Décembre 2016

Rapport sur le paysage des menaces

McAfee Labs

Le centre d'opérations de sécurité (SOC)

État des lieux et projets futurs du centre SOC

Près de 9 entreprises sur 10 possèdent un centre SOC.

91 %
des grandes entreprises possèdent un centre SOC.

84 %
des moyennes entreprises possèdent un centre SOC.

74 %
s'efforcent de mettre en place des opérations de sécurité proactives et optimisées, mais 26 % continuent de fonctionner en mode réactif et adoptent une approche ponctuelle en matière d'opérations de sécurité, de traque de menaces et de réponse aux incidents.

64 %
reçoivent une forme quelconque d'assistance de la part de leur fournisseur de services de sécurité managés (MSSP) pour leurs opérations de sécurité.

69 %
déclarent utiliser aujourd'hui une solution SIEM. 45 % des entreprises sans solution SIEM comptent déployer cette fonctionnalité dans les 12 à 18 prochains mois.

93 %
des entreprises sont incapables de catégoriser toutes les menaces pertinentes, et la plupart sont submergées par les alertes.

65 %
des entreprises disposant d'un centre SOC ont mis en place des équipes formelles de prévention des menaces.

Domaines prioritaires de développement pour les entreprises

Capacité d'intervention
en cas d'attaques avérées, y compris la coordination, la neutralisation, l'élimination et la prévention de nouvelles attaques du même type

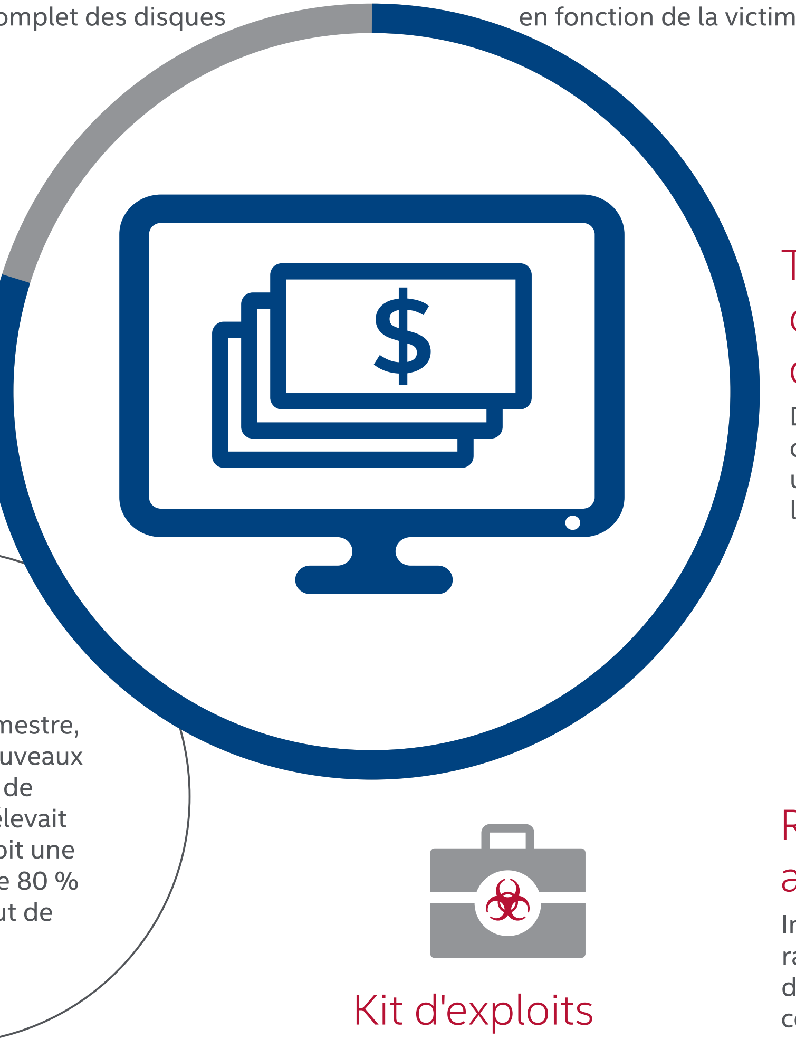
Capacité de détection
des signes d'attaques potentielles, notamment la génération d'alertes et d'événements pertinents, le tri et la priorisation

Capacité d'investigation
des attaques potentielles, notamment l'évaluation de l'ampleur et de l'impact d'une attaque

L'année de tous les ransomwares

L'année 2016 est caractérisée par une forte hausse des attaques de ransomware et quelques avancées techniques majeures dans ce domaine. Le secteur de la sécurité n'a pas manqué de riposter.

Les avancées techniques majeures des ransomwares en 2016 :



Chiffrement des disques
Chiffrement partiel ou complet des disques

Demandes de rançon variables
Adaptation des montants en fonction de la victime

Chiffrement de sites web
Chiffrement des sites web utilisés par des applications légitimes

Techniques de contournement de sandbox
Détection et contournement des solutions sandbox utilisées pour tester le code suspect

80 %
À la fin du 3e trimestre, le nombre de nouveaux échantillons de ransomware s'élevait à 3,9 millions, soit une augmentation de 80 % depuis le début de l'année.

Kit d'exploits
Kits d'exploits plus sophistiqués pour la distribution des ransomware

Ransomware-as-a-Service (RaaS)
Infrastructure et ransomware mis à disposition d'attaquants, contre paiement, par des fournisseurs de service

La riposte du secteur de la sécurité

Collaboration

NO MORE RANSOM!

No More Ransom!
Fondée en juillet, cette initiative a pour but d'offrir des conseils de prévention, une assistance lors des enquêtes ainsi que des outils de déchiffrement.

Opérations des forces de l'ordre

WildFire
Démantèlement du ransomware

Shade
Démantèlement du ransomware

Logiciels légitimes infectés par des chevaux de Troie

Les chevaux de Troie infectent le code légitime et s'y dissimulent dans le but de passer inaperçus le plus longtemps possible pour maximiser les gains.

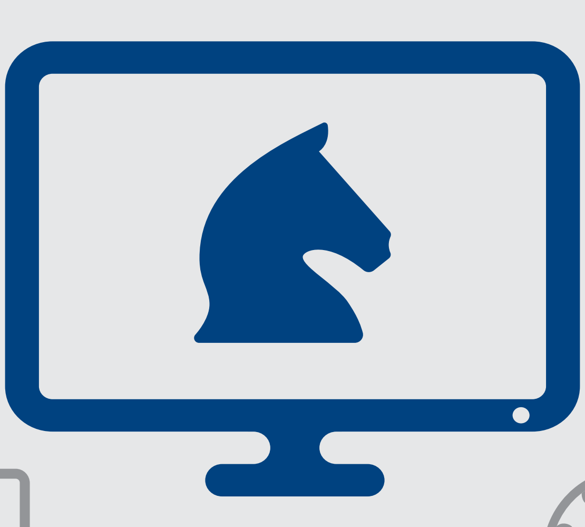
Avantages des chevaux de Troie

Apparence de légitimité
La reconnaissance des marques usurpées donne de la légitimité au code contenant la charge active.

Bonne couverture
L'utilisation de logiciels légitimes offre une excellente couverture lors des analyses de sécurité et des investigations numériques.

Persistance sans limite
L'infection des applications légitimes par des chevaux de Troie offre une persistance sans limite.

Méthodes d'infection des logiciels légitimes par des chevaux de Troie



Modification
de code source ouvert, interprété ou décompilé

Altération
des fichiers exécutables à mesure qu'ils sont téléchargés, par une attaque de type man-in-the-middle

Combinaison
de fichiers sains et infectés à l'aide de binders ou de joiners

Modification des fichiers exécutables
à l'aide de patchers sans perturber le fonctionnement normal de l'application

Infection
du code source maître, surtout dans les bibliothèques redistribuées

700 000

700 000
Au 3e trimestre, plus de 700 000 fichiers binaires infectés par des chevaux de Troie de trois grandes familles Android ont été détectés.

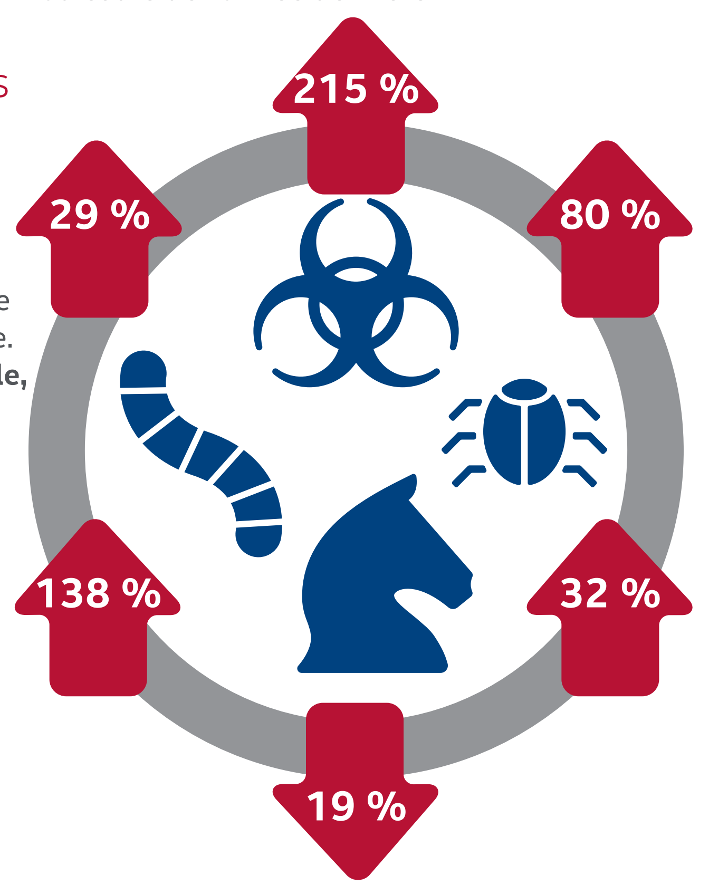
30 000

30 000
Au 3e trimestre, 30 000 fichiers binaires Android ont été infectés par des chevaux de Troie avec deux kits de porte dérobée (backdoor) populaires.

Statistiques sur les menaces

On enregistre 245 nouvelles menaces par minute, soit plus de 4 par seconde.

Logiciels malveillants sur Mac OS
Même s'il reste faible en comparaison aux menaces Windows, le nombre de nouveaux échantillons malveillants sur Mac OS a progressé de 65 % au 3e trimestre. **Le nombre total de logiciels malveillants sur Mac OS a augmenté de 215 % au cours de l'année dernière.**



Logiciels malveillants (malware)
Le nombre de nouveaux échantillons de logiciels malveillants au 3e trimestre s'élève à 32 millions, en baisse de 21 % depuis le 2e trimestre. **Toutefois, dans leur ensemble, les logiciels malveillants ont progressé de 29 % l'année dernière, pour atteindre la barre des 644 millions d'échantillons**.

Logiciels de demande de rançon (ransomware)
Le nombre total d'échantillons de ransomware a augmenté de 18 % au cours du 3e trimestre, soit une progression de **80 % pour les 3 premiers trimestres de l'année 2016**.

Logiciels malveillants sur mobiles
Le nombre de nouveaux échantillons de logiciels malveillants sur mobiles découverts au 3e trimestre constitue lui aussi un record, avec plus de 2 millions. **Le nombre total de logiciels malveillants sur mobiles a augmenté de 138 % au cours de l'année dernière**.

Logiciels malveillants de macro
Les nouveaux logiciels malveillants de macro continuent d'augmenter à un rythme rapide. **Le nombre total de logiciels malveillants de macro a augmenté de 32 % au cours du dernier trimestre**.

Réseaux de robots (botnets) de spam
Les e-mails de spam générés par le réseau de robots Kelihos ont chuté de 97 % au 3e trimestre, mais ceux du réseau Necurs ont progressé de 554 %. **Globalement, les e-mails de spam diffusés par des réseaux de robots ont diminué de 19 % au 3e trimestre**.

McAfee Global Threat Intelligence

44,1 milliards de requêtes reçues par McAfee GTI en moyenne chaque jour

McAfee GTI

57 millions
Les protections de McAfee GTI contre les URL malveillantes **ont diminué et sont passées de 100 millions par jour au 2e trimestre à 57 millions au 3e**.

32 millions
Les protections de McAfee GTI contre les programmes potentiellement indésirables ont connu une légère augmentation entre le 2e et le 3e trimestre. En revanche, elles ont considérablement chuté par rapport à la même époque en 2015. **Leur nombre est passé de 175 millions par jour au 3e trimestre 2015, à 32 millions par jour au 3e trimestre 2016**.

150 millions
Les protections de McAfee GTI contre les fichiers malveillants **ont augmenté, passant de 104 millions par jour au 2e trimestre à 150 millions ce trimestre**. L'année dernière, à la même époque, elles avaient baissé.

27 millions
Les protections de McAfee GTI contre les adresses IP dangereuses **ont légèrement diminué et sont passées de 29 millions par jour au 2e trimestre à 27 millions au 3e**. Cette baisse est bien plus faible que celle observée entre le 2e trimestre et le 3e trimestre 2015.

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

Pour obtenir le rapport complet : www.mcafee.com/December2016ThreatsReport.

1941_1016_info_threats-report-dec-2016