Emotet de retour, POC Exchange, 0-day Windows : à quelle sauce les attaquants prévoient de nous manger cette semaine ?

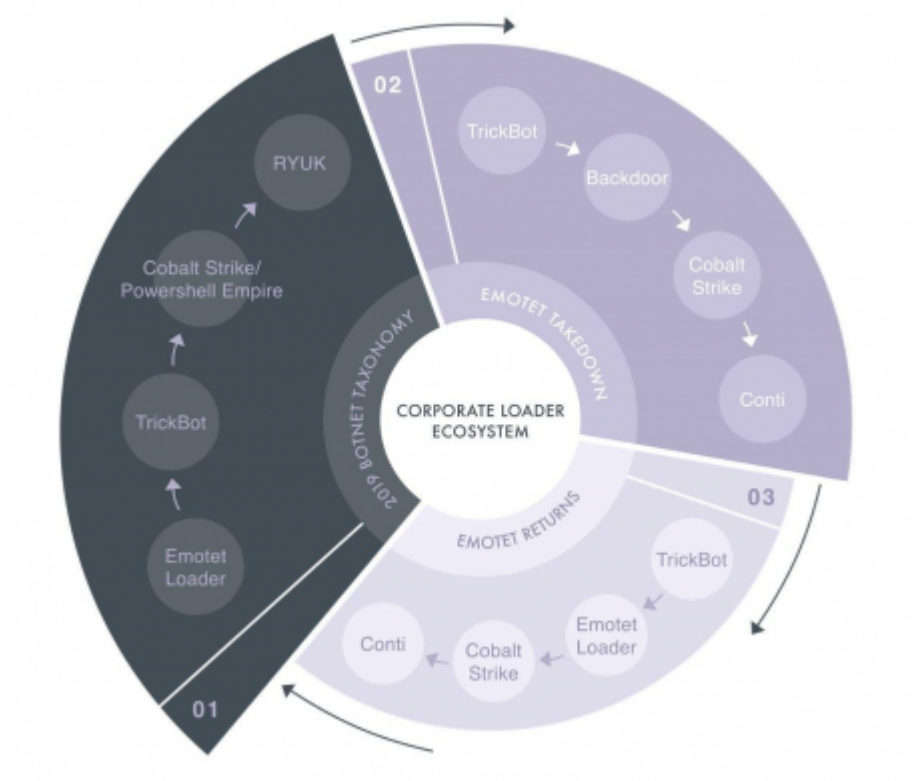
By DSIH

Published: 2021-11-25 · Archived: 2026-04-06 01:02:11 UTC

Emotet

Dans le domaine de la sécurité numérique, les bonnes nouvelles sont plutôt rares...
Le 27 janvier dernier, Europol annonçait une neutralisation de l'infrastructure permettant le contrôle des botnets Emotet [1]. Il était prévisible que cette bonne nouvelle n'allait être que de courte durée. Pour rappel, Emotet [2] est un « cheval de Troie », souvent considéré comme le plus répandu entre 2014 et 2020 et généralement distribué via des pièces jointes ou liens Web accompagnants des courriels malveillants. Les machines compromises étaient contrôlées par quelques centaines de serveurs à travers le monde et regroupées en trois grands botnets : Epoch 1, Epoch 2 et Epoch 3.

Depuis le 14 novembre, plusieurs chercheurs connus et reconnus, comme Vitali KREMEZ s'accordent à dire qu'Emotet est de retour [3].
Il semblerait que l'on retrouve toujours le même groupe d'acteurs dans la boucle, avec les attaquants derrière le cheval de Troie Trickbot et les rançongiciels Conti et Ryuk notamment.



Source : ADV INTEL

En m'appuyant sur les serveurs recensés via le projet Feodo Tracker d'Abuse.ch [4], je constate que tous les serveurs de commande et de contrôle (C2) actifs présentent une similarité permettant d'identifier assez facilement une connexion vers l'un d'entre eux. Même s'ils présentent des certificats TLS autosignés différents, les informations spécifiées dans les certificats restent les mêmes :

C=GB
ST=London
L=London
O=Global Security
OU=IT Department
CN=example.com

Il serait donc possible de détecter une potentielle compromission avec la règle Suricata suivante :

alert tls $EXTERNAL_NET any -> $HOME_NET any (msg:" Suspicious TLS Certificate - Possible Emotet C2 Server"; tls.cert_subject; content:"CN=example.com"; nocase; content:"L=London"; content:"ST=London"; content:"O=Global Security"; content:"C=GB"; reference: url,https://malpedia.caad.fkie.fraunhofer.de/details/win.emotet; metadata:created_at 2021_11_24, updated_at 2021_11_25; sid:2021112402; rev:4; classtype:trojan-activity;)

À noter que même si plusieurs certificats ont été générés aux alentours du 14 novembre, certains sont plus anciens et remontent à fin août / début septembre :

Si les hostilités n'ont pas été lancées avant le 14 novembre, date à laquelle les nouvelles détections ont été observées, cela nous laisse supposer qu'ils préparaient le terrain depuis quelques mois, ou qu'ils sont restés discrets jusque-là.

Exchange

Si vous avez des serveurs Exchange, dont l'interface OWA est exposée sur Internet, ce n'est pas la joie en matière de sécurité, mais il est parfois difficile de lutter… Sachez que la vulnérabilité CVE-2021–42321 corrigée le 9 novembre et annoncée comme déjà exploitée par Microsoft a désormais son POC d'exploitation publique [5], en ligne depuis le 21 novembre. Même si la vulnérabilité permettant d'exécuter du code arbitraire à distance avec des droits « system » nécessite un compte utilisateur pour être exploitée, contrairement à ProxyShell [6], le vol d'identifiants et mots de passe est assez courant, notamment via des campagnes de phishing.

L'application rapide du correctif s'impose…

Il est également possible de vérifier que la vulnérabilité n'a pas été exploitée en recherchant dans les logs à l'aide de la commande PowerShell suivante :

*Get-EventLog -LogName Application -Source "MSExchange Common" -EntryType Error | Where-Object { $_.Message -like "*BinaryFormatter.Deserialize*" }*

Des tentatives d'exploitations peuvent également être observées au niveau des traces d'accès Web (reverse proxy, waf, firewall...) à l'URL : /ews/exchange.asmx

Windows

Pour finir avec les mauvaises nouvelles, un POC permettant d'exploiter une vulnérabilité mal corrigée dans Windows (CVE-2021-41379) et donc exploitable dans un système Windows à jour des derniers correctifs de sécurité a été rendu publique le 22 novembre [7]. D'après un post sur le blog de Talos [8], certains attaquants utiliseraient déjà cette vulnérabilité dans Windows Installer permettant à un utilisateur non privilégié de devenir administrateur.

---

[1] https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

[2] /article/3889/emotet-qui-est-ce-demon-qui-vient-hanter-les-nuits-des-rssi.html

[3] https://www.advintel.io/post/corporate-loader-emotet-history-of-x-project-return-for-ransomware

[4] https://feodotracker.abuse.ch/browse/emotet/

[5] https://peterjson.medium.com/some-notes-about-microsoft-exchange-deserialization-rce-cve-2021-42321-110d04e8852

https://www.youtube.com/watch?v=Fmx6JlSABAQ

https://twitter.com/testanull/status/1462363736815988744

[6] https://www.apssis.com/actualite-ssi/532/serveurs-exchange-et-proxyshell-comment-eviter-de-laisser-rentrer-n-importe-qui-dans-son-si.htm

[7] https://github.com/klinix5/InstallerFileTakeOver

[8] https://blog.talosintelligence.com/2021/11/attackers-exploiting-zero-day.html

---