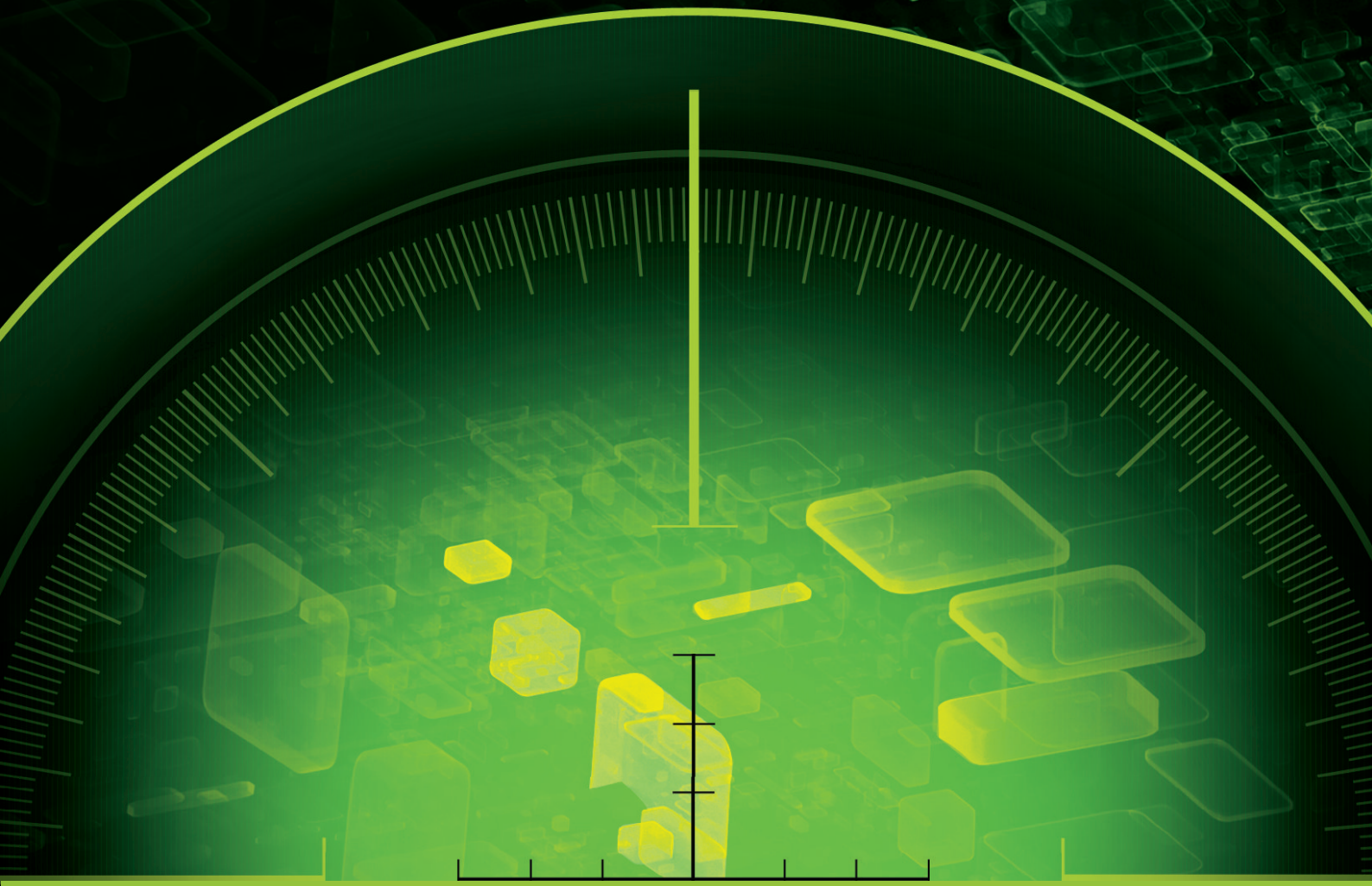
eScan™

Anti-Virus & Content Security

Malware Report

[June 2013]

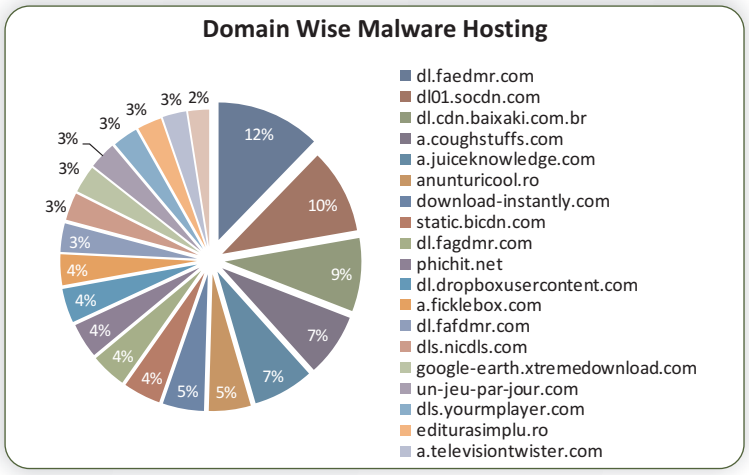


sales@escanav.com

www.escanav.com

Malware Report - June 2013

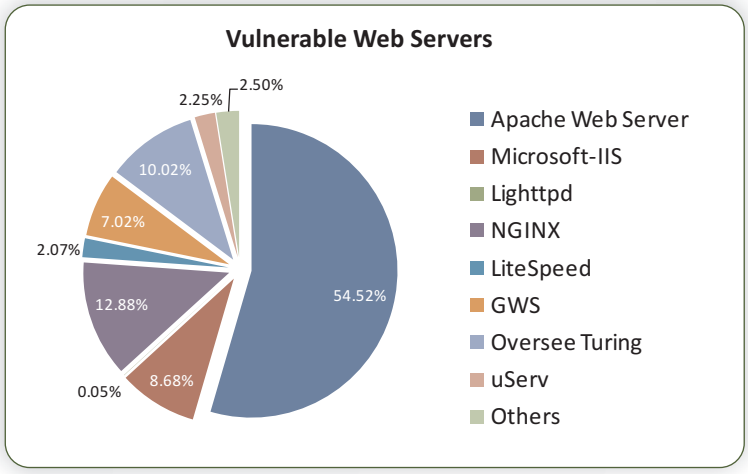
The World Wide Web is home to a number of malicious programs. But mostly programs that work without being dependent on one another. The month of June saw the discovery of two malicious programs that help each other stay on the infected machine. The programs work together by alternatively downloading the other but with slightly different variations to help evade antivirus software.



The Malware belongs to a family of worms that spreads via removable drives and mapped network drives. The worm (Vobfus) is a Visual Basic malware that is compiled in pseudo-code or native code. It first started with a simple string manipulation method and has evolved to more complex string decoding.

The worm shares a close relationship with Beebone – another Visual Basic compiled Trojan downloader that is capable of downloading threats from a range of families, such as Vobfus, Zbot, Sirefef, Fareit, Nedsym and Cutwail. When executed, Vobfus contacts a command and control server to obtain encrypted instructions on where to download Beebone.

Based on the research by Microsoft, Beebone variants download other variants of Vobfus, which basically creates an infection cycle. This recurring relationship is the reason why the malware Vobfus and Beebone are resilient to Antivirus products. Updated virus scanners might detect one variant of the worm; however newer downloaded variants may just go undetected. So even if Vobfus is detected and removed, the malware could have downloaded an undetected Beebone which further downloads an undetected variant of Vobfus.

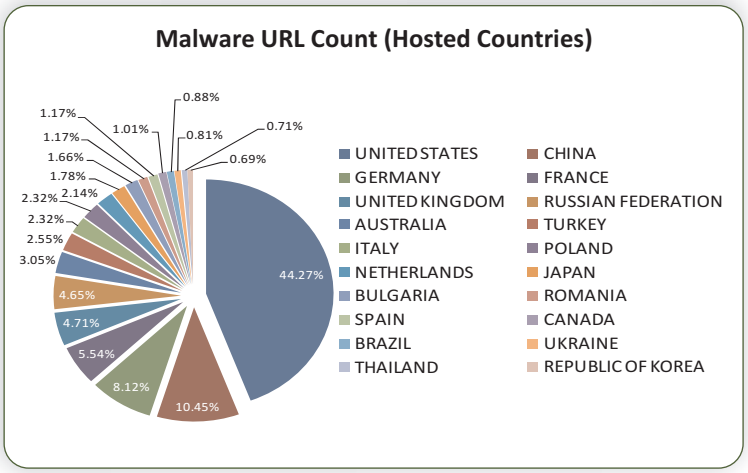


Vobfus can spread by copying itself along with an Autorun.inf file in a mapped network environment or via removable drives. Moreover since Beebone is capable of downloading threats from a range of malware families, the infected machine is quite likely to have all the mentioned variants.

To be on the safe side, users should always use caution when clicking external links. Browsers and other installed software should be kept up to date with the latest patches to help prevent software exploits. Also, disabling Windows autorun functionality will further help prevent execution of the malware via USB based devices.

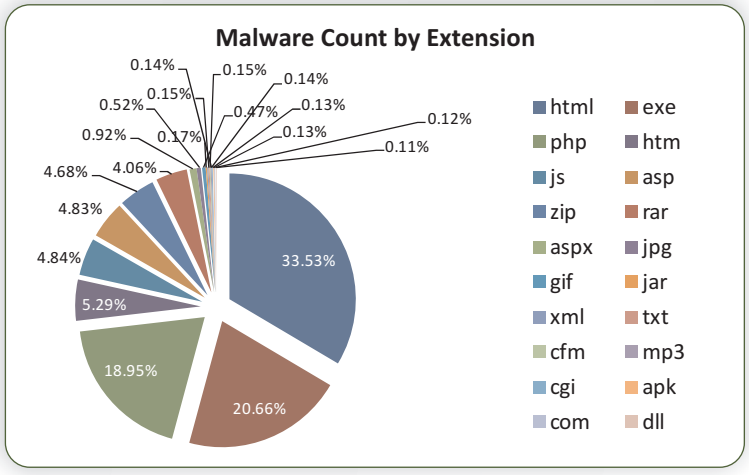
Android Malware

Malware for the android OS has been a concern for a while now. However, they have been easy to detect and remove. But a newly discovered Trojan targeting the Android platform is said to be more advanced than ever. It exploits multiple unknown vulnerabilities and makes use of complex obfuscation techniques and even blocks users from uninstalling it.



Obad.a makes use of a vulnerability found in Android's manifest (AndroidManifest.xml) file. This particular manifest file tells the OS about its various structure and components. The manifest file that Obad.a uses is twisted which basically hides it from detection and ensures installation. The Trojan exploits Android's Administrator function which further prevents apps with administrator rights from getting uninstalled by the user. To further prevent it from being detected Obad.a comes with no interface and runs in the background as a service.

The Trojan can export your personal information, download and install additional malicious apps, spam the contacts on your phone and is also capable of sending premium rate SMS message. Obad.a can also scan for nearby Bluetooth devices and then attempts to send copies of itself to all located devices. The Trojan goes a step further when the device has root access; it can then connect to the C&C server and execute terminal commands and do virtually anything.



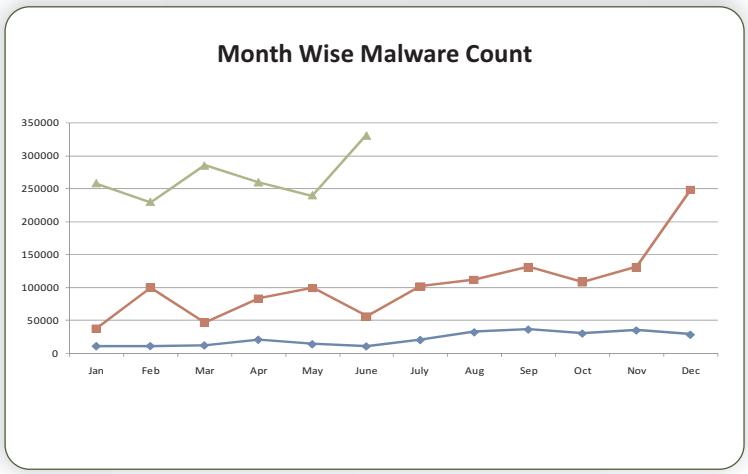
A Trojan such as Obad.a simply signifies that the Android OS has become a large enough target for malicious script writers. It also signifies that the OS has serious issues that need to be looked into by Google.

Citadel Malware

A new variant of the Citadel malware makes use of in-browser injection techniques to steal log-in credentials and credit card details from users in different countries. The malware has the ability to modify or replace websites opened by users on infected computers.

This new variant is specifically aimed at users from social networks, banks and major e-commerce sites, including Amazon across France, Spain, Italy and Germany.

When the websites are accessed from computers infected with the new variant, the malware replaces them with rogue versions that claim that the users account was blocked due to suspicious activity. They are then asked to input their personal information to confirm that they are legitimate owners and can further proceed to unlock the said account.



What makes this malware interesting is the use of customized drop down menus and in its ability to request for information in local languages.

Earlier during the month Microsoft and FBI units worked in sync to help disrupt more than 1400 botnets based on the Citadel malware. It is also estimated that the malware was responsible for more than half a billion dollars in financial loss. Microsoft might have put in a lot of effort to disrupt the operations of the Citadel botnets, but anyone with a Citadel builder can create a new variant and start a new operation.

Our Offices

USA:
MicroWorld Technologies Inc.
31700 W 13 Mile Rd, Ste 98
Farmington Hills, MI 48334,
USA.

Tel: +1 248 855 2020/2021
Fax: +1 248 855 2024.
TOLL FREE: 1-877-EZ-VIRUS
(USA Only)

E-mail: sales@escanav.com
Web site: www.escanav.com

India:
MicroWorld Software Services Pvt. Ltd.
Plot No.80, Road No.15, MIDC,
Marol, Andheri (E),
Mumbai- 400 093, India.

Tel: +91 22 2826 5701
Fax: +91 22 2830 4750

E-mail: sales@escanav.com
Web site: www.escanav.com

Germany:
MicroWorld Technologies GmbH
Drosselweg 1,
76327 Pfinztal,
Germany.

Tel: +49 72 40 94 49 0920
Fax: +49 72 40 94 49 0992

E-mail: sales@escanav.de
Web site: www.escanav.de

Malaysia:
MicroWorld Technologies Sdn Bhd.
(722338-A)
E-8-6, Megan Avenue 1,
189, Jalan Tun Razak,
50400 Kuala Lumpur, Malaysia.

Tel: +603 2333 8909 / 8910
Fax: +603 2333 8911

E-mail: sales@escanav.com
Web site: www.escanav.com

South Africa:
MicroWorld Technologies South Africa (Pty) Ltd.
376 Oak Avenue, Block C
(Entrance at 372 Oak Avenue),
Ferndale, Randburg, Gauteng,
South Africa.

Tel: Local 08610 eScan (37226)
International: +27 11 781 4235
Fax: +086 502 0482

E-mail: sales@escan.co.za
Web site: www.escan.co.za

Mexico:
eScan Mexico
Manzana 3, SuperManzana 505,
Lote 13, Fraccionamiento Pehaltun,
C.P. 77533, Cancun, Quintana Roo,
Mexico.

Tel: +52 998 9893157

E-mail: ventas-la@escanav.com
Web site: www.escanav.com.mx