Recrudescence d'activité Emotet en France

Archived: 2026-04-06 00:11:37 UTC

[mise à jour du 22 septembre 2020]

L'ensemble des échantillons obtenus par l'ANSSI jusqu'à maintenant a permis de comparer ces derniers avec les listes de marqueurs en sources ouvertes référencés dans la section "Moyens de détection relatifs à Emotet".

La fiabilité de ces flux a été assurée et nous vous encourageons à les intégrer dans vos systèmes de détection.

Contrairement aux recommandations indiquées dans la version précédente de cette alerte, il n'est donc plus nécessaire de nous faire parvenir vos échantillons.

[version initiale]

Depuis quelques jours, l'ANSSI constate un ciblage d'entreprises et administrations françaises par le code malveillant Emotet. Il convient d'y apporter une attention particulière car Emotet est désormais utilisé pour déposer d'autres codes malveillants susceptibles d'impacter fortement l'activité des victimes.

Caractéristiques du cheval de Troie Emotet

Observé pour la première fois mi-2014 en tant que cheval de Troie bancaire, Emotet a évolué pour devenir un cheval de Troie modulaire. Ses différents modules actuels lui permettent :

- de récupérer les mots de passe stockés sur un système ainsi que sur plusieurs navigateurs (Internet Explorer, Mozilla Firefox, Google Chrome, Safari, Opera) et boîtes courriel (Microsoft Outlook, Windows Mail, Mozilla Thunderbird, Hotmail, Yahoo! Mail et Gmail) ;
- de dérober la liste de contacts, le contenu et les pièces jointes attachées à des courriels ;
- de se propager au sein du réseau infecté en tirant parti de vulnérabilités SMB ainsi que des mots de passe récupérés.

Le code malveillant est distribué par le botnet éponyme (lui-même composé de trois groupements de serveurs différents Epoch 1, Epoch 2, Epoch 3, opérés par le groupe cybercriminel TA542) au travers de **campagnes massives de courriels d'hameçonnage**, souvent parmi les plus volumineuses répertoriées. Ces courriels d'hameçonnage contiennent généralement des pièces jointes Word ou PDF malveillantes, et plus rarement des URL pointant vers des sites compromis ou vers des documents Word contenant des macros.

Ces campagnes d'attaques touchent tous types de secteurs d'activités à travers le monde.

Emotet : loader de codes malveillants tiers

Depuis 2017, Emotet n'est plus utilisé en tant que cheval de Troie bancaire mais distribue, fréquemment au sein des systèmes d'information qu'il infecte, des codes malveillants opérés par des groupes d'attaquants qui sont

clients de TA542. Par exemple, les chevaux de Troie bancaires Qbot, Trickbot, IcedID, GootKit, BokBot, Dridex et DoppelDridex peuvent être distribués en tant que seconde charge utile, avec une prédominance en 2020 de Qbot et TrickBot.

En outre, ces derniers peuvent télécharger des rançongiciels au sein du système d'information compromis. C'est par exemple le cas de TrickBot auquel il arrive de télécharger les rançongiciels Ryuk ou Conti.

Ainsi, la détection et le traitement au plus tôt d'un évènement de sécurité lié à Emotet peut prévenir de nombreux types d'attaques, dont celles par rançongiciel avant le chiffrement.

Recrudescence des campagnes d'attaque durant le second semestre 2020

Après une absence de cinq mois, Emotet a refait surface en juillet 2020. Depuis, nombre de ses campagnes d'hameçonnage exploitent une technique de détournement des fils de discussion des courriels (*email thread hijacking technique*).

Une fois la boîte courriel d'un employé de l'entité victime (ou la boîte courriel générique de l'entité elle-même) compromise, le code malveillant Emotet exfiltre le contenu de certains de ses courriels. Sur la base de ces derniers, les attaquants produisent des courriels d'hameçonnage prenant la forme d'une réponse à une chaîne de courriels échangés entre l'employé et des partenaires de l'entité pour laquelle il travaille. L'objet légitime du courriel d'hameçonnage est alors précédé d'un ou plusieurs « Re : », et le courriel lui-même contient l'historique d'une discussion, voire même des pièces jointes légitimes.

Ces courriels, d'apparence légitime, sont envoyés à des contacts de la victime, et plus particulièrement aux tierces parties de l'entité (clients et prestataires notamment) ayant participé au fil de discussion originel, afin d'accroître leur crédibilité auprès des destinataires.

Outre cette technique, TA542 construit également des courriels d'hameçonnage sur la base d'informations récupérées lors de la compromission des boîtes courriel, qu'il envoie aux listes de contact exfiltrées, ou usurpent plus simplement l'image d'entités, victimes préalables d'Emotet ou non (sociétés de transport, de télécommunication ou encore institutions financières).

Dans tous les cas, il apparaît que les boîtes courriel compromises ne sont pas utilisées pour envoyer des courriels d'hameçonnage mais que ces derniers sont envoyés depuis l'infrastructure des attaquants sur la base d'**adresses courriel expéditrices souvent typosquattées**.

La France représente une cible des campagnes récentes d'Emotet.

SOLUTION

Moyens de détection relatifs à Emotet

Plusieurs flux existent contenant des indicateurs de compromission actualisés relatifs à Emotet, ce code faisant l'objet de nombreuses investigations dans les secteurs public et privé. Parmi ces flux, https://paste.cryptolaemus.com/ et https://feodotracker.abuse.ch/browse/ représentent des **sources fiables qu'il est recommandé d'intégrer dans ses moyens de détection et de blocage.**

A noter aussi :

- Les chercheurs de Cryptolaemus fournissent notamment des expressions régulières permettant de détecter des liens utilisés dans les courriels malveillants. Ils sont disponibles dans les bulletins quotidiens de l'équipe de chercheurs, dans le paragraphe « Link Regex Report ».

- Des règles de détection YARA d'Emotet ont été produites par ReversingLabs : https://github.com/reversinglabs/reversinglabs-yara-rules/blob/develop/yara/trojan/Win32.Trojan.Emotet.yara.
- Emocheck, un outil créé par le CERT japonais, permet de détecter la présence du trojan Emotet sur une machine Windows. Emotet utilisant un dictionnaire prédéfini pour le nom de ses processus, ce programme vérifie si un programme en cours d'exécution correspond à ce dictionnaire précis. L'outil est disponible en source ouverte : https://github.com/JPCERTCC/EmoCheck.

Recommandations

Sensibiliser les utilisateurs à ne pas activer les macros dans les pièces jointes et à être particulièrement attentifs aux courriels qu'ils reçoivent et réduire l'exécution des macros.

Limiter les accès Internet pour l'ensemble des agents à une liste blanche contrôlée.

Déconnecter les machines compromises du réseau sans en supprimer les données.

De manière générale, une suppression / un nettoyage par l'antivirus n'est pas une garantie suffisante. Seule la réinstallation de la machine permet d'assurer l'effacement de l'implant.
