‘e Scan

Malware Report

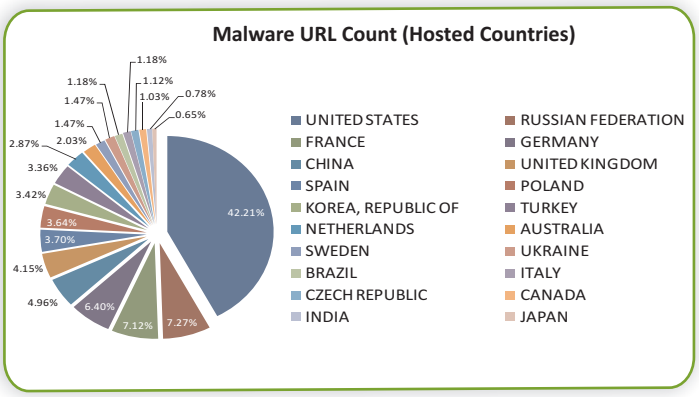
(August 2012)

E-mail: marketing@escanav.com

Web site: www.escanav.com

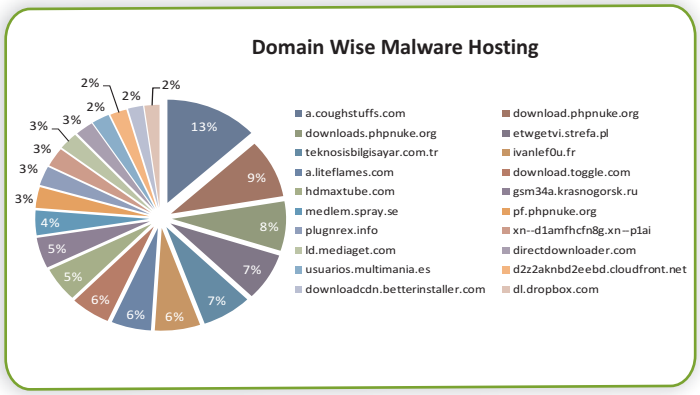
Malware Report - August

The underground economy associated with malware has grown rapidly in the last few years. Recent studies demonstrate that malware authors

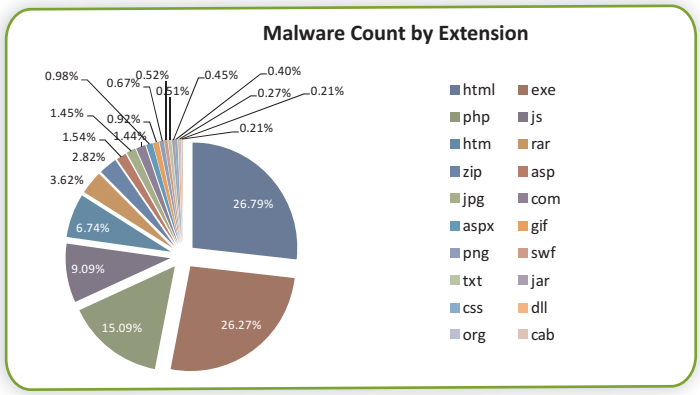


no longer need concern themselves with the distribution of malware to end user systems; they can leave that task to specialized pay-per-install services. In such an environment, the primary concern of the malware creator is to evade detection on infected machines as and when it carries out its malicious task, as end-user machines are protected by real-time detection systems that rely heavily on static analysis. Static analysis is favored because it is faster and consumes fewer resources relative to dynamic methods. Being able to defend itself against new anti-malware, signatures are therefore considered as high priority for malware obfuscation technologies.

Back in the past, the hacking scenario was such that it only demanded a single hacker to gain access into a vulnerable system. More often than not, their intent was self explanatory and it was looked at as an opportunity to make a quick buck.

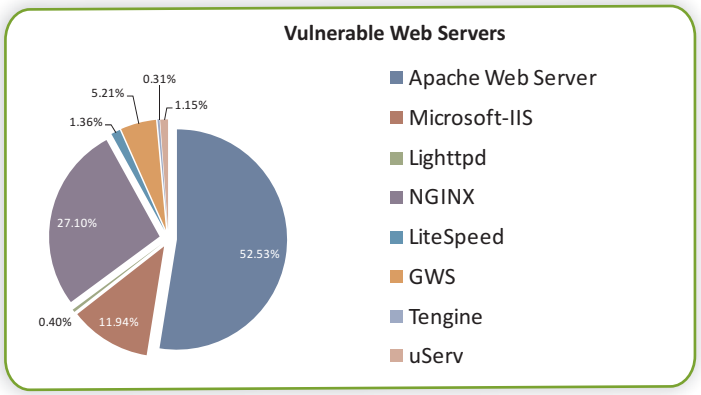


However, the same cannot be said now, as online crime has grown far beyond what it was years back. It has now turned into a 24/7 business that's riddled with bidding markets for malware, botnets for hire and cyber warfare. Many successful organized criminal rings are a culmination of various criminal groups that comprise of Full-time Employees, HR Departments, Project Management Teams and Team Leaders. Here too, each individual's specialization is looked into and divided accordingly where all processes are orchestrated to near perfection. Each team will specialize in different areas dedicated to creating the malware, marketing it and setting up the distribution channel, while the other is in charge of creating and renting botnets. It therefore goes without saying that cybercrime has evolved into a multi-level, service oriented industry where predated IT practices will simply not work against newly crafted malware.



The malware threat scenario has increased exponentially and this is not just in terms of volume. The techniques used in evading signature based security programs have also become more effective. In terms of averages we are seeing an increase in malware of by at least 10% for the month of August – in comparison to the previous month (July). Both small and large organizations are experiencing over 600 web based malicious threats every week. Such threats can either be malicious executables or they could be files with exploits that are specifically targeted towards vulnerable applications. This upward trend in malware basically illustrates that users are extremely vulnerable to clicking malicious links –

this is especially true when the perpetrated links use social engineering tactics.



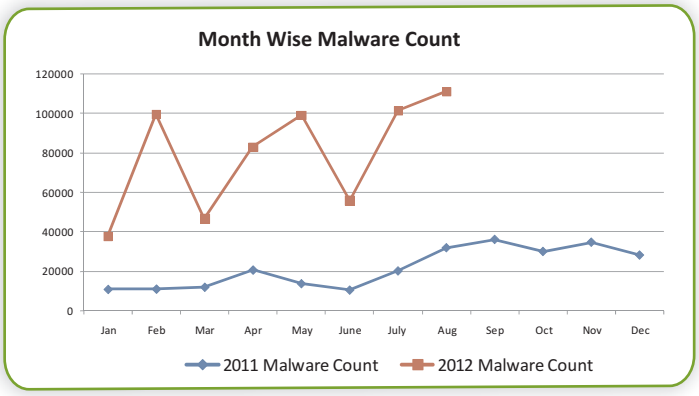
Email still holds the throne for being the primary attack vector for most targeted attacks. Operation Aurora, Night Dragon, RSA breach, etc. have all been documented to have some connection to spear phishing emails. In the last six months we have witnessed a 60% increase in email based attacks out of which 45% of those attacks have successfully penetrated various organizations that rely on using traditional security measures. However, in terms of malware delivery, there has been a significant rise in malicious links. Malicious links represented about 17% of malicious emails. However, in the last 2 months they have outnumbered malware ridden attachments.

In the coming months we can expect to see a rise in the above mentioned categories. However, their change will not be dramatic nor will it become the most sought after in the coming years. The main aspect that we need to be aware about is, these types of threats do exist in large numbers and the need to deploy policies and system wide patches are most important. However, as vulnerabilities are patched, the use of infected file attachments dwindle thus giving rise to Web-based attack vectors. The use of application vulnerabilities will never see an end as there will always be a new set of application vulnerabilities waiting just around the corner.

Malware writers put in a lot of effort to bypass security measures. Various tactics are employed by cybercriminals. It goes without saying that the use of malicious URLs are short lived before they move on to use others. Moreover, these domains are so infrequently used that their overall detection goes largely ignored by most scanners. Using socially engineered tactics, cybercriminals are personalizing emails and then making use of throw-away domains to bypass company based security policies that help filter out malicious emails.

As mentioned previously, email based attack tactics are used in various penetration methods and are considered as the first tactic that cybercriminals employ to bypass deployed defenses. What security analysts should understand is the fact that they are now facing an evolving threat that is both dynamic and potent in nature.

Vulnerability exploitations have also played a major role in the spreading of malware. Take the instance of the flashback Trojan outbreak, one of the most prominent incidents to have occurred in 2012. This malware exploited a known vulnerability in Java to gain control of Mac OS X machines. Even though previous various variants had been detected back in 2011, the malware



had been successful at keeping its infections hidden from users – till a buggy variant was released that triggered the alarms on a number of security software. Having said that, vulnerability exploitation has also been a part of the rootkit 'Zeroaccess'. This complex and ever changing malware has also become one of the most dominant threat of its kind. This ingenious little rootkit comes with multiple capabilities and once it infects its target, the machine can be used to help spread malicious applications and spam.

The trend set amongst mobile malware continues to see a rise however the overall infection rate has definitely slowed down in comparison to last year. With that said, the slow growth in malware has given way to new infection techniques. We are now beginning to see a number of effective techniques beginning to get implemented for the mobile platform – such as drive-by-download for Mobiles.

Drive-by-downloads has been a standard when it comes to infecting Windows based PCs – until now. First seen in the month of May, Android.Trojan.NotCompatible.A is not designed to steal data but it in fact acts as a device proxy, making the infected phone a part of a bot network. The malware can only get installed when the device is configured to accept installation of programs from unknown sources. The malware automatically downloads when the user accesses a compromised website. The malware is then automatically downloaded and sits in the notification tray, waiting for the user to install it. The downloaded file comes under the name 'Update.apk' and the running program name is shown as 'com.Security.Update' – both names come in as trick to fool the user into believing that the running file is innocent.

Disclaimer

The above report is based on malware URL collected for the month of August, 2012 and is a representation of the growth in malware infected URLs in the span of 1 month. The domains mentioned were found infected at the time of report creation. However, the domain/site/URL might be safe now as the infection may have been removed by the host. MicroWorld Technologies Inc. is not liable to any party for any direct, indirect, special or other consequential damages caused.

Any concerns as to the legality of reproduction should be directed to:

The Marketing Department
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.
Web site: www.escanav.com
E-mail: marketing@escanav.com

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