‘e Scan

Malware Report

(May 2012)

E-mail: marketing@escanav.com

Web site: www.escanav.com

INDEX

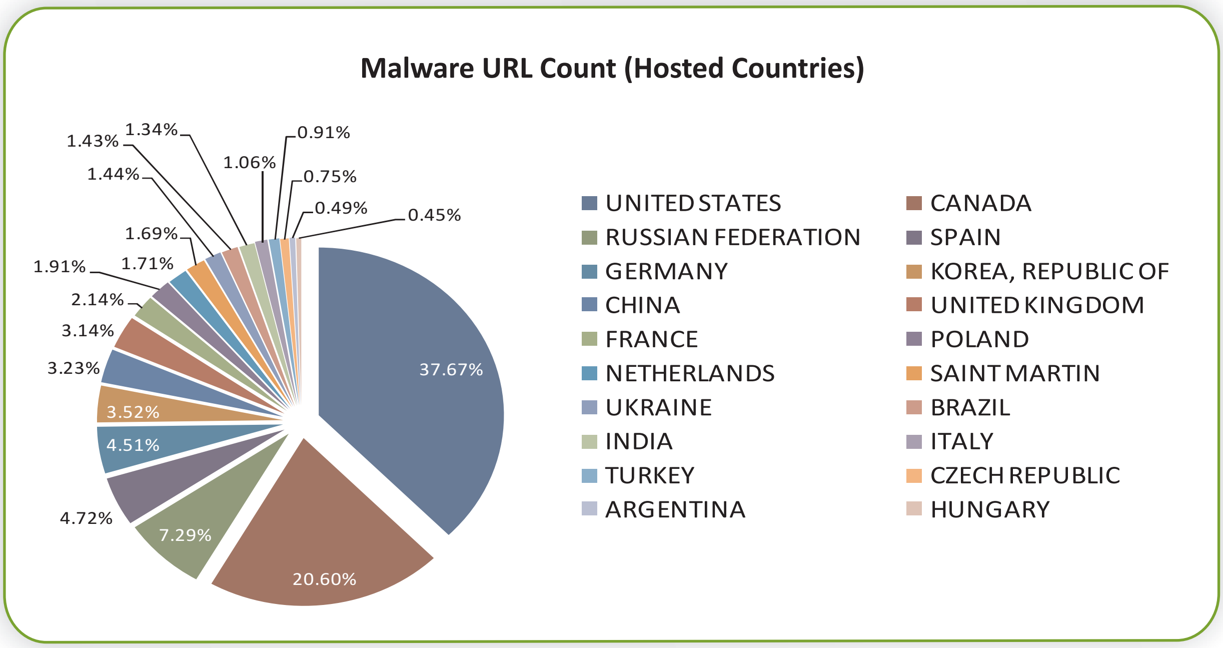
Malware Report

With the passing of each year threats are becoming even more complex and hard to detect. And as mentioned earlier, year 2012 will bring in a whole new breed of malware and a much wider range of attacks. 2011 itself was an eye-opener to most enterprises as a number of companies found important bits of information leaked on the web. Companies like RSA, Sony, HBGary all faced similar consequences of having their data hacked into. Yet enterprises fail to learn from such incidents. There are hundreds of small and large companies that are exposed to outside threats – where neither data nor personal information is managed securely.

The World Wide Web will undoubtedly play a major role in the distribution of malware as cybercriminals focus mostly on weak unsecured spots. Furthermore, various techniques are used to make these unsecured spots less effective. We have seen this transition taking place with spam emails, which are still present but less popular amongst cybercriminals. The web will remain to be the one source of malware distribution where usage of socially engineered attacks will specifically be built to target browsers and linked applications. Reason for this to grow and succeed in time is solely due to the fact that this platform has in fact become popular amongst cybercriminals.

In effect to the above mentioned, the huge influx of consumer owned smartphones and tablets is becoming a major security challenge for most organizations. IT departments are facing major issues securing data on these devices which they have very little or no control over. As mentioned in our previous report, the benefits which are brought in by mobile devices are plenty but there are also concerns that need to be addressed.

Cloud computing is another growing revolution that is capturing the industry by storm. The implementation of the cloud can significantly improve the overall effectiveness and manageability of various security solutions. This would cover security based on the web, data protection, endpoint and mobile security managed via the cloud. However the



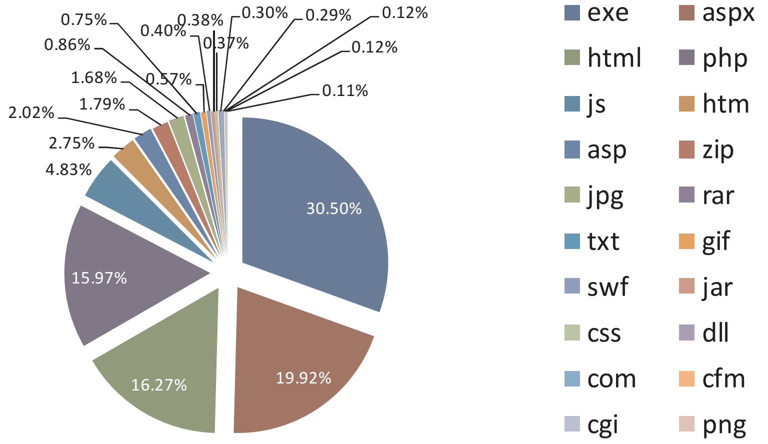
same also introduces new issues with regard to security and privacy for data at rest and in motion.

We are also beginning to see a rapid change in the way information is beginning to flow freely using the World Wide Web and this in fact brings in a whole new set of challenges that include people, process and technology. Moreover, as we change the way we communicate and share data, we can expect cybercriminals to infiltrate and hook themselves into these systems to brag about their malicious code.

News is something everybody enjoys talking about – be it by security experts or the media. Hacktivist groups such as LulzSec and Anonymous fished in a lot of news as they brought chaos and disruption of services by leaking documents and bringing down websites. It therefore goes without saying that Cybercriminals are becoming more and more professionalized as the availability of commercial crime-ware kits such as the growing popularity of the Blackhole kit. The distribution and growth of this kit basically translates into creation of new malware codes and exploits which significantly increases the overall volume of malware. Businesses will face newer and tougher challenges to curb and manage such threats. However, with newer ways being implemented to access data and applications on the go, the need to secure both mobile and cloud services will need to be addressed by both SMBs and Enterprises.

With that said, the overall volume of malware attacks and compromised websites will grow at a steady pace which will evidently make both governments and organizations place more importance on cyber-security. We are witnessing more than a steady growth in the distribution of malicious software and malicious links which translates to a 30% increase in malicious activity as compared to last year (See chart 'Month Wise Malware Count'). Intermediate threats also showed the ineffectiveness of deploying weak passwords. Moreover OS and application patching also comes in as a challenge as far as IT security is concerned. What we have witnessed is an increase in infection from hacked legitimate websites and drive-by-downloads – this further fortifies the need to patch vulnerable applications, browsers and operating systems. And with newer platforms and devices being introduced there is a growing need to upgrade our existing security tools.

Malware Count by Extension



Flame – Dawn of a New Era in CyberWarfare

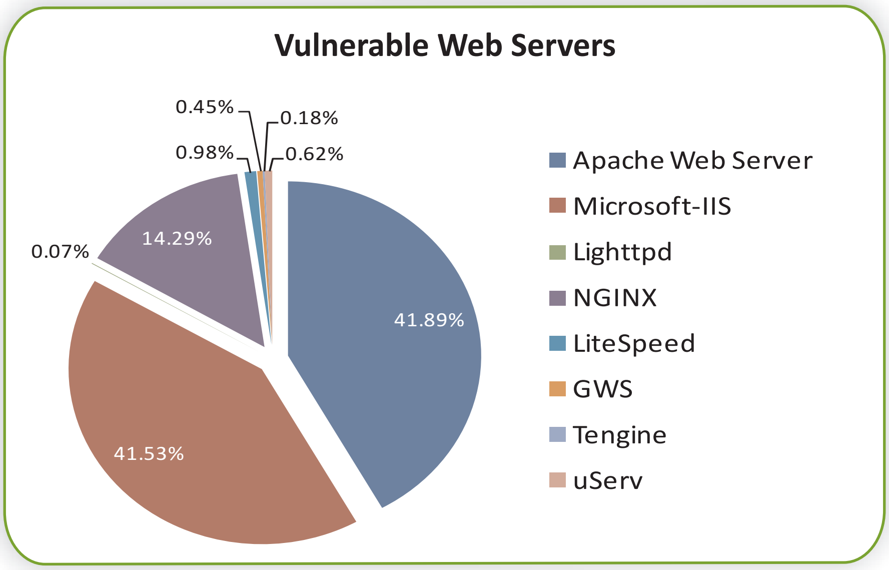
For those of you who are tech savvy and understand the web will definitely know the effects of getting infected by malware. We have all heard of the once famous Stuxnet – a computer worm specifically designed to infect and sabotage industrial systems in Iran. It was also the most complex piece of code developed by both United States and the Israeli government in 2009. However, the discovery of Flame has left most security researchers gasping for breath. Close to approximately 20 MB in size, the Flame virus easily surpasses Stuxnet in size and complexity, making it the most complex and biggest malware till date. Dissecting the Flame virus also shows that the malware not only predates Stuxnet but also shares bits of code thus giving the probability of it being used as a platform for building the Stuxnet malware.

Stuxnet was a proven weapon of choice to sabotage Iran's uranium enrichment infrastructure while Flame was built for espionage and information acquisition. In other words, the malware comes with features that allow it to steal documents, record conversations and keystrokes, take screenshots, disable security products, spread to connected systems and log network traffic. One very unique mode of transport Flame implements is the use of Bluetooth. The malware comes with a preconfigured set of instructions which when triggered results in two actions: one, it scans for Bluetooth devices – following which it steals details like IDs, contact information; two, can turn infected computers into Bluetooth beacons. The gathered data is then sent or uploaded to one of the several command and control servers scattered around the world. The files targeted in particular were AutoCAD drawings, PDFs and Text files.

The malware effectively evades detection by first determining the installed antivirus software following which it customizes its own behavior by changing the filename extensions it uses. Moreover, to effectively remove all traces the malware comes with a 'Kill' function that deletes all known files and operations from the infected system.

The Flame malware comes with an approximate infection of 1500 machines which include government organizations, educational institutions and high ranking individuals. The countries most infected at time of writing were Israel, Sudan, Lebanon, Egypt, Saudi Arabia and Syria. However, Iran tops the charts with the highest number of Flame infections.

The discovery of Flame clearly shows that State Sponsored Cyber Attacks are going to grow but to be able to predict the depths of such attacks is something we will have to wait and watch.



Drive-by-Downloads

Drive-by downloads are nothing new and they've been around for a number of years. Such attacks are built around multiple un-patched vulnerabilities found in browsers, plugins, applications and even operating systems. Such attacks are orchestrated by luring users to malicious sites that have been injected with malicious code. Ever since mid last year we have seen a number of legitimate sites being hacked to host malware. This has been a growing trend as legitimate sites are generally popular and trusted by large number of users. And because they attract a decent amount of traffic they are on the whole very successful in distributing malware to unsuspecting users. Blackhole is currently the most popular kit used to make drive-by malware. Currently marketed and sold within the underground marketplace, the Blackhole drive-by malware comes in as a crime-ware kit built around highly complex techniques that help it generate malicious code. To add to its complexity the malware kit comes with server side polymorphism and highly obfuscated scripts to avoid antivirus detection.

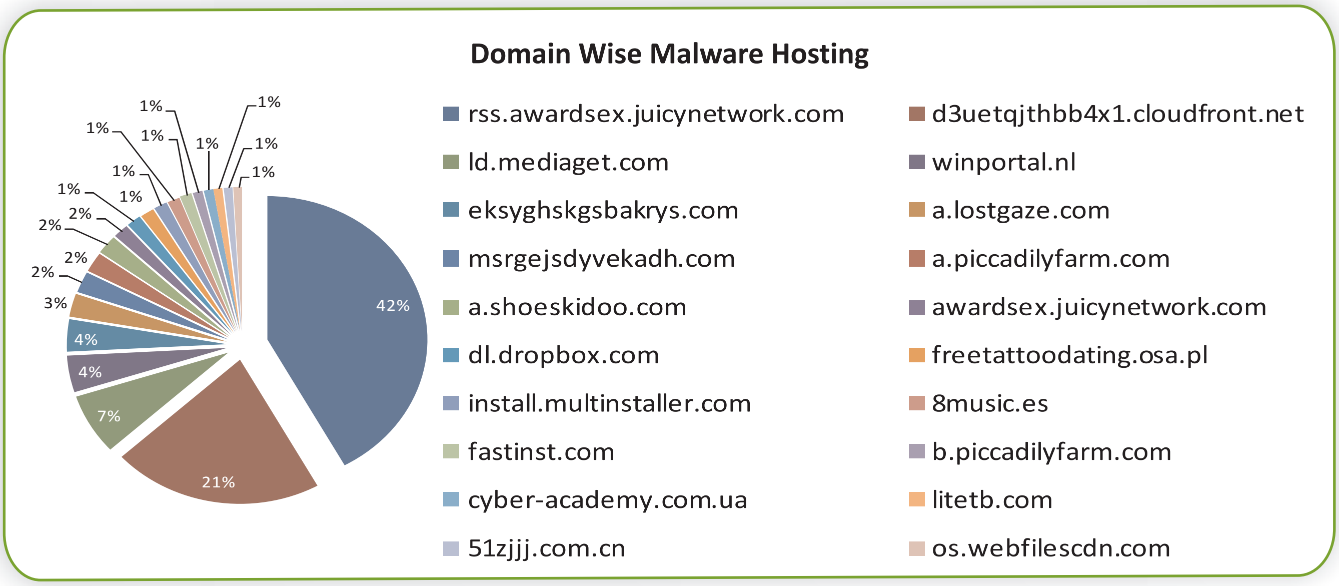
Typical Payload of Blackhole

The malware mainly spreads through compromised websites and is also capable of spreading using spam. Both methods redirect users to malware hosted sites.

In respect to this, there have also been instances of cybercriminals making use of a number of free hosting sites made to specifically host the Blackhole malware. And just like the kit, the injected script relies on heavily obfuscated and polymorphic codes that make it hard to detect. A typical payload an infected site hosts would include:

- Bot-type malware such as Zbot (aka Zeus)
- Rootkit droppers (such as TDL and ZeroAccess)
- Fake antivirus

It is also seen that the malware on these sites are built to target vulnerabilities in Java, Flash and PDF. We have and will be witnessing a continuous use of exploits specifically targeted towards Flash, PDF


Domain Wise Malware Hosting

and Java based components. Exploiting such components will remain to be a malware coders delight as their patch process is slow in detecting and blocking multiple vulnerabilities. This basically brings us to the next topic for discussion.

Vulnerabilities

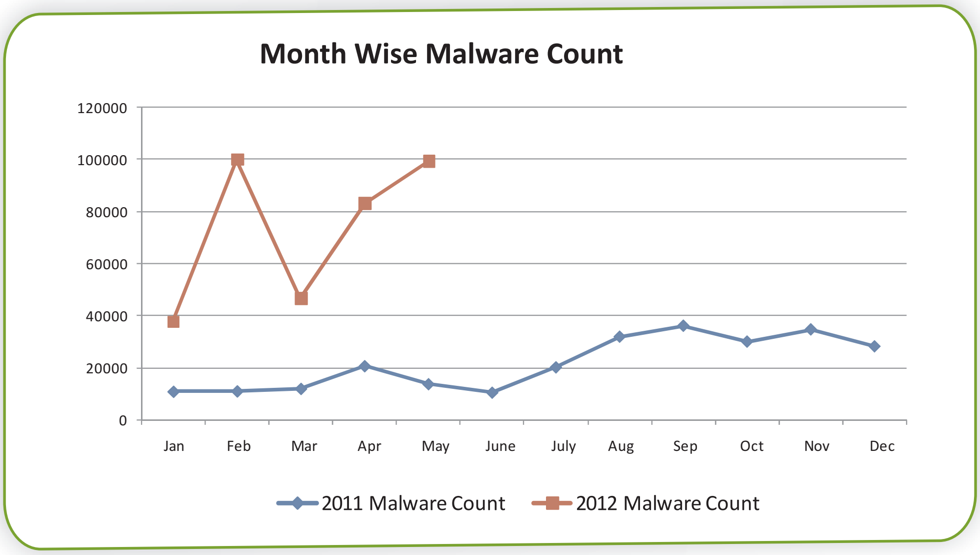
Windows is by and large the most targeted OS. However, its main vector of attack doesn't lie thoroughly in the Operating System. Its primary and highly used attack targets lie in vulnerabilities found in PDFs and Flash, despite Microsoft's efforts in releasing regular updates to patch Windows OS.

Software vulnerabilities are scanned for and patched at regular intervals. However, software companies often lag behind cybercriminals when it comes to counter zero-day attacks and unknown vulnerabilities. Speaking of which, Microsoft Office and Internet Explorer lead the charts when it comes to the distribution of malware as they are effectively the most used programs by users.

In addition, SQL injection and cross site scripting also account for a majority of hacks in web applications. 2011 accounted for a number of such hacks and by exploiting such security flaws hacktivists such as Anonymous exposed and took down several high-profile sites. This trend still continues into 2012. Take for example, the recent incidents that plagued Indian shores itself. We have large companies such as Reliance Communications that was hacked in about 5 minutes. There were other victims too – the Supreme Court, Congress, BJP and MTNL websites also felt the cold brunt of Anonymous.

In contrast the best protection against such attacks is to keep your software updated at regular intervals. This, in lieu with a regular OS patches, will further enhance the overall security of the system. Let's not forget the all importance of having a security suite installed and running at all times. Both small and large enterprises need to understand the importance of implementing a patch management system as this will effectively close the window of opportunity for hackers.

But before we jump in with all guns blazing in terms of security we need to learn from our past mistakes. Security at its basic level is what we need to understand to prevent uncalled for breaches.



Disclaimer

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