‘e Scan

Malware Report

(September 2011)

E-mail: marketing@escanav.com

Web site: www.escanav.com

INDEX

Malware Report

September has been quite an eventful month with all the necessary gossips porting around the Web. Take for instance, the bot army that was plagued around the Conficker worm was the topic of discussion in September. Needless to say, the worm was put to rest two years back. News is what drives the online community and it is exactly what cybercriminals look out for to help spread malware. In other words, greater the popularity of a particular topic greater will be the online traffic and where there is decent online traffic; SEO poisoning is one main aspect that is used to spread malware.

Contrary to this, application vulnerabilities are also the main reason for the inconsistent spread of Windows based malware. According to a report published by CSIS (Center for Strategic and International Studies), drive by downloads became the main aspect for malware distribution where distribution of email were replaced with exploits as the main attack vector 4-5 years ago. Browser exploits were the main stock in trade that was used to spread malware but the trend has changed over time. As studies show, a substantial 85% of all virus infections take place via drive-by downloads. Moreover in a study that involved analyzing the behavior of 50 different exploit kits over a three month period, CSIS observed 32% of 500,000 users were exposed to toolkits that discretely force-fed malware due to missing security updates.

Systems particularly vulnerable to attacks mostly consisted of Java, Adobe Reader/Acrobat and Adobe Flash. According to the research conducted by CSIS the following products were abused by malware to infect machines running Windows: Java accounted to around 37% of detected flaws, 32% in Adobe Reader/Acrobat and 16% flaws found in Flash. Systems that are infected are typically loaded with a number of malware instances that more often than not include fake Anti-Viruses and spyware programs which are typically used for stealing personal information. Statistically speaking, approximately 99% of all malware infections that are caused by exploit kits are a result of not updating or patching necessary software applications.

Amongst browsers, Internet Explorer summed up a major chunk of drive-by-download attacks – 66% in contrast to 21% of users using Mozilla, 8% for Chrome, 2% and 3% of users for Opera and Safari respectively. The data also provides insights on the Operating System which are most vulnerable. Windows XP stands at an astounding 41%, Windows Vista at 38%, Windows 7 at 16%, Windows 2000 & Windows 2003 had the least exposure to malware with the scores 2% and 5% respectively. The scores also directly signify the total number of users for that particular OS.

Having said that, aspects that surfaced in the month of September mainly consisted of polymorphic malware of which 70% were all email borne malware. The sudden rise also signifies the nature by which criminals are targeting business industries by exploiting traditionally used security measures. Let's not forget, social engineering is also on the rise with a wide variety of evolving techniques which include email based malware pretending to be forwarded by a colleague.

Speaking about security, one major concern that has everyone concerned is the new privacy policy that has been implemented by Facebook. The changes itself makes it vulnerable to a number of security hazards. This would include the recent removal of certain privacy policies which would otherwise prevent unknown Facebook users from viewing your list of friends. However, the bigger concern lies with the spreading of malware using social networking sites where scammers are also looking at various mediums to compromise user information. Take for example, the much talked about 'Dislike' button was a major hit in gaining user information. So much so, that a dedicated Facebook page was created to have the dislike button implemented. While this didn't result in the spreading of malware it definitely was one of the most successful attempts made to siphon off user information.

Breaking news is the second most important aspect that cyber criminals watch out for. Why? Higher the number of users or searches made greater will be the chance of spreading the infection. Take for instance, the passing away of Steve Jobs was the topic of discussion on October 5th, 2011. Within hours of his passing away scammers were out claiming Apple is giving away 1000 iPads in memory of Steve Jobs. It goes to show that scammers will stop at nothing to spread malware.

The following report is generated to give you a brief analysis of the overall malware statistics that is prevalent around the world. We have broken them down into 4 different sections to help you get a better analysis of the report.
The sections will include:

- Malware Insights
- Malware URL Count by Hosted Countries
- Malware Count by File Extension
- Domain Wise Malware Hosting

Malware Insights

Over the day's phishers and cyber criminals have been sending out huge volumes of fraudulent emails, specifically designed to spread password-stealing banking Trojans. Judging by the monthly and yearly chart shown it seems clear that a number of individuals and Small and Medium businesses have taken the bait.
As previously mentioned, September has seen a high jump in spam containing polymorphic malware that are hard to detect by most security suits. The main reason behind the use of such malware is mainly due to their ever changing code that uses a polymorphic engine to mutate while keeping the original algorithm intact. This basically means that the code changes each time the malware is run, but the main function of the code remains the same – allowing the malware to go undetected.

Even implementing the best technology will not stop malware from spreading, but preventing your banking credentials from getting stolen is the biggest step. The most practical and safest way to approach such a discerning factor is to use a dedicated computer for online banking. Which basically means the PC is not used for anything else other than accessing banking accounts.

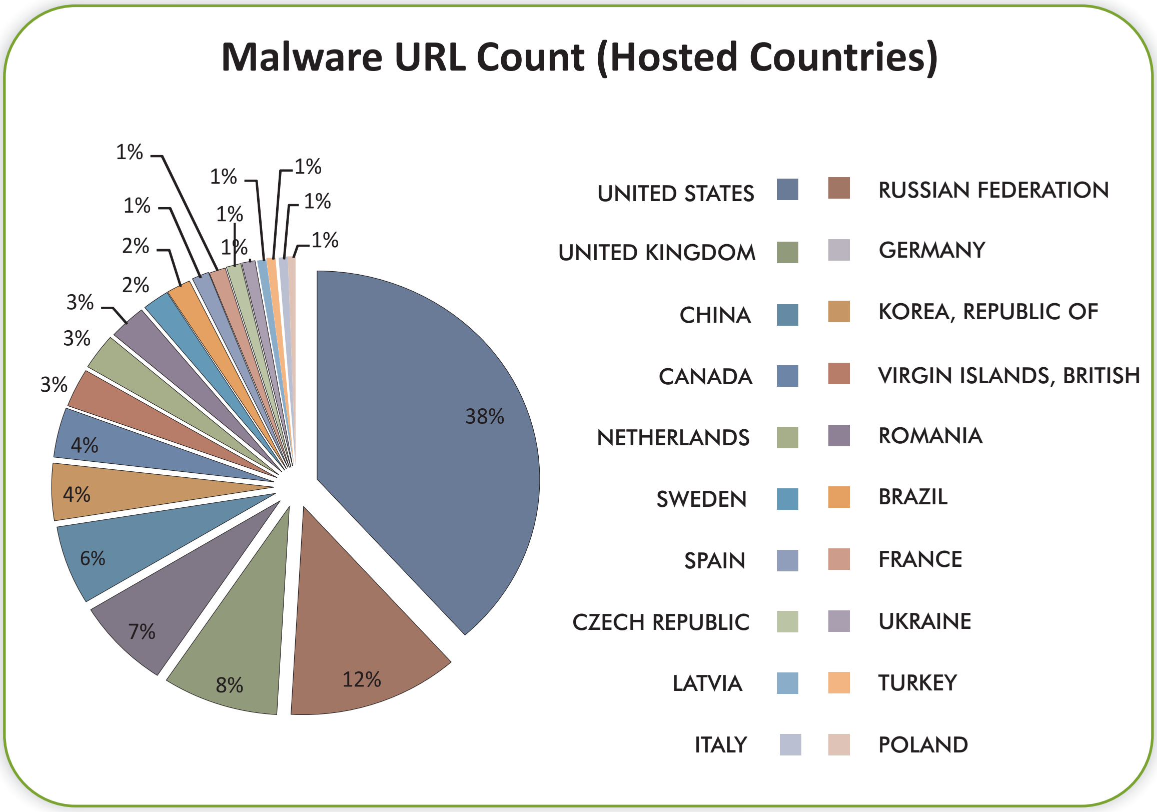
Having said that, blocking such attacks doesn't have much to do with state of the art computer systems or even having your system scanned using an anti-virus. From the attacks that have been recorded there has been significant usage of both ZeuS and SpyEye toolkit. However, organizations will need to understand that the attacks have a lot more to do with social engineering and tricking humans than with bypassing technologically advanced solutions. For instance, take the recent breach of US air base for piloting drones. News has it that cockpits piloting unmanned US drones have been infected with malware capable of logging pilots' keystrokes. What's perplexing is the fact that the US army is finding it difficult to remove the malware. Come to think of it, it was only less than a year that the US military faced a major security breach. An infected USB was the root cause of the breach and spread undetected on both classified and unclassified systems, allowing data to be transferred to servers under foreign control. This only goes to show the importance of securing endpoints as they are the first source of infection and needs to be secured at all times. However, don't confuse the word 'secured' with having a security suite installed. Blocking access to all endpoints is most important.

Malware URL Count (Hosted Countries)

Social networks such as Facebook, Twitter and Google+ have not only changed the way people communicate but have also helped businesses as a marketing medium. However the sheer increase in the number of users has also made it one of the most targeted. With that being said companies as well as individuals are not adopting enough safety standards to guard themselves against possible attacks. In a recent survey conducted by Ponemon Institute, 4000 respondents polled in 12 countries and territories displayed that 63% of users at work came by as a serious security risk and only 29% reported of having the necessary security controls in place to mitigate internal as well as external threats.

Moreover in another survey conducted by Time Doctor, there is a clear depiction of the productivity loss that companies face from non work related Internet surfing. As per the survey, an average worker with access to the Internet spends approximately 21 hours a week online. However, of the 220 decision makers surveyed at large companies, 34% reported loss of sensitive information which impacted business. The report further goes on to say a total of 55 minutes per day are spent by the average user on Facebook. In context this over 33% of workers check their personal mail at least 3 times a day while 14% of workers (of 568 companies surveyed) used email to pass on confidential information.

Social media is a necessity in some organizations and comes in as a business opportunity for most, making it a difficult proposition to block. What is required are defenses that go beyond signature and fixed policies that traditional security suites rely on. The World Wide Web has grown from what it was and is no more considered static. We have flash, embedded objects that keep changing over time while the page and web link remain the same. All it requires is a successful hack to redirect listed links or embedded objects to a malicious website.



What is required in such circumstances is a link scanner that can analyze and block all listed links irrespective of their signature or payload.

The results of research into which countries contain the most malware-hosting websites reveal some interesting changes. The US has experienced unprecedented growth in this area, hosting close to 38% of infected websites – however down by 3% when compared to last month's report. China, was responsible for hosting more than half of the infected websites on the web, playing host to just 6% of infected websites. A newcomer to this list is Sweden, accounted for 2% of the infected websites. Latvia, Italy and Poland make a comeback to this list, all accounting for just 1% of the infected websites.

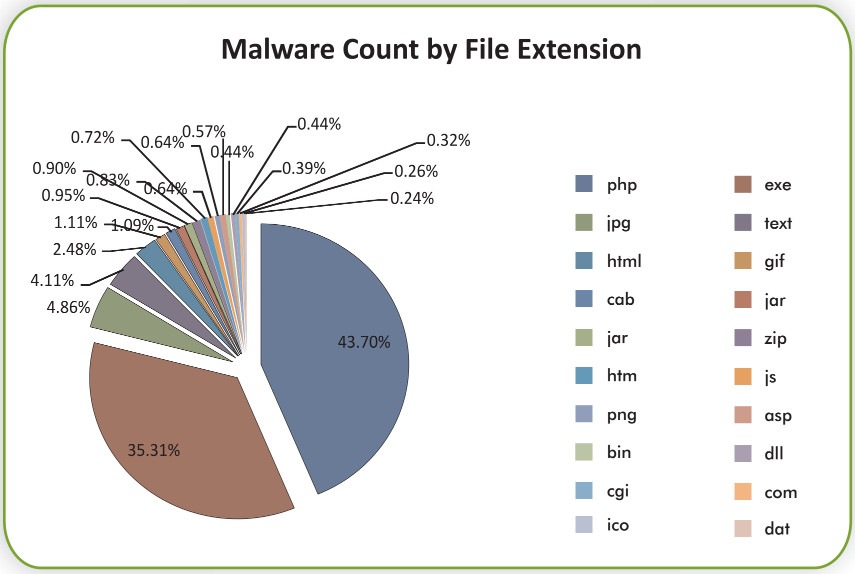
Malware Count by File Extension

The following research is based on analysis of threats found in the month of August. The figures shown is a basic study of malware hosting web sites that focus on stealing everything from credit card information to an individual's identity to banking credentials to spreading malware via links or even social networking sites.

There are a number of ways hackers are infiltrating the web but the most prominent way of making the user click on a malicious link is either by SEO poisoning or by specially crafted social engineering tactics. SEO poisoning tactics are basically used to increase the rankings of malicious websites in search results thereby making them look legitimate. Over the years this particular method has proven extremely successful since it can adapt to the ever changing news trend. Malicious websites looking to cash in on trending news make use of botnets to artificially inflate search rankings. As soon as the sites are discovered and filtered from search results, botnets are then configured to move on to the next hot trending topic.

However, hackers are also known to go after legitimate sites especially sites that top the search results. Why? Such sites are not only trusted by most users but are also considered safe by security filters. The top 100 most visited sites represent the majority of traffic on the web and consist mainly of social networking and search sites. Malware is injected via "user-generated content," such as news items, posted links, and comments.

With that said, 85% of all email is still mostly spam while 81% contain links to malicious websites. What remains prominent is the use of vulnerabilities. Vulnerabilities found in browsers such as Internet Explorer, Apple Safari, Firefox and Chrome remain to be used to a great extent with PDF exploits being the most sort after. Personalized emails sent from hacked Hotmail, Gmail and Yahoo accounts are

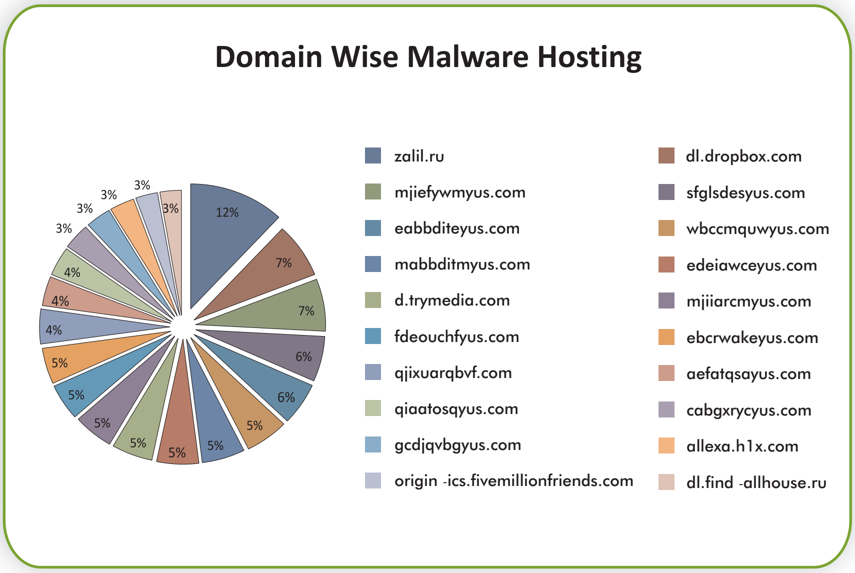


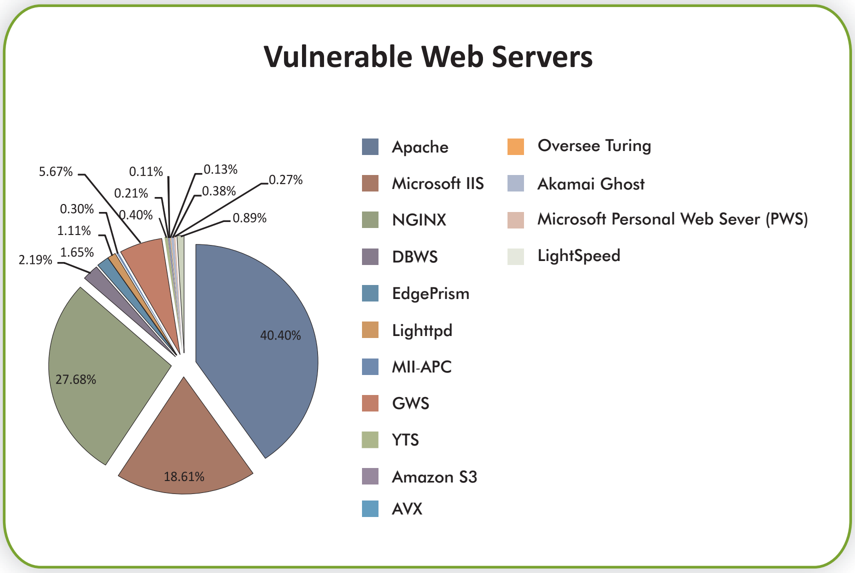
Malware Count by File Extension

specifically used to fool the receiver into believing the email is from a legitimate source. But in retrospect, they basically link back directly to malware or phishing sites or it could also link back to a hacked legitimate site which is further linked to a malicious website. All said and done, the increase in malicious websites and content are simply making it harder for the average user to differentiate between what's legitimate and malicious.

Domain Wise Malware Hosting

The web continues to be the preferred hunting ground for malware authors to deliver potent attacks. More so, our ever growing dependence on the World Wide Web makes it ideal for cyber criminals to chase poorly protected users.





Malacious Java iFrames and Obfuscated JavaScripts continue to dominate the chart as attackers continue to take advantages of vulnerabilities in websites and web servers to implant malicious code. Web users should surf from a fully protected machine, while companies will need to ensure their web servers are protected against attacks.

Having said that, server-side attacks are gaining popularity and is on the rise. Strategies are being worked upon to take advantages of new technologies and architectures which have forced organizations to look into hardening user endpoints like desktops and laptops. This in turn have lead attackers to shift focus to servers.

Looking at the current scenario, threats are most often than not multi staged and are advanced and persistent in attacks. The initial steps might involve spear-phishing attack against an end user – however this will involve getting around the initial defenses of the Web server. The second aspect or the second phase of the attack would involve dropping control codes for remote management and exploitation onto the server. Following which the attacker scans for vulnerabilities, executes sniffer and other monitoring tools to compromising administrator accounts.

So to develop a protection strategy for the server environment, it is worth reviewing server side risk profiles, evaluate currently deployed security strategy, and identify key characteristics of the server environment thereby establishing a protection strategy for servers.

Disclaimer

The above report is based on malware URL collected for the month of September, 2011 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