‘e Scan

Malware Report

(February 2012)

E-mail: marketing@escanav.com

Web site: www.escanav.com

INDEX

Malware Report

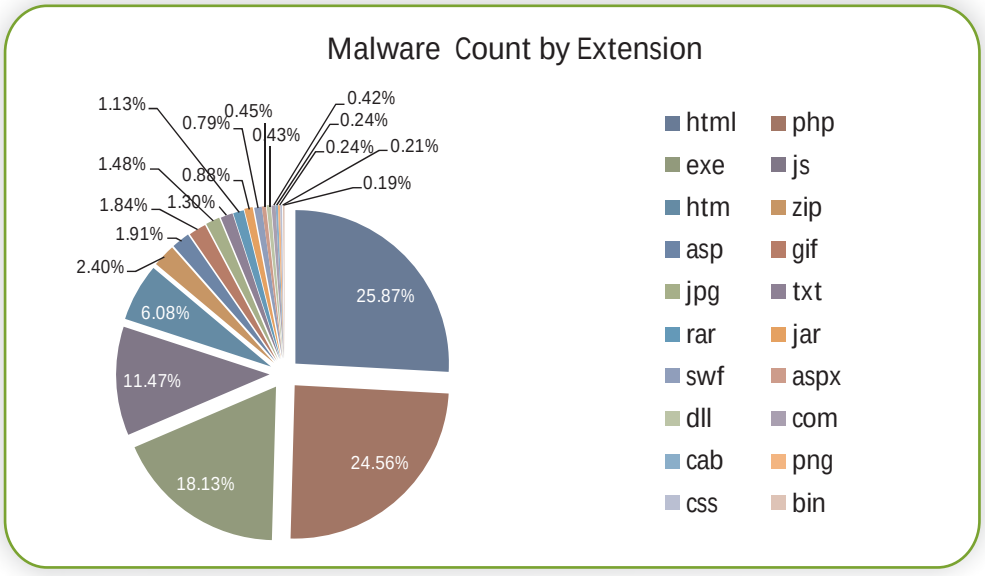
Cybercrime has become a silent global digital epidemic. The majority of Internet users worldwide have fallen victim and they feel incredibly powerless against faceless cyber criminals. The most intriguing aspect of today's viruses is, most malware are not being newly created but are in-fact being re-written or re-coded to a great extent.

We all know that the malware threat to IT and web users will continue to grow, irrespective of whether we bring out the best AV suite. But the burning question is 'Can this growing threat be curbed?'
To state facts, malware is not only on the rise but is evolving as are the methods by which they are transmitted. According to statistics the total number of recorded malware incidents surged in 2011 with a record high of close to 2.5 billion. Break them up and you'll find, approximately one third came via browser attacks while others came through spam, application vulnerabilities and network based attacks.

In a bid for survival, Peer-to-Peer networks have become the key source of malware infection. In fact P2P have grown into the most common source of malware infection making it second to browser based attacks. Moreover, the threats coming from this area are diverse and consist mostly of Trojans, Worms, Rogue AVs and Backdoors. Cisco also stated that the attacks on three leading P2P networks are growing by the numbers – namely eDonkey, BitTorrent and Gnutella. Take the example of the Zeus/Spyeye malware. The jump to P2P has eliminated the need for a command and control server as the botnet itself functions in a peer-to-peer manner.

As for the number one source of malware infection which basically originate via Internet browsers, 2011 recorded more than 600 million incidents. Adding to this, Internet Explorer is by far the most vulnerable, as with programs that work within browsers such as Adobe Reader and Flash Player. Furthermore, a number of low-cost high-impact infection techniques rely on social engineering attacks which till date have been a task for IT administrators to stop.
The overall percentage of the method used to lure users is as follows:

SEO Poisoning:	45%
Spam / Phishing eMails:	25%
Social Networking Attacks :	20%
Malware Embedded Within Adult Movies :	10%



The prevalence of SEO poisoning is also on the rise with 45% of malware writers using search engine as a medium to spread viruses. As always, they are by far the most requested category for any sort of content search. In fact in the last year request for this category has grown by almost 5% - basically demonstrating that this medium is still the most preferred by a number of users. Also, social networking rose to being the third most preferred medium of attack.

And why not? With over a billion active users and growing (Cumulative: Facebook + Twitter) the sheer size of users make it difficult for malware writers to overlook. Moreover, social networks have grown beyond the need of individual users but are being widely accepted by businesses too. From employee recruitment to brand promotion to partner portals/ customer environments, businesses are actively embracing the benefits of social media.

Now, if you analyze the growing need of social networking it comes in as a different breed as far as online content is concerned. The move to social networking lies mostly on the trend that first began from the consumer side. Since 2009, social networking sites have eclipsed web based email. Moreover, it is also observed that a user's behavior within the social networking circle is different from the behavior on the Internet. To state facts, the social networking domain is dominated by games and various daily updates.

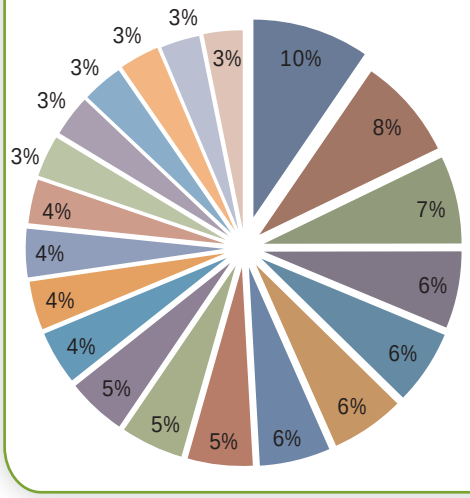
Given below are some of the most requested content within social networking

Games:	48%
Society /Daily Living:	31%
Personal Pages /Blogs:	10%
Pornography:	6%
Entertainment:	5%

Social Networking Dominance

In fact, social networking activity is dominated by Games and Society/Daily Living. These two categories were responsible for more than 60 percent of all requests, a significant growth over 2010, where they represented just over 14 percent. Looking at it from another perspective, almost one in every four new Social Networking requests fell into the Society/Daily Living category compared to one in every 16 in 2010. Among the other top five categories are Personal Pages/Blogs, Pornography and Entertainment. Within the top five categories alone there is a mix of content that might be acceptable within a workplace, content that would consume large amounts of bandwidth and employee productivity. It is essential to understand that social networks are portals that effectively host a variety of content. Moreover, it is important for businesses to foresee the effects of social networking as it will help put policies in place which would further protect against the risk of data loss, increase the overall employee productivity and reduce the effect of web based threats.

Domain Wise Malware Hosting

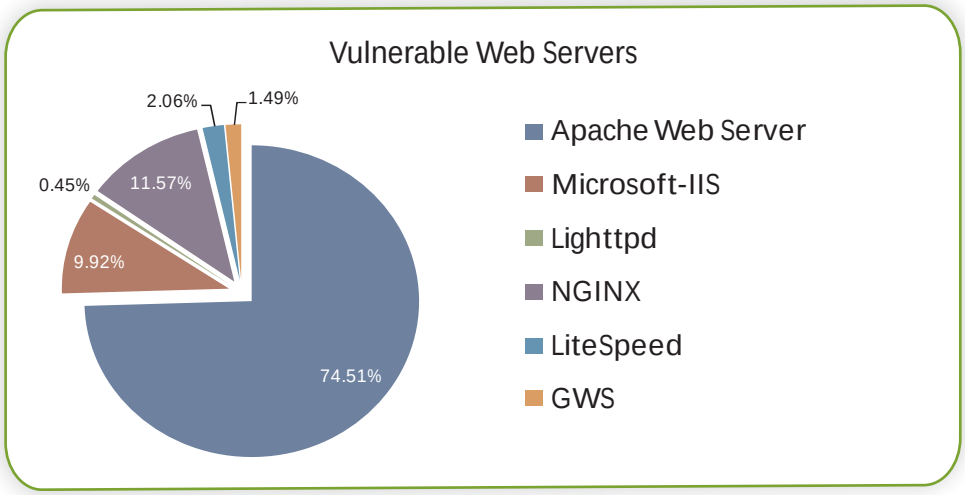


- rusmagistr.ru
- origin-ics.ravenbleu.com
- gay.lmg.pl
- origin-ics.fivemillionfriends.com
- dl.dropbox.com
- feelc.org
- besturlfinder.com
- rpg.kingzdomain.com
- deafnorthwest.com
- utenti.multimania.it
- membres.multimania.fr
- members.multimania.nl
- membres.lycos.fr
- phichit.net
- toptenreport.com
- mitglied.multimania.de
- beritaberitainspiratif.com
- origin-ics.clickpotato.tv
- alpasvart.interfree.it
- ics.fivemillionfriends.com

Business Impact

Businesses can no longer simply block social networking, but require more granularity and control to mitigate the risks associated with it. To fully leverage the benefit of web applications and content, businesses must have detailed analysis and control, not just of social networking sites, but also of the individual web applications and content within those sites. Additionally, they need to be able to filter out any malicious links from within the allowable content.

February also saw the rise of the Waldec Botnet. While it was taken offline in February 2010 and remains very much dead, the code used to create the spambot has been re-coded to steal passwords instead. The new variant comes with the ability to sniff user credentials for FTP, POP3, SMTP and steal .dat files from FTP and BitCoin users. The original bot still remains offline and under the control of Microsoft. The exact scope of the malware still remains a mystery but the new bot is clearly smaller and more targeted than any typical spamming botnet. From spamming to password stealing, the sudden change has in fact perplexed most security analyst.



Moreover, the connection between malware coders and computers have long lived since the 1970s. From the first Creeper virus (1971) to date (2012) malware writers have thrived on creating the most complex of viruses. From floppy disks to vulnerabilities found on server based applications – malware have existed in almost all forms. Their ability to spread has further grown with the rise of email and the web. Exe's or executables have by far become the most common way to trick users into installing malware on their systems. With that said, these types of attacks were relatively easy for tech savvy users and IT departments to block and stop, as there was very little reason for anyone to have an exe sent via email. Blocking of exe's were relatively easy for users and IT Administrators as were the needs to permit sending of documents such as MS Word / Microsoft Office Suite files or PDFs.

But with time the overall functionality of documents have changed. They were and no longer are simple static files and come with scripting capabilities, thereby making it possible to execute programs and processes to silently install various bits of code on the users system – which brings us to the first virus that spread using Word. Melissa brought down networks and mail servers and spread quickly across the Internet and it achieved this by making use of Microsoft Word's macro capabilities.

We've come a long way since Melissa. Modern document-based malware spreads in a variety of ways – not just through email but sometimes just by viewing the wrong website with the wrong browser and applications installed on your system. And while vendors continually try to patch the holes malware writers use to spread

their code, they are usually well behind the bad guys. Today, documents are one of the most common ways malware is spread across the Internet.

Having said that, there are ways to prevent yourself from opening or even downloading malicious documents – be it in PDF or Word format. Awareness is key and knowing which documents to download and open will help prevent your machine from getting infected.

.

Document Based Malware

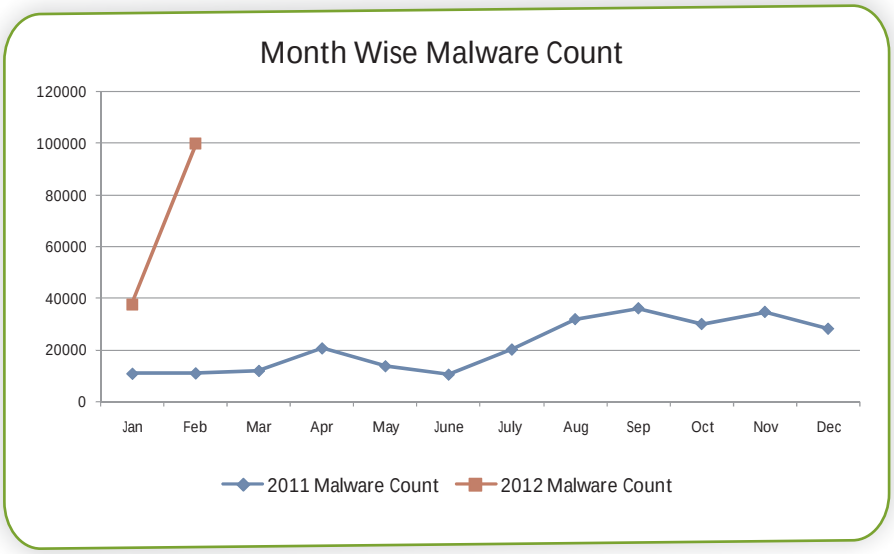
There are innumerable number of ways in which a user can be intimidated into opening a malicious document. It could come in the form of an email attachment with a subject line stating: 'Hear is the doccumnet u asked for!' Take note of the grammatical errors the subject line holds. That in itself should be good enough to raise a doubt on the received email.

But it doesn't end there. There are a number of mails that come with links pointing to documents on websites. Again it is worth looking into the content of the mail to know if it's legitimate or not. Any sort of grammatical error should immediately be flagged as malicious. And just as there are various numbers of document based malware, the ways in which they attack are also innumerable.

Now, if we go by the presented figures, you will note that web pages rank high in terms of hosting malware. Moreover, malware exploit kits serve as an engine for drive-by-downloads. These kits are professionally written software components that are hosted on a server with a database backend. The kits, which are sold on underground hacker sites, are fitted with exploits for vulnerabilities in a range of widely deployed desktop applications, including Apple's QuickTime player, Adobe Flash Player, Adobe Reader, RealNetworks' RealPlayer and WinZip. These exploit kits are then purchased by malware authors and deployed on malicious servers.

Browser-specific exploits have also been used, targeting Microsoft's Internet Explorer, Mozilla's Firefox, Apple Safari, Google Chrome and Opera. Several targeted exploit kits are fitted only with attack code for Adobe PDF vulnerabilities or known flaws in ActiveX controls.

As predicted, February saw a surge in malicious activity taking the overall count close to a lakh from just forty thousand in January. It is also helpful to understand that the same malware (viruses, spyware, Trojans, bots, rootkits, and fake security software) can and often is, delivered in different ways – sometimes by e-mail, sometimes by visiting a Web page and sometimes by using other means. The month also saw a surge in botnet activity that further strengthens the existence of the Waldec bot.



Disclaimer

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

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