الوكالة الوطنيّة للسّلامة المعلوماتيّة
Agence Nationale de la Sécurité Informatique

Comment se protéger contre le malware polymorphe « Emotet »

Introduction

Le cheval de Troie Emotet est vraiment l'un des malwares les plus dangereux de l'histoire de la cybersécurité. N'importe qui peut en être victime - particuliers, entreprises, et même les autorités mondiales. Car une fois que le cheval de Troie s'est infiltré dans un système, il recharge d'autres logiciels malveillants qui vous espionnent. En effet, Emotet est un malware avancé et modulaire qui fonctionne, principalement, comme un téléchargeur ou un dropper d'autres chevaux de Troie bancaires. Emotet continue de figurer parmi les logiciels malveillants les plus coûteux et les plus destructeurs affectant plusieurs machines à l'échelle internationale. Il peut s'échapper à la détection typique basée sur la signature et dispose de plusieurs méthodes pour maintenir sa persistance, notamment des clés de registre et des services à démarrage automatique. Emotet utilise des bibliothèques de liens dynamiques (DLL) modulaires pour évoluer et mettre à jour ses capacités en permanence. Pour s'échapper de la détection, Emotet peut générer de faux indicateurs s'il est exécuté dans un environnement virtuel.

Comment le cheval de Troie Emotet se propage-t-il ?

Emotet est principalement distribué par le biais de la méthode « Outlook harvesting ». En effet, le cheval de Troie lit les courriels des utilisateurs déjà touchés et crée un contenu faussement réel. Ces courriels semblent légitimes et personnels et se distinguent ainsi des courriels de spam ordinaires. Emotet envoie ces e-mails de

phishing à des contacts enregistrés tels que des amis, des membres de la famille et des collègues de travail.

La plupart du temps, les e-mails contiennent un document Word infecté ou un lien dangereux. Le nom correct de l'expéditeur est toujours affiché. Les destinataires pensent donc que c'est sûr : tout ressemble à un courriel légitime. Ils cliquent ensuite (dans la plupart des cas) sur le lien dangereux ou téléchargent la pièce jointe infectée.

Une fois qu'Emotet a accès à un réseau, il peut se propager. Au cours de ce processus, il tente de craquer les mots de passe des comptes en utilisant la méthode de force brute. Parmi les autres moyens de propagation d'Emotet figurent l'exploit « EternalBlue » et la vulnérabilité « DoublePulsar » sur Windows, qui permettait d'installer des logiciels malveillants sans intervention humaine.

Qui se cache derrière Emotet ?

Selon l'Office général allemand pour la sécurité en matière de technologie de l'information (BSI) : « Les développeurs d'Emotet sous-louent leur logiciel et leur infrastructure à des tiers ». Ils s'appuient également sur des programmes malveillants supplémentaires pour atteindre leurs objectifs. Le BSI estime que les motivations des cybercriminels sont financières et considère ce type d'attaques comme des cybercrimes, et non comme de l'espionnage. Pourtant, personne ne semble savoir précisément qui se cache derrière Emotet. Plusieurs rumeurs circulent concernant les pays d'origine, mais rien n'a été prouvé.

Comment se protéger d'Emotet ?

Pour se protéger d'Emotet et d'autres chevaux de Troie, il ne suffit pas de se fier uniquement aux programmes antivirus. La détection d'un virus polymorphe n'est que la première étape pour les utilisateurs finaux. Il n'existe tout simplement pas de solution permettant de se protéger à 100% contre Emotet ou d'autres chevaux de Troie en

constante évolution. Ce n'est qu'en prenant des mesures organisationnelles et techniques que l'on peut réduire au minimum le risque d'infection.

Voici quelques conseils pour vous protéger d'Emotet :

- Installez le plus rapidement possible les mises à jour fournies par les fabricants afin de combler les éventuelles failles de sécurité. Cela s'applique aux systèmes d'exploitation tels que Windows et macOS ainsi qu'à tous les programmes d'application, navigateurs, modules complémentaires de navigateur, clients de messagerie, Office et programmes PDF.
- Veillez à installer un programme complet de protection contre les virus et les logiciels malveillants, analyser régulièrement votre ordinateur à la recherche de vulnérabilités. Vous bénéficierez ainsi de la meilleure protection possible contre les derniers virus, logiciels espions, etc.
- Ne téléchargez pas les pièces jointes douteuses des courriels et ne cliquez pas sur les liens suspects. Si vous n'êtes pas sûr qu'un courriel soit faux, ne prenez pas de risques et contactez l'expéditeur. Si l'on vous demande d'autoriser l'exécution d'une macro sur un fichier téléchargé, ne le faites en aucun cas, mais supprimez immédiatement le fichier. Ainsi, vous ne donnerez pas à Emotet l'occasion de s'introduire dans votre ordinateur.
- Sauvegardez régulièrement vos données sur un périphérique de stockage externe. En cas d'infection, vous aurez toujours une sauvegarde sur laquelle vous appuyer et vous ne perdrez pas toutes les données de votre appareil.
- Utilisez uniquement des mots de passe forts pour toutes les connexions à vos serveurs et à vos services (banque en ligne, compte de messagerie, etc … En outre, de nombreux programmes offrent aujourd'hui la possibilité d'une authentification à deux facteurs.
- Demandez à votre ordinateur d'afficher les extensions de fichiers par défaut. Cela vous permet de détecter les fichiers douteux tels que "Photo123.jpg.exe", qui sont généralement des programmes malveillants.

Indicateurs de compromis

Emotet se cache dans les dossiers système et s'enregistre en tant que service système. Il peut modifier les paramètres du registre Windows afin de s'exécuter automatiquement au démarrage du système. Emotet se trouve généralement dans un chemin arbitraire situé dans les répertoires AppData\Local et AppData\Roaming. Il imite les noms d'exécutables connus. Il est maintenu par des tâches programmées ou par des clés de registre. En outre, Emotet crée des fichiers au nom aléatoire dans les répertoires racine du système qui sont exécutés en tant que services Windows. Les systèmes compromis contactent régulièrement les serveurs de commande et de contrôle (C2) d'Emotet pour obtenir des mises à jour et des nouvelles charges utiles.

D'autres indicateurs de compromission peuvent être trouvés via les urls suivantes :

1. **AlienVault IOC**

   https://otx.alienvault.com/pulse/5bb4f4156e489a1abbbd1d28/

2. **Malwarebytes IOC**

   https://blog.malwarebytes.com/detections/trojan-emotet/

3. **PrecisionSec's IOC**

   https://precisionsec.com/threat-intelligence-feeds/emotet/

4. **Cybersecurity & Infrastructure Security Agency (CISA) IOC**

   https://us-cert.cisa.gov/ncas/alerts/aa20-280a

5. **Feodo Tracker**

   https://feodotracker.abuse.ch/browse/emotet/

Comment puis-je supprimer Emotet ?

- Ne paniquez pas si vous pensez que votre PC est peut-être infecté par Emotet. Informez votre entourage personnel de l'infection, car les personnes faisant partie de vos contacts de messagerie sont potentiellement en danger.
- Isolez votre ordinateur s'il est connecté à un réseau afin de réduire le risque de propagation d'Emotet.
- Modifiez toutes les données de connexion de tous vos comptes (comptes de messagerie, navigateurs web, etc.). Faites-le sur un appareil distinct qui n'est pas infecté ou connecté au même réseau.
- Utilisez un programme antivirus pour vous aider à nettoyer votre appareil infecté.
- Vous devez vérifier si tous les ordinateurs connectés à votre réseau ne soient pas infectés, les uns après les autres car Emotet étant polymorphe et son code change légèrement à chaque accès à chaque connexion.

Références

KASPERSKY
https://www.kaspersky.com/resource-center/preemptive-safety/ransomware-removal

MALPEDIA
https://malpedia.caad.fkie.fraunhofer.de/details/win.emotet

US : DEPARTMENT OF JUSTICE
https://www.justice.gov/opa/pr/emotet-botnet-disrupted-international-cyber-operation

US-CERT : Alert (TA18-201A)
https://us-cert.cisa.gov/ncas/alerts/TA18-201A

CERT-FR

https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-003/

CIRT.GY

https://cirt.gy/node/474

MALWAREBYTES

https://blog.malwarebytes.com/threat-analysis/2021/01/cleaning-up-after-emotet-the-law-enforcement-file/