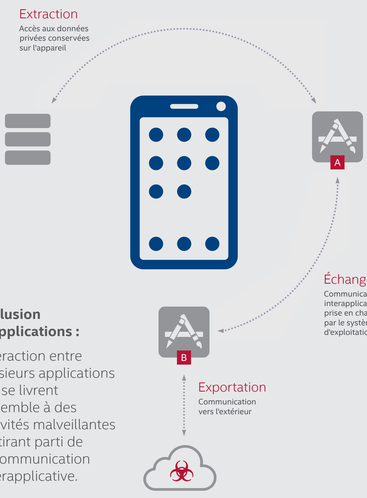
Juin 2016

Rapport sur le paysage des menaces

McAfee Labs

Une complicité dangereuse : enquête sur la collusion entre applications mobiles

Des applications mobiles apparemment inoffensives peuvent agir de connivence pour exécuter des attaques.



Collusion d'applications :

Interaction entre plusieurs applications qui se livrent ensemble à des activités malveillantes en tirant parti de la communication interapplicative.

5 000 packages d'installation

Un kit de développement logiciel (SDK) Android comprenant des fonctions de communication interapplicative est en circulation depuis 2015. Il est inclus dans plus de 5 000 packages d'installation comprenant 21 applications mobiles.

Le réveil de Pinkslipbot

Une nouvelle souche du cheval de Troie Pinkslipbot propose des fonctions de chiffrement multiniveau et de contournement des analyses.

Mode opératoire de Pinkslipbot

Déplacement latéral
Déplacement latéral vers d'autres systèmes d'un réseau approuvé

Enregistrement et exfiltration
Enregistrement et exfiltration des frappes au clavier, des identifiants de connexion et des certificats

Contournement de la détection
Détection des machines virtuelles ou des fichiers de débogage et interruption de son exécution

Vol de clés
Exportation des clés privées du magasin de certificats

Désactivation de la protection
Désactivation des produits d'analyse de la réputation web

Déc. 2015 — 1er trim. 2016

4 200 détections depuis décembre

McAfee Labs a détecté plus de 4 200 fichiers binaires uniques de Pinkslipbot entre décembre 2015 et la fin du premier trimestre 2016.

2007 — 1er trim. 2016

165 000 détections depuis 2007

Plus de 165 000 fichiers binaires uniques de Pinkslipbot ont été identifiés depuis son apparition en 2007.

Statistiques sur les menaces

On enregistre 305 nouvelles menaces par minute, soit plus de 5 par seconde.

Logiciels de demande de rançon (ransomware)

Les nouveaux logiciels de demande de rançon ont progressé de 24 % ce trimestre en raison de l'arrivée constante de nouveaux venus peu qualifiés dans la communauté cybercriminelle du ransomware.

Logiciels malveillants de macro

Les logiciels malveillants de macro poursuivent leur progression entamée en 2015 avec une augmentation trimestrielle de nouveaux échantillons de l'ordre de 42 %.

Logiciels malveillants sur mobiles

Les nouveaux logiciels malveillants sur mobiles ont enregistré une hausse de 17 % au cours du premier trimestre 2016 par rapport au précédent. Le nombre total de nouveaux logiciels malveillants sur mobiles a progressé de 23 % par trimestre et de 113 % pour les quatre derniers trimestres.

Logiciels malveillants pour Mac OS

Les logiciels malveillants pour Mac OS ont connu une belle envolée au 1er trimestre, essentiellement en raison de l'augmentation du logiciel publicitaire VSearch. Même si le volume d'échantillons Mac OS reste faible dans l'absolu, leur nombre total a progressé de 68 % par rapport au dernier trimestre et de 559 % sur les quatre précédents.

McAfee Global Threat Intelligence

McAfee GTI reçoit, en moyenne, 49,9 milliards de requêtes par jour.

4,3 millions

Par heure, plus de 4,3 millions d'incitations à la connexion à des URL dangereuses (présentes dans des e-mails, des résultats de recherche par navigateur, etc.)

5,8 millions

Par heure, plus de 5,8 millions de fichiers infectés identifiés dans les réseaux des clients

1,8 million

Par heure, 1,8 million de tentatives d'installation ou de démarrage de programmes potentiellement indésirables

500 000

Par heure, 500 000 tentatives de connexion réseau de nos clients depuis ou vers des adresses IP dangereuses

Rapport de McAfee Labs sur le paysage des menaces — Juin 2016

Pour obtenir le rapport complet : www.mcafee.com/June2016ThreatsReport.

intel Security

McAfee fait désormais partie d'Intel Security.