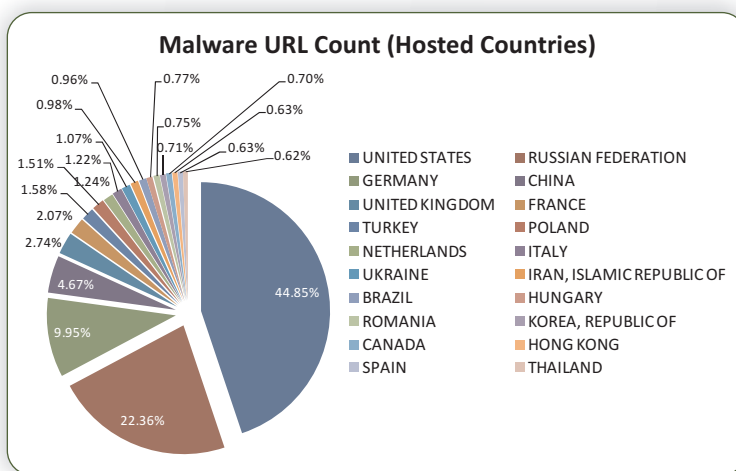# eScan™

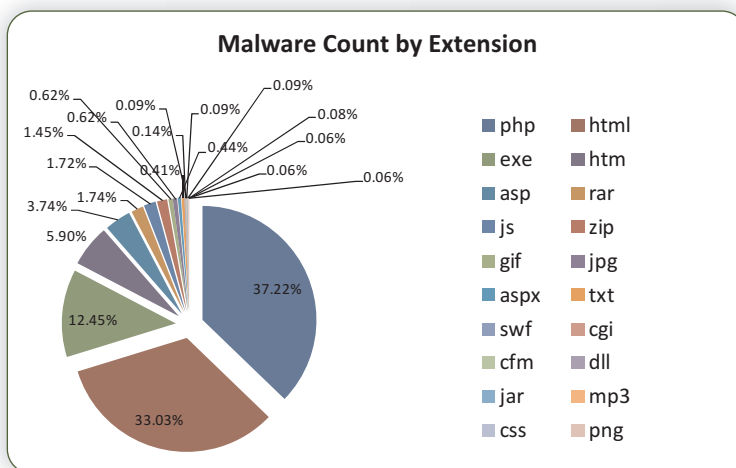## Anti-Virus & Content Security

Malware Report

[February 2013]

Malware Report – February 2013

Malware is a growing epidemic that cannot be washed out but can only be curbed. Controlled by a chain of cybercriminals, its growth is indefinite in the digital world. In all practicality, the ability to prevent this community or industry (which it is slowly turning into) from growing is clearly impossible. Why? The reason is clearly due to the fact that hackers and malicious coders are becoming highly successful in covering their digital tracks, making it very difficult for cyber sleuths to track and analyze their online movement. Malicious coders have also grown in complexity such that their digitized presence can go undetected in the presence of the user, irrespective of whether a security suite is installed. However, the inability of a security suite to detect the presence of malware is relatively low but what we as users must understand that a security suite alone cannot prevent malware from infecting a system. The user himself plays as big a role as the installed security suite. While an anti-virus product will prevent an infection 99% of the time there is always that 1% window of opportunity for hackers. And this 1% comes in the form of users, patches, updates, etc.

Malware URL Count (Hosted Countries)

UNITED STATES	RUSSIAN FEDERATION
GERMANY	CHINA
UNITED KINGDOM	FRANCE
TURKEY	POLAND
NETHERLANDS	ITALY
UKRAINE	IRAN, ISLAMIC REPUBLIC OF
BRAZIL	HUNGARY
ROMANIA	KOREA, REPUBLIC OF
CANADA	HONG KONG
SPAIN	THAILAND

0.96%, 0.98%, 1.07%, 1.51%, 1.22%, 1.24%, 1.58%, 2.07%, 2.74%, 4.67%, 9.95%, 22.36%, 44.85%, 0.77%, 0.75%, 0.71%, 0.70%, 0.63%, 0.63%, 0.62%

Email has always been the choice attackers use for infecting a target. However, with technology progressing and with the growing number of malware related tools, this trend is seeing a rapid change. Email based malware will certainly continue but we will see this method decrease over time; giving way to real-time attacks. We will see a rise in malicious web applications which have more than proved to be advantageous for an attacker. Moreover, recent incidents go on to prove that hackers have been highly successful in evading traditional antivirus signatures.

Malware Count by Extension

php	html
exe	htm
asp	rar
js	zip
gif	jpg
aspx	txt
swf	cgi
cfm	dll
jar	mp3
css	png

0.62%, 0.62%, 1.45%, 1.72%, 3.74%, 1.74%, 5.90%, 12.45%, 33.03%, 37.22%, 0.09%, 0.09%, 0.09%, 0.14%, 0.44%, 0.41%, 0.08%, 0.06%, 0.06%, 0.06%

There are a number of reasons for traditional antivirus to fail when it comes to detecting web based malware. We need to realize that the internet is home to a magnitude of web based applications; all of which are rendered in real time within a browser. So it would be right to say that an antivirus is only as effective as its virus database; be it based on a cloud server or signature based. Not only are they highly adaptable to their host environment but are also polymorphic in nature. Which basically means that the malware can effectively be re-encoded
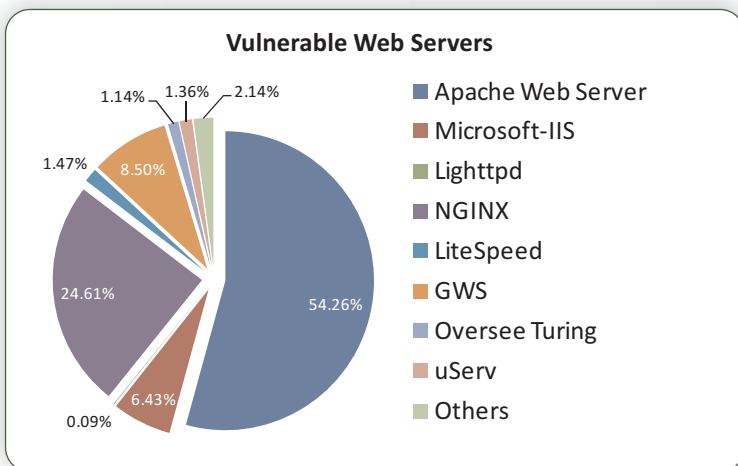
remotely, making it difficult to detect. With that being said, the likelihood of getting infected is linked – but not limited – to the sites the user visits. Hacked and redirected links which further spawn drive-by-downloads are also beginning to see an increase of over 20% in the last 2 months.
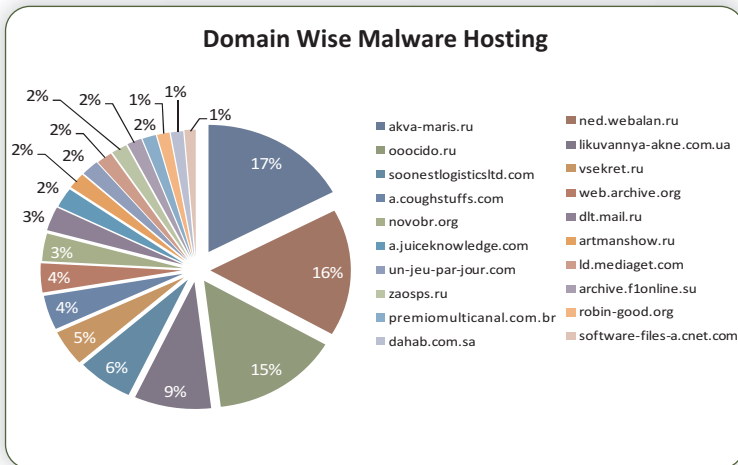
Going by the samples captured, web based malware lead the malware pack both in terms of detected malware and undetected malware. PHP, HTML & EXE made up for 82 percent of the detected malware, while MP3, CSS and PNG summed to less than 1 percent. This just goes on to show that malicious HTML and Scripts are going to be the area of choice for hackers when it comes to spreading malware.

Domain Wise Malware Hosting

akva-maris.ru	ned.webalan.ru
ooocido.ru	likuvannya-akne.com.ua
soonestlogisticsltd.com	vsekret.ru
a.coughstuffs.com	web.archive.org
novobr.org	dlt.mail.ru
a.juiceknowledge.com	artmanshow.ru
un-jeu-par-jour.com	ld.mediaget.com
zaosps.ru	archive.f1online.su
premiomulticanal.com.br	robin-good.org
dahab.com.sa	software-files-a.cnet.com

Vulnerable Web Servers

- Apache Web Server
- Microsoft-IIS
- Lighttpd
- NGINX
- LiteSpeed
- GWS
- Oversee Turing
- uServ
- Others

Social networks have also had a lot to add in terms of distribution of malware. Take the instance of the circulating Facebook banner which promised to change the color of the page to red, blue, yellow etc. It was however detected to be survey scam rather than a malware related issue. Here, your identity is stolen that gets used or sold for profit to various online organizations.

Malware in February stands at a high of 44.85 percent followed by Russia, Germany and China at 22.36%, 9.95% and 4.67% respectively. The top 10 viruses for the month stand as Ramnit, Sality, Autostart, Virut and Conficker. Taking these threats into consideration we shall also see a rise in malicious activity for the month of March.

Month Wise Malware Count

- 2011 Malware Count
- 2012 Malware Count
- 2013 Malware Count
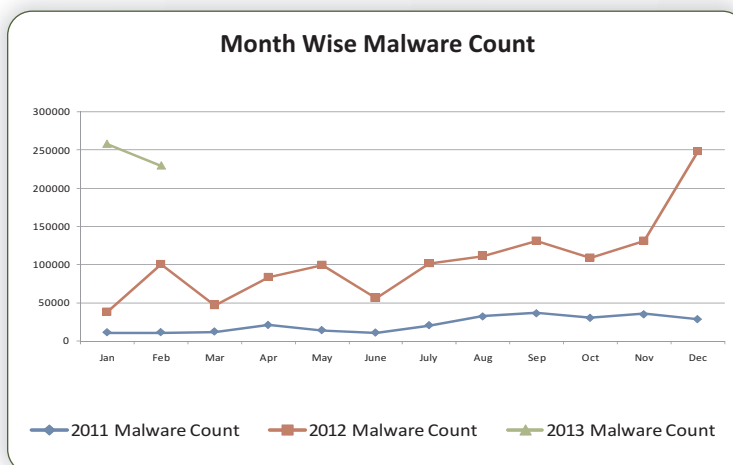
The distribution of malware is definitely not going to slow down in the coming months. Malware awareness therefore comes in as a necessity that online users need to initiate. And this awareness should not only be limited to laptops and PCs but to all devices that make use of the Internet.

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

Mexico:
eScan Mexico
Manzana 3, SuperManzana 505,
Lote 13, Fraccionamiento Pehaltun,
C.P. 77533, Cancun, Quintana Roo,
Mexico.

Tel: +52 998 9893157

E-mail: ventas-la@escanav.com
Web site: www.escanav.com.mx