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 janvier 2022
Version : v1.0
Auteur : NCSC/GovCERT.ch
Contact : outreach@govcert.ch
Distribution : Secteur de la Santé MELANI, H+, HIN

Actualités (Décembre 2021)

L'exposition aux risques cyber dans le secteur de la santé reste élevée. Les pirates ont profité de la période entre Noël et le Nouvel An pour lancer des cyber-attaques contre des organisations. En effet, de nombreux spécialistes informatiques sont en vacances et une cyberattaque contre le réseau de l'entreprise risque ainsi d'être détectée trop tard.

Cette édition aborde les thèmes suivants :

- Vulnérabilité critique dans la bibliothèque Java "Log4j".
- Attaques de ransomware contre le secteur de la santé
- A notre sujet…

Vulnérabilité critique dans la bibliothèque Java "Log4j"

Début décembre, une vulnérabilité critique dans la bibliothèque largement répandue Java "Log4j" a été rendue publique[1], permettant à un attaquant d'exécuter du code arbitraire à distance ("Remote Code Execution" - RCE). Peu de temps après l'annonce de la faille, celle-ci a déjà été largement exploitée par des cybercriminels pour compromettre des organisations. Le NCSC a constaté des centaines d'attaques de ce type au mois de décembre et a pris des contre-mesures peu après l'annonce de la faille de sécurité afin de protéger les organisations disposant de logiciels vulnérables en Suisse. En outre, le NCSC a informé des dizaines d'organisations en Suisse qui utilisent des logiciels potentiellement vulnérables. Jusqu'à présent, les acteurs ont surtout distribué des maliciels Linux ("Mirai", "Kinsing" et "Tsunami"), mais aussi des maliciels Windows ("Dridex" et "CoinMiner") via cette faille de sécurité.

[1] https://www.ncsc.admin.ch/ncsc/fr/home/aktuell/im-fokus/log4j.html

Le NCSC a également connaissance de cas d'attaques contre "Log4j", dans lesquels des pirates ont chiffré le réseau de la victime avec un ransomware[2]. Le ministère belge de la Défense a lui aussi été récemment victime d'une attaque exploitant "Log4j"[3], sans que l'on connaisse pour l'instant les intentions exactes des auteurs.

Log4j est utilisé dans de nombreux produits tiers. Par conséquent, de nombreux produits et logiciels open source sont concernés par cette vulnérabilité. Le NCSC recommande donc de veiller à ce que tous les logiciels soient toujours maintenus au niveau de patch le plus récent. Il est important de surveiller non seulement le logiciel proprement dit, mais aussi toutes les dépendances du logiciel et de définir clairement la responsabilité de leur maintenance.

Vous trouverez de plus amples informations sur la vulnérabilité de "Log4j" sur le site web du NCSC et de GovCERT.ch.

Faille de sécurité critique dans la bibliothèque Java «Log4j»
https://www.ncsc.admin.ch/ncsc/fr/home/aktuell/im-fokus/log4j.html

Zero-Day Exploit Targeting Popular Java Library Log4j:
https://govcert.ch/blog/zero-day-exploit-targeting-popular-java-library-log4j/

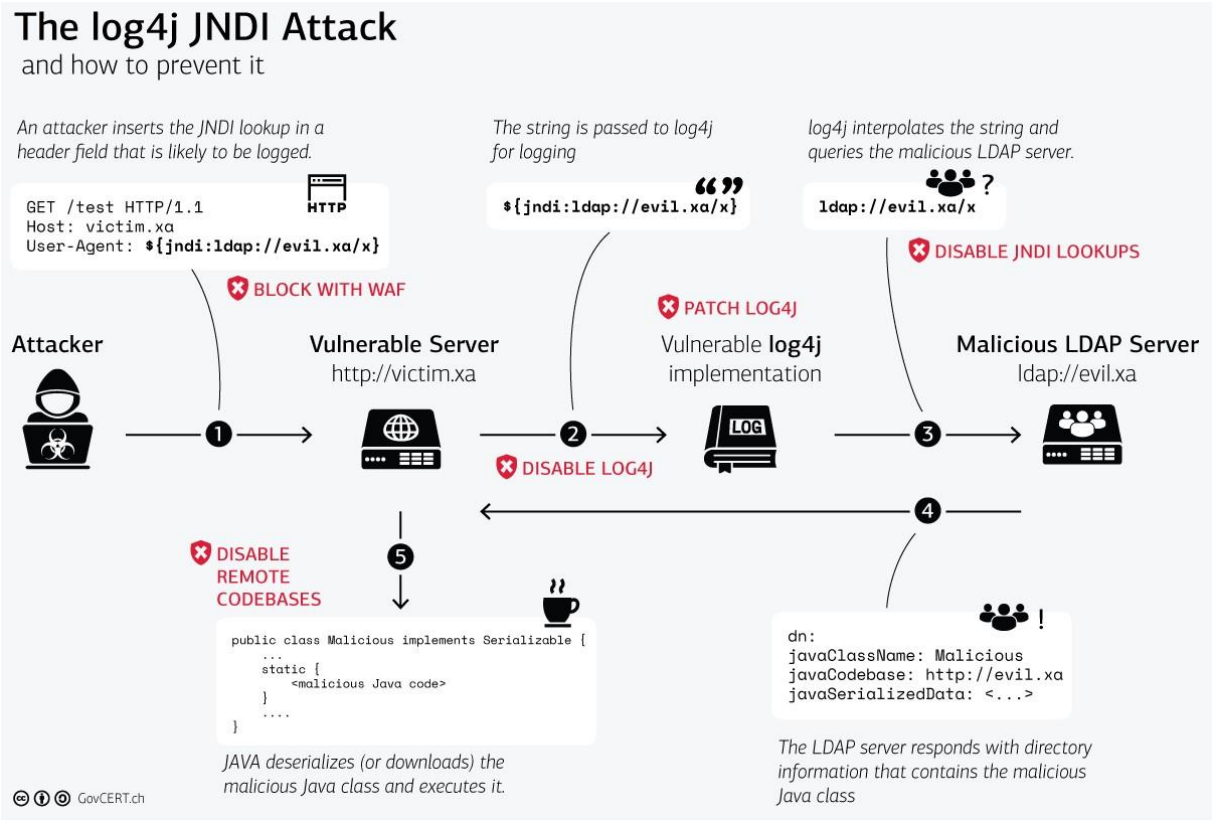

Figure 1 - Déroulement d'une attaque exploitant "Log4j"

[2] https://www.zdnet.com/article/conti-ransomware-attacking-vmware-vcenter-servers-through-log4j-vulnerability/
[3] https://www.cyberscoop.com/intruders-leverage-log4j-flaw-to-breach-belgian-defense-department/

Attaques de ransomware contre le secteur de la santé

Le mois de décembre a été marqué par de nouvelles attaques de rançongiciels contre des organisations du secteur de la santé :

- Début décembre, l'exploitant américain de centres de traitement aux opioïdes "Behavioral Health Group" (BHG) a été victime d'une cyberattaque[4]. BHG gère plus de 80 cliniques dans 17 États américains. Selon ses propres informations, BHG a temporairement désactivé son réseau informatique afin d'éviter que l'attaque ne se propage. Selon les médias, la panne des systèmes informatiques a entraîné des problèmes dans la distribution des médicaments. Dans un premier temps, on ignorait s'il s'agissait d'une attaque par ransomware.

- Fin décembre, la société allemande Compugroup Medical (CGM) a annoncé avoir été victime d'une attaque par ransomware[5]. CGM est, selon ses propres dires, le leader du marché des logiciels pour les cabinets médicaux, les laboratoires et les cliniques. Selon le communiqué de presse de l'entreprise, la grande majorité des systèmes des clients n'ont pas été touchés et sont toujours en service. On ne dispose pas d'autres informations et on ne sait pas si une rançon a été payée.

- Les données du CyberPeace Institute[6] montrent qu'au cours des 18 derniers mois, au moins 39 groupes de ransomware ont lancé des attaques contre des entreprises du secteur de la santé dans plus de 27 pays. La plupart des attaques contre ces entreprises ont été menées par "Conti", "Pysa" et "Hive".

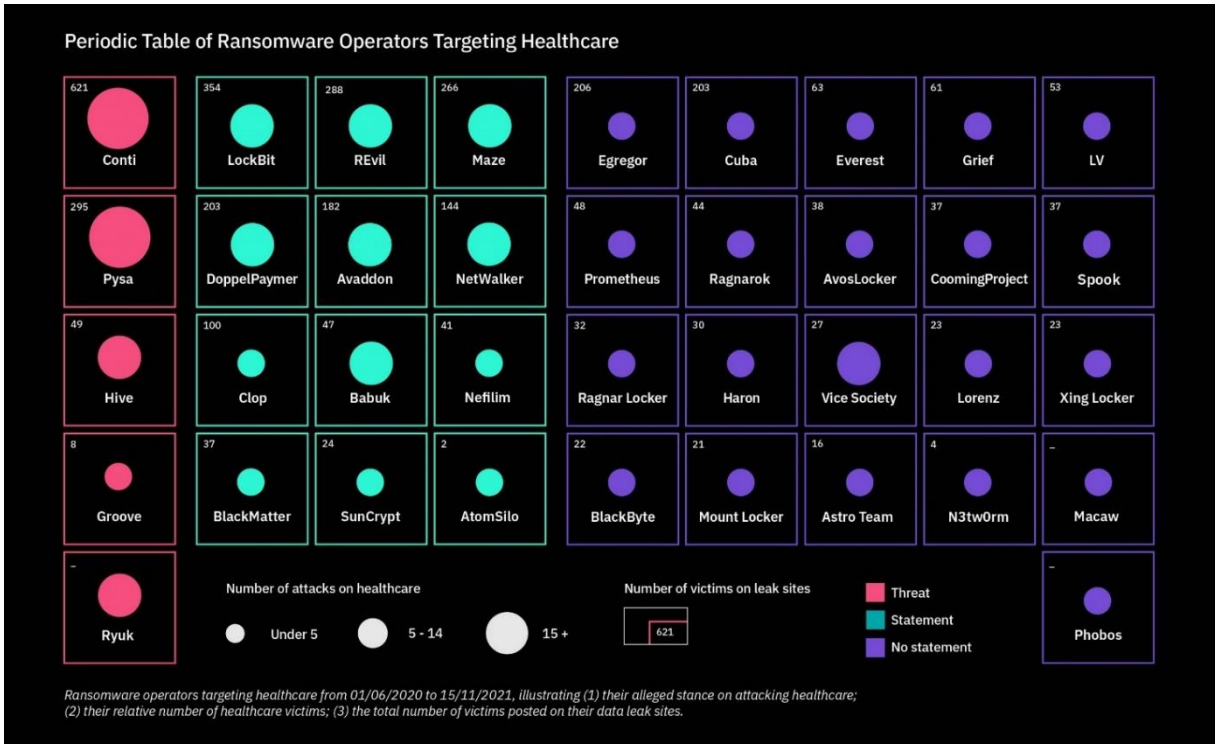

Figure 2 - Nombre d'attaques par rançongiciel sur le secteur de la santé par famille de ransomware

[4] https://www.bleepingcomputer.com/news/security/cyberattack-on-bhg-opioid-treatment-network-disrupts-patient-care/

[5] https://www.cgm.com/corp_en/magazine/articles/emergency-note/technical-failure.html

[6] https://cyberpeaceinstitute.org/blog-series-reconceptualizing-ransomware/

A notre sujet…

Le "Cyber Security Update pour le Secteur de la Santé" sera publié à partir de 2022 par l'Operation Information Center (OIC) du Service de Renseignement de la Confédération (SRC). Nous remercions nos lectrices et lecteurs de leur fidélité et espérons pouvoir continuer à vous compter parmi notre lectorat.

L'interlocuteur pour les questions techniques, les annonces de cyberincidents ou la mise en œuvre des prestations du NCSC reste le GovCERT (voir "Contact GovCERT" ci-après).

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

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