FL INT.

21/01/2021

SEKOIA THREAT INTELLIGENCE **FLASH REPORT**

EMOTET

OBJECTIFS :
GAIN FINANCIER

STATUT :
En cours

ATTRIBUTION :
MUMMY SPIDER, aka TA542

TTPs (MITRE ATT&CK) :
Phishing: Spearphishing Link (T1566.002)
Phishing: Spearphishing Attachment (T1566.001)
Account Discovery: Email Account (T1087.003)
Archive Collected Data (T1560)
Email Collection: Local Email Collection (T1114.001)
Credentials from Password Stores: Credentials from Web Browsers (T1555.003)
User Execution: Malicious Link (T1204.001)
User Execution: Malicious File (T1204.002)
Valid Accounts: Local Accounts (T1078.003)
Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder (T1547.001)
Brute Force: Password Guessing (T1110.001)
Command and Scripting Interpreter: PowerShell (T1059.001)
Command and Scripting Interpreter: Visual Basic (T1059.005)
Command and Scripting Interpreter: Windows Command Shell (T1059.003)
Create or Modify System Process: Windows Service (T1543.003)
Exfiltration Over C2 Channel (T1041)
Exploitation of Remote Services (T1210)
Obfuscated Files or Information (T1027)
OS Credential Dumping: LSASS Memory (T1003.001)
Process Discovery (T1057)
Process Injection: Dynamic-link Library

Injection (T1055.001)
Scheduled Task/Job: Scheduled Task (T1053.005)
Windows Management Instrumentation (T1047)

SECTEURS AFFECTÉS : **TOUS**

PAYS IMPACTÉS **: MONDE**

Synthèse

Détectées pour la première fois en 2014, les premières souches d'Emotet ont été conçues comme des trojan bancaires, opérant pour cibler les clients des banques dans le monde entier.

Le malware a été créé par Mummy Spider, alias TA542, un groupe cybercriminel à motivation financière. Ce groupe mène généralement ses attaques pendant quelques mois avant de cesser ses activités, pour revenir plus tard avec une nouvelle variante du malware. Les opérations d'Emotet ont redémarrées à la fin du mois de décembre de l'année dernière après avoir été interrompues en octobre et novembre.

Depuis 2016, la nouvelle variante d'Emotet n'agit plus comme un trojan bancaire, mais plutôt comme un ver qui s'auto-propage et un loader qui installe d'autres codes malveillants. Emotet a ainsi été le vecteur d'infection des malware Trickbot, Dridex, IcedID et Qbot en 2020, ces derniers étant responsables de l'installation de rançongiciels tels que Maze, Ryuk et ProLock.

Analyse

Emotet est un malware modulaire dans lequel chaque module sert un objectif spécifique qui permet au malware de :

- collecter les mots de passe stockés sur le système infecté et dans les navigateurs web
- voler la liste de contacts, le sujet, le corps du message et les pièces jointes présentes dans Outlook
- se propager sur d'autres systèmes du réseau infecté par force brute, en utilisant les mots de passe volés ou par exploitation de vulnérabilités

Vecteur d'infection

Emotet utilise des documents Word (.doc) compromis avec des macros VBA comme vecteur d'infection. Ces documents sont diffusés via des emails contenant des pièces jointes ou des liens malveillants. Une fois ouverts, ils lancent leur charge utile. Plus précisément, Emotet a recours à une technique appelée "thread hijacking" qui consiste à répondre à une chaîne de courriels (en utilisant une identité usurpée) en y joignant le document piégé. Dans sa version la plus récente, les documents piégés sont envoyés dans des archives protégées par un mot de passe (par exemple, des fichiers Zip) pour contourner les passerelles de sécurité et les antivirus.

Dans les documents malveillants les plus récents, la macro VBA exécute un script Powershell soit directement via WMI, soit indirectement via WMI qui invoque ensuite cmd.exe. Le code Powershell exécute également msg.exe en premier lieu pour afficher un faux message "Word experienced an error trying to open the file." avant de contacter un site web compromis.

Communications C2

Emotet est une menace connue pour utiliser des centaines de serveurs de commande et de contrôle (C2). L'infrastructure C2 est divisée en trois botnets distincts appelés Epoch 1, Epoch 2 et Epoch 3 qui sont identifiables par la clé RSA utilisée pour chiffrer le trafic réseau. Cette clé RSA change chaque mois. Chaque échantillon d'Emotet intègre en moyenne une quarantaine de serveurs C2 suivant le format IP:Port. Les ports les plus fréquemment utilisés sont 80, 8080 et 443.

L'infrastructure du botnet C2 est également très hiérarchisée. Pour chaque Epoch, une souche de malware communique directement avec un serveur Tier 1 ou avec un "Bot", qui se trouve être un système compromis utilisé comme proxy. Ces Bot ne se chargent pas de répondre au malware, mais agissent plutôt comme un proxy en transmettant la communication à un serveur Tier 1. Contrairement aux Bots, les serveurs Tier 1 sont généralement des sites web compromis qui transmettent ensuite la communication C2 à un serveur Tier 2. Il y a de fortes chances que le serveur C2 réponde avec un statut "404 : page non trouvée", même si le corps de réponse contient les réponses chiffrées.

Persistance

Actuellement, Emotet établit la persistance en ajoutant l'exécutable à la clé de registre : HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run.
D'autres techniques ont également été utilisées dans le passé :

- Planificateur de tâches
- Service
- Dossier de démarrage

Actions

Emotet exfiltre les emails et les informations de contact stockés dans Outlook pour les utiliser ensuite dans le but de se propager davantage. Emotet vole les mots de passe stockés sur l'ordinateur infecté et les navigateurs, qu'il peut ensuite utiliser pour tenter de se propager latéralement sur d'autres ordinateurs du réseau, via les partages réseaux ou en réalisant des attaques par force brute.

Emotet peut également vendre l'accès à un ordinateur infecté à d'autres acteurs de la menace et y déposer leur backdoor. Les opérateurs de Trickbot, Qakbot, Dridex et IcedID sont des clients réguliers de Mummy Spider. Ces clients peuvent ensuite essayer de compromettre l'Active Directory dans le but de lancer une attaque par rançongiciel.

Toute infection d'Emotet doit être considérée comme une menace sérieuse.

Afin d'empêcher une infection, vous pouvez désactiver le déclenchement des macro pour les documents de MS Office. Il convient également de former régulièrement les utilisateurs à la détection d'e-mails malveillants. Vous pouvez également restreindre l'exécution des scripts Powershell pour n'autoriser que les scripts signés.

Afin d'identifier les ordinateurs infectés, nous vous recommandons d'utiliser EmoCheck, un outil créé par le CERT japonais, permettant de vérifier si un ordinateur est infecté par Emotet, ou bien vous pouvez utiliser les indicateurs de compromission présents dans SEKOIA.IO ou d'autres dépôts publics tels que :

- Feodo Tracker
- URLHaus
- Cryptolaemus

Vous pouvez également surveiller les processus Powershell invoqués directement par WMI ou indirectement par cmd.exe, lui-même invoqué par WMI.

La surveillance des modifications suspectes dans les clés de registre qui contrôlent le démarrage automatique des programmes, dans les dossiers de démarrage, dans le planificateur de tâches et dans l'exécution de services peut permettre de détecter l'installation d'Emotet.

Si vous détectez une infection, vous devriez examiner l'étendue de la compromission et vérifier si d'autres codes malveillants ont été téléchargés sur la machine infectée. Si vous réagissez dès le début de l'événement, vous devriez isoler l'ordinateur infecté du réseau afin d'éviter une propagation latérale. Si vous réagissez quelques jours après l'infection, vous devriez éviter de couper l'hôte compromis du réseau avant qu'une enquête forensique complète ne soit effectuée, car cela pourrait déclencher le chiffrement par un rançongiciel si de tels adversaires se trouvaient sur le réseau.

Pour éviter toute latéralisation, appliquez une politique de mots de passe forts. Pensez également à utiliser des postes de travail dédiés pour l'administration du réseau et du système.

La meilleure solution de rétablissement consiste à réinstaller le système d'exploitation sur le ou les ordinateurs compromis et à réinitialiser toutes les autorisations d'accès liées au(x) systèmes(s) compromis.

Enfin, une infection par Emotet doit être considérée comme une perte de confidentialité. Recherchez dans les courriels compromis des informations sensibles telles que des documents confidentiels, des informations sur les clients, des informations sur l'infrastructure du réseau, des codes d'authentification pour des applications, etc. Signaler le vol de données personnelles à l'autorité compétente.

IOCs & détails techniques

La liste des IOCs est disponible sur notre dépôt GitHub.

Tous les indicateurs sont liés au botnet Epoch2 d'Emotet.

CONFIANCE

Elevée

RÉFÉRENCES

- [ANSSI] Le Malware-as-a-Service EMOTET
- [JP-CERT] Alert Regarding Emotet Malware Infection
- [JP-CERT] EmoCheck
- [CISA] Emotet Malware
- [AnyRun] Emotet
- [Deutsche Telekom] Dissecting Emotet – Part 1
- FLINT 2020-163 - Beware of Emotet resurgence targeting France, Japan and New Zealand