Emotet : le poids lourd des botnets vraiment mis K.-O. ?

En est-ce fini d'Emotet ? Europol veut y croire au sortir d'une opération qui a impliqué les forces de police de huit pays dont la France.

> *[#CoopérationInternationale] La #PoliceJudiciaire □□ participe au démantèlement du logiciel malveillant #Emotet lors d'une opération internationale coordonnée par @Europol. Ce #botnet a infecté des centaines de milliers d'ordinateurs dans le monde. https://t.co/iMuJApcpMD*
>
> *— Police nationale (@PoliceNationale) January 27, 2021*

La démarche a atteint son point culminant le 26 janvier, avec des perquisitions et des arrestations en Ukraine. C'est là que se trouvait l'épicentre supposé de ce *botnet* au sujet duquel le CERT-FR avait encore récemment émis une alerte.

La « famille Emotet » avait émergé en 2014. Elle comprend plusieurs variantes du *trojan* bancaire Feodo, lui-même proche parent de Dridex*.

Emotet-TrickBot-Ryuk : une chaîne bien connue

Avec les années, l'attribut « cheval de Troie » est resté. Mais avec des capacités élargies allant du piratage de boîtes mail à la propagation au sein des réseaux infectés.
Emotet est aussi devenu un support de diffusion d'autres *malwares*. Notamment TrickBot, lui-même vecteur de propagation du *ransomware* Ryuk.

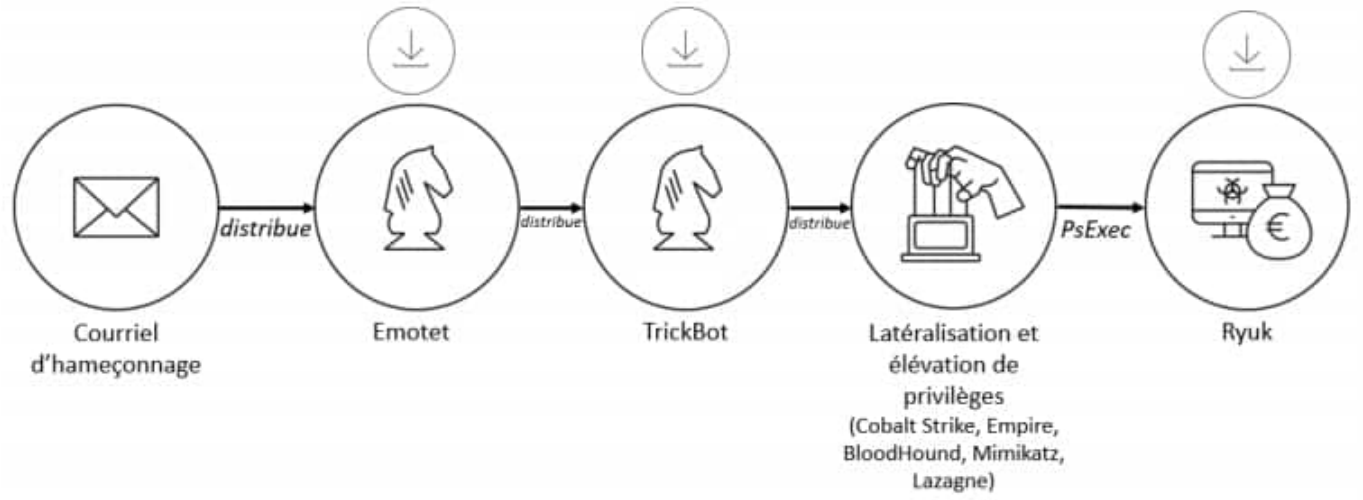

Fig. 2.1 : Déroulé simplifié de la chaîne d'infection Emotet-TrickBot-Ryuk

Les premières version d'Emotet reposaient sur un script mis en pièce jointe d'e-mails imitant des

avis de paiement, des rappels de factures ou encore des notifications de suivi de colis. Les sources d'infection se sont progressivement diversifiées, en particulier à travers l'utilisation de macros dans les logiciels de la suite Office.

Pour ne pas éveiller les soupçons de ses cibles, Emotet s'immisce dans les conversations qu'elles ont eues par le passé. Capable de détecter VM et bacs à sable, il est aussi polymorphe. C'est-à-dire qu'il peut changer sa représentation pour échapper aux détections basées sur les signatures. Le registre Windows et le planificateur de tâches lui permettent d'établir une persistance sur les systèmes infectés.

> *Emotet is known for its penchant for using holiday-themed emails, but this week's campaign also uses what's proven effective for the operators: a wide range of lures in massive volumes of emails, the use of fake replies or forwarded emails, password-protected archive attachments. pic.twitter.com/tgJpvC3hKV*
>
> *— Microsoft Security Intelligence (@MsftSecIntel) December 29, 2020*

2,5 milliards de dollars de dégâts ?

L'architecture d'Emotet se constituait semble-t-il de trois groupements de serveurs (Epoch 1, 2 et 3). L'opération qu'a coordonnée Europol aurait permis d'en mettre environ 700 hors ligne.

L'activité a effectivement bien diminué, si on en croit les statistiques d'abuse.ch. Elle n'a cependant pas tout à fait cessé… en partie du fait des forces de police. À l'initiative de l'Allemagne, celles-ci ont commencé à utiliser l'infrastructure pour diffuser un module aux ordinateurs infectés. Ce module entraînera la désinstallation d'Emotet le 25 mars prochain.

> *All Emotet epochs now are delivering the payload (https://t.co/Tv21VmJm4s) which has the code to remove Emotet on 25 March 2021 12:00. I believe that #Emotet #Killed pic.twitter.com/FnrdqZmQcd*
>
> *— milkream (@milkr3am) January 27, 2021*

D'après les estimations de la NCA, les coûts annuels de maintenance de l'infrastructure ont pu s'élever à 250 000 $. Du côté des forces de l'ordre ukrainiennes, on évalue à 2,5 milliards de dollars le montant global des dégâts.

** Dridex est aujourd'hui considéré comme inactif. On avait cru à son démantèlement en 2015 après une opération concertée du FBI et des autorités britanniques. Mais il avait refait surface, y compris en France.*

Illustration principale © lolloj – shutterstock.com