‘e Scan

Malware Report

(December 2011)

E-mail: marketing@escanav.com

Web site: www.escanav.com

INDEX

Malware Report

The threat landscape is exploding by the numbers – be it with enterprise security, desktop security or even the mobile space. And as the year comes to a close, 2011 will easily be remembered as the year of the malware. While there has been innumerable number of incidents that made 2011 there isn't enough room to cover all. However, what we have covered are incidents or events that shook the corporate world.

1. The Year of the Data Breach

From Epsilon to RSA Security SecurID to Sony, we have witnessed a change in the security landscape. Cyber criminals are now targeting organizations that hold data for millions of customers. In all known cases, cyber-criminals targeted and attacked most well known high ranking organizations in order to gain access to personal information which could further lead to a broader scope of employee and consumer attacks – also known as spear phishing. All said and done 2011 will be known as the worst year for data breach incidents.

2. Mobile Malware

With Smartphone's (namely Google's Android OS) coming into play, it was only a matter of time before the security industry witnessed a rapid rise in malicious software. This kind of malware has slowly but effectively crawled into unofficial Android marketplaces where existing good apps are repurposed and uploaded as bad ones. Once downloaded and installed, cyber criminals can essentially gain full rights over the infected phone, allowing access to any information shared which can amount to emails, text messages, bank login information, etc. And this can be done without the knowledge of the mobile phone owner.

3. Social Media as a Platform for Cyber Criminals

Social Media is not only growing amongst end users but cyber criminals are using this as a medium to promote and coordinate their efforts. For example, June's Operation Anti-Security, a joint effort by LulzSec and Anonymous, was tweeted by the minute which involved cyber attacks on the FBI and various other security agencies.

4. Malware Takedown

Public-private partnerships have resulted in the takedown of numerous online criminal networks. Take for example, the FBI's involvement with various private sector entities on November 8th aptly called Operation Ghost Click, was one of the largest coordinated cyber-takedown efforts. Their whole operation was solely directed to bring down a malware called DNSChanger – which was believed to have infected over 4 million machines in over 100 countries. With that said, the month of September also saw the fall of a well known botnet named Kelihos. The botnet reportedly consisted of a network of 41,000 infected computers capable of sending billions of spam emails per day.

5. Attacks on Domain Registrars

Criminals are publicly stating that foiled cyber attacks have prompted them to turn to targeting the "domain name company," otherwise known as a registrar. For example, hijacking of ups.com, theregister.co.uk and other major Internet properties in September, cybercriminals targeted their registrars to indirectly hijack the domains. By targeting the registrar, cybercriminals have access to their original target through this extended enterprise connection that is often overlooked. And in the case of a domain hijacking, that means complete control of the targeted organization's Web presence, email, and Internet-based transactions.

6. Targeted Attacks

Malware is no longer being used just for the thrill of hacking, or as a means of siphoning off credit card numbers. Criminals are purposefully targeting enterprises in order to gain access to proprietary organizational assets. For instance, the recently discovered Remote Access Trojan "Duqu" was built as a weapon for espionage and targeted attacks against certificate authorities (CAs). By bypassing security measures and gaining access to trusted CAs, cyber criminals can then gain access to vital data from enterprises. Industries previously thought to be well protected from cyber threats, like CAs, have clearly been caught in the criminal crosshairs.

7. SSL Certificate Flaws

The breach of Netherlands-based CA Diginotar in September showed that blind trust placed in SSL (Secure Sockets Layer) encryption certificate providers must be examined. The hack into Diginotar basically shows that even experts in the field of Internet Security can have their proprietary information hijacked just like any other company.

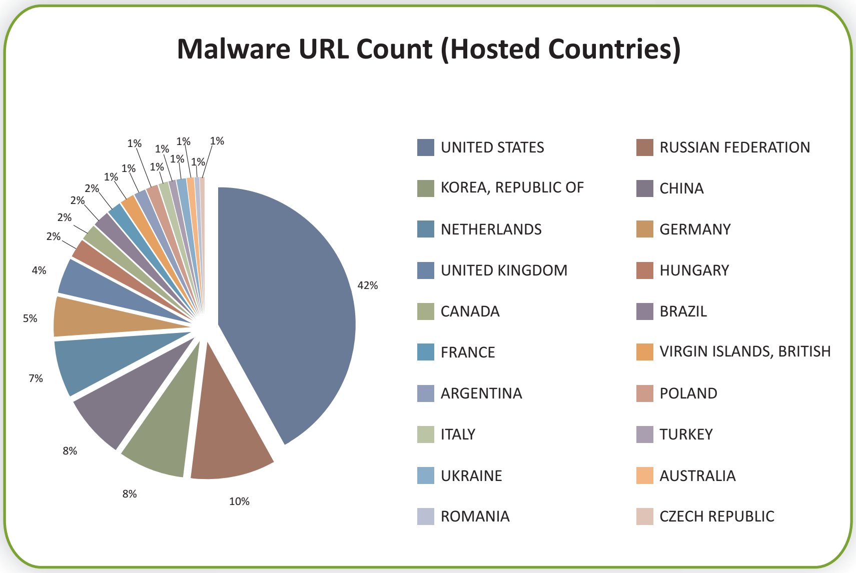
The following report is generated to give you a brief analysis of the overall malware statistics that is prevalent around the world.

Malware Insights

If you take a look at all previous years, you will notice that the shift in malware trend is almost identical. The point that we are trying to nail here is the sharp upward curve we are beginning to see with the passing of each year. With that said, there has been a certain slowdown in certain types of malware. Reasons for this slowdown would definitely point towards the efforts of law enforcement agencies and antivirus vendors along with Microsoft's efforts in clamping down illegal services and cyber criminal gangs. However, there has been a rather high contributing factor, namely rogue AV's that have brought about a number of malicious programs in circulation. What we need to keep in mind is the fact that malware is growing complex by the day and it holds true from year to year. Secondly, browser and application vulnerabilities is used to gain access to various other compromised computers – thereby allowing the same malicious program to be distributed via multiple vulnerabilities, leading to an increase in the number of infections.

Making use of vulnerabilities has become the most used method for penetrating a user's computer. The attacks are performed using various different sets of exploits for various vulnerabilities in browsers and plugins. Adobe exploits were leaders in 2011 in terms of incidents due to vulnerabilities.

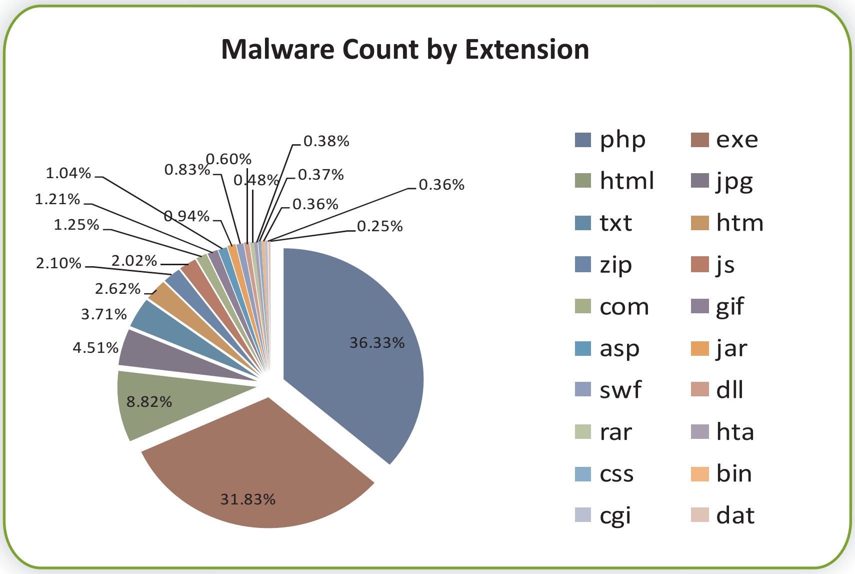
The rate at which malware is progressing it is only fair to say that P2P networks now come in as a major distribution channel for the spreading of malware. However, in terms of infection rate this comes second to browser attacks. The propagation of viruses via P2P is such that it helps spread a number of threats in minimum time. This would include file viruses, Rogue AVs, backdoors and various worms that effectively make use of P2P based networks. Take for instance, the hack on Bit-Torrent and uTorrent sites caused visitors to download malware ridden file sharing software. The malware executes just like any typical fake AV, where it prompts the user for payment before claiming to disinfect the machine. Only users who downloaded and installed the program from bittorrent.com and utorrent.com during the 2 hour

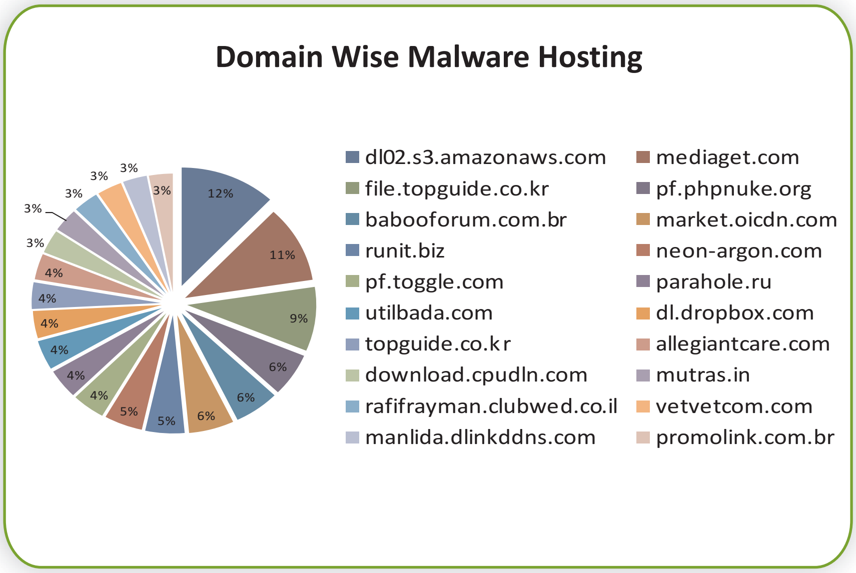


window were compromised. The sudden eruption in P2P based malware is not going to come to a sudden halt and the figures come to a close 4 million for year 2011.

Rise in Complex Malware

High profile attacks have dominated the security landscape in 2011. The result is that other security issues which could pose greater threat to businesses, governments and consumers such as fake anti-virus, search engine poisoning and social networking scams have received far less attention and therefore slipped beneath the radar. With new unique malware threat seen almost every second, it's vital to understand how these new threats work and what exactly is required to build the proper defenses.


Malware Count by Extension


Domain Wise Malware Hosting

Malware attacks are fast becoming the biggest threat to most computer users as fake AV scanners and SEO poisoning are slowly but effectively being used to spread malware. 2011 has seen a massive upward progress in the overall volume of malware while the Web remains to be the most used vector for targeted and mass attacks. SEO poisoning is also on the rise as cybercriminals effectively manipulate the results from Google, Bing and Yahoo to lure web surfers to malicious pages. How is it done? Popular search terms and events that make headlines are used to lure users to malware ridden sites that are home to viruses, worms, Trojans or fake anti-virus software. Search engine poisoning attacks are extremely effective, and account for more than 30 percent of all malware. OSs, applications and browsers have been under constant fire from malware writers and 2012 is not going to be any different.

2011 has also been the year of the Smartphone and we have witnessed a considerable rise in the sale of these devices. So much so that cell phones have become so personal that it comes with features and functions that mimic a personal computer. However, with that said their growing popularity poses new risk within the IT eco-system. Fraudsters have been populating the app stores with malicious software that masquerade as free apps which could either be in the form of a game, general app or even a security app. Once infected the malware allows cyber criminals to make calls, send and receive SMSs to premium numbers, intercept voicemail messages and download/browse online content. In addition personal information and payment data can also be siphoned off, which are then sold to and used by identity thieves.

With that said it is more than obvious that there are a number of users who make use of their Smartphone's to send across personal as well as financial information over the Internet and this definitely doesn't go un-noticed by cyber criminals. Take for instance, the Android Trojan Zitmo that came into being on July 2011 worked in conjunction with the infamous ZeuS malware. Together they allowed cyber criminals to bypass the two-factor authentication systems used by most banks for online transactions.

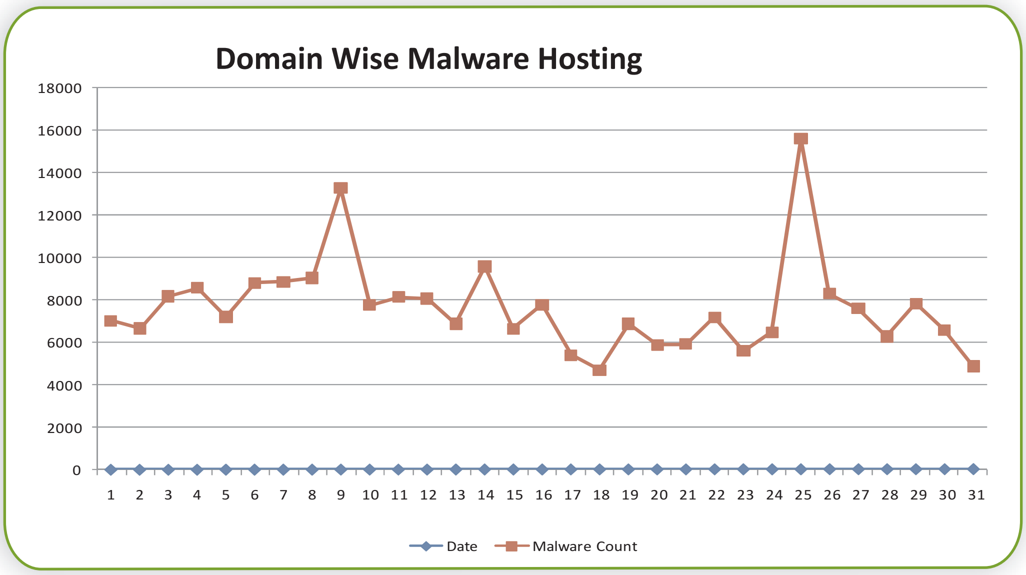
Malicious QR codes are on the rise and are a new technique cyber criminals are using to spread malware. With their growing popularity it is only inevitable for hackers to make use of this. The thing with malicious QR codes is their capability to directly download malware which then sends SMSs to premium numbers.

Accessing the web can be fun and productive by using such devices, but it is equally important to be careful. Here are a few tips to secure your identity from being stolen-

- Download apps only from the official app market
- View all permissions that are required by the app
- Check reviews and ratings of the selected app
- Last but not the least – install an Anti-Virus

Attacks on Corporations and Enterprises

The IT threat evolution has seen a considerable upward swing in the last year. What we have witnessed is a sustained growth in cyber attacks against some of the world's largest corporations. We saw corporate networks attacked which included targets such as the FBI, Italian Cyber Police along with several US police units. Defense contractors such as Mitsubishi Heavy Industries and Vanguard Defense also saw the brunt of malware attacks. These are just a handful number of attacks that shook the corporate world. However, there are



other attacks which allowed cyber criminals to get hold of information pertaining to employee/customer data, company documentation and classified data.

In July 2011, certificate authority servers of DigiNotar and as mentioned above, were hacked which resulted in the creation of 531 rogue certificates. The fake SSL certificates allowed cyber criminals to access data sent to or from those sites even with a secure and encrypted connection. The main resources that were targeted were not only government agencies but online services such as Google, Yahoo!, TOR and Mozilla were also hacked.

It is more than clear that 2011 has been the year of hacks and this trend is just the beginning of things to come. The incidents which took place should serve as a warning for other large corporate players to strengthen their security policies.

●●●●●●

Disclaimer

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