‘e Scan

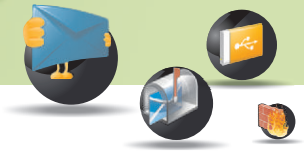
Malware Report

(August 2011)

E-mail: marketing@escanav.com

Web site: www.escanav.com

INDEX



'e Scan
Anti-Virus

Malware Report

The World Wide Web remains the biggest playground for malware infection where eMails are a host to malicious attachments and links while websites come in as a host to a wide variety of exploits and drive-by downloads – mainly targeting browsers and applications alike.

Malware in general have always posed a significant threat to online users – be it individuals or organizations. The overall threat landscape is seeing a rapid rise that is more than capable of compromising, damaging or acquiring sensitive data which can either be personal or can lead to loss of intellectual property. According to statistics, users are more likely to be tricked into downloading malware rather than be hacked by using an exploit. It therefore goes without saying that detecting and preventing such threats will continue to be a challenge as cybercriminals make this their prime attack vector.

Not all of these attacks are socially engineered. The technique, however, is being used to evade security programs and is being applied to the web that increasingly triples the distribution of malware, of which 55% (Malware) is now delivered via Internet downloads whereas only 14% is delivered through malicious emails. Therefore from a hackers perspective, tricking users into installing malware is much preferred as there are more than a handful that don't understand the complexity of web based threats.

Looking back a year, cybercrime itself cost the world a whopping $114 Billion in loss, of which, India alone stood at a loss of $7.6 Billion with over 2.9 million users falling as victims to cybercrimes. To be precise, $4 Billion was the total financial loss while $3.6 Billion was the amount spent to resolve reported theft. Of the total amount reported a mere 21% of victims actually reported the crime to the police. Despite the efforts made by security vendors only 16% had security software installed on their cell phone while 21% had security suites installed on their PCs. More than two thirds of all adults who used the Internet more were victims of cybercrime. While most issues are more than preventable, over 54% of online users have experienced malware followed by 11% in online scams and 10% in phishing scams. In comparison to 2009 and 2010 there has been a significant increase in malware amounting to 19%.

The overall number of infected users itself signify a defect in the way cybercrime is dealt by people online. Studies indicate that in the last one year the total number of users (read: Adults) infected with regard to online cybercrime have tripled in comparison to offline crime. Furthermore, we have noticed a major flaw in the way users perceive online threats as there is a disconnect between awareness and the action that needs to be taken. What this basically translates to is the fact that close to 80% of PC users are aware of cybercrime as a growing threat but the necessary precautions are not being taken to curb this threat. Security is either outdated or the necessary updates are never implemented to protect users from complex threats. Take for example credit cards, with frauds amounting to billions of dollars, it's been noted that over 60% of users do not make use of complex passwords. Having said that, over 41% do not take the effort to change their default credit card password.

In contrast, cybercriminals are taking advantage of the way social networking sites (Facebook, Twitter, LinkedIn) connect users – not only do they allow anonymity but are also used to phish out personal information. Moreover, it is the speed at which threats are spread that come as a challenge to both users and security vendors alike.

Come to think of it, when it comes to enterprises – cybercriminals are more than capable of hacking into security defences, that too at an alarming rate – even with over $30 Billion being invested annually on corporate defences. What we are witnessing is an era of dynamic cyber-theft where hackers are invariably being able to bypass conventional defences being laid down by large enterprises. Point worth mentioning are the number of industries that are vulnerable to online attacks – even the most security conscious industries. These would include financial services, health care and government sectors. To justify the statement, incidents that shook the corporate world would include HBGary, Epsilon, RSA and Sony – to name a few.

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

It's inevitable but true – there will never be a fall in malware, no matter how hard we try to stop it. The common way of spreading Trojans (be it financial, backdoors, bots etc), are not only done by embedding exploit kits within malicious websites but they can also be spread using a hacked legitimate website. The hacked or malicious links are then passed on to unsuspecting users either via instant messaging platform or spam emails or can be posted within questionable websites. For instance, when a user reaches a malicious domain unaware, the exploit will automatically decide the type of exploit that needs to be executed – all depending on the users system configuration. Once successful the exploits opens up a backdoor on the infected machine, allowing hackers to use it for nefarious activities such as spamming, execution of DDoS attacks, financial/identity theft – without the knowledge of the user. Other methods of infection can be based on JavaScripts or by implementing iFrames. However, we can enforce caution and deploy certain rules that would help curb this growing threat.

Cybercriminals are continuingly coming up with smarter and effective ways of creating malware. Do It Yourself crime-ware kits are available on the underground market for as little as $1500 USD. Take for instance, ZeuS was considered the god of all financial malware in 2010 and is currently being sold for as little as $600 USD. However, 2011 saw the rise of more potent twin – SpyEye. While it's overall functionality remains the same, its ability to delete known ZeuS mutexes and remain hidden from most AV suites is what makes it equally virile. The fact that a cracked version of the SpyEye kit remains readily available basically translates to a more effective and widespread number of Trojans.

Let's not forget Cyber-Criminals are not only devoting time and resources to create new malware but are effectively re-modifying the code of known deceased malware. A very good example would be that of the Ramnit Worm which has now been re-coded into a financial malware. The malware comes with a man-in-the-middle web injection module that allows it to modify client side web pages and transaction details on the fly. Moreover the month has also seen an enormous increase in malicious programs accounting for at least 25% rise in fresh threats when compared to similar months in 2010. Trojans dominated the line of newly detected threats comprising of at least 70% of all newly created malicious software.

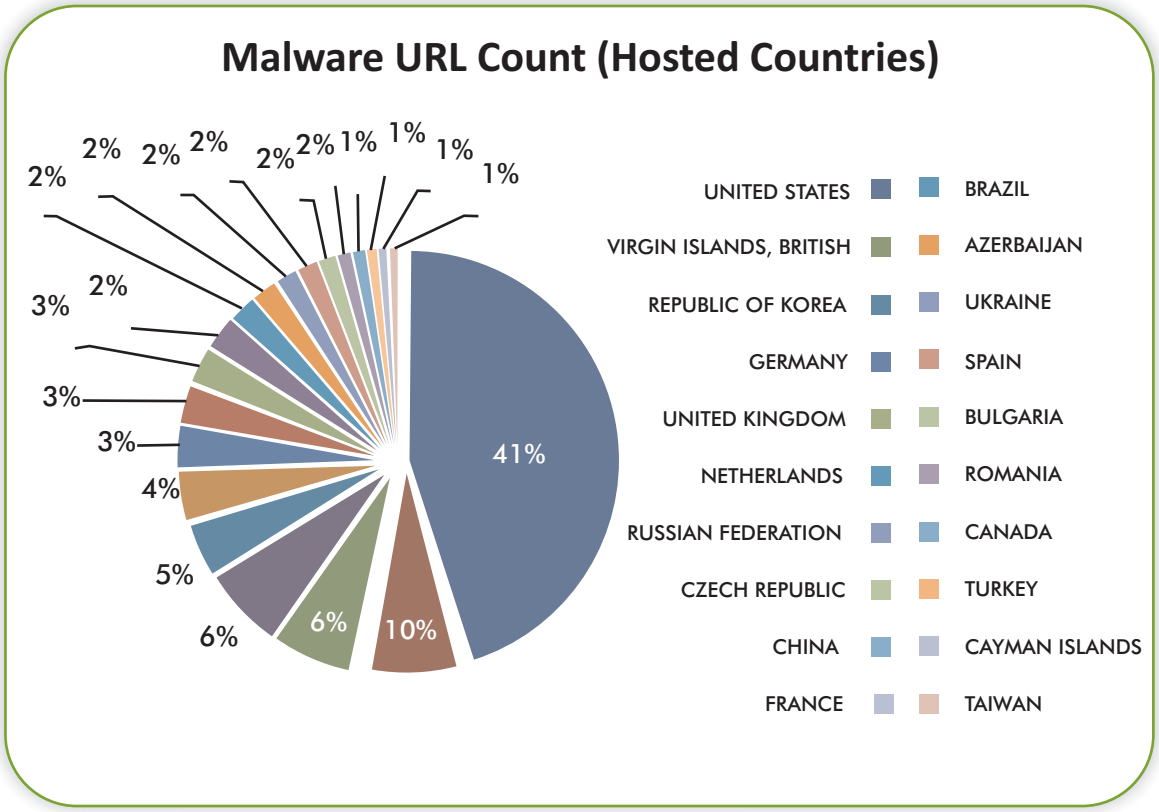
Malware URL Count (Hosted Countries)

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.

With cloud computing coming into play there has been a number of companies that have opted to harvest the power of the cloud. But large or even small companies are not the only players to take notice; cybercriminals are also making the best use of the cloud. Take for instance, Amazon's Web Services (AWS) were used to distribute banking Trojans using Amazon's Simple Storage Service (S3). It goes to show how stolen identities and AWS credentials can be used to create fake accounts even in the most robust of environments. However, this isn't the first time malware writers abused Amazon's Web Services. The mentioned service was also used as a ZeuS Command and Control centre in 2009.

Traditional methods of executing a web attack is generally based by creating malicious crafted websites to help lure victims with false promises. While the technique still continues to flourish, alternate methods have crept in where viral codes are injected into sites that are not properly secured. Moreover the reason these sites are attacked are mainly because of the large amount of traffic they attract. And the success of penetrating a wider degree of people also goes hand in hand.

Malvertising or advertisements containing malicious code has also seen a steady rise in the last 12 months. Two famous websites which fell to such attacks included New York Times and Gizmodo.com. It goes to show that it is people's trust that is being breached as this is the weakest aspect of any human being. That apart, the need to patch server side vulnerabilities are also aspects that are being overlooked by a handful of IT heads.



The month of August clearly states an increase in the number of web borne attacks which stood at an astounding 89%. US

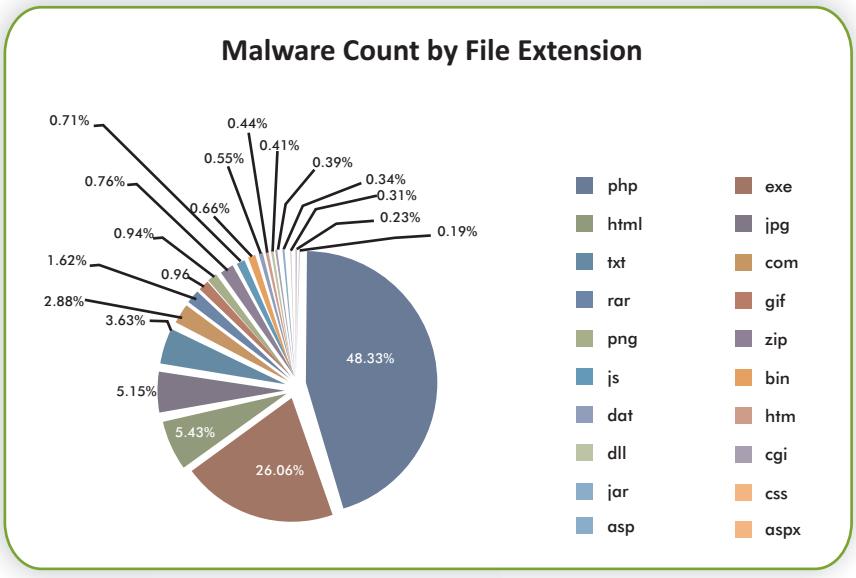
still tops the charts with the highest number of infected websites at 41%. It has also been noted that the overall bulk of malicious activity is mostly found to be located on compromised legitimate sites. The number of malicious sites continues to rise in Korea and Virgin Island (British) while those facing the highest risk of infection via the Internet were Germany and the UK. Other high-risk countries would include Netherlands, Russia, Czech Republic, China, France and Brazil. In comparison the safest would include Canada, Romania, Spain, Turkey, Taiwan and Cayman Islands. The statistics collected primarily show that developing countries carry the highest risk of both local and web borne infection. It has also been noted that IT risks are seen rapidly increasing in these countries and the required level of security awareness may not always be the same. However, Trojans such as TDL4, ZeuS, SpyEye, etc are primarily targeted at users in developed countries as developed countries primarily make use of plastic money or credit cards, to be more precise.

Malware Count by File Extension

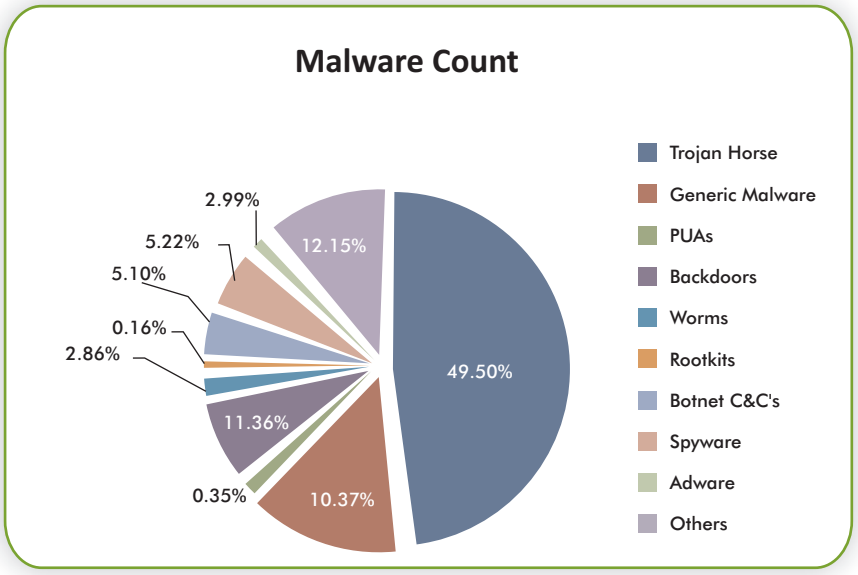
There has been a constant repacking of malicious executables which basically make them appear new each time they appear in the wild. The MD5 hashes that the files come with are so dynamic that their time to live is probably little more or less than an hour. Moreover in recent months there has been a swarm of web hosted infections. Besides, WordPress attacks seem to be on the rise along with other PHP-based platforms. From mass injection within ads to inserting rogue codes within JavaScripts, there has been a steady growth in malware injection over the years.

The Autorun.inf made a rather strange comeback and was by far the most popular threat in the month of July 2011. Besides Backdoor.IRCBot.Dorkbot.A comes in as a beginner with 1.47% prevalence in Latin America. Much like the Autorun.inf, the worm includes a backdoor that allows it to be controlled remotely.

The previous report mentioned about the virtually indestructible TDL-4 and the rise of fake AV products. While they continue to grow at a steady pace financial malware has also seen a sudden surge in recent months. Detected back in 2007 ZeuS was the first of its kind to siphon off money in real-time. It later turned rampant in 2009 and has been modified ever since. ZeuS controlled machines are spread across 196 countries with Egypt, United States, Mexico, Saudi Arabia and Turkey being the most significantly infected. Development pertaining to this malware has stopped but is still widely used by cybercriminals. However, with its source code leaked back in March it has given way to more notorious malware such as SpyEye, Ice IX, Ramnit – let's not forget to mention they come with added improvements that make them far more difficult to detect. The



improvements are relatively minor but are effective in evading most security programs. In addition, developers have made it harder to track its command and control servers that are hosting the necessary configuration files. These files are basically instruction sets that are used to control the infected computer. With the necessary improvements in place the configuration files are now hidden behind scripts which require a specific key to download.



The month has also seen a drastic rise in botnet activity – the highest in the last one year. The month of August witnessed an increase in the volume of email messages that came with malicious links or attachments. Possible rise could be the effect of the takedown of the Rustock botnet which has apparently left a deep scar in the supply of compromised computers, thus leaving bot operators scrambling to build bigger and more effective botnets.

Domain Wise Malware Hosting

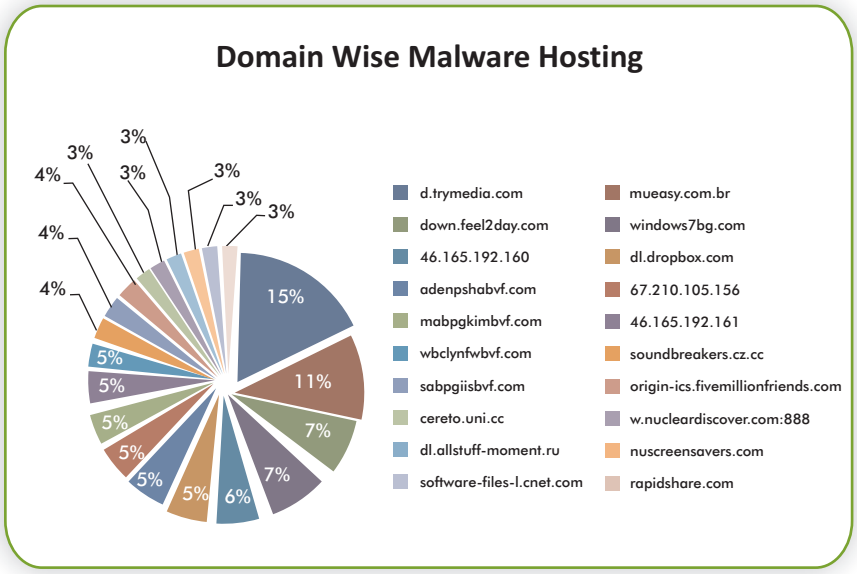
The Domain Name System or DNS is a hierarchical naming system for a number of resources connected to the Internet. It helps locate resources such as web servers, mail hosts and various other online services, which makes it one of the most important components of the Internet. However, it is also one of the most sort after by cyber criminals. Take for example, the botnet command and control centres are the most prevalent when it comes to hosting malicious sites. Whenever an attacker succeeds in infecting an end-user, the destination machine is silently turned into a bot whose basic functionality is to listen and react accordingly to remote commands which are sent across to the bot-master. Remotely controlled hosts are prevalent across the Internet and are used for a wide range of attacks. These would include DDoS attacks, theft of user/corporate information and the ability to send a large number of spam messages with the aim of making a profit.

The month of August has seen a sudden surge of infected files which are being distributed by making use known popular services such as Rapidshare and Dropbox. The links are distributed using various Internet forums and social networking sites. However, it is not just Rapidshare that is affected, other file hosting services such as mediafire.com, megaupload.com, filefactory.com and the likes are being taken advantage of to help spread malware. The files that get distributed are often software that come repacked with malware – which could either be in the form of an infected keygen or could be embedded within the application. Therefore users who are looking for something free are highly likely to get infected. Users should not be intimidated with such offers even if they come from well known sites such as Rapidshare and Mediafire.

Phishing websites are also another aspect that hackers set up to lure unsuspecting

users into entering sensitive information such as banking credentials and credit card numbers. These sites look and feel the same way as that of the original along with a domain name that sounds similar. But when it comes to targeting a wider array of users, complex infrastructures are required by hackers to be able to collect stolen information, distribute malware, launch social engineering attacks and host a number of malicious pages which are used to phish out personal information.

The use of domain names allow malware writers to deal with the complexity of large distributed infrastructure. DNS provides flexibility to change IP addresses of malware ridden servers. Moreover, critical servers can be hidden behind proxy services making malicious servers more difficult to key out and take down.



Disclaimer

The above report is based on malware URL collected between 1st January 2011 & 31st June 2011 and is a representation of the growth in malware infected URLs in the span of 6 months. 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