Juin 2017

McAfee
Together is power.

Rapport sur le paysage des menaces

McAfee Labs

Tendances et techniques de contournement des logiciels malveillants

Les auteurs de logiciels malveillants disposent d'un très large choix de techniques de contournement, toujours plus performantes.

Historique des techniques de contournement

1980
Virus Cascade
Premier virus à utiliser le chiffrement pour brouiller son contenu.

1990
Virus de la famille Chameleon
Premiers virus polymorphes.

1998
Logiciels malveillants métamorphes
Regswap utilise le métamorphisme pour exécuter les mêmes fonctions via des registres différents.

Années 1990
Programmes de compression (packers)
Les packers de chiffrement ou de compression deviennent populaires en raison de la taille réduite des disques et mémoires RAM.

De 1999 à 2003
Rootkits
En 1999, apparition du premier rootkit Windows, NTRootkit, suivi par HackerDefender en 2003.

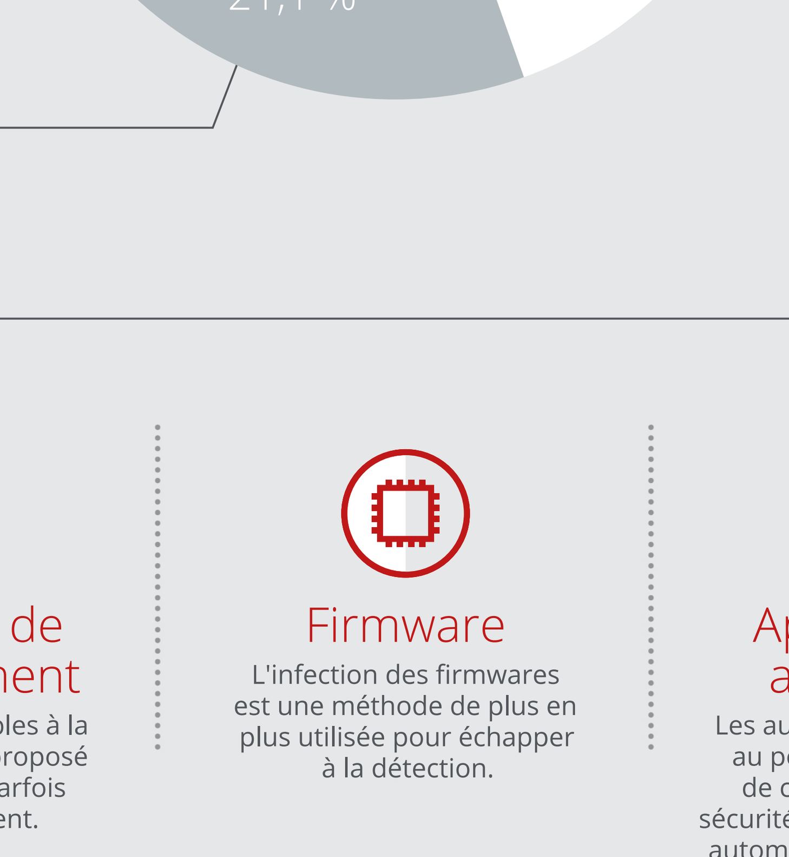
2008
Algorithmes de génération de domaines (DGA)
Le ver Conficker utilise un algorithme de ce type pour contourner la détection réseau.

2011
Marché d'outils prêts à l'emploi
Silkroad est le premier marché clandestin du Web (darknet) à vendre des produits et services de contournement pour logiciels malveillants.

De 2015 à 2017
Dridex et Locky
Première dissimulation à grande échelle, utilisation de PowerShell et contournement de sandbox.

De 2015 à 2017
Logiciels malveillants ciblant les firmwares
Les fuites dont ont été victimes Equation Group et Hacking Team ont révélé l'utilisation de logiciels malveillants ciblant les firmwares pour échapper à la détection.

Techniques de contournement utilisées par les logiciels malveillants



Techniques de contournement
Celles-ci sont disponibles à la vente. Leur code est proposé « prêt à l'emploi », parfois même gratuitement.

Firmware
L'infection des firmwares est une méthode de plus en plus utilisée pour échapper à la détection.

Apprentissage automatique
Les auteurs d'attaques mettent au point des techniques afin de contourner les outils de sécurité basés sur l'apprentissage automatique (machine learning).

La stéganographie au service des menaces

La stéganographie est l'art de la dissimulation d'informations secrètes.

Fonctionnement de la stéganographie numérique

1. Fichier de couverture / message caché
2. Algorithme d'insertion
3. Stégo-fichier
4. Support de communication
5. Stégo fichier
6. Algorithme d'extraction
7. Message caché

Utilisation de la stéganographie numérique par les logiciels malveillants

2010	2012	2014	2016

- Duqu, Shady RAT, Alureon (rootkit)
- Zbot, Lurk, ZeusVM, MiniDuke, CosmicDuke
- Vawtrak, Stegoloader, Sundown, AdGholas, Magento CC, DNSChanger

Message secret
La stéganographie sert à cacher un message secret dans un autre message anodin en apparence.

440 av. J.-C.
La stéganographie est utilisée sous différentes formes au moins depuis 440 av. J.-C.

2011
Le premier usage de la stéganographie numérique date de 2011 et est attribué à Duqu.

Réseau
La stéganographie numérique appliquée au réseau est forme la plus récente appliquée par des logiciels malveillants.

Fareit, un voleur de mots de passe de plus en plus dangereux

Les voleurs de mots de passe sont utilisés dans les premières phases de presque toutes les principales menaces persistantes avancées (APT). Fareit a probablement été utilisé dans la compromission subie par le parti démocrate américain en 2016.

Évolution de Fareit

2011
- Première variante de Fareit contenant des fonctions de vol d'identifiants et DDoS.

2012
- Le kit d'exploit Blackhole (BHEK) propage Fareit avec Zeus et FakeAV.

2013
- Fareit télécharge Medfos et Nymaim et se propage via une campagne de spam.
- Fareit se lance dans le minage de bitcoins.

2014
- Fuite du code source de Pony Loader 1.9.
- Pony Loader 2.0 est capable de dérober des portefeuilles de bitcoins.
- Un ransomware qui verrouille l'écran du système infecté utilise Fareit pour le vol d'identifiants.

2015
- Fuite du code source de Pony Loader 2.0.
- Fareit se propage au moyen d'attaques par empoisonnement du cache DNS.
- Attaque du parti démocrate américain à l'aide d'Onion Duke.
- Détection de l'utilisation du module de vol d'identifiants de Fareit en association avec Stegoloader

2016
- Fareit se propage à l'aide de W97, PowerShell, JavaScript et MHT.
- Implication de Fareit dans l'opération Grizzly Steppe.

2017
- Plusieurs variantes personnalisées de Pony Loader disponibles, jusqu'à la version 2.2.

5 599
Fareit a été détecté pour la première fois en 2011. 5 599 incidents subis par des clients de McAfee l'an denier sont imputables à Fareit.

Fareit peut effectuer de nombreuses actions :
- Voler des mots de passe
- Télécharger et exécuter du code malveillant arbitraire
- Mener des attaques par DDoS
- Voler des portefeuilles de cryptomonnaie
- Dérober des informations d'identification FTP

Statistiques sur les menaces

Au 1er trimestre 2017, 244 nouvelles menaces ont été détectées par minute, soit plus de 4 par seconde.

Incidents
Nous avons recensé 301 incidents de sécurité révélés publiquement au 1er trimestre 2017, soit une augmentation de 53 % par rapport au 4e trimestre 2016. Les secteurs public, de la santé et de l'enseignement ont concentré plus de 50 % de leur nombre total. Et 78 % de ces incidents ont eu lieu sur le continent américain.

Logiciels malveillants (malwares) — 22 %
Le 1er trimestre a connu une reprise du nombre de nouveaux échantillons de malwares, qui est passé à 32 millions. **On dénombre au total 670 millions d'échantillons, soit une hausse de 22 % au cours des 4 derniers trimestres.**

Logiciels malveillants sur Mac OS — 53 %
Au cours des 3 derniers trimestres, la profusion de logiciels publicitaires est venue doper le taux de nouveaux malwares sur Mac OS. Même s'il reste faible en comparaison aux menaces Windows, **le nombre total d'échantillons malveillants sur Mac OS a progressé de 53 % au 1er trimestre**.

Logiciels malveillants sur mobiles — 79 %
En ce qui concerne cette catégorie, les signalements en provenance d'Asie ont doublé au 1er trimestre, entraînant une hausse de 57 % du taux d'infection à l'échelle mondiale. **Le nombre total de malwares sur mobiles a progressé de 79 % au cours des 4 derniers trimestres, pour atteindre 16,7 millions d'échantillons.**

Logiciels malveillants de macro — 66 000
Le nombre de nouvelles détections a décliné par rapport à la moyenne sur 3 ans. **66 000 nouveaux échantillons de malwares de macro ont été recensés au 1er trimestre.**

Logiciels de demande de rançon (ransomware) — 59 %
Les nouveaux échantillons de ransomwares ont augmenté à nouveau au 1er trimestre, principalement en raison des attaques d'appareils Android menées à l'aide de Congur. **On dénombre au total 9,6 millions d'échantillons, en progression de 59 % au cours des 4 derniers trimestres.**

McAfee Global Threat Intelligence

McAfee GTI a reçu en moyenne 55 milliards de requêtes par jour au 1er trimestre.

McAfee GTI

95 millions
Les protections de McAfee GTI contre les URL à risque modéré ont **diminué, passant de 107 millions par jour au 4e trimestre à 95 millions au 1er** grâce à l'amélioration de leur précision.

56 millions
Les protections de McAfee GTI contre les programmes potentiellement indésirables ont **augmenté, passant de 37 millions par jour au 4e trimestre à 56 millions au 1er**.

34 millions
Les protections de McAfee GTI contre les fichiers malveillants ont **diminué, passant de 71 millions par jour au 4e trimestre à 34 millions au 1er**, grâce à une détection plus précoce et à une cyberveille locale plus performante.

59 millions
Les protections de McAfee GTI contre les adresses IP à risque ont elles aussi **connu une baisse, passant de 88 millions par jour au 4e trimestre à 59 millions au 1er**, grâce à une détection plus rapide.

Rapport sur le paysage des menaces de McAfee Labs — Juin 2017

Pour obtenir le rapport complet : www.mcafee.com/June2017ThreatsReport.

McAfee
Together is power.