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 : 1er avril 2021
Version : v1.0
Auteur : NCSC/GovCERT.ch
Contact : outreach@govcert.ch
Distribution : Secteur de la Santé MELANI, H+, HIN

Actualités (mars 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.
- Un risque élevé d'exposition existe en raison d'une vulnérabilité de type "0day" dans Microsoft Exchange.
- De nouvelles campagnes de malspam en Suisse conduisent à nouveau à des compromissions par ransomware.

Vulnérabilité "0day" dans Microsoft Exchange

Début mars 2021, plusieurs vulnérabilités ont été divulguées dans Microsoft Exchange, dont l'une a été classée comme "critique". Il s'agit de CVE-2021-26855[1], une vulnérabilité qui peut être exploitée à distance pour exécuter du code non autorisé sur le système de la victime (Remote Code Execution - RCE). Cette vulnérabilité est également connue sous le nom de "ProxyLogon[2]". Selon Microsoft, la vulnérabilité a déjà été activement exploitée dans des attaques ciblées par des acteurs étatiques sous le nom de "HAFNIUM[3]" et attribuée à la Chine. Microsoft a fourni un correctif d'urgence en dehors du cycle de mise à jour mensuel ("out-of-band patch"). Dans la nuit du 2 au 3 mars, le NCSC a informé les exploitants d'infrastructures critiques en Suisse de cette vulnérabilité critique, recommandé des mesures immédiates et publié un tweet dans les quatre langues nationales. Quelques heures après la publication de la vulnérabilité, d'autres groupes, notamment cybercriminels, ont commencé à rechercher activement cette vulnérabilité et à l'exploiter automatiquement.

[1] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855
[2] https://proxylogon.com/
[3] https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

En outre et peu de temps après l'annonce de la vulnérabilité, le NCSC a débuté l'analyse des données recueillies par des organisations partenaires ainsi que par ses propres capteurs afin d'identifier les serveurs Microsoft Exchange vulnérables et accessibles au public et d'en informer leurs propriétaires par courrier électronique. Au total, **4316 notifications de ce type** ont été envoyées par le NCSC à ce jour. Les PME ont été les plus touchées, mais aussi les organisations du secteur de la santé qui travaillent avec des données sensibles sur les patients.

Le graphique suivant montre les attaques détectées par ESET exploitant la vulnérabilité en question. Il est clair que cette vulnérabilité était déjà exploitée avant la publication de la mise à jour de sécurité le 3 mars 2021. Également visible est le fait que la vulnérabilité a été massivement exploitée dans les premiers jours suivant sa publication :

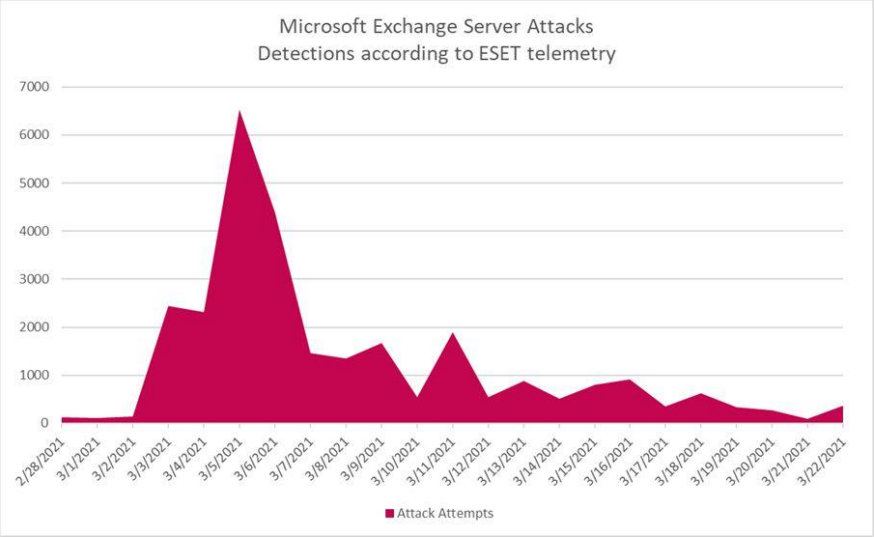

Figure 1: Nombre d'attaques exploitant la vulnérabilité Microsoft Exchange (source : ESET)

Bien que le NCSC ait rapidement informé par tous les canaux disponibles à propos de cette vulnérabilité critique et que le sujet ait été largement couvert par les médias, un grand nombre d'infections ont malheureusement eu lieu en Suisse. Dans la majorité des cas, seule une ou plusieurs portes dérobées sous forme de "web shell" ont été déposées, permettant aux attaquants d'accéder ultérieurement sans restriction au système affecté (et ce même après l'installation de la mise à jour de sécurité de Microsoft). Dans certains cas, cette faille a également été abusée pour installer des mineurs de cryptomonnaie (cryptominer) voire des rançongiciel. Dans quelques cas, cela a conduit à un chiffrement complet de l'infrastructure informatique de la victime par un ransomware, entrainant l'arrêt de processus critiques pour l'entreprise.

Au moins deux acteurs criminels sont entre-temps actifs et utilisent "ProxyLogon" pour des attaques de rançongiciel : "DoejoCrypt (également connu sous le nom de "DearCry") et "Black Kingdom". Les deux groupes utilisent la vulnérabilité ProxyLogon comme point d'entrée dans le réseau des entreprises. Ils tentent ensuite de se déplacer latéralement dans le réseau de la victime via Microsoft Exchange Server afin de chiffrer autant de systèmes que possible avec le ransomware.

Offensive du malware "IcedID"

Suite au démantèlement du botnet Emotet au début du mois de février, GovCERT constate une augmentation d'autres familles de logiciels malveillants. GovCERT a notamment enregistré une augmentation des campagnes de malspam qui distribuent un cheval de Troie appelé "IcedID". Les acteurs s'appuient sur des documents Excel piégés envoyé par email et contenant un code macro malveillant. Lorsque la macro est exécutée, elle télécharge IcedID depuis Internet.

IcedID est actif depuis un certain temps déjà, mais avait jusqu'ici surtout ciblé les États-Unis. Or, le NCSC a pris connaissance de cas en Suisse dans lesquels les acteurs ont utilisé IcedID pour pénétrer dans des réseaux d'entreprise, ont obtenu l'accès à d'autres systèmes par un mouvement latéral dans le réseau de la victime et ont ainsi pu les chiffrer avec un rançongiciel.

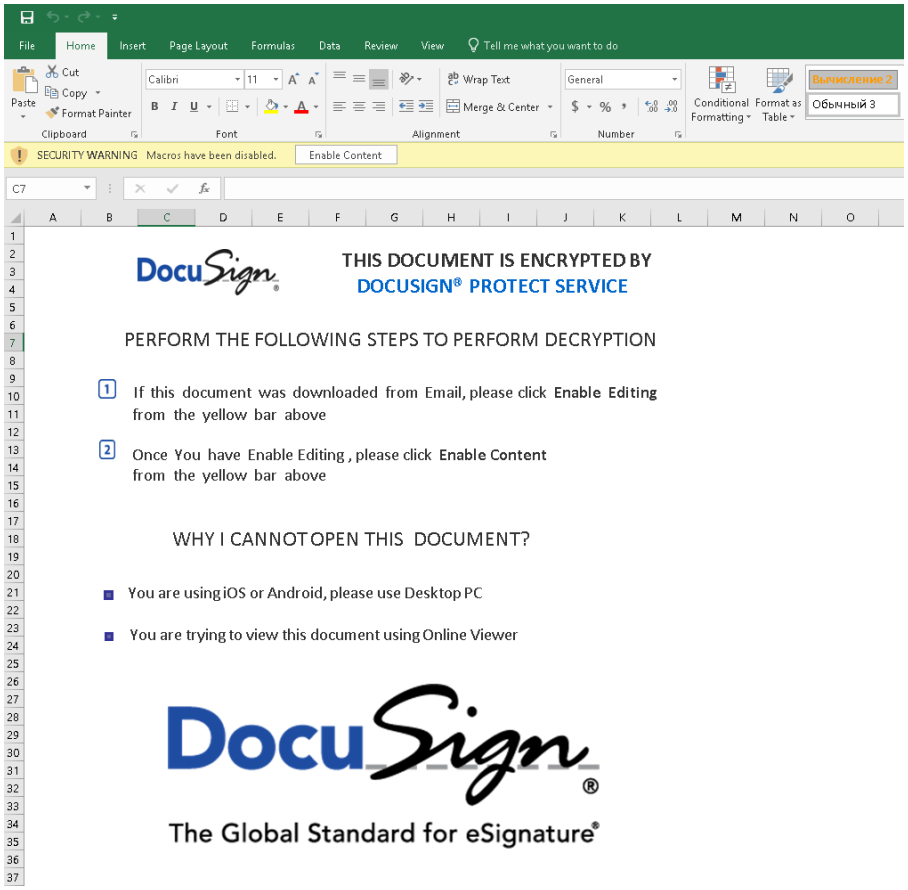

Figure 2: Fichier Excel contenant un code macro malveillant

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

- Mettez en œuvre la solution **LAPS (Local Administrator Password Solution)** et utilisez des comptes de type "Managed Service Accounts".
  - https://www.microsoft.com/en-us/download/details.aspx?id=46899
  - https://docs.microsoft.com/de-de/windows-server/security/group-managed-service-accounts/getting-started-with-group-managed-service-accounts

- 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[4] pour **empêcher ou du moins détecter le téléchargement de logiciels malveillants**.

- **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.

- Les appareils infectés **doivent toujours être réinstallés**. Le nettoyage (ou l'installation de correctifs après coup) n'offre pas une garantie suffisante que l'attaquant a effectivement perdu tout accès. Il convient par ailleurs de vérifier si un mouvement latéral a déjà eu lieu et quels comptes d'utilisateurs ont potentiellement été compromis.

- 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).

[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.