



Threats Report

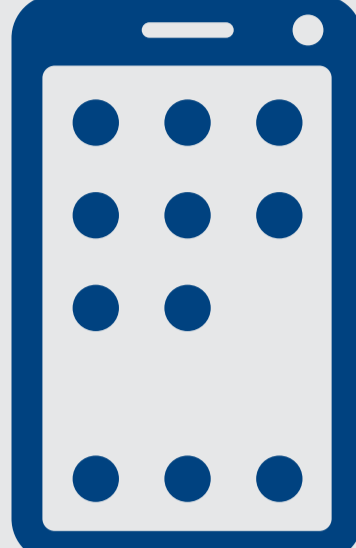
McAfee Labs

Partners in crime: investigating mobile app collusion

Seemingly benign mobile apps can collude to execute attacks.

Extract

Access to locally stored private data.



Exchange

OS-supported interapp communication

Colluding apps:

Two or more apps that together can carry out harmful activity using interapp communications in a collaborative fashion.



Export

Communication outside mobile device



5,000 installation packages

A collusion-capable Android SDK, included in more than 5,000 installation packages representing 21 mobile apps, has been in the wild since 2015.

Pinkslipbot: back from its slumber

A new strain of the Pinkslipbot Trojan features antianalysis and multilayered encryption.

Pinkslipbot attempts to



Move laterally

Move laterally to other systems within a trusted network.



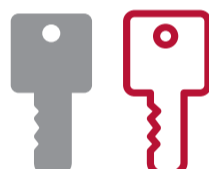
Log and exfiltrate

Log and exfiltrate keystrokes, login credentials, and certificates.



Avoid detection

Detect virtual machines or debug files, and quit.



Steal keys

Export private keys from the certificate store.



Disable protection

Disable web-reputation security products.

Dec 2015

Q1 2016



4,200 since December

McAfee Labs detected more than 4,200 unique Pinkslipbot binaries from December 2015 through the end of Q1 2016.

2007

Q1 2016



165,000 since 2007

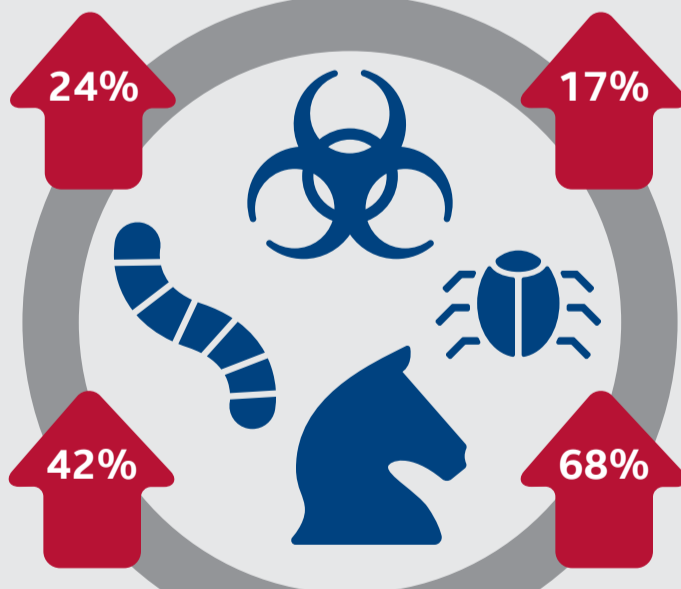
More than 165,000 unique Pinkslipbot binaries have been detected since it emerged in 2007.

Threat Statistics

There are 305 new threats every minute, or more than 5 every second.

Ransomware

New ransomware rose 24% this quarter due to relatively low-skilled criminals into the ransomware cybercrime community.



Mobile malware

New mobile malware grew 17% quarter over quarter in Q1 2016. Total mobile malware grew 23% quarter over quarter and 113% over the last four quarters.

Macro malware

Macro malware continues on the growth trajectory begun in 2015 with a 42% quarter over quarter increase in new macro malware samples.

Mac OS malware

Mac OS malware grew quickly in Q1, primarily due to an increase in VSearch adware. Although the absolute number of Mac OS samples is still low, the total number has increased 68% quarter over quarter and 559% over the last four quarters.

McAfee Global Threat Intelligence

McAfee GTI received on average 49.9 billion queries per day.



4.3 million

Every hour, more than 4.3 million attempts were made to entice our customers into connecting to risky URLs (via emails, browser searches, etc.).



1.8 million

An additional 1.8 million Potentially Unwanted Programs attempted installation or launch every hour.



5.8 million

Every hour, more than 5.8 million infected files were exposed to our customers' networks.



500,000

were made by our customers to connect to risky IP addresses or those addresses attempted to connect to customers' networks.

McAfee Labs Threats Report: June 2016

Visit www.mcafee.com/June2016ThreatsReport for the full report.

