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

Actualités (février 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 spam que nous avons détectées restent à un niveau élevé.
- Des fraudeurs tentent de plus en plus de vendre de prétendus "vaccins" à des organisations gouvernementales et non gouvernementales.
- Des acteurs étatiques ont tenté de voler les données sur les vaccins de Pfizer.
- Des hôpitaux ont également été victimes d'attaques par des rançons en février 2021.

Fraude impliquant de faux vaccins

Début février 2021, le NCSC a reçu des informations selon lesquelles des fraudeurs profitaient de la pénurie actuelle de vaccins en Europe pour s'enrichir financièrement. Le NCSC a connaissance de cas, en Suisse et à l'étranger, où des cybercriminels ont proposé des vaccins par email à des organisations gouvernementales et non gouvernementales. À cette fin, les fraudeurs ont enregistré des noms de domaine crédibles, à partir desquels le contact a été établi avec les victimes potentielles. Les courriels sont rédigés en anglais et proposent la livraison d'un vaccin, en omettant de spécifier son producteur.

Le NCSC recommande de se méfier des courriels provenant de personnes inconnues et de ne pas ouvrir de pièces jointes ni de cliquer sur des liens présents dans de tels messages. En outre, les courriels suspects peuvent toujours être signalés directement à GovCERT :

incidents@govcert.ch

Nouvelles cyber-attaques contre des hôpitaux européens

En février 2021, des cyberattaques ont à nouveau touchées divers hôpitaux dans le monde entier. Les institutions médicales en Europe n'ont pas été épargnées. Ainsi, deux hôpitaux français ont été victimes de rançongiciels. Le 15 février, l'Hôpital Nord-Ouest situé à Villefranche-sur-Saône a été chiffré par "Ryuk". Selon les médias[1], les patients ont dû être transférés des services d'urgence vers d'autres hôpitaux à la suite de la cyber-attaque. L'accès à divers services, dont la téléphonie et le site web de l'hôpital, a été restreint ou impossible pendant plusieurs jours.

Des attaques réussies impliquant le rançongiciel Ryuk ont eu lieu en Suisse par le passé. Le malware "TrickBot" est généralement utilisé comme vecteur d'infection, se propageant par email à l'aide de documents Office malveillants (docx, xlsx).

Aucun détail n'a été divulgué concernant l'incident à l'hôpital de Dax, une autre victime de rançongiciel en France. Un centre de vaccination a cependant dû être fermé à la suite de l'attaque selon les médias.

Des acteurs étatiques tentent de mettre la main sur les données relatives au vaccin de Pfizer

En février, des acteurs étatiques, prétendument originaires de Corée du Nord, ont tenté de voler des données sur les vaccins auprès du fabricant de vaccins Pfizer. L'agence de presse sud-coréenne Yonhap[2] a rapporté que des attaquants ont tenté de s'introduire dans les systèmes informatiques des fabricants de médicaments sud-coréens. Ces informations proviennent de députés qui en ont été informés par le service de renseignement sud-coréen NIS.

En plus des données de Pfizer sur les vaccins, d'autres fournisseurs de vaccins ont probablement été touchés par des cyberattaques similaires. Reuters mentionne par exemple que les acteurs étatiques ont tenté d'utiliser l'ingénierie sociale pour obtenir des données du développeur de vaccins Astra Zeneca.

Entretien avec un opérateur de rançongiciel

Le fournisseur de services de sécurité informatique TALOS a publié une interview[3] d'un opérateur du rançongiciel "LockBit", offrant un aperçu intéressant sur ses activités :

- **Hôpitaux "cibles faciles"** : les acteurs derrière "LockBit" considèrent les hôpitaux comme des "cibles faciles". Dans la grande majorité des cas, les institutions de santé ciblées se conforment aux demandes de rançon des cybercriminels. Le criminel estime que les chances qu'un hôpital paie une rançon se situent entre 80 et 90 %.
- **Systèmes vulnérables** : les cybercriminels continuent de considérer les systèmes non mis à jour et donc vulnérables comme l'un des moyens les plus faciles de réussir leurs attaques. Et ce, malgré le fait que des correctifs correspondants soient déjà disponibles pour lesdites vulnérabilités, permettant de combler la faille de sécurité.

[1] https://www.inside-it.ch/de/post/immer-mehr-ransomware-attacken-auf-krankenhaeuser-20210217

[2] https://www.heise.de/news/Nordkorea-versuchte-angeblich-Pfizers-Impfstoff-Daten-zu-stehlen-5056656.html

[3] https://talos-intelligence-site.s3.amazonaws.com/production/document_files/files/000/095/481/original/010421_LockBit_Interview.pdf

- **RGPD** : Les réglementations strictes de l'UE en matière de protection des données (RGPD / GDPR) font le jeu des agresseurs. Les entreprises européennes qui sont victimes d'attaques par rançongiciels sont plus disposées à se conformer aux demandes de rançon des cybercriminels afin d'éviter les conséquences juridiques d'une éventuelle publication des données.

(10:47:35 PM) **REDACTED:** I told you that I don't like to focus on quantity and don't after everything
(10:49:43 PM) **Talos Analyst :** There are laws in the US that force the victim to publicly disclose breaches – something like the Sarbanes-Auxley Act and alike
(10:50:20 PM) **REDACTED:** they definitely don't disclose everything
(10:50:38 PM) **REDACTED:** but in reality the ransom payout is a bit more difficult in the US recently

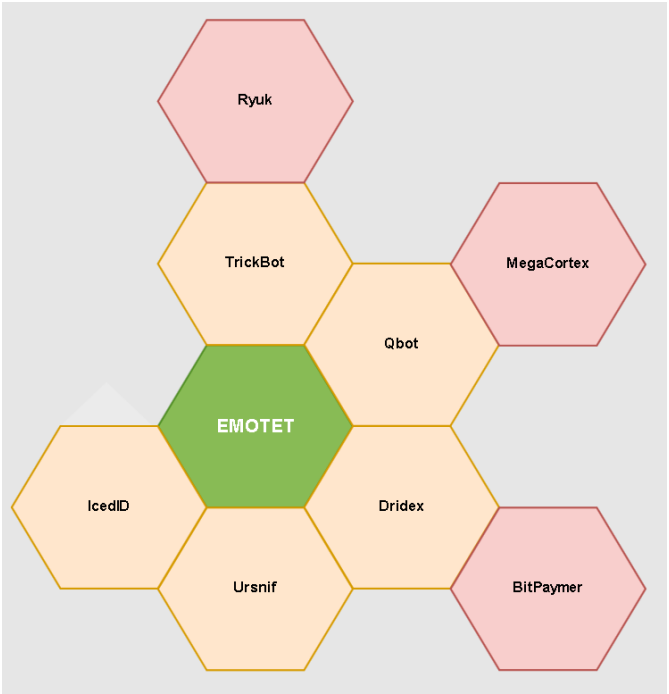
(10:51:09 PM) **Talos Analyst :** because everyone has insurance now?
(10:51:19 PM) **REDACTED:** actually those who have insurance pay up quickly
(10:51:24 PM) **REDACTED:** because the insurance covers it
(10:52:16 PM) **REDACTED:** but I hear that there will soon be a law that will ban victims from paying ransomware

(10:52:29 PM) **Talos Analyst :** what about in Europe?
(10:52:45 PM) **REDACTED:** Europe pays, they are scared of GDPR

Extrait de l'interview avec un opérateur du rançongiciel "LockBit" (source : TALOS)

TrickBot, Qbot et Dridex

Le démantèlement par les forces de l'ordre mi-janvier 2021, dans le cadre de l'opération Ladybird, du botnet "Emotet" a fait cesser un vecteur d'infection populaire pour les rançongiciels. Nous estimons cependant que cela n'a eu qu'un impact limité, voire nul, sur l'activité des ransomware. D'autres familles de logiciels malveillants restent actives et sont utilisées pour infecter puis chiffrer les victimes, comme le démontre l'incident susmentionné à l'Hôpital Nord-Ouest. Le graphique suivant illustre le rôle d'Emotet jusqu'à récemment :



Source : https://twitter.com/pollo290987/status/1214596853771227137

Jusqu'en janvier 2021, "Emotet" était commercialisé par ses créateurs principalement sur le Darkweb sous forme de "Pay-Per-Install" (PPI). D'autres acteurs, également mentionnés ci-dessus, achetaient l'accès à des systèmes infectés par "Emotet" pour y placer leurs propres logiciels malveillants. Cette méthode était généralement utilisée pour mener une reconnaissance puis une infiltration du réseau avant que les cybercriminels ne procèdent au chiffrement d'un maximum de systèmes à l'aide d'un rançongiciel.

Depuis la disparition d'Emotet, ces différents acteurs se chargent eux-mêmes de la diffusion et de l'infection initiale de nouveaux systèmes. Ainsi, nous constatons une augmentation des campagnes de spam qui tentent directement d'infecter le destinataire avec TrickBot, Qbot (alias Quakbot) ou Dridex. Le mode opératoire reste toutefois toujours le même : les cybercriminels envoient des documents Excel ou Word malveillants contenant des macros. Lors de leur exécution, ces macros infectent le système avec un logiciel malveillant, qui est généralement téléchargé depuis un serveur sur Internet au moment de l'exécution.

Recommandations

- 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.

- Veiller à avoir suffisamment de **fichiers de log disponibles** (logs des serveurs proxy contenant les URL consultées, journaux Active Directory, visibilité sur les terminaux à l'aide de SysMon ou d'un autre outil de type EDR - Endpoint Detection and Response).

- Utilisez une liste telle que URLHaus[4] pour empêcher ou du moins détecter le téléchargement de logiciels malveillants.

[4] 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.