Threats Report
McAfee Labs

Mobile Users Exposed

SSL vulnerabilities open the door to cybercriminals by enabling man-in-the-middle attacks without users' knowledge.

Victims
have no idea their mobile apps have been exploited.

The Man-in-the-Middle
can manipulate sessions in multiple ways.

Trusted Websites
have no idea cybercriminals are intercepting information passing between the mobile apps and their websites.

Eighteen of the 25 most downloaded apps from a CERT list of vulnerable apps[1] that send credentials via insecure connections are still vulnerable to man-in-the-middle attacks.
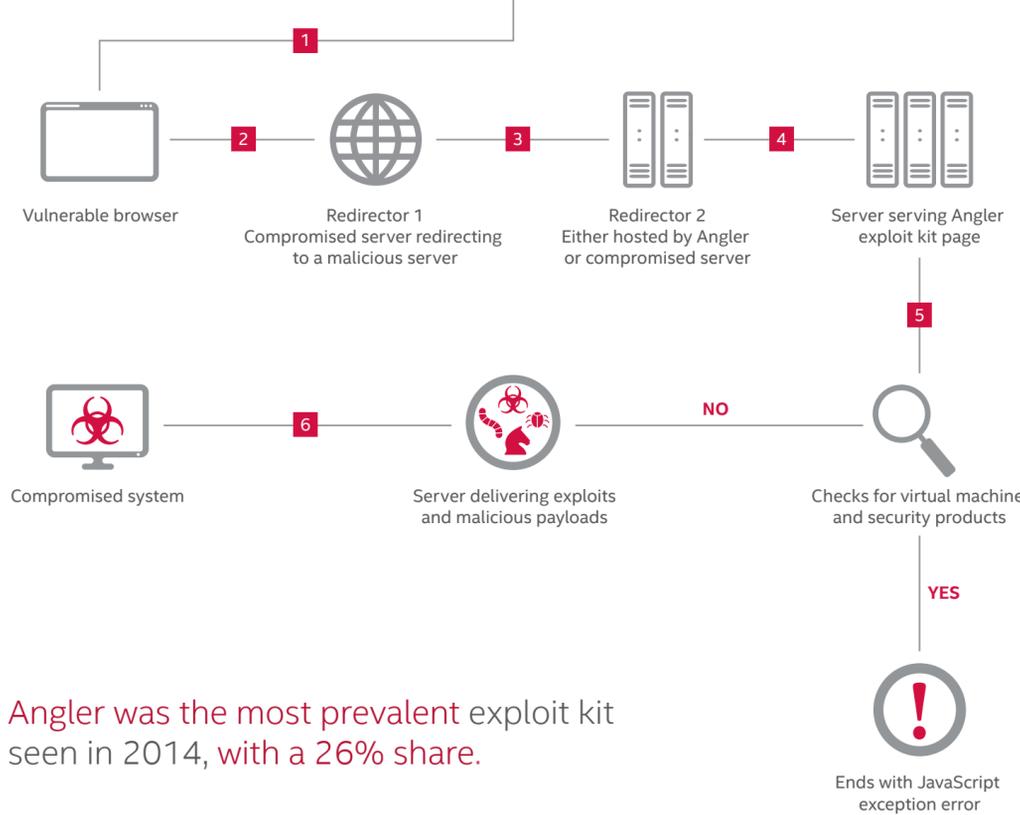
Angler Exploit Kit

Angler has taken over from Blacole as one of the most popular and powerful exploit kits.

Angler employs
a variety of evasion techniques to remain undetected by virtual machines, sandboxes, and security software.
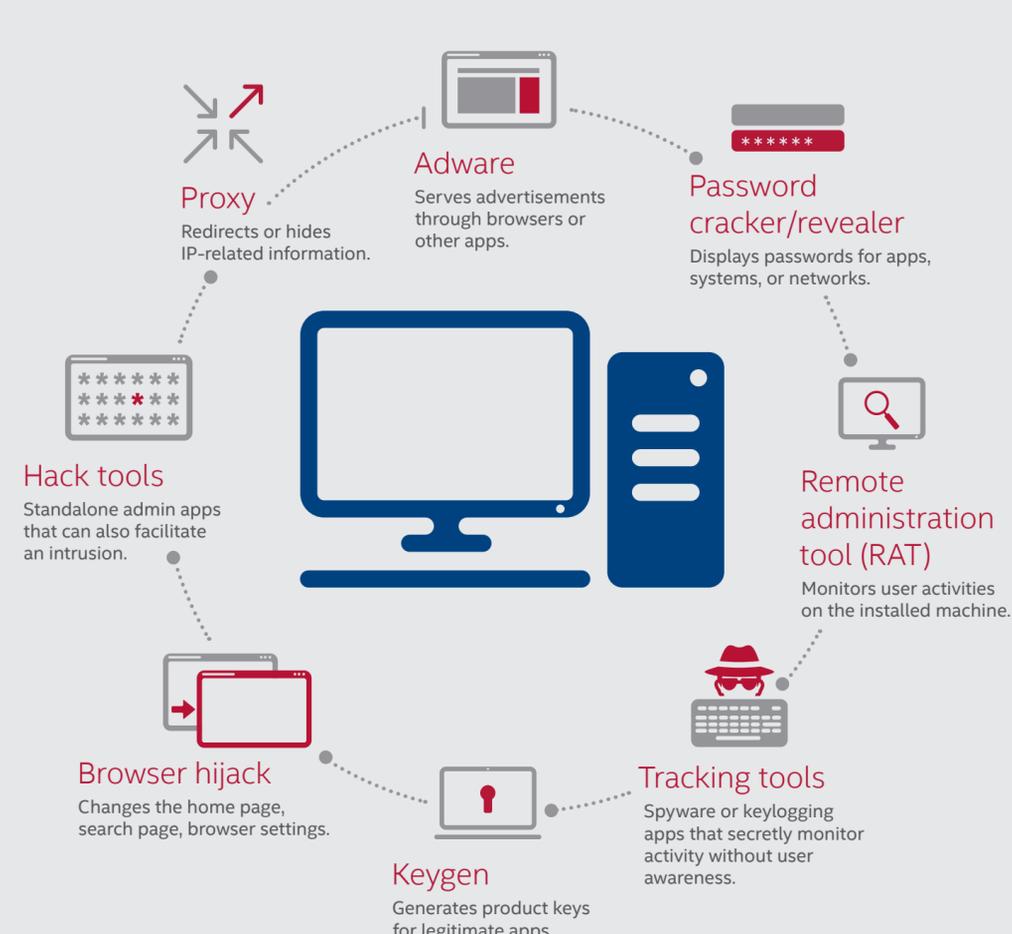
Victim

1

2 Vulnerable browser

3 Redirector 1
Compromised server redirecting to a malicious server

4 Redirector 2
Either hosted by Angler or compromised server

Server serving Angler exploit kit page

5

Checks for virtual machine and security products

NO

Server delivering exploits and malicious payloads

6 Compromised system

YES

Ends with JavaScript exception error

Angler was the most prevalent exploit kit seen in 2014, with a 26% share.

Fifty Shades of Gray

Potentially unwanted programs (PUPs) live in the world between nuisance and malicious malware and are becoming more aggressive.
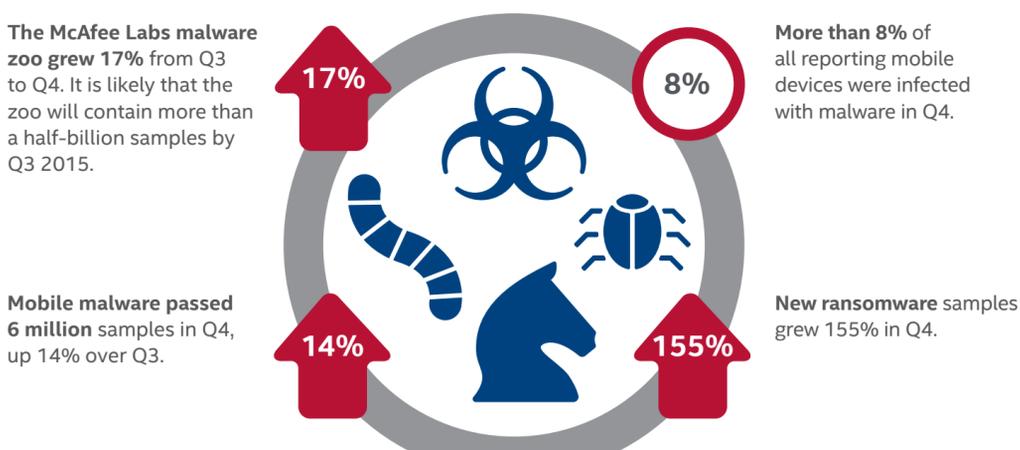
Proxy
Redirects or hides IP-related information.

Adware
Serves advertisements through browsers or other apps.

Password cracker/revealer
Displays passwords for apps, systems, or networks.

Hack tools
Standalone admin apps that can also facilitate an intrusion.

Remote administration tool (RAT)
Monitors user activities on the installed machine.

Browser hijack
Changes the home page, search page, browser settings.

Keygen
Generates product keys for legitimate apps.

Tracking tools
Spyware or keylogging apps that secretly monitor activity without user awareness.

In a typical 24-hour period, McAfee Labs detects PUPs on more than 91 million systems.

McAfee Labs observed more than 9 billion PUP samples in 2014.

Threat Statistics

February 2015

There are 387 new threats every minute, or more than 6 every second.

The McAfee Labs malware zoo grew 17% from Q3 to Q4. It is likely that the zoo will contain more than a half-billion samples by Q3 2015.

17%

8%

More than 8% of all reporting mobile devices were infected with malware in Q4.

Mobile malware passed 6 million samples in Q4, up 14% over Q3.

14%

155%

New ransomware samples grew 155% in Q4.

McAfee Labs Threats Report: February 2015

Visit **www.mcafee.com/February2015ThreatsReport** for the full report.

1 http://www.kb.cert.org/vuls/id/582497.

intel Security