'e Scan

Malware Report

(November 2011)

E-mail: marketing@escanav.com

Web site: www.escanav.com

INDEX

Malware Report

Our last month's report covered a number of incidents while also providing key highlights on the growth of malware through the years. The one incident that made headlines was use of malware by German law enforcement agencies. Having said that, the current month has a lot to be wary about. With Christmas and the holiday season drawing closer by the day hackers/cybercriminals would be on the hunt to fish out unsuspecting users. But before we get into the highlights of the events for the month of November, let's shed some light on what enterprises need to do to stay secure.

To start with, a whole lot of aspects need to be looked into before a proper deployment is put in place; it could be anything from overall costs to meeting policies laid down by various operating heads. But even with a number of policies deployed across the network, why do large corporations lose millions year after year? What companies lack is a proper enforcement of policies where all connected users need to adhere to certain rules laid down by the IT admin. Protection of Information and Information Systems from unauthorized access/modification, disruption of services or destruction/theft of intellectual property is basically what broadly defines the term Information Security. Moreover, the term greatly surrounds the goal of protecting the confidentiality, integrity and availability of information – be it electronic, print or any other form it translates into. As a breach could amount to anything from loss of personal data to loss of business and its reputation – be it with end users, institutions (educational or financial), governments, defense, hospitals or private businesses. Therefore, securing information is not only a business requirement but also a personal necessity.

It goes without saying that there has been a sharp increase in cybercrime in the last few years. With hackers taking advantage of various vulnerabilities within Windows OS's and third party applications, it goes to show the extent to which malware can be created. While the impact of the Stuxnet malware is old news – there have been bigger instances where enterprises have lost millions. Take for instance Duqu – a malware that was specifically designed for data exfiltration. This particular malware came with no payload and was built with just one motive – to gather and send back information to its command and control centers. Studies show that attacks are mainly carried out on power plants, oil refineries and pipelines. With that said, 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.

If you look at large Enterprises and MNCs of today, you get to see that a great deal of attention is given in protecting the company's electronic assets (mostly from) outside threats. From intrusion prevention systems to vulnerability management – while the mentioned few are what most companies implement – the aspect that needs to be addressed are the access rights that are deployed within the company. Email, instant messaging, webmail, website surfing or even file transfers, electronic communications exiting the company apparently go largely uncontrolled and unmonitored – with the potential of confidential data falling into the wrong hands. However, should there be a breach in information; it could create havoc within the organization through fines, bad publicity, loss of strategic customers, loss of competitive intelligence and legal action. Thereby, looking into today's scenario and competitive environment, data loss prevention is one of the most critical issues that are being faced by large companies.

Before even getting into employee rights, companies need to develop a thorough understanding and should break down the various types of sensitive data that exist within the organization. This would give a better view of the policies required to control and strategically enforce the kind of data that is needed to be shared.

Having said that, it is critical for companies to understand the kind of security policies that need to be deployed not only organization wide but to break them down individually as per users, departments and remote offices are also of importance. While the need to determine relevant areas that need to be protected, organizations also need to look into the impact the deployed policy has on workflow. This ensures that the solution implemented is by far dynamic and flexible enough to meet the ever changing workflow and processes.

The following report is generated to give you a brief analysis of the overall malware statistics that is prevalent around the world. Having said that, we have taken a different approach towards this month's malware report. With the holiday season coming in, the month of November will see a number of users shopping online. November is also the month where we see a number of online phishing sites coming alive along with credit card fraud. To help you get a better understanding we have spoken about certain aspects that you need to look out for this December. In addition, the report also provides an insight of online threats users can expect towards the coming year - 2012.

The statistical graphs provided are purely based on the month of November.

Malware Insights

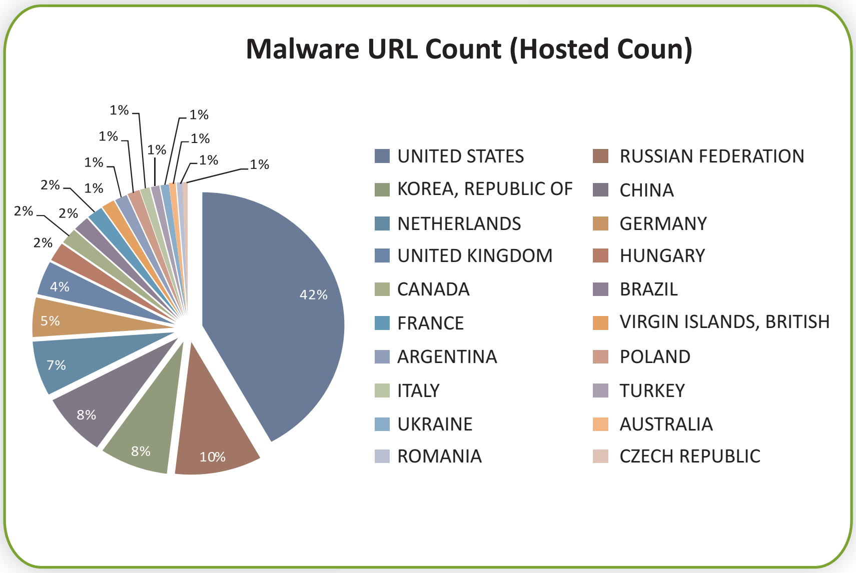
November by far is the most awaited month of the year – not only for online shoppers but for hackers too. It is also a month which sees the maximum number of online transactions. Here is what you can expect to see during this holiday season:

Malicious Mobile Apps:

With Google's Android OS getting famous by the day we are slowly beginning to see a number of malicious applications running amok within the Android Marketplace. Little do people know that a handful of apps are designed to steal user information without his/her knowledge. What users fail to see is the security permissions these free apps ask for.

Fake Facebook Contests & Promotions:

Free is the word that attracts a number of users. Who wouldn't want something free, especially during the holidays? Unfortunately, scammers have been around long enough to know exactly what attracts users. With millions of inter-connected users in Facebook the probability of spreading malware using this medium is very high. Scams such as free Facebook shoe or free airline tickets sounds extremely appealing at this time of the year – where participants are requested to fill out personal information.



Fake Anti-Virus Software:

2011 has seen a rise of a handful of fake Antiviruses. Some so well designed that it would be difficult for an untrained eye to notice the difference. Their main aim is to trick the user into believing that the computer is at risk or is already infected. Once installed, these rogue apps download more malware from predefined command and control centers. They are also regarded as the most common and dangerous threats on the Internet today; with an estimated rate of infection that's close to a million users per day.

Holiday Phishing Scam:

Holiday phishing scam such as the fake notice from UPS has become one of the most common. The form may ask for personal and financial details that go straight into the hands of the scammer. Another growing area is Smishing (phishing by text messages). Fake text messages are sent to unsuspecting consumers stating that his bank account has been compromised. The unsuspecting user is then directed to call a phone number where the user's personal information is taken.

Online coupon scams and offers:

The holiday seasons are always rife with attractive online offers – but let's not forget eye popping offers come in as malicious ones too. Scammers know that by offering irresistible online offers they can get a number of people to hand over personal information. One popular way of luring consumers are done by giving them the hope of winning something totally free – say a tablet such as the iPad for instance. Online coupon codes are another instances where, if they agree, they are asked to provide personal information which can include credit card details, passwords and financial data too.

Hotel "wrong transaction" malware emails:

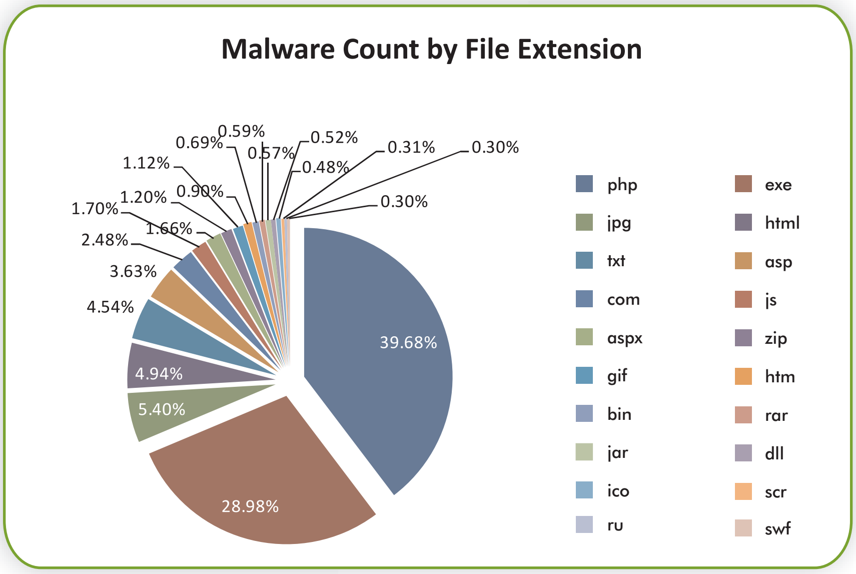
Malicious emails in the form of hotel transactions have been cropping up lately. Scammers send out emails claiming that a wrong transaction had been discovered on the recipients credit card which then asks them to fill out a refund form that is attached to the mail. However, when opened the attachment downloads malware onto the user's machine.

Mac malware:

These words never made sense if you look back a couple of years. But with the growing popularity of Apple products, cyber criminals have designed a new wave of malware targeted solely at Mac users. A year back there were approximately 5000 pieces of malware code produced for Macs and with the passing year this number is increasing at approximately 10 percent by the month.

Malware Trend - 2012

The trends that were set in 2011 wholly suggest that security threats are fast becoming more targeted and personal. Hackers are switching to social engineering and data mining to carry out attacks not only against important individuals but also their corporate networks. Let's not forget to mention that the growth of such threats have in fact brought about advances in network protection and tighter security regulation which have just about made it more difficult for hackers to disrupt and compromise systems. Social engineering attacks are fast becoming the chosen line of attack as the yield all the necessary data that basically help to carry out highly organized systematic attacks while the use



of traditional techniques such as SQL injection, web app hijacking and unauthorized server access are slowly taking a back seat.

Security Trends to Watch Out for in 2012

Security breaches are no more about bypassing protocols laid down by the IT Administrator but it has grown more user specific in nature. Social Engineering is fast becoming the attack vector for Advanced Persistent Threats (APTs) as cybercriminals are beginning to gain data directly from the user itself. This is achieved by forcing them into giving vital information by making them click on email attachments or web links.

Expectation:

We shall see further examples of socially engineered attacks that are combined with zero day exploits in the coming years. Couple of famous incidents that took place would be the one against RSA and its client base, Operation Aurora and GMail.

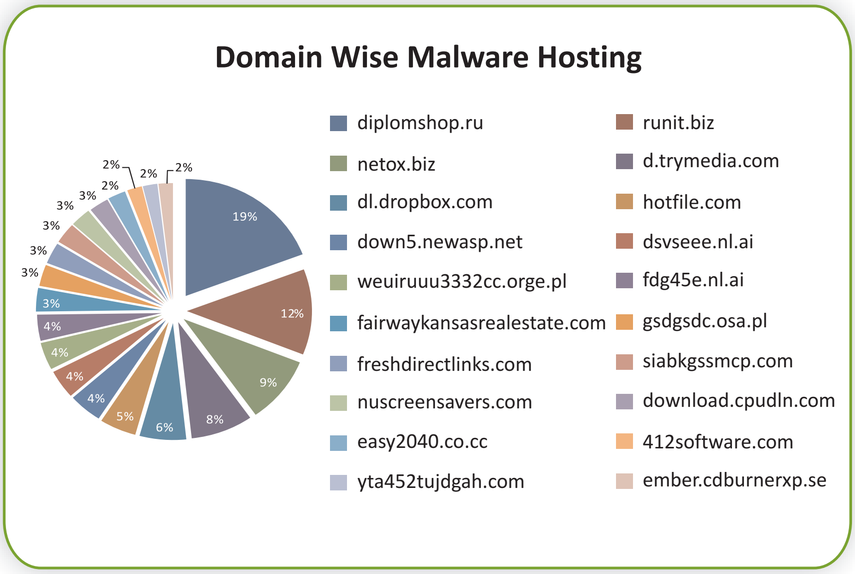
Prevention:

Staff training and regulated courses are important to ensure employee productivity. Moreover, security processes maybe looked as a damper for everyday working processes – therefore IT Admins will need to ensure that the deployed procedures are not only tailored made to fit the ever growing business needs but should also prevent users from evading deployed security policies.

Data Theft:

With the launch of social networking sites, users are now connected to a wider range of users which would transcend from email to social networking sites (Facebook, Twitter & LinkedIn) to forums and sites that are interactive. Their importance will only increase with time as they provide a larger and wider networking base to work on at an extremely cost effective rate.

Contactless payment such as the Google Wallet or even phones that implement Near Field Communication (NFC) is also going to see a rise, not only in usage but we shall also see a rise in vulnerabilities that compromise the use of wireless technologies.



Domain Wise Malware Hosting

Expectation:

There will be an increase in identity theft using social media sites where hackers will more than willingly try to crack passwords and find ways to hack into particular networks. Other aspects where data theft can happen are via Radio Frequency Identification (RFID) and Cell Phones as they provide a major chunk of user information. We shall see an increase in voice mail hacking or intercepting calls.

Prevention:

With the current progress in technology the divide between work and leisure has taken a back seat.

Users need to be briefed on how to protect their anonymity on social networking sites by providing clear guidelines on usage within the work premises.

Device issues:
There has been a growing number of users switching to Smartphones and Tablets. And just a handful of enterprises have gone the extra mile to implement policies which enable them to monitor authentication and file transfers. However, issues such as shoulder surfing are rarely addressed. This not only is the case for portables but desktop environments too. With the latest products incorporating super clear and AMOLED screens, it makes them more than easy to read log-in and other personal details in public locations from various angles.

Expectation:
We will see a rise in theft as hackers record log-in details and observe transactions and then try to replicate these.

Prevention: Reconfigure network access for remote and wireless connections. Implement control through regular password renewal, two factor authentication. Carry out IT auditing, penetration testing and review role based access privileges.

SSL Certificates and Cloud Issues:
2011 did see attacks against SSL certificate authorities. The general use of web certificates is to authenticate computers over web servers which also include online browsers. Despite their claims of being secure, the certificates were easily compromised. Having said that, the coming year can see a rise in Advanced Persistent Threats (APTs) targeting data in the cloud.

Prevention:
We need to make it a point that only non-sensitive data is stored in the cloud while sensitive information is stored offline or on a separate network drive. Guidelines should also be laid out on the usage of data when on the cloud infrastructure.

What to Expect This December

The Internet offers users the convenience to shop from the comfort of your home. Moreover, the web also provides the option to search for items from countless vendors, make price comparisons and purchases with just a few mouse clicks – eliminating the need to wait in long queues. Having said that, the Internet is also home to hackers, giving them multiple ways to access personal and financial information.

What are the aspects Hackers look for when targeting online shoppers?
There are three common ways attackers use to take advantage of online shoppers:

Intercepting vulnerable computers:
Your computer becomes vulnerable when you do not take the necessary steps to protect your PC from viruses and malicious code – allowing attackers to gain access not only to your computer but also personal/private information. The same rules apply to vendors to protect their computers from external attacks; the need to block hackers from gaining access to customer data is vital.

Creation of fraudulent sites and email messages:
Unlike traditional shopping malls, where you know that a store is actually what it claims to be, attackers can create malicious websites that appear to be legitimate or can even fake email messages that appear to have been sent from a legitimate source. Breaking

incidents such as natural disasters or even special offers during holiday seasons are also eyed on by hackers. The sites are created to basically convince the user to supply personal and financial information.

Intercepting Online Transactions:
Irrespective if you are a vendor or user, if your connection between you and the Web is transmitted in an unencrypted format, an attacker will easily be able to intercept information that gets transferred.

How to Protect Yourself?

It is highly important for users to have an anti-virus and firewall installed. The use of protection software helps secure your PC against viruses and Trojans that can steal or modify data that would essentially leave your PC vulnerable to other web threats. Another very important aspect that needs to be updated on a regular basis is the web browser as it is the first aspect hackers look into to penetrate systems. Apply operating system updates as they block hackers from taking advantage of known vulnerabilities (enable automatic updates).

Evaluate the Settings of Installed Software:
Software's mostly take their default functionality when installed, allowing hackers to take advantage of this. Reason why it is important to check various software settings; especially the ones that connect to the Internet (browsers, email clients, messengers, etc). The best way to go about this is by applying the highest security level available while still maintaining overall functionality.

Evaluate Online Vendors:
Be wary of online vendors. Make sure you are carrying out transactions with reputable and established vendors. The web is infested with malicious websites that appear to be legitimate – so it is important to cross check the website before giving out information. Stolen site certificates are also used to make a malicious site look authentic. It would therefore be wise to review site certificates before carrying out important online transactions.

Defining Passwords and Implementing Security Features:
Passwords and other security features add layers of protection if used appropriately.

Malicious eMails Requesting Personal/Financial Information:
There are a number of ways an attacker can gather personal information. It could be through malicious Word documents, PDFs, Excel sheets – all asking the user to fill them up with personal details. It could come in as a purchase order, wrong hotel transaction, etc. What needs to be noted is that legitimate emails will not ask for such information. Do not give out personal and financial details via email and always check email links before clicking on them.

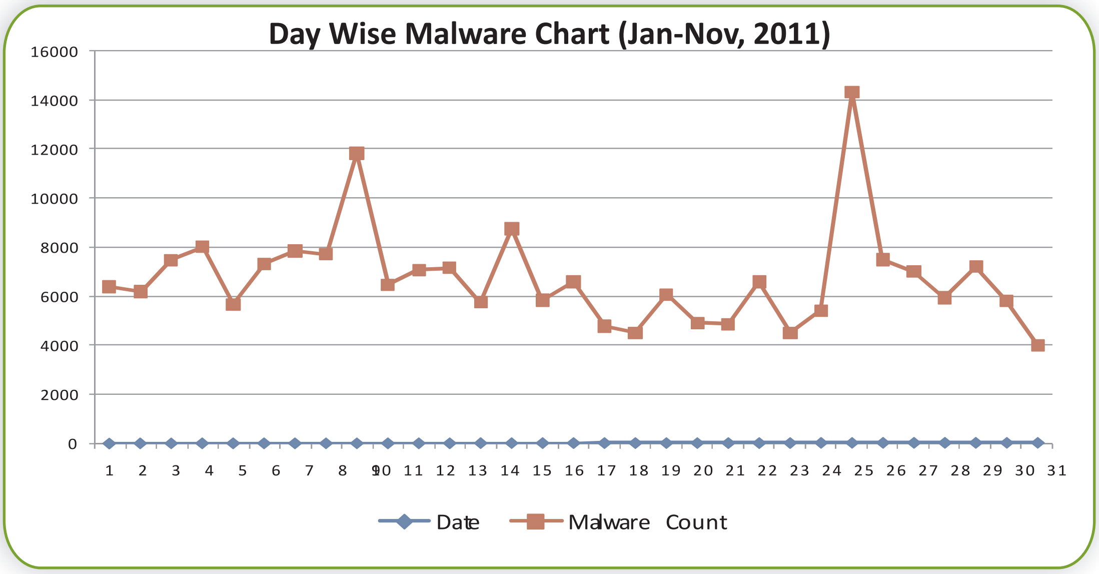
Check Privacy Policies:
Check the privacy policy of websites before providing personal & financial information. Understand the way your information will be used by the given websites.

Make Sure Your Information is Encrypted:
Many sites implement SSL – better known as Secure Sockets Layer to encrypt information. A site can be defined as encrypted if the URL begins with 'https:' instead of 'http:' – followed by an icon that

resembles a padlock. However, the location of the padlock can differ from browser to browser – it can be towards the left of the address bar or to the right. It can also be located towards the bottom of the page. Do keep in mind, that there are instances where hackers try to trick users by adding a fake padlock on malicious sites. Make sure the icon appears in the appropriate location within your browser.

Use a Credit Card:

There are laws that keep fraudulent credit card charges in check while it might not be the same with debit cards. Reason why this is being said is due because using a debit card has an immediate effect on your bank account. Unauthorized charges can easily leave you with insufficient funds to pay other bills. What you can do here is – use a credit card with a low credit limit for your online transaction as it minimizes the overall damage.



Disclaimer

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