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

Actualités (Avril 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.
- Nous constatons une augmentation de l'activité des rançongiciels en Suisse.
- Les vulnérabilités de type "0day" corrigées récemment dans Pulse Connect Secure, SonicWall Email Security (ES) ainsi que de vulnérabilités dans MS Exchange exposent un risque élevé.
- Des cybercriminels vendent 1'300'000 identifiants RDP sur le marché noir. Plusieurs milliers d'organisations en Suisse sont potentiellement concernées.

Augmentation de l'activité des rançongiciels en Suisse

Un nombre inhabituellement élevé de cas de ransomware ont été signalés au NCSC dans le courant du mois d'avril 2021. Les familles les plus actives sont *QLocker, Avaddon, Lockbit, Conti, Himynameis-ransom, Ryuk, Sodinokibi, BlackKingdom* et *Makop*.

Le vecteur d'infection habituel des ransomwares demeure l'utilisation de documents bureautiques malveillants propagés par email, l'exploitation de vulnérabilités connues non corrigée dans des équipements connectés à Internet ou par l'abus d'identifiants volés ou devinés. Le NCSC a également reçu des rapports de cas dans lesquels un malfrat appelle la victime en se faisant passer pour un employé d'un service de livraison. L'auteur tente ensuite d'obtenir l'adresse électronique de la victime par le biais de l'ingénierie sociale. Souvent, le prétendu service de livraison utilise le prétexte qu'un bon de livraison doit être envoyé par e-mail. L'e-mail malicieux contient un lien qui mène à un fournisseur bien connu de services de stockage en nuage. Si la victime ouvre le fichier qui lui est proposé, son ordinateur est infecté par un logiciel malveillant qui charge immédiatement l'outil "Cobalt Strike". Par ce biais, l'auteur peut se déplacer latéralement dans le réseau de la victime, accéder à d'autres systèmes et

finalement les chiffrer à l'aide d'un rançongiciel. Ce type d'attaque est souvent accompagnée d'une exfiltration des données volées. La victime fait ensuite l'objet d'une extorsion supplémentaire autour de la publication ou de la vente de ces données.

Depuis la mi-avril, nous observons également une importante campagne de ransomware dans laquelle les attaquants tentent de chiffrer les produits NAS du fabricant Qnap avec un ransomware appelé QLocker[1]. Les attaquants exploitent une vulnérabilité connue dans les modules complémentaires (apps) Multimedia Console, Media Streaming et Hybrid Backup Sync pour accéder aux NAS de QNAP qui sont accessibles via Internet. En l'espace de cinq jours seulement, les inconnus opérants QLocker ont encaissé plus de 250'000 USD selon les médias[2].

En Suisse, on dénombre plusieurs dizaines d'incidents QLocker, souvent dans des PME. Dans certains cas non seulement les fichiers mais également leurs sauvegardes ont été chiffrées, car stockées sur le même support.

Vulnérabilités "0day" dans Pulse Secure et SonicWall

Après les vulnérabilités critiques de Microsoft Exchange en mars, deux autres éditeurs ont été affectés en avril. Les produits des fabricants de solutions de sécurité informatique "Pulse Secure" et "SonicWall" sont concernés[3] :

SonicWall Email Security (ES)

Vulnérabilité	Description
CVE-2021-20021	Unauthorized administrative account creation
CVE-2021-20022	Post-authentication arbitrary file upload
CVE-2021-20023	Post-authentication arbitrary file read

Pulse Connect Secure

Vulnérabilité	Description
CVE-2021-20021	Remote Code Execution (RCE)

Les vulnérabilités mentionnées sont critiques et, selon les informations dont nous disposons, sont déjà exploitées dans des cas isolés par des acteurs pour accéder à des réseaux d'entreprise (exploitation de type "0day"). Le NCSC a connaissance d'organisations en Suisse dont les réseaux ont été compromis par les vulnérabilités mentionnées.

Le NCSC souligne également de manière explicite que des vulnérabilités similaires ont été utilisées ces derniers mois par des acteurs pour pénétrer dans des réseaux d'entreprise, les chiffrer à l'aide de rançongiciel et voler d'importants volumes de données, avec lesquels la victime pouvait faire l'objet d'extorsions. Le NCSC estime donc que le danger posé par ces vulnérabilités est très élevé.

[1] https://www.qnap.com/en/security-news/2021/response-to-qlocker-ransomware-attacks-take-actions-to-secure-qnap-nas

[2] https://www.bleepingcomputer.com/news/security/a-ransomware-gang-made-260-000-in-5-days-using-the-7zip-utility/

[3] https://www.ncsc.admin.ch/ncsc/fr/home/aktuell/news/news-aktuell/pulse-secure-sonicwall.html

1'300’000 identifiants RDP vendus

En mars, des chercheurs en sécurité ont découvert 1'300’000 identifiants RDP volés qui étaient vendus sur un marché noir appelé "UAS". Ces informations d'identification ont très probablement été obtenues par des attaques par force brute ciblant des serveurs RDP accessibles depuis Internet.

Le NCSC a connaissance de plusieurs milliers d'organisations touchées en Suisse. Il convient toutefois de noter qu'une grande partie des données datent déjà de plusieurs années. Le NCSC a informé des identifiants volés récents (découverts en décembre 2020 ou janvier 2021) les organisations concernées en Suisse, que ce soit directement ou via leur fournisseur d'accès à Internet (FAI).

Recommandations

- Les systèmes exposés à 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 **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.

- Si vous utilisez **SonicWall** Email Security (ES) dans votre entité :
  - Assurez-vous que le produit dispose des dernières mises à jour de sécurité (hotfix 10.0.9.6173 ou 10.0.9.6177).

- Si vous utilisez **Pulse Connect Secure** :
  - Assurez-vous que le produit exécute la dernière version du logiciel (9.1R.11.4).

- - Si vous utilisez **QNAP** :
  - Assurez-vous que le produit utilise la dernière version du logiciel et que toutes les applications/compléments installés sont également à jour.
  - Évitez d'exposer le produit directement à l'Internet.

- 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[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.

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.

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