



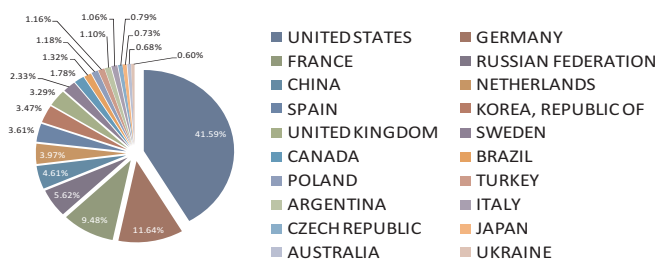
Malware Report

(July 2012)

Malware Report - July

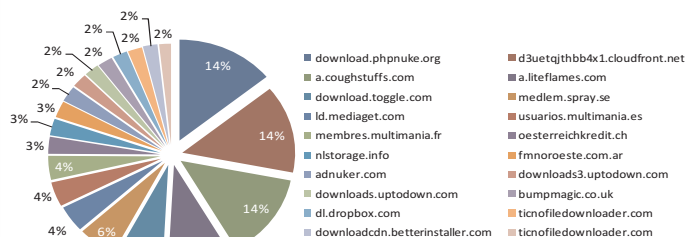
Mac's have always been touted as being the most secure OS. Sadly, it isn't the same as there have been a growing number of malware specifically

Malware URL Count (Hosted Countries)



targeted towards Mac users. Having said that, malware targeted specifically towards Mac users isn't something new; it has been slowly but effectively taking shape over the years. Traditionally, Mac users have always felt safer in comparison to Windows users. And why not? Given the dominance of Windows, it would be foolish to target Mac users when a larger chunk of the profit can be gained by targeting a larger base of Windows users. But it can well be said that the first major security threat to the Mac platform took shape with the discovery of the Mac Defender (May 2nd, 2011). With over 70,000 calls made to AppleCare – the Mac Defender was a turning point in Mac malware. Moreover to deceive users into installing the rogue program, the Mac Defender also morphed into what was called the Mac Protector, Mac Security, Mac Guard and Mac Shield. With the Mac Defender, Apple saw the largest number of infections at its time. But if you have been keeping track of malware, you

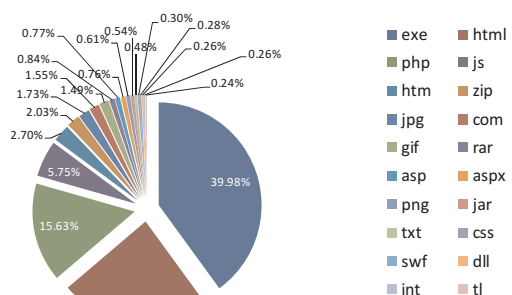
Domain Wise Malware Hosting



would know that the fame a malware reaches is short lived. In April 12th, 2012 - Flashback became the largest known malware to have compromised the security of Apples Mac, with over 700,000 infected Macs.

The high number of infected Macs goes to show just that Macs are as vulnerable as Windows. Also, the rate at which Mac users are being targeted should come as a concern to both vendors and buyers alike. Take the instance of the recently discovered Morcut malware that masquerades as a fake Adobe Flash installer – the malware is capable of turning infected Mac systems into a remote spying platform that can intercept email and instant message communications. To many it might come in as just another malware but in fact it is the first of its kind to have grown in complexity. For instance, the Morcut malware requires no administrative

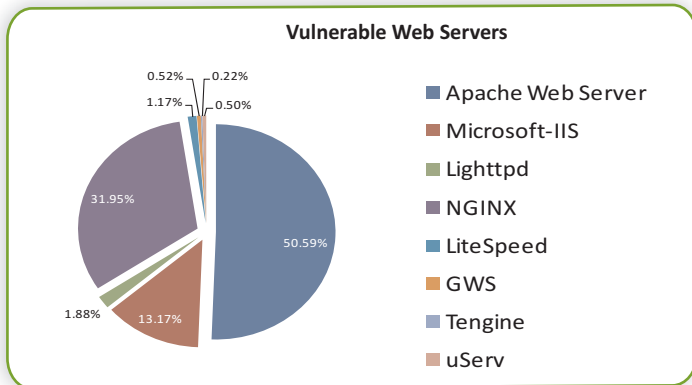
Malware Count by Extension



password to be installed, survives reboots and can intercept Skype, Adium and MSN messenger conversations. In other words, this little malware is capable of gathering a lot of information from the machine it infects. However, the detected malware doesn't come in as a major threat to Mac users as there have been no reports of it being active in the wild. The malware is not currently a threat but it goes to show you that Mac based malware will see a steady growth in numbers and complexity in the coming years.

While the Mac malware are a growing concern, the threat landscape to the Windows OS has been increasing almost three fold. Attacks on Small and Medium Businesses have seen a significant

growth in the last 3 months – as compared to 2011. Close to 40% of all targeted attacks have



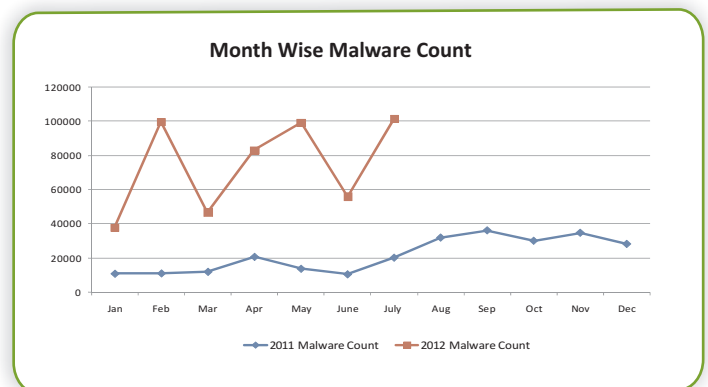
been directed towards businesses with less than 250 employees. This however hasn't diverted the growing trend in attacks towards large enterprises. Approximately 55% of businesses (large) are still bearing the brunt of targeted attacks.

In comparison to the month before, July has seen an upward trend in the overall number of malicious emails. At least 35% of all emails examined contained links to sites that were designed to automatically download and run malicious software. In addition, the distribution of EXEs have also increased by approximately 5% in comparison to June, also giving rise to infected zipped files. With that said, we are also seeing an increase in the distribution of files with hidden extensions.

There has also been an increase in malicious links in some of the most active locations in the world. Germany, France, Netherlands and Spain have all witnessed a relative increase in hosting and distributing malicious URLs. With that said, two of the still most trending worms within the United States and European countries include Sality and the Autorun virus. In total, both Sality and the Autorun virus sum up to a total 27% of infected computer both in the US and European countries. At 42.68%, US still tops the chart at hosting the maximum number of malicious URLs. In context to the European countries mentioned, four specific threats have contributed to the rise in malware infection rates. This would be EyeStye, Zbot (AKA. Zeus), Infected Keygens & Blacole. Germany has

also witnessed the highest number of data stealing Trojans known to target users who use online banking services. In contrast, both Vulnerabilities and Exploits have played as a major contributing factor to the increasing malware trend worldwide. European countries have witnessed an increased number of generic tools such as 'Keygen.exe' – a tool that generates keys for illegally-obtained versions of various software products.

The threat landscape is dynamically changing and hackers are continuously probing deployed defences; trying to find new ways of penetrating organizations. This they achieve by deploying a wide range of vectors that require complex forms of social engineering. They achieve this by cleverly persuading employees to open up security loop holes within the corporate network. Well established hack tools such as rootkits, zero-day vulnerabilities and cross-site scripting are continually being worked upon and refined to evade detection. In contrast, Spam mails have definitely seen a decline over time with only 65% mails adding up to spam but they have grown increasingly authentic and effective at making



recipients click malicious links. It is therefore critical to update and apply patches on regular basis. Moreover, with the increasing number of threats it is critical to have a security suite installed and running at all times. As far as enterprises are concerned, being proactive and deploying real-time security measures will not only protect businesses from incurring severe losses but will also help in earning customer/employee confidence.

Disclaimer

The above report is based on malware URL collected for the month of July, 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