



Threat-Report

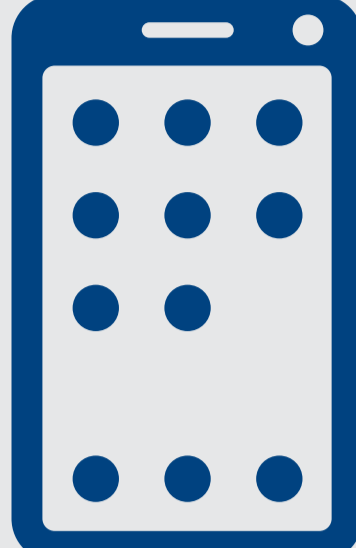
McAfee Labs

Gefährliche Komplizen: Konspirative Mobilgeräte-Apps

Scheinbar harmlose Mobilgeräte-Apps können mit konspirativem Vorgehen Angriffe durchführen.

Extrahieren

Zugriff auf lokal gespeicherte private Daten



Austauschen

Vom Betriebssystem unterstützte Kommunikation zwischen Mobilgeräte-Apps

Konspirative Apps:

Zwei oder mehr Apps können gemeinsam schädliche Aktivitäten durchführen, indem sie gemeinschaftlich vorgehen und dazu von App zu App kommunizieren.



Exportieren

Kommunikation aus dem Mobilgerät heraus



5.000 Installationspakete

Ein Android-SDK, das konspiratives Verhalten unterstützt und mehr als 5.000 Installationspakete für 21 Mobilgeräte-Apps umfasst, ist seit 2015 im Umlauf.

Pinkslipbot: Zurück aus dem Winterschlaf

Der Trojaner Pinkslipbot umfasst jetzt auch Analyseschutz und mehrstufige Verschlüsselung.

Möglichkeiten von Pinkslipbot



Bewegung innerhalb des Netzwerks

Kann sich innerhalb eines vertrauenswürdigen Netzwerks auf andere Systeme verbreiten.



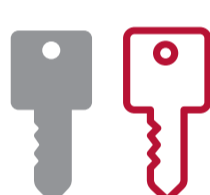
Schutz vor Erkennung

Erkennt virtuelle Maschinen oder Debug-Dateien und beendet sich selbst.



Erfassung und Exfiltration

Erfasst und exfiltriert Tastatureingaben, Anmeldeinformationen und Zertifikate.



Schlüsseldiebstahl

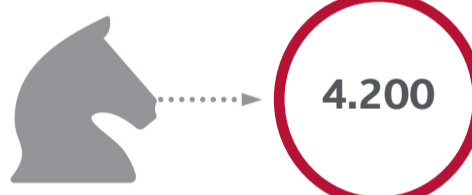
Exportiert private Schlüssel aus dem Zertifikatspeicher.



Schutzdeaktivierung

Deaktiviert Sicherheitsprodukte, die die Web-Reputation auswerten.

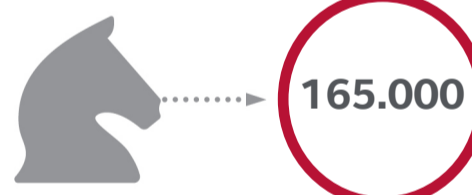
Dez. 2015 1. Quartal 2016



4.200 seit Dezember

McAfee Labs erfasste von Dezember 2015 bis Ende des 1. Quartals 2016 mehr als 4.200 individuelle Pinkslipbot-Binärdateien.

2007 1. Quartal 2016



165.000 seit 2007

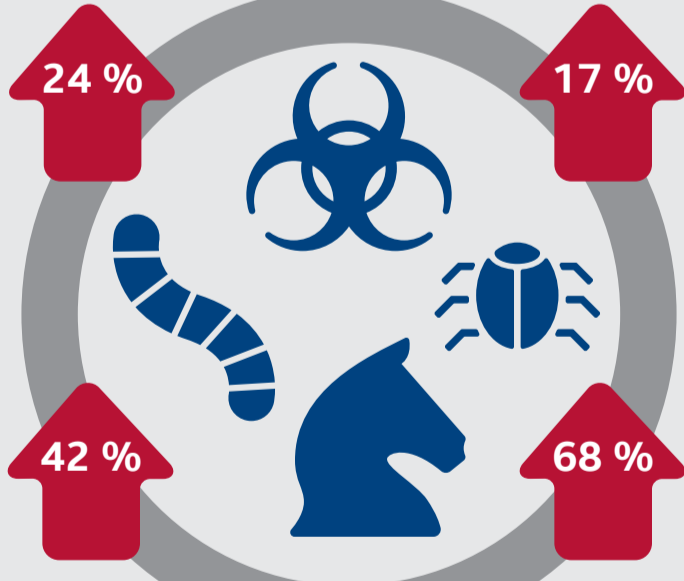
Seit dem ersten Auftreten im Jahr 2007 wurden mehr als 165.000 individuelle Pinkslipbot-Binärdateien erfasst.

Statistische Bedrohungsdaten

Pro Minute werden 305 neue Bedrohungen erkannt. Das entspricht mehr als 5 pro Sekunde.

Ransomware

Die Ransomware-Zahlen stiegen in diesem Quartal um 24 %, da die Ransomware-Community kontinuierlich durch relativ unerfahrene Kriminelle wächst.



Mobilgeräte-Malware

Im 1. Quartal 2016 stieg die Zahl neuer Mobilgeräte-Malware-Varianten im Vergleich zum vorherigen Quartal um 17 %. Die Gesamtzahl der Mobilgeräte-Malware-Varianten stieg im letzten Quartal um 23 % und im Verlauf der letzten vier Quartale um 113 %.

Makro-Malware

Makro-Malware setzt das Wachstum fort, das 2015 begann und im letzten Quartal 42 % betrug.

Mac OS-Malware

Mac OS-Malware nahm im 1. Quartal schnell zu, vor allem aufgrund des Anstiegs bei der Adware VSearch. Obwohl die Gesamtzahl der Mac OS-Varianten weiterhin niedrig ist, stieg sie im letzten Quartal um 68 % und im Verlauf der letzten vier Quartale um 559 %.

McAfee Global Threat Intelligence

McAfee GTI erhielt täglich durchschnittlich 49,9 Milliarden Anfragen.



4,3 Millionen Pro Stunde gab es mehr als 4,3 Millionen Versuche, unsere Kunden zum Aufrufen von riskanten URLs zu verleiten (per E-Mail, Browser-Suchen usw.).



1,8 Millionen Pro Stunde versuchten weitere 1,8 Millionen potenziell unerwünschte Programme, sich zu installieren oder zu starten.



5,8 Millionen Pro Stunde wurden in den Netzwerken unserer Kunden mehr als 5,8 Millionen infizierte Dateien entdeckt.



500.000 Pro Stunde versuchten unsere Kunden 500.000 Millionen Mal, sich mit riskanten IP-Adressen zu verbinden, oder solche Adressen versuchten, eine Verbindung mit den Kundennetzwerken herzustellen.



McAfee GTI

McAfee Labs Threat-Report: Juni 2016

Den vollständigen Report finden Sie unter www.mcafee.com/June2016ThreatsReport.

