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

Actualités (décembre 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 par COVID19.

- Les attaques DDoS contre des grandes entreprises et des opérateurs d'infrastructures critiques en Suisse, signalées en novembre 2020, se sont poursuivies en décembre 2020. Toutefois, leur nombre a considérablement diminué.
- Les campagnes de malspam (malware spam) que nous détections restent à un niveau élevé.
- Après une pause en novembre, nous avons peu avant Noël à nouveau détecté de l'activité liée au virus Emotet.
- Mi-décembre ont été publié les détails d'une attaque par chaîne d'approvisionnement ("supply chain attack"), attribuée à des acteurs étatiques, contre des cibles de haut rang dans le monde entier et menée en compromettant un logiciel légitime et largement utilisé du fabricant SolarWinds (SolarWinds Orion)[1].

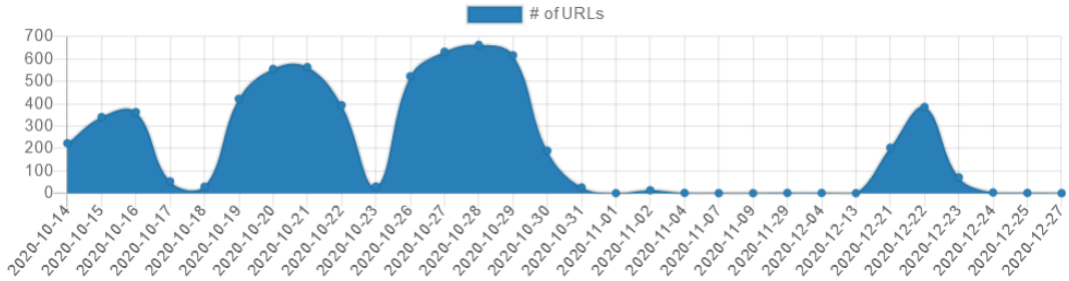
Emotet est de retour

Emotet, également connu sous les noms de "Heodo" et "Geodo", est de retour après une interruption de plus d'un mois. Les acteurs derrière Emotet continuent d'utiliser, comme vecteur d'infection, des courriels (malspam) qui contiennent soit un lien vers un document Word malveillant hébergé sur un site compromis ou attachent directement un document Office correspondant en tant que pièce jointe. Le document Word tente de convaincre l'utilisateur d'activer les macros du document grâce à de l'ingénierie sociale ("social engineering"). En cas de succès, la macro malveillante télécharge et installe un binaire Emotet depuis Internet.

[1] https://www.solarwinds.com/securityadvisory

Le NCSC a détecté la dernière campagne de malspam le 31 octobre 2020. Après une longue interruption de plus d'un mois, les acteurs opérant Emotet ont recommencé à envoyer du malspam le 21 décembre pour étendre leur botnet.

Le graphique suivant montre l'activité d'Emotet, mesurée par le nombre d'URLs signalées diffusant ce virus, au cours des deux derniers mois. Les campagnes de spam, parfois très importantes en octobre, la pause d'Emotet en novembre puis son retour peu avant Noël sont clairement visibles.



Activité d'Emotet d'octobre à décembre 2020

Les acteurs continuent d'utiliser Emotet pour observer les réseaux d'entreprises et revendre ensuite ces accès à d'autres acteurs sur le Darkweb. Dans la plupart des cas, ces infections conduisent tôt ou tard à des attaques par rançongiciels, chiffrant de grandes parties du réseau. **Le NCSC continue donc d'évaluer la menace constituée par Emotet comme étant élevée.**

Recommandation

- Bloquer les adresses IP connues des serveurs de commande et contrôle (C&C) des botnets en mettant en œuvre le **flux MELANI BGP et/ou la zone de politique de réponse (RPZ) ou le résolveur DNS sécurisé** (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.

Attaque par chaîne d'approvisionnement via SolarWinds

Mi-décembre 2020 ont été publié les détails d'une attaque menée par des acteurs étatiques ayant réussi à compromettre le mécanisme de mise à jour automatique de SolarWinds Orion. Ce logiciel est utilisé par des grandes entreprises et des agences gouvernementales dans le monde entier pour surveiller et gérer leurs infrastructures informatiques. En compromettant le mécanisme de mise à jour légitime du logiciel SolarWinds Orion, les attaquants ont pu, sans intervention d'un administrateur, infecter des entreprises du monde entier en y installant les logiciels malveillants appelés SUNBURST et SUPERNOVA. FireEye et plusieurs autres entreprises ont effectué une analyse approfondie du logiciel malveillant[2] [3].

Le NCSC a connaissance de quelques victimes en Suisse et les a informées peu de temps après que le piratage ait été rendu public. Si vous utilisez SolarWinds Orion sur votre réseau, le NCSC recommande les actions suivantes.

Recommandation

- **Examiner les systèmes** et les journaux existants en fonction des indicateurs de compromission. Pour les infrastructures critiques, les IOCs appropriées sont disponibles dans l'événement MISP 6154. Des IOCs accessibles au public peuvent, entre autres, être trouvés sur le GitHub de FireEye[4].

- **Restreindre l'accès des serveurs aux ressources Internet** dont le fonctionnement est explicitement requis, comme Windows Update (approche par liste blanche). Bien que cela n'empêche pas forcément une infection, cela empêche le logiciel malveillant de communiquer avec l'auteur, empêchant ainsi la fuite de données.

- Gestion hors bande (via un LAN ou VLAN dédié) des composants particulièrement sensibles (surveillance du réseau, routeurs, pare-feu, commutateurs).

- Si vous avez souscrit à Microsoft 365 Defender, consultez le guide suivant: https://www.microsoft.com/security/blog/2020/12/28/using-microsoft-365-defender-to-coordinate-protection-against-solorigate/

Attaques contre des fabricants de vaccins COVID-19

Diverses annonces d'attaques[5] contre des fabricants de vaccins COVID-19 ont été publiées récemment. Aucuns détails quant à ces attaques ne nous sont connus mais nous continuons d'observer la situation et vous avertirons si nécessaire. Un des acteurs probablement impliqués dans ces attaques est, selon Kaspersky, le groupe "Lazarus". Vous trouverez les IOCs y relatifs sur https://securelist.com/lazarus-covets-covid-19-related-intelligence/99906/.

[2] https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html

[3] https://www.fireeye.com/blog/threat-research/2020/12/sunburst-additional-technical-details.html

[4] https://github.com/fireeye/sunburst_countermeasures

[5] https://www.bleepingcomputer.com/news/security/us-treasury-warns-of-ransomware-targeting-covid-19-vaccine-research/

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.