‘e Scan

Malware Report

(October 2011)

E-mail: marketing@escanav.com

Web site: www.escanav.com

INDEX

Malware Report

Wars are not fought with firepower - it's all about possessing the right resources. Resources such as money and knowledge that will help build the ultimate online security threat. Digital warfare is what we see cybercrime slowly but effectively transcending into. And why not? Ever since information has turned digital, data has never been easier to get hold of. Think about it - there used to be a time when hackers used to hack just for recognition. Come to think of it, cybercrime wasn't even a word that was used to link hackers. But if you compare it with the current trending scenario, we will notice a drastic change within the hacking community. Over the years targeted attacks have grown significantly where corporate organizations have had to beef up their current security solutions to thwart web based attacks. Having said that, there are still instances where organizations get pawned or owned by hackers. Question is – would you hold employees responsible for the spreading of infection? With the widespread increase of fraudulent, malicious and scamming sites, it is inevitable for every employee within the organization to understand this growing threat. The question that needs to be answered here is – can you trust an employee to not visit a website that has been compromised and infected by malware? To be precise, 99% of the infections that occur within organizations happen due to inadequate security solutions in place. It's just not email security that needs to be taken care of but securing an employee's browsing habits is just as important.

Among Small and Medium Businesses it is said, close to 40% suffered from a security breach due to bad surfing habits. This basically resulted in navigating to websites that were home to malware, malicious downloads that might have been corrupted by malicious code. The aspect that needs to be understood is that the Internet is more like a hive for malware and cybercriminals are always on the hunt to fish out unsuspecting users. What remains a worrying concern is the fact that a handful of organizations are not implementing the needed precautions that would prevent employees from clicking a malicious link or even browse unwanted sites.

According to research held by CSIS (Center for Strategic and International Studies), it is seen even in the event of infections, a number of users who use web monitoring software do not take into account the importance of considering their network as the main vector for deploying the necessary solution or policies. Over 52% of SMBs state that it isn't in their top priority list to set up a perimeter against web threats. Statistically speaking, a total of 24% of IT Administrators who did consider setting up a perimeter deployed it mainly to enforce employee productivity while 15% used policies to maintain the overall speed of the network and just 13% used policies to forbid employees from accessing illegitimate sites. However, the question that still needs to be answered is – are these reasons valid enough for organizations to use just a web monitoring software? Doesn't security play a major role?

The results however, clearly show the overall lack of awareness of what web monitoring software is capable of. Securing the network or endpoints from malicious downloads, websites or even endpoints such as USB ports should be of top priority. Probably superseding concerns such as bandwidth management and employee productivity. The survey also found a high number of organizations that didn't consider using filtering or even a web monitoring software. With the increasing number of threats this becomes a major concern as company as well as user information can easily be siphoned off without knowledge.

What needs to be looked into here is – a proper deployment of web monitoring software that co-exists with a robust security suite which provides an additional layer of defense against web threats. The need to secure an employee from accessing malicious or illegitimate sites will definitely go a long way for SMBs in maintaining a proper balance that would more or less nullify the overall risks an employee creates when accessing the World Wide Web.

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

We have all heard of the infamous Stuxnet (Malware), however, the current star of the month is none other than the recently discovered Duqu. Believed to be closely related to the Stuxnet worm from which it borrows code and functionality. The Trojan is specifically designed for data exfiltration. But unlike its elder sibling, Duqu comes with no payload. It's built with only one motive – to gather and send back information to its command and control centers. It goes beyond a doubt that this particular virus was developed by a bunch of knowledgeable hackers to help lay the ground work. Studies show that attacks were mainly carried out on power plants, oil refineries and pipelines. It is not only the US, Iran, Sudan and Europe that is being targeted to host malware but India is slowly becoming a breeding ground for malware authors. The very fact that Indian servers were used to collect information from machines infected with Duqu goes on to show the overall vulnerability of servers hosted in India. What most SMBs need is a strong line of defense that will not only help in monitoring employee productivity but will help secure endpoints thereby preventing complex malware such as Duqu from spreading.

As the saying goes – everything that has a beginning has an end. The lifespan of Duqu will be short-lived, as seen with all malware, probably weeks or a couple of months till it gets overthrown by yet more effective and dangerous malware.

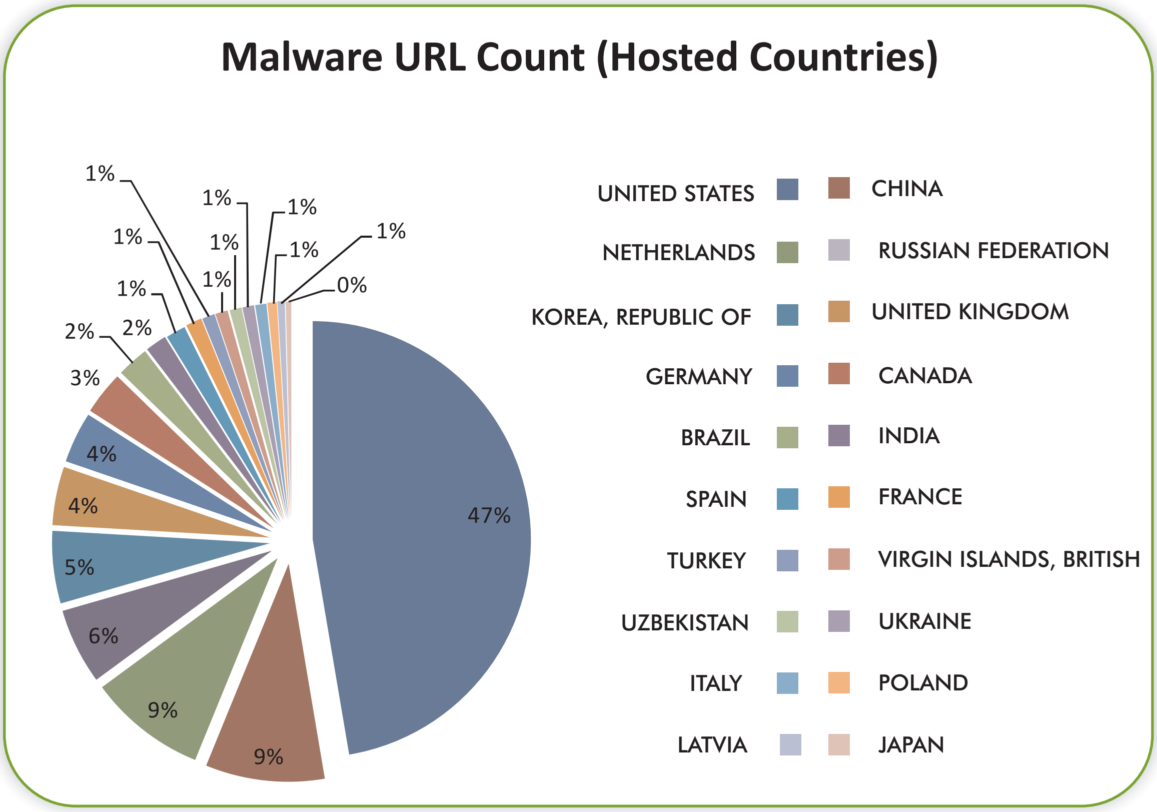
Before Duqu a vast number of threats claimed top spot to be the most advanced, dangerous and pervasive malware in the wild. It is like a game malware writers have played with users and the entire AV industry to get noticed. It was in 2010 that the world saw the rise of one of the most sophisticated and advanced malware – malware that was designed to hinder the normal workflow of nuclear power plants. Irrespective of this, sophisticated malware has also been used to infect end users. 2008 saw the rise of Koobface – a sophisticated malware that used social networking sites such as Facebook, Twitter and Hi5 to spread. Once infected, users would be used as pawns to infect other users within their contact lists.

However, if you turn back the clock to 2004 – you did probably remember the effects of the MyDoom worm. A rapidly spreading mass mailer worm used for sending unsolicited mails via other infected PCs. 1999 on the other hand brought in a game changer named Melissa – a mass mailing macro virus – that overloaded the Internet mail system to such an extent that it almost brought it to a point of shutdown. The worm spread using vulnerability within Microsoft's Word document. With that said, the early 90s saw a change in the detection behavior of most Antiviruses. Signature based scanning was replaced with more advanced detection technologies such as heuristics and sandboxing. Again, it was due to a specific malware that brought this significant change – a malware that was able to alter its internal coding after each infection. This method successfully evaded detection by tricking known AV scanners.

As news would have it, the talks on a massive bot army being formed were nothing more than a passing phase. Experts as well as tech journalists believed that this army was being built to cripple the worldwide web. The point that needs to be seeded into the minds of users and other IT experts is the fact that the Internet will not face a shutdown. Why? Here is why – First and foremost the malware industry is a multibillion dollar business where revenue is generated via millions of infected PCs. Now imagine shutting or bringing down the Internet – with no Internet access where would the revenue come from? How will credit cards or even user (includes the corporate world) details be siphoned off? It therefore goes without saying that crippling the Internet is not an option for cyber criminals.

Malware URL Count (Hosted Countries)

According to a report released by Microsoft Security Intelligence, India has witnessed a sudden rise in contaminations from viruses. The sudden increase has increased India's contribution to the amount of spambots globally in the last month. According to statistics infections spread using worms and Trojans accounted for 38% and 34% of all detections, making it the most common while Adware hung on at a moderate level. A total of 25% accounted for general virus contaminations while spyware infections were more than negligible to overlook.
The report also stated the overall number



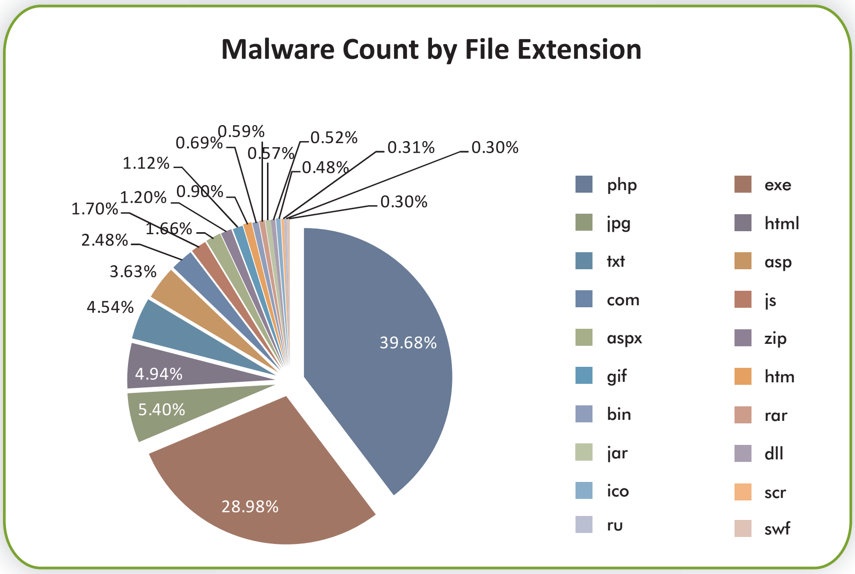
of PCs sanitized for every 1,000 touched 16%, highlighting an increase in contaminations rates as compared to 15% during the third quarter. This increase not only points to the number of un-patched applications but also takes into account the number of users not using authentic software, inefficient anti-virus and rather weak passwords. While there are several methods that can be used to spread malware, the Autorun virus is still the most widely used. In addition to the mentioned, malware ridden websites are commonly used to trace user activity. This in turn not only allows hackers to carry out phishing assaults but it also helps them spread malware via sites that come across as genuine.

Malware Count by File Extension

In a rather strange turn in events German officials or the law enforcement agencies, to be precise, were found making use of malware that was used to monitor activities of local citizens. The discovery was made by a Europe's largest hackers club called – Chaos Computer Club (CCC). Evidence of the malware was found when a German lawyer gave a clients laptop for examination. It has been noted that the detected malware can not only siphon intimate data but can also provide remote accessibility or backdoor functionality to upload and execute arbitrary programs. Significant design and implementation flaws make it easily available to anyone on the Internet – a major aspect to be concerned about.

Dubbed as the "State Trojan" or "R2D2" – the malware is capable of intercepting Skype, Yahoo and MSN messenger communications. If that was not enough, the malware is also capable of logging browser keystrokes, screenshots and can be updated remotely – according to CCC. In retrospect, the malware can also be used to plant and also delete files on the targeted computer. The malware comes with security flaws that not only opens up the infected machine to outside attacks but also puts the law enforcement agency into great risk.

According to CCC, all recorded screenshots and audio files are encrypted in an incompetent way and it not only ends there. All commands sent to the Trojan lie completely unencrypted. Their recent post goes on to say, 'Neither the commands to the Trojan nor its replies are authenticated or have their integrity protected. Not only can unauthorized third parties assume control of the infected system, but even attackers with mediocre skill level can intercept already established connections by authorities, claim to be a specific instance of the Trojan, and upload fake data. It is even conceivable that the law enforcement agencies IT infrastructure could be attacked through this channel.' – CNET



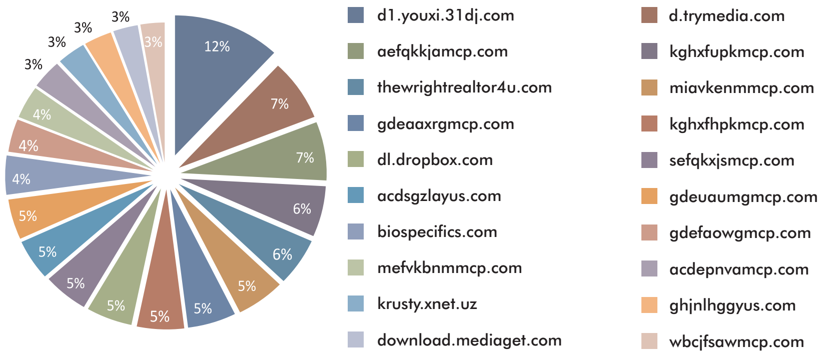
With respect to the reading in September, there has been a decrease in PHP (4%) and executable malware (6%). However, vulnerabilities continue to play a significant part in spreading malware. Many malware campaigns carried out have been successful and the rate of infection is directly proportional to the number of malware mailed. In other words, greater the number of malware emailed higher will be the number of infections. A number of malware have been detected in the past, namely Sasfis, SpyEye, Zeus, Fake Antivirus along with others. In almost all cases the malware first contacts the command and control servers, which then downloads a number of other malicious files which are then executed on the infected machine.

Domain Wise Malware Hosting

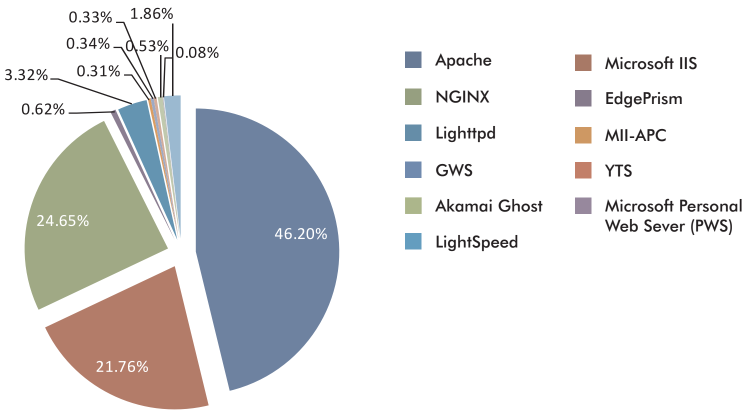
Botnets have always been used to send high volumes of spam. Technically speaking, the distribution of malware was aimed to increase the number of spam mails. However this is not the case now as the last couple of months clearly depict a decreasing trend in the number of spam being sent out. However, there are a handful of other ways for botnets to operate. These would clearly include – large scale banking fraud, account theft of email and social networking sites, Distributed Denial of Service (DDOS) – to name a few.

- Courier (UPS, Fedex, DHL) package notifications – package notification that is due or help up, with details attached within the mail
- Hotel charge error – incorrect hotel bill that would need to be corrected by opening the attached document.
- The “map of love” – promising juicy information about global sites of “interest” in the attached map.
- Credit card errors – an incorrect credit transaction needs to be reversed with more details in the attached.
- HP scanner doc – a document scanned on the office scanner has been delivered
- Inter-company invoice – includes a confusing message about an attached invoice.
- NACHA errors – an inter-banking transaction has been rejected. The reasons for the rejection are in the attached document.

Domain Wise Malware Hosting



Vulnerable Web Servers



Various instances that are used for tricking users into opening attachments would include:

Pharmacy spammers tend to use direct emails which explicitly state the types of medicines being offered. Even with most spams that end up within the junk email folders, there are a selective few who would still be interested in opening such mails. With that said, Facebook continues to draw attention of malware writers. The month of October saw a series of campaigns or so called scams that were spread as events with catchy titles-

- First 40,000 participants get an iPhone free
- First 30,000 that signup get a free pair of Beats by Dre headphones
- First 2,000 participants to like this page will get a Facebook Phone free
- First 20,000 participants will get a free Facebook shoe

Disclaimer

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