‘e Scan

Quarterly Malware Report

(April, May, June, 2012)

E-mail: marketing@escanav.com

Web site: www.escanav.com

INDEX

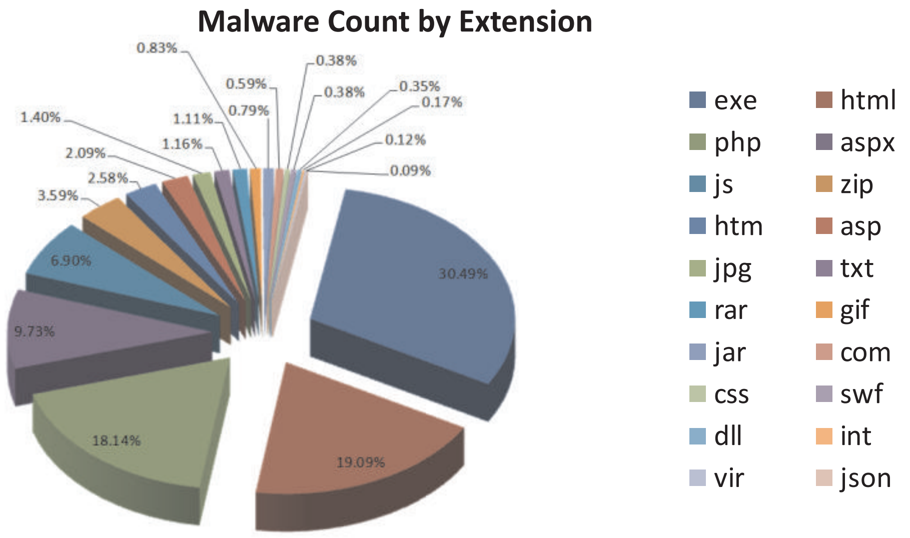
Quarterly Report

The last three months have been a roller coaster ride in terms of technology. In April, we saw the launch of Google's 'Cloud Drive', which if I must say isn't something overly new as Cloud based services have existed for a while now. And as mentioned, 'Sugarsync' , 'Dropbox', 'iCloud', 'Box', 'Carbonite', and 'Mozy' have always implemented Google's so called concept 'Keep Everything, Share Everything'. The cloud is a great concept to host and share files with people you know, but it also has its own set of drawback. For instance, hosting sensitive information in the cloud should come as a BIG NO for any organization (Big or Small). The loss of vital information can not only put the brakes in progress for the firm, but can also discourage clients from continuing with the company in question. Small and medium businesses are simply putting their data in the hands of third parties without taking note of the security being implemented. Over 75% of organizations are making use of at least one of the many cloud based service but a mere 30% ensure that the data held by external providers are being encrypted.

Malware URL Count (Hosted Countries)

The chart below shows the countries that are host to a number of infected sites. In the last 3 months, US itself has scaled to being the largest country to host at least 41% of malicious websites. That's more than even Canada (11%), Russia (8%), Germany (5%), Korea (5%), China (4%) and the United Kingdom (4%) combined. With that said, April also saw a heightened level of malware distribution of over 80,000 new samples as compared to just 20,000 (approx.) back in 2011.

The last three months have also seen a major shift in the overall trend in malware. The numbers speak for itself – with over 800,000 infected Mac users, it just goes to show that the Mac OS is equally penetrable as Windows. The only reason for it to stay out of harms reach was mainly due to the low number of users. The



growing number of buyers for the Mac further reinstates that this OS will see an increase in the number of malware attacks in the coming months.

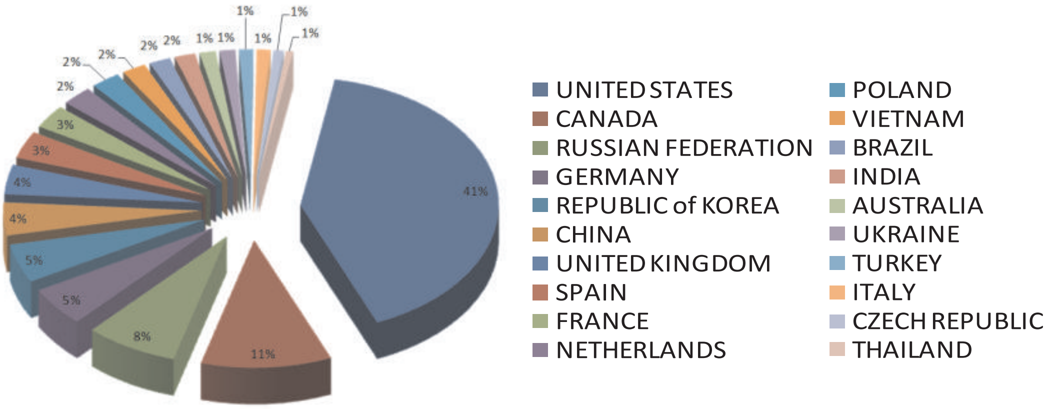
We have all witnessed the overall effectiveness of APTs (Advanced Persistent Threats). Stuxnet was a proven example of how effective targeted attacks can be. It also came to be known as the most complex malware written in history. However, the discovery of Flame made it surpass Stuxnet not only with its complex coding structure, but was also twenty times bigger than any other malware. At 20 MB, it is the largest piece of code to have ever been written. Key features allow it to steal documents, record conversations and keystrokes, take screenshots, disable installed security products, spread to connected systems (can also be done wirelessly) and log network traffic. In addition, it can steal details like IDs, contact information and also turn infected computers into Bluetooth beacons. It is also the first malware to have integrated this many features into one single module.

Malware Count by Extension

As far as extensions are concerned, EXE's have always been the most preferred in spreading malware and infecting other legitimate programs. As shown in the chart below, EXE's make up for 30.49% of malware. The last three months have also seen a rise in the number of infected web pages, giving it a weighted percentage of 19.09%.

Another growing concern is the significant usage of Smartphones. Close to 90% of employees in any given organization not only own such devices, but the very fact that they are allowed to access company network should come in as a concern to IT administrators. Even then, some organizations believe that implementing BYOD will help improve the overall productivity of the employees. But the question is – to what extent? As IT administrators, would we consider putting the company's network at risk over employee satisfaction? With their growing usage, there are many aspects that need to be looked into before giving

Malware URL Count (Hosted Countries)



the necessary permissions to an employee.

- What level of accessibility do the employees have?
- Do they have access to confidential information stored on the network?
- What is the total number of employees that have network access at any given point in time?

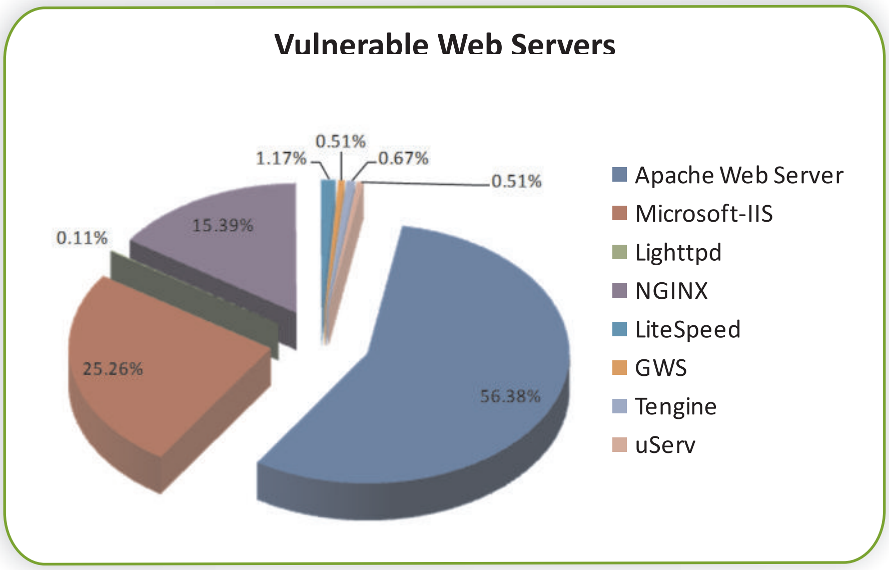
One of the major difficulties in managing BYOD is the ability to track and control access within a corporate environment. The overall sensitivity of implementing BYOD requires the utilization of a secure wireless network – WPA2-Enterprise. Moreover, the use of WPA2-Enterprise protocol ensures all three forms of wireless security:

- Over-the-Air Encryption – to ensure that the traffic in transit is protected
- User authentication – to ensure an authorized user is accessing the network
- Network authentication – to ensure the user is connecting to the real network (and not an Evil Twin network)

BYOD isn't just about keeping tabs on a particular platform, it's about securing the perimeter, no matter what the OS. Take the example of bringing in a Smartphone. Here, we aren't just talking about one particular platform but at least 5 various platforms - Android, iOS, Symbian, Windows for Mobile, Blackberry. The question here is – 1. Will you be able to implement access policies on all given platforms? 2. Will there be a need to block certain devices from accessing company resources when they enter the office perimeter?

Vulnerable Web Servers

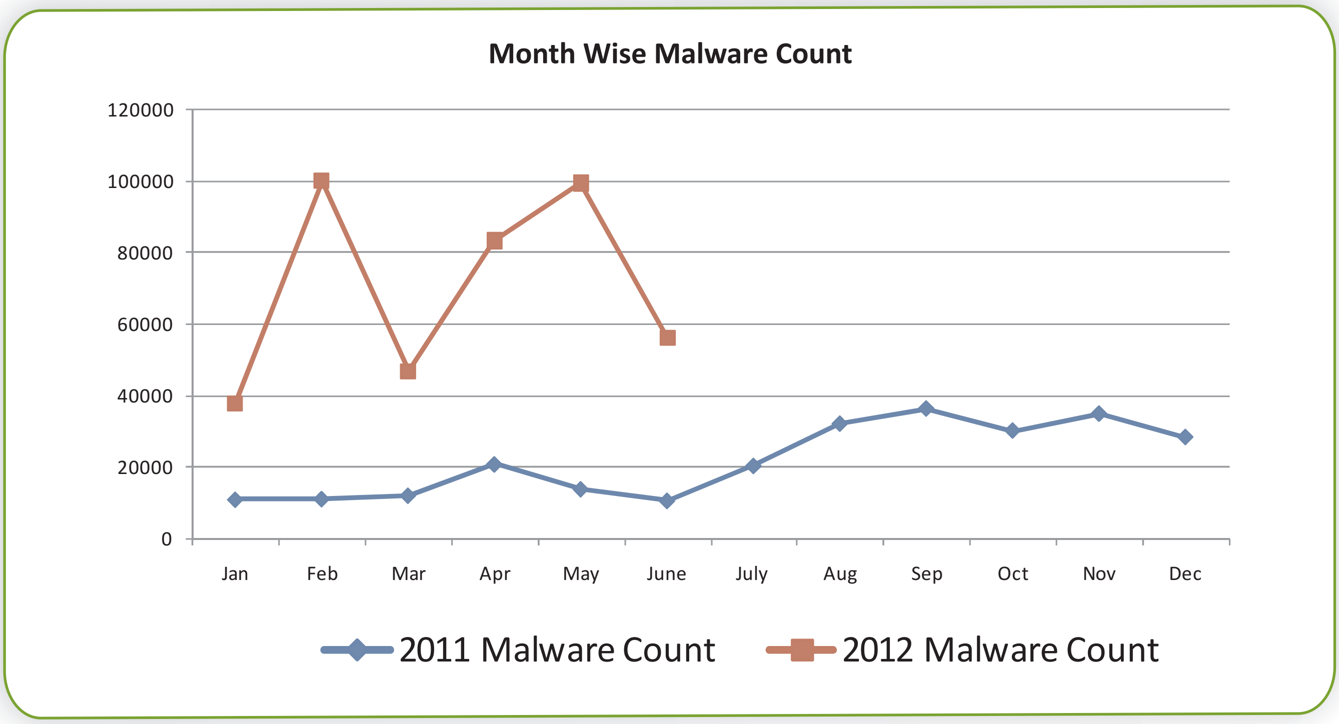
Website hosting is the most common function of web servers, but there are other uses such as gaming, data storage and running of enterprise level applications that they also provide. However, their primary function is to deliver web pages on the request to clients using the Hypertext Transfer Protocol (HTTP) service. Web servers also tend to be vulnerable to attacks especially when left un-patched. In the last three months, over 56% of Apache Web Servers have gone un-patched leaving them open to hacks. Furthermore, they can be used to host malware, thus increasing the chances of infecting unsuspecting users. Having said that, Apache Web Servers weren't the only ones left un-patched, Microsoft-IIS and NGNIX totaled to 25.26% and 15.39% respectively.



Month Wise Malware Count

Malware samples have been growing by the number and according to statistics, they have almost tripled in comparison to last year. On an average, we are beginning to see over 76,000 new and unique malware samples a month.

We have a growing number of targeted attacks that have outwitted most security companies, with Flame now being the benchmark for most malware writers. Zero day vulnerabilities also play a major role in creating an effective malware. More so, they are present in any given software product. It could be related to an Operating System, free, or even paid software, browser applications, etc. Web browsers are a particular target because of their widespread distribution and usage. E-mail attachments is also another method of bypassing a targets defenses as they are built to exploit vulnerabilities in the application opening the attachment. The attack could be in the form of a Word, Excel, PowerPoint or even a PDF document.



Disclaimer

The above report is based on malware URL collected for the month of April to June, 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.

All artwork and content is property of MicroWorld Technologies Inc. and cannot be used or reproduced by any person or company without the written consent of MicroWorld Technologies Inc. Any unauthorized reproduction of artwork or content is subject to legal action. The information is provided by MicroWorld Technologies Inc. without any assurance or guarantee of its correctness, be it express or implied. Neither do we make any implied affirmations regarding the negotiability, the suitability for certain purposes, or the nonviolation of laws and patents.

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

All other trademarks, registered trademarks, company names, product names, domain names and brand names are the property of their respective owners, and MicroWorld Technologies Inc. disclaims any ownership in such third-party marks. The use of any third party trademarks, logos, or brand names is for informational purposes only, and does not imply an endorsement by MicroWorld Technologies Inc. or vice versa or that such trademark owner has authorized MicroWorld Technologies Inc. to promote its products or services.

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