Cyber Security Update - Secteur de la Santé

À USAGE INTERNE UNIQUEMENT

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

Actualités (Novembre 2021)

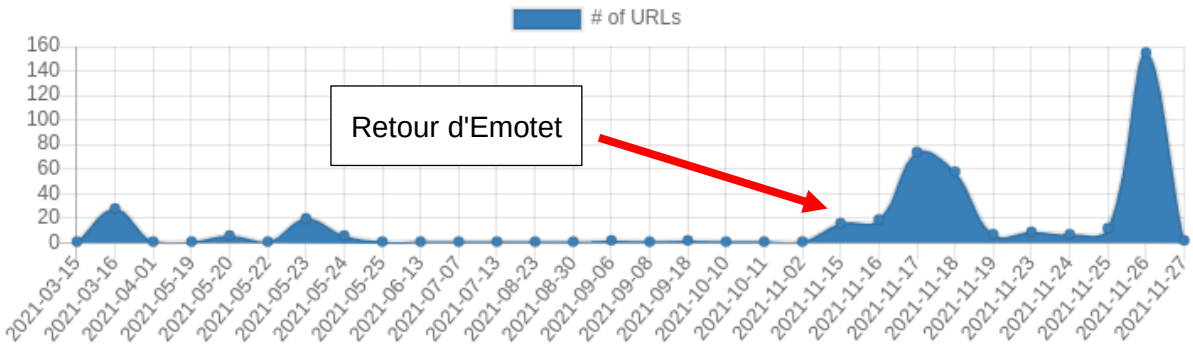
Le retour mi-novembre du cheval de Troie "Emotet" a fait couler beaucoup d'encre. En outre, plusieurs cyberattaques ont à nouveau été signalées à l'étranger contre des organisations de santé. Heureusement, aucune attaque de ce type n'a été signalée en Suisse au mois de novembre.

Cette édition aborde les thèmes suivants :

- Retour d'Emotet
- Le gang lié au rançongiciel BlackMatter cesse ses activités
- Cyber-attaques contre des établissements de santé

Le retour d'Emotet

Le 15 novembre 2021, des experts en sécurité informatique[1] ont annoncé le retour du tristement célèbre cheval de Troie "Emotet". Emotet a été utilisé à grande échelle en 2019 et 2020 pour lancer des cyberattaques contre des entreprises et des réseaux gouvernementaux, afin de les chiffrer à l'aide d'un rançongiciel puis les soumettre à du chantage. Plusieurs dizaines de cas ont notamment été recensés en Suisse. Le réseau de zombies a été neutralisé en janvier 2021 par EUROPOL[2] dans le cadre de l'action de "takedown" Ladybird. Suite à cette action, Emotet s'est tu, du moins jusqu'à mi-novembre et son retour :



Le cheval de Troie "TrickBot" a contribué à la résurrection d'Emotet. Des experts ont observé[3] que TrickBot a installé mi-novembre Emotet sur des appareils Windows déjà infectés. Il est probable que le gang Emotet ait acheté aux acteurs derrière TrickBot des victimes ("Pay-Per-Install" - PPI) pour redémarrer leur propre service. Emotet a également volé des conversations électroniques dans les boîtes aux lettres de Microsoft Outlook et Mozilla Thunderbird afin de les utiliser pour sa diffusion par le biais du détournement de conversation par courriel (également connu sous le nom de "dynamite-phishing"). Cette technique avait déjà été utilisée par Emotet en 2020 pour se propager. Elle consiste à voler des conversations e-mails existantes pour y ajouter le maliciel. L'usurpation d'un correspondant connu et la réutilisation d'une précédente conversation tenue avec ce dernier rend la détection du maliciel plus difficile et augmente sensiblement la probabilité que le destinataire clique sur la pièce jointe infectée.

Le mode opératoire d'Emotet n'a pas beaucoup changé. Ce cheval de Troie continue d'utiliser des macros inclues dans les documents Microsoft Office Excel et Word pour télécharger à partir de sites piratés le binaire malicieux puis l'exécuter sur le poste de sa victime.

Actuellement, le réseau de zombies Emotet et son infrastructure semble toujours en cours de reconstruction, notamment vu le faible volume de spams envoyés par Emotet ainsi que le nombre réduit de serveurs de type Command and Control (C&C) actifs dans le réseau de zombies. Alors que les campagnes de spam étaient initialement dirigées contre les internautes européens et américains, d'autres pays, dont le Japon, l'Australie et la Suisse, se sont ajoutés au cours de la semaine 47. En Suisse, seul le réseau de zombies Emotet "epoch5" est actuellement actif (Emotet étant divisé en différents sous-réseaux, qui reçoivent chacun de nouvelles charges utiles à des moments différents et qui disposent d'une infrastructure C&C dédiée).

[1] https://twitter.com/Cryptolaemus1/status/1460302706954981385

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

[3] https://www.zdnet.com/article/emotet-once-the-worlds-most-dangerous-malware-is-back/

GovCERT observe de près la situation et a commencé dès le 15 novembre à bloquer les serveurs C&C actifs du réseau de zombies Emotet. Les organisations qui utilisent le pare-feu BGP (MELANI BGP feed) et MELANI RPZ (ou le résolveur DNS sécurisé) bénéficient automatiquement d'une protection de base contre Emotet et TrickBot.

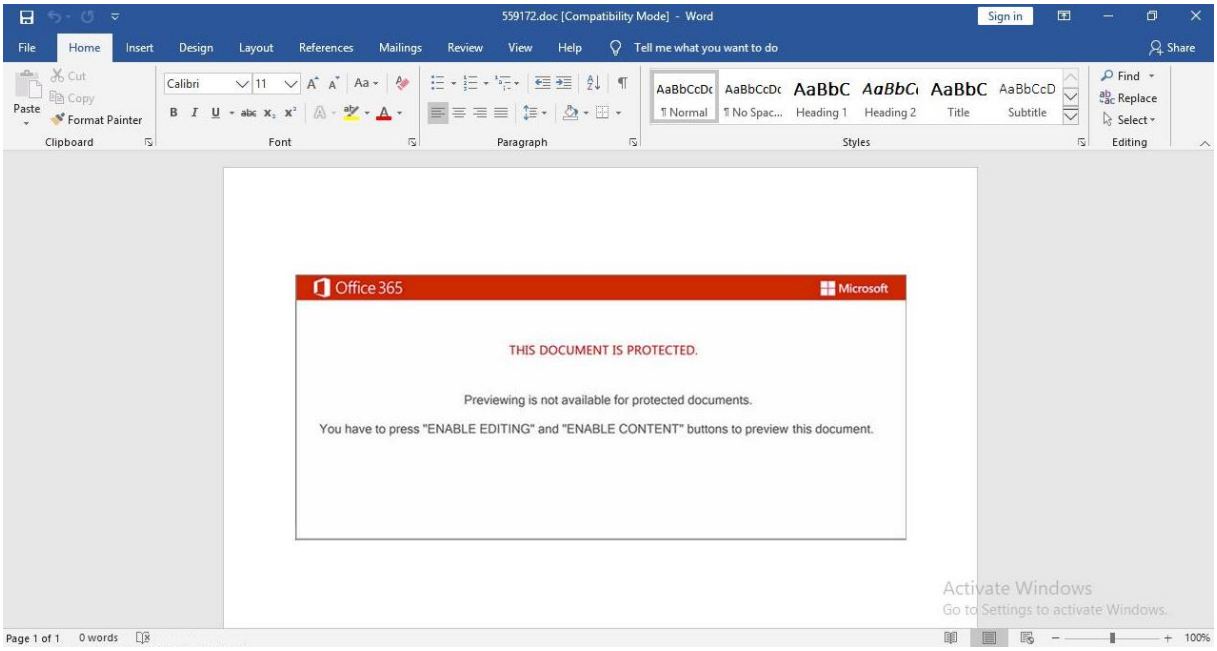


Figure 1 - Document Word malicieux utilisé par Emotet

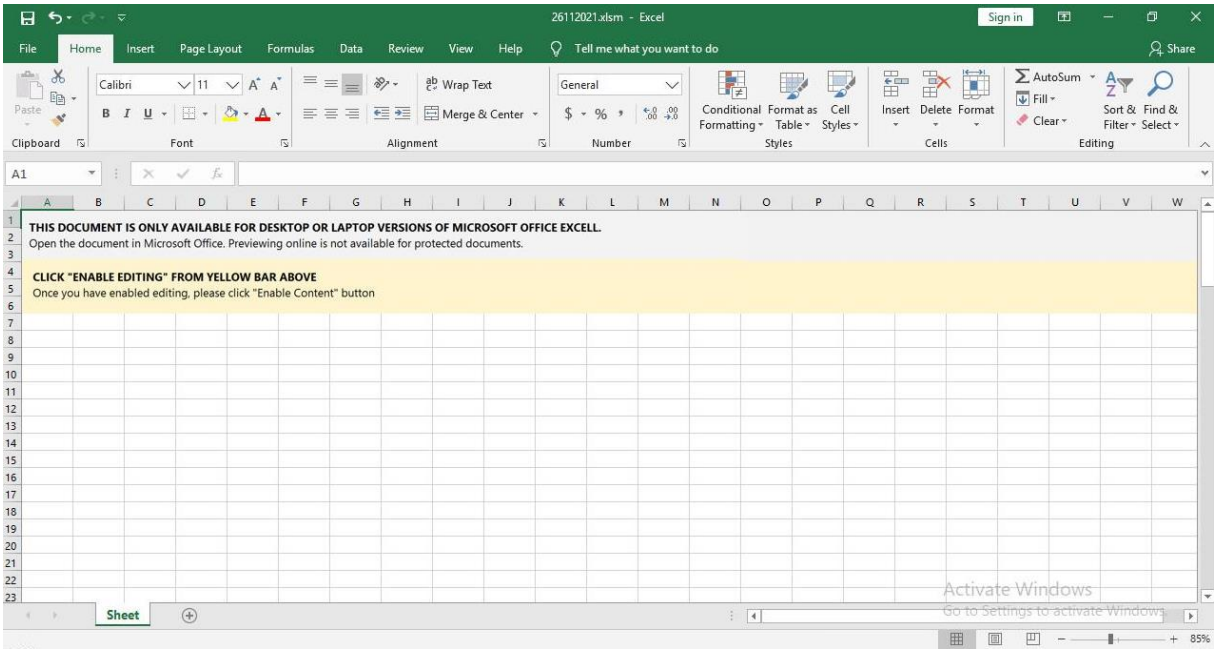


Figure 2 - Document Excel malicieux utilisé par Emotet

Le gang lié au rançongiciel BlackMatter cesse ses activités

En novembre, le gang à l'origine du ransomware "BlackMatter" a annoncé qu'il allait probablement cesser ses activités. BlackMatter était une nouvelle version du ransomware "DarkSide", qui s'est fait entre autres connaître pour le chiffrement de l'exploitant de pipeline américain Colonial Pipeline et du groupe technologique Toshiba. Le groupe BlackMatter a annoncé le 1er novembre 2021 sur son portail en ligne qu'il allait cesser ses activités "en raison de la pression des autorités locales". Selon leurs propres déclarations, "une partie de l'équipe n'est plus disponible". On peut supposer que certains acteurs du groupement ont été arrêtés ou ont annoncé qu'ils se retiraient des activités de BlackMatter par crainte de la répression des autorités.

```
Due to certain unsolvable circumstances associated with
pressure from the authorities (part of the team is no
longer available, after the latest news) - the project is
closed. After 48 hours, the entire infrastructure will be
turned off, it is allowed to:

-Issue mail to companies for further communication.
-Get decryptors, for this write "give a decryptor" inside
the company chat where they are needed.

We wish you all success, we were glad to work.
```

Source: VX-UNDERGROUND

Cyber-attaques contre des établissements de santé

En novembre également, plusieurs cyber-incidents impactant des établissements de santé à l'étranger ont été rendus publiques. En voici un bref aperçu :

Au Canada, plusieurs cyberattaques ont affecté des organisations du secteur de la santé[4] [5]. Des incidents ont également touché le numéro d'urgence "911" qui, selon des citoyens, n'était plus accessible pendant plusieurs heures. Des cabinets médicaux et des hôpitaux ont parfois dû repasser au papier et au crayon, car l'accès aux systèmes informatiques étaient impossibles. Des rendez-vous pour des chimiothérapies, des radiographies et des opérations ont notamment été reportés ou annulés. Bien qu'aucun détail sur la cyberattaque ne soit connu, on peut supposer qu'il s'agit des effets d'une attaque par rançongiciel.

Aux États-Unis, le centre de cancérologie de Las Vegas a été chiffré par un ransomware[6]. L'attaque n'a été rendue publique qu'en novembre 2021, mais elle s'était déjà produite en septembre. Aucune autre information sur cet incident n'est connue à l'heure actuelle.

En Allemagne, le prestataire de services informatiques Medatixx a été victime d'une attaque par rançongiciel[7]. Ce prestataire de services informatiques propose entre autres des logiciels

[4] https://www.bleepingcomputer.com/news/security/canadian-province-health-care-system-disrupted-by-cyberattack/

[5] https://ottawacitizen.com/news/local-news/rideau-valley-health-centre-service-disrupted-due-to-cyber-security-incident

[6] https://www.databreaches.net/las-vegas-cancer-center-hit-by-ransomware-over-labor-day-weekend-3000-patients-notified/

[7] https://www.heise.de/news/Ransomware-Attacke-auf-Medatixx-Grossalarm-im-Gesundheitswesen-6260613.html

pour les médecins, qui sont utilisés par un quart environ des cabinets médicaux allemands. Comme ce prestataire de services informatiques dispose également d'accès en télémaintenance chez ses clients, un grand risque existe pour le système de santé allemand si ces accès ont également été compromis. L'ampleur de la cyberattaque et la demande de rançon n'ont pas été précisées dans l'immédiat.

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.

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

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

- **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.

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.