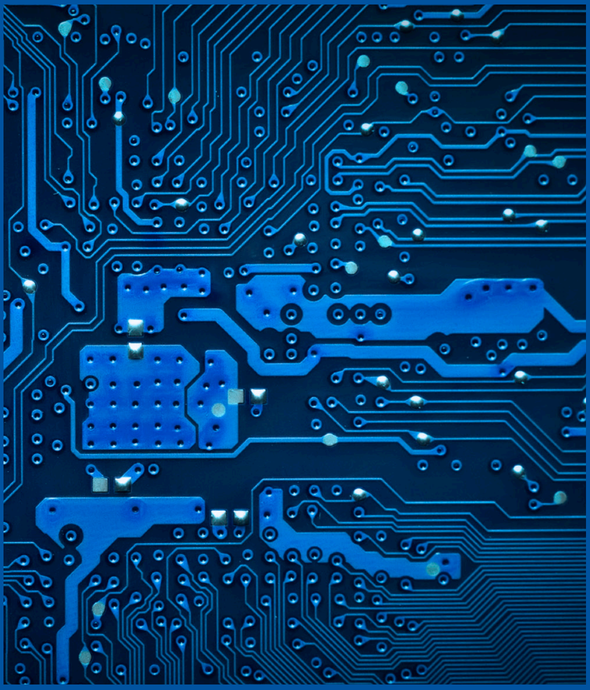
SecurityCoverage®

SECUREIT MALWARE REPORT

Q2 2013

About this Report

SecurityCoverage, Inc.’s Q2 2013 Threat Detection report is based on insights from the SecureIT™ Research Team, which monitors threat activity and studies new threats. This report contains data collected from hundreds of thousands of SecureIT protected computers from April 1, 2013 to June 30, 2013. The report reviews the malware landscape thus far in 2013 and provides a look at current and anticipated trends.



39%

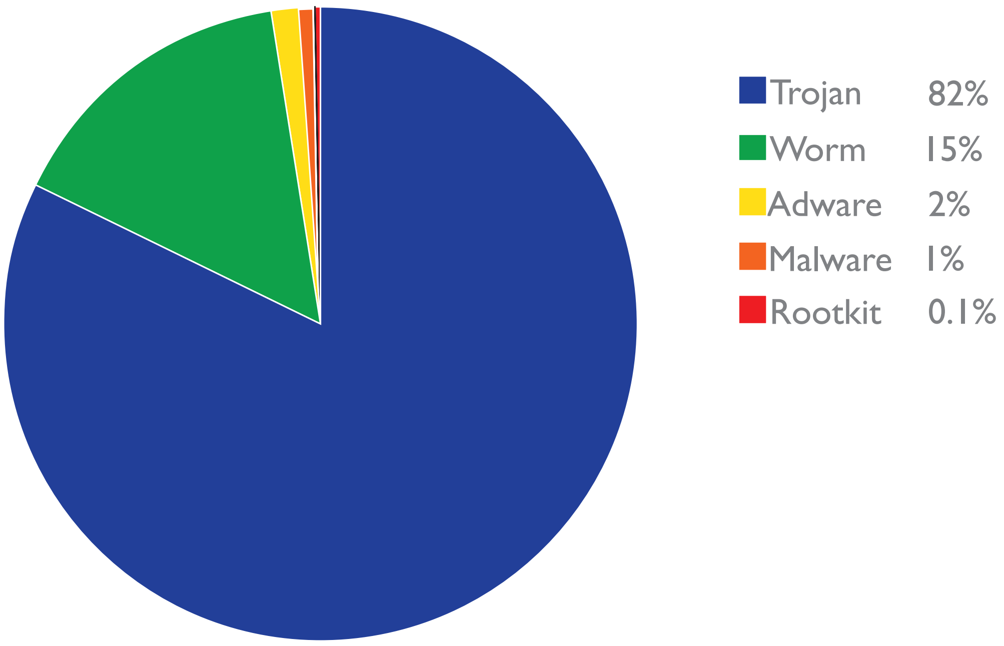
increase over Q1 2013

1.8M

malware detections in Q2 2013

450K

detections exploit Java vulnerabilities



Total Malware Detections Q2 2013

Key figures

The second quarter of 2013 saw a 39 percent increase in virus detections versus first quarter 2013.The total number of virus detections in the second quarter of 2013 was 1.8 million and roughly 25% of those detections exploited a Java vulnerabilty in their attempt to gain access.

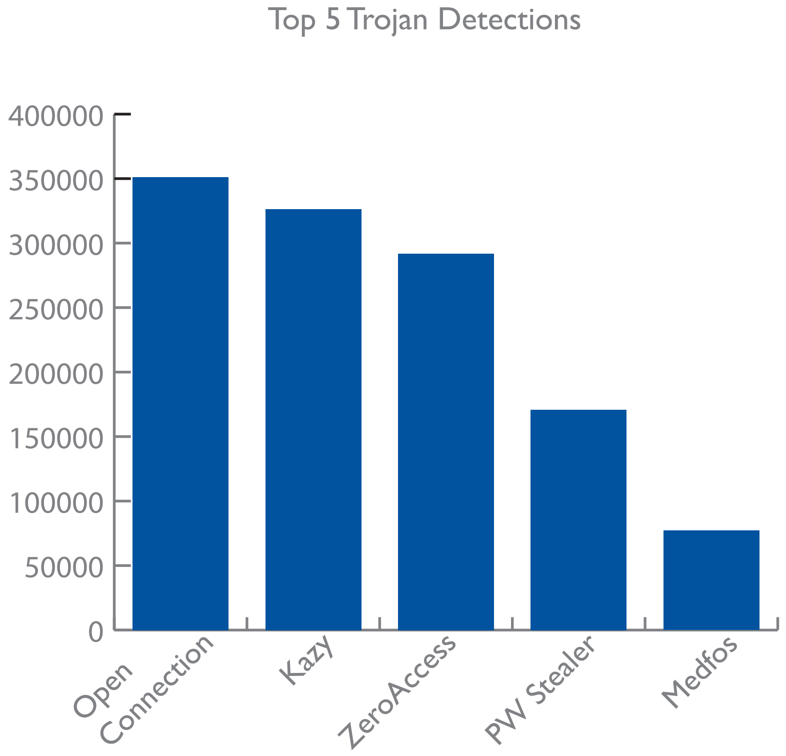
The majority of this increase was driven by Trojan detections, particularly OpenConnection, Kazy, ZeroAccess, Password Stealer, and Medfos. In fact, Trojans accounted for 82 percent of all virus detections in 2013. We will discuss what these Trojans do in the next section of our report.

SecureIT Researchers also reported a 34 percent increase in adware like GameVance and Hotbar, which bog down a computer with pop-up ads. Adware, though not generally malicious, can be a nuisance on an infected computer due to the persistence of the advertisements causing overloads and crashes. In some cases, Adware is used as a cover-up to hide more malicious activity such as virus installations, communication with command and control servers, or click jacking. Our researchers saw a small amount of cases where Kazy was installed onto computers via Adware.

Top Trojan Detections

OpenConnection is a family of Java-based Trojan downloaders. Once installed, it can circumvent browser security to install other malicious software. The end result depends on whatever that particular variant is programmed to download. It may install fake anti-virus software or other types of malware. OpenConnection is essentially designed to open the security gate from the inside so the author can install whatever malicious items they want.

> ***Adware, though not generally malicious, can be a nuisance, causing overloads and crashes.***



Kazy is a relatively standard Trojan infection that is typically installed using social engineering scams. These types of scams employ emails with attachments that look like documents, but are actually malicious executables that can install fake anti-virus programs to scam victims for money.

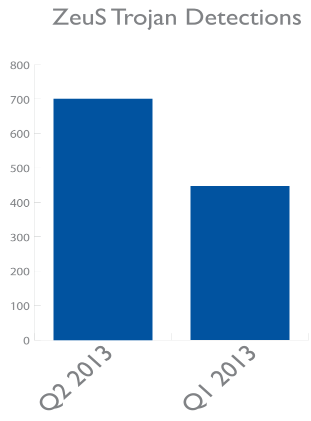
ZeuS TROJAN +57%

ZeroAccess, also known as Sirefef, is a persistent Trojan rootkit that is able to embed itself deep into a system and hide itself very well. Once embedded, users see symptoms such as installing fake anti-virus programs or reading keystrokes. SecureIT Researcher Matt Forbis says, "In my experience it can be an exceptionally difficult infection to remove once it hits a system, and has continued to evolve over time."

PW Stealer refers to a family of Trojans that are designed to steal password and log-in information from the infected computer. This can be accomplished by reading specific login fields from applications and websites, or by the use of keyloggers that can track all keystrokes made by the user, not just usernames and passwords.

Medfos (a.k.a. Midhos or Symmi) is a Trojan that installs malicious extensions into web browsers. The malicious extensions can then redirect search results to bad pages and/or allow for click-fraud by generating cost-per-click profit for an illegitimate enterprise.

The ZeuS Trojan, though not detected in large numbers, is worth noting as our SecureIT researchers spotted a 57% increase in ZeuS Trojan or Zbot detections in Q2 2013 versus Q1 2013. ZeuS makes use of a widespread botnet targeted toward stealing banking information. It was used to steal millions of dollars from U.S. banks and has the potential to cause serious financial damage to infected users.



BitCoin Mining

SecureIT researchers noticed approximately 200 detections of BitCoin Miner for the first time this quarter. BitCoin Mining is not generally malicious, but does use all of the available memory and bandwidth available on a computer, making it impossible to perform other actions. Many BitCoin enthusiasts purchase a high-power computer whose sole purpose is to mine BitCoins, and the Miner software commandeers the processing power of the machine. Recent reports of BitCoin Mining being done via botnet are concerning because that means it has the potential to be distributed and take over many more computers.

Conclusion

The first two quarters show 2013 is shaping up to be an active year. SecureIT researchers expect the detections of Trojans to increase again through the next quarter as the authors continue to evolve their infection methods.

Our researchers will continue to keep a close watch on ZeuS to see if it is indeed trending to make a comeback, or if this was just a short cameo for second quarter. One bright spot is an anticipated decrease in OpenConnection detections as patches are applied, or new computers with Windows 8 are purchased as OpenConnection is based on a rather old exploit within Internet Explorer. The same probably cannot be said for the ZeroAccess rootkit, as its efficiency and popularity on the malware black market will push it to evolve even further and detection rates will climb.

With the increasing popularity of mobile devices, many malware authors have shifted their focus to target smart phones and tablets. However, SecureIT researchers continue to see an active malware environment for desktop and laptop computers as many households will likely continue using their home desktop devices. As businesses continue their heavy use of desktop hardware, for both security and budget reasons, malware creators will still target these machines as potentially lucrative sources.

About SecurityCoverage

SecurityCoverage's mission is to simplify the use of technology and provide world class customer service. Known for award winning digital security, data protection, and exceptional support services, SecurityCoverage secures online identities and devices across desktop, mobile handset and tablet environments. It serves customers through a partnership group of electronic retailers, wireless distributors, Internet Service Providers, and telecommunications and cable companies across the nation. Product and company information is available at www.securitycoverage.com.

Media inquiries about this report or the mobile security space may be directed to:

Mike Fleming
Public Relations & Marketing Manager
SecurityCoverage, Inc.
230 2nd St. SE Suite 312
Cedar Rapids, IA 52401
Tel: (319) 298-4709
E: mfleming@securitycoverage.com