'e Scan

Malware Report

(January 2012)

E-mail: marketing@escanav.com

Web site: www.escanav.com

INDEX

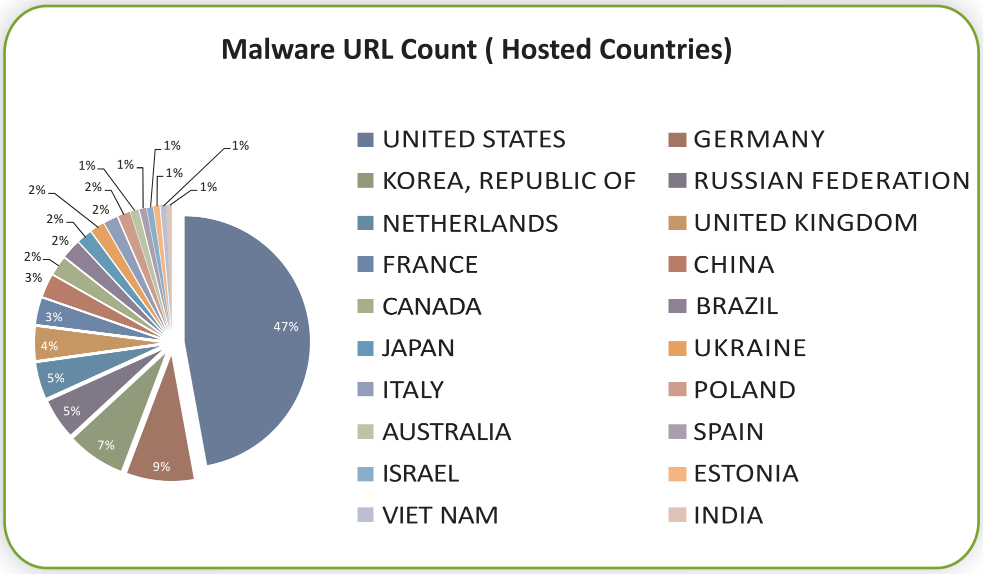
Malware Report

2011 has been an eventful year in the field of malware - though it cannot be termed as eventful for the people who were snipped by hackers. A number of high-ranking officials and enterprises felt the full brunt of cyber criminals. The hacks carried out were not done with the purpose of becoming famous but their sole intention was to create havoc within small and large companies. However, if you do happen to look into a breach it would be surprising to know that there are a handful of companies which don't quite adhere to policies laid down to prevent uncalled for security breaches. Take the example of Sony's PlayStation Network – one of the largest hacks, which involved names, addresses, birthdates and credit card numbers for any of the 77 million customers.

Come to think of it, online malicious activity was a major headache in 2011 and 2012 is not going to be any different. Scammers are targeting social networking sites such as Twitter and Facebook. And, it doesn't only end there – with the sale of Smartphone's hitting a new high (Think: Android OS), the Android Marketplace is exploding with suspicious applications that do more than what they are meant to do. Cyber criminals are figuring out new ways to infect your system – be it your Smartphone or PC. However, the good news is that the latest security suites are designed to do a much better job at detecting and removing malware. Nevertheless, common sense also needs to prevail, as there are times when the best security suites are never enough to protect you from the latest threats. Whether it be a fake Anti-Virus scam, malware using social networks to spread or even e-mail attachments which come loaded with viruses – it pays to be aware of the pages you visit or applications you download as it helps to identify a potential threat. Here is a summation of the top 5 threats which have grown substantially in the last year.

Mobile Threats

It comes as no surprise that mobile devices are the new hot targets by malware writers. With over 90 percent of adults owning a general mobile phone, it is the Smartphone category that is being targeted the most by malware writers, as they are the next big jump in both communication and entertainment. To state facts – more than 50 third-party applications on Google's Android Marketplace were infected with a Trojan named Droid Dream. The Trojan was designed to gain administrative privileges over your phone without the user's permission. That means it could download more malicious programs to your phone without your knowledge and steal data saved on your device. Google was able to stop the DroidDream outbreak by deleting the bad apps from the Market and remotely removing malicious apps from Android users' devices, but it will only be a matter of time before the next outbreak occurs.

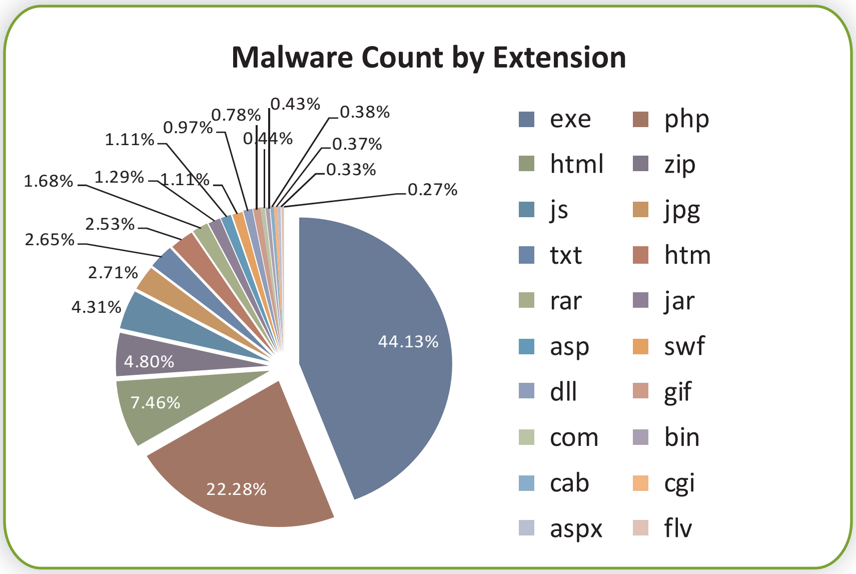

Malware URL Count (Hosted Countries)

Malicious apps on the Android Market are not the only way malware authors can target phones: A recent Android malware outbreak in China spread through repackaged apps distributed on forums and through alternative app markets.
The threat of malware,

coupled with other security threats (such as data leakage from a lost phone) may soon impact your ability to use personal devices at work, according to Andrew Jaquith, Chief Technology Officer of Perimeter E-Security. "Companies may begin to set some serious ground rules for putting company data on personal mobile devices by enforcing policies for passwords, device locking, remote wipe, and hardware encryption", Jaquith says.

Social Network Based Scams

Social networks such as Facebook and Twitter may be a great place to connect with friends, but they are also a breeding ground for malicious activity. Some of the most rapid growth in online attacks comes from social networks. Moreover, at least 20 percent of all Facebook users are active targets of malware.



Social networking scams often take the form of phishing attacks that try to lure you in with photos or videos, and harvest your personal information or Facebook login--or worse, infect your PC with malware--along the way. Often, these links will come from Facebook friends who fall victim to these scams. You could also run across rogue Facebook applications that try to access your Facebook data and that of your friends. While it's probably no big deal if scam artists find out what your favorite movies or quotes are, it's your profile that contains critical data -- such as your date or place of birth, cell phone number, and e-mail address —all of which that can be used to build a fake profile about you and even steal your identity. Such bits of information can supposedly be the final data point a bad actor needs to impersonate you online.

You could even become a specific target for criminals through social networks. In September, three young men ran a burglary ring in Nashua, New Hampshire, by looking at Facebook postings about people going out and then targeting homes they believed were likely to be empty. Police said they recovered over $100,000 in stolen property after cracking the ring – according to a news channel in New Hampshire.

Fake Anti-Virus:

Although they have been around for a few years now, fake Anti-Virus scams are on the rise. In the last eight months, there have been more than 850,000 instances of fake Anti-Virus. Also known as 'scareware', these scams start by convincing you to download a free Anti-Virus program, sometimes appearing to be software from a reputable security company. Then the software claims your computer is under threat from a virus and you can save your system by buying a full version of the Anti-Virus program for a one-time fee.

Once that is done, you have not only allowed more potential malware onto your computer but you have in fact handed over your credit card credentials to identity thieves. From this point on, the rogues are capable of draining your bank account and are even capable of faking you online.

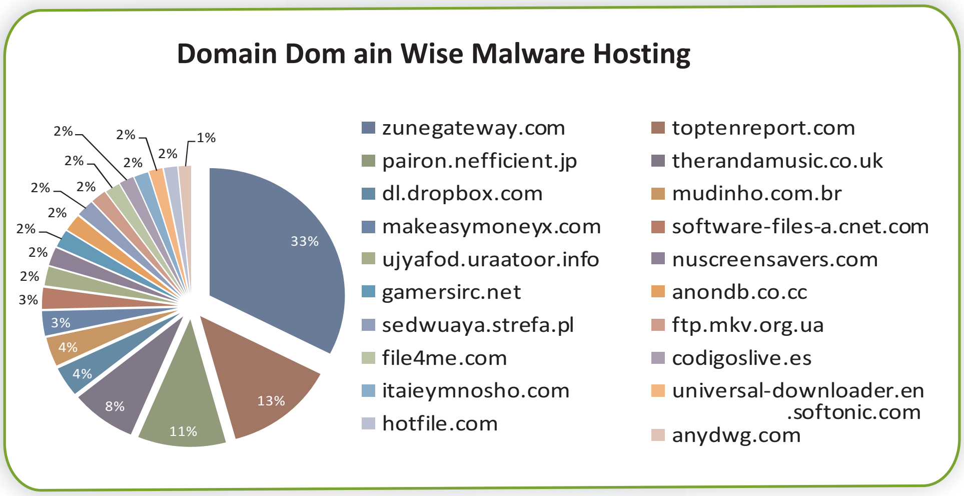
The irony of all this, is that the success of these scams are helping us become more aware of computer security and since we find the need to protect ourselves to a great extent from malware threats, we easily get lured by software promising enhanced security. The downside, however, is that we tend to panic when we come across pop-ups that state an infection on the PC.

PDF

Clearly, the oldest and the most versatile scam of the lot – malicious PDF attachment is still considered to be a big problem even with the high degree of awareness. They have even been successful in bypassing robust Anti-Virus scanning clients such as Gmail and Yahoo mail. Millions of malware related e-mails are sent every day and they are not about Viagra or fake degrees, but are turning malicious in nature. PDF documents appear to be a prime method for these attacks. PDFs are potentially one of the most dangerous file formats available and should be treated with caution because it is significantly easier to generate legitimate and concealed malicious content with PDFs.

2011 itself accounted for 65 percent of targeted e-mail attacks, which used PDFs containing malware – a 12.4 percent rise when compared to 2010. According to statistics, at least 80 percent of targeted malware attacks could be using PDFs as their primary method of intrusion.

Domain Dom ain Wise Malware Hosting



Sponsored Attacks

State-sponsored malware attacks, industrial espionage, and hacktivism are on the rise, according to Perimeter E-Security's Jaquith. They may not be considered as a threat for individual users, but if you manage security for a business, they are the sorts of issues you should be paying attention to.

Take for example the hacktivist group

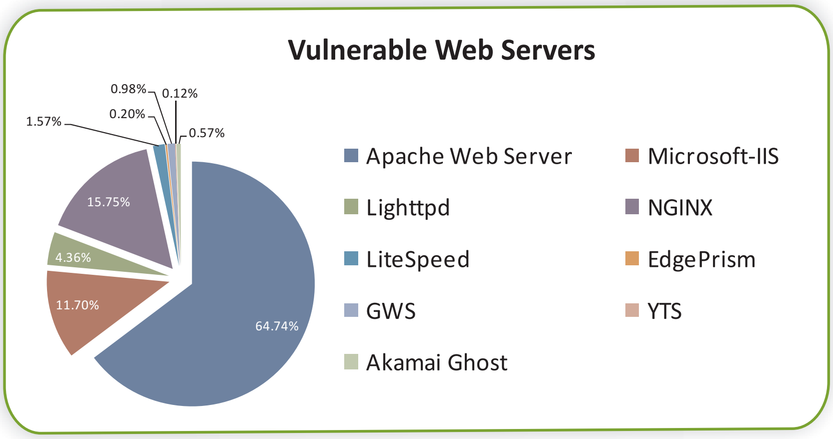
Anonymous, grabbed headlines last year for mounting attacks in defense of whistle-blower site WikiLeaks, and attacking government Websites in support of recent protests in Egypt, Tunisia, and Libya. The group also leaked a cache of e-mail messages from a security researcher who was trying to identify Anonymous members. Whether it is WikiLeaks, Anonymous, or a Chinese or Russian attacker, theft of industrial secrets is shaping up to be one of the key issues in 2012.

Growing threat to Security

Security – An essential aspect of the IT ecosystem - a necessity for any business to survive the onslaught of malicious codes patrolling the World Wide Web. All it takes is a miniscule error to bring down small and large enterprises – leaving them drowning in financial loses. Come to think of it, security cannot be considered as an option as it comes in as a building block that will help your business to survive web based threats.

What is the biggest and growing threat to Businesses?

To be precise, no threat is small enough to be taken lightly. It could be in the form of an eMail Spoof or Denial-of-Service Attack or even a Packet Sniffer – all of which can lead to a loss in data. However, what seems to be inching its way into the corporate world would be the rise on social engineering attacks. There are a number of tactics that could be played out when carrying out a socially engineered attack. Given below are a mentioned few –



Pretexting – An act of creating and using an invented scenario to engage a targeted victim in a manner that increases the chance the victim will divulge information or perform actions that would be unlikely in ordinary circumstances

Phishing – A technique of fraudulently obtaining private information. Typically, the phisher sends an e-mail that appears to come from a legitimate business—a bank, or credit card company—requesting 'verification' of information. The e-mail usually contains a link to a fraudulent web page that seems legitimate—with company logos and content—and has a form requesting everything from a home address to an ATM card's PIN.

Baiting – Baiting is like the real-world Trojan Horse that uses physical media and relies on the curiosity or greed of the victim. In this attack, the attacker leaves a malware infected floppy disk, CD ROM, or USB flash drive in a location sure to be found (bathroom, elevator, sidewalk, parking lot), gives it a legitimate looking and curiosity label, and simply waits for the victim to use the device.

Attacks such as Man-in-the-Browser (MITB) will see a rise in the coming years. MITB based attacks are designed to infect web browsers, which result in the modification of web pages. An attack such as this could lead to illegal money transfer, identity theft or could be used to compromise valuable enterprise information.

Disclaimer

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