bloqués par le flux BGP de MELANI ces derniers jours. On y voit clairement l'effondrement du nombre de serveurs C&C actifs entre le 25 et le 26 janvier :

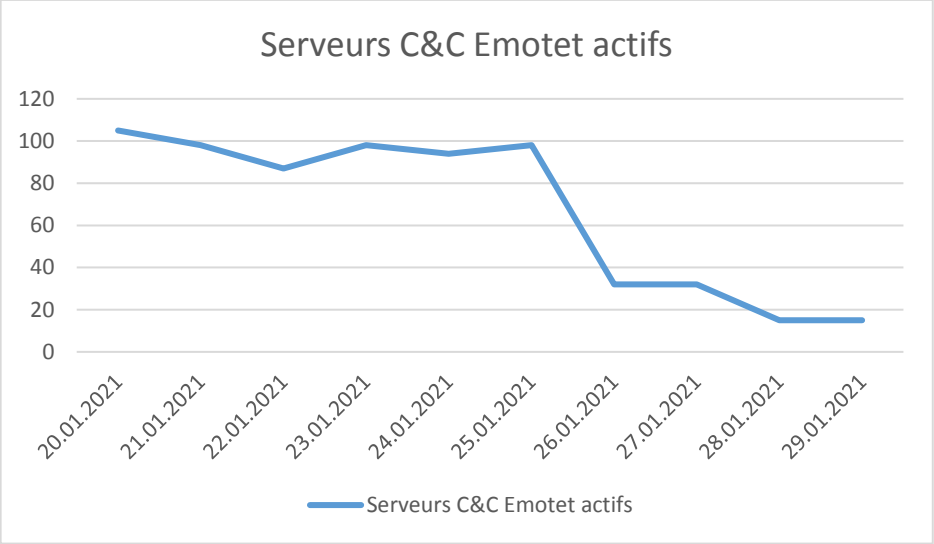

Figure 1 - Serveurs C&C Emotet actifs durant les 10 derniers jours

En outre, des personnes soupçonnées d'être impliquées dans la gestion et la distribution d'"Emotet" ont été arrêtées et remise à la justice. Depuis plusieurs jours, GovCERT.ch reçoit des informations sur les adresses IP infectées par "Emotet" en Suisse et en informe les fournisseurs d'accès Internet (FAI) responsables afin qu'ils puissent à leur tour informer les clients finaux concernés dans le but de nettoyer l'infection.

D'un point de vue technique, NCSC considère que l'action menée par les autorités est très réussie. Bien que certains acteurs derrière "Emotet" n'aient pas pu être identifiés et arrêtés, leur infrastructure a été considérablement démantelée. Cependant, nous nous attendons à ce que ces personnes reviennent dans les mois à venir avec de nouveaux logiciels malveillants et une nouvelle infrastructure. D'ici là, nous recommandons d'utiliser ce moment de répit pour planifier et mettre en œuvre d'autres mesures de protection, telles que la protection / le blocage des macros ou accroire la visibilité sur les stations de travail. Il convient également de noter que les accès aux réseaux d'entreprise obtenus grâce à Emotet ont été revendus et que, par conséquent, d'autres groupes peuvent avoir déjà installé d'autres logiciels malveillants indépendants d'Emotet sur les machines des victimes.

Le NCSC continue de surveiller "Emotet", non seulement en utilisant les données de ses propres capteurs et analyses, mais aussi en s'appuyant sur une coopération internationale

[1] https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

intensive avec les États partenaires. Cela nous permet de réagir rapidement et à tout moment aux nouvelles évolutions du cyberespace et de prendre sans délai les mesures préventives appropriées.

Nouvelle cyber-attaque contre un hôpital européen

Mi-janvier 2021, un hôpital européen avait été victime d'une cyberattaque majeure. Des inconnus ont eu accès au réseau de l'hôpital et à ses serveurs, les chiffrant à l'aide d'un rançongiciel. L'impact sur le fonctionnement de l'hôpital et la disponibilité de ses services a été jugée "significative". Des identifiants VPN volés ont servi de point d'entrée. Le NCSC met en garde depuis des mois contre le risque de vol d'identifiants VPN et les vulnérabilités de sécurité des services VPN et a déjà émis des recommandations à ce sujet :

- Les accès à distance tels que les serveurs **Citrix, RDP et VPN** doivent être **constamment maintenus à jour**.
- Tous les accès distants qui peuvent être obtenus via un login (par exemple, nom d'utilisateur et mot de passe) sur Internet doivent être sécurisés par une **authentification à deux facteurs (2FA)**. Cela concerne les accès à distance susmentionnés tels que les serveurs **Citrix, RDP et VPN**, mais également, l'accès au **webmail** ou à **Sharepoint** par exemple.

Autres cybermenaces

Nombres de cyber incidents qui nous sont signalés peuvent être attribués à des identifiants d'accès compromis. Ceux-ci ont été précédemment volés ou devinés par une attaque de type "brute-force". Si les attaques "brute-force" sont techniquement relativement faciles à détecter, la mise en œuvre d'une authentification à deux facteurs (2FA) permet de minimiser l'exposition au risque. En principe, nous recommandons la mise en œuvre de la 2FA pour tous les services accessibles depuis Internet (tels que l'accès à distance, les services de rendez-vous, le webmail, l'accès VPN, etc.) ainsi que pour tous les services en nuage. En outre, les tentatives de connexion doivent être enregistrées et régulièrement évaluées.

Si le niveau de la cybermenace a été réduit par le démantèlement du botnet Emotet, d'autres acteurs sont prêts à s'engouffrer dans la brèche. Le NCSC surveille notamment régulièrement les campagnes de malspam qui utilisent des fichiers Excel malveillants attachées en tant que pièces jointes ou des liens vers des sites web compromis dans le but d'infecter l'ordinateur de la victime avec le virus "Dridex".

En janvier, nous avons également constaté une augmentation de l'infrastructure utilisée par un acteur connu sous le nom de UNC1878. UNC1878 s'est surtout distinguée par son utilisation du rançongiciel Ryuk contre Universal Health Service (UHS) en octobre 2020[2].

Les serveurs C&C Dridex et UNC1878 que nous connaissons sont répertoriés sur la liste MELBL (MELANI Botnet List), ce qui minimise le risque lié à ces botnets pour les utilisateurs de MELBL.

[2] https://www.fireeye.com/blog/threat-research/2020/10/kegtap-and-singlemalt-with-a-ransomware-chaser.html

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.