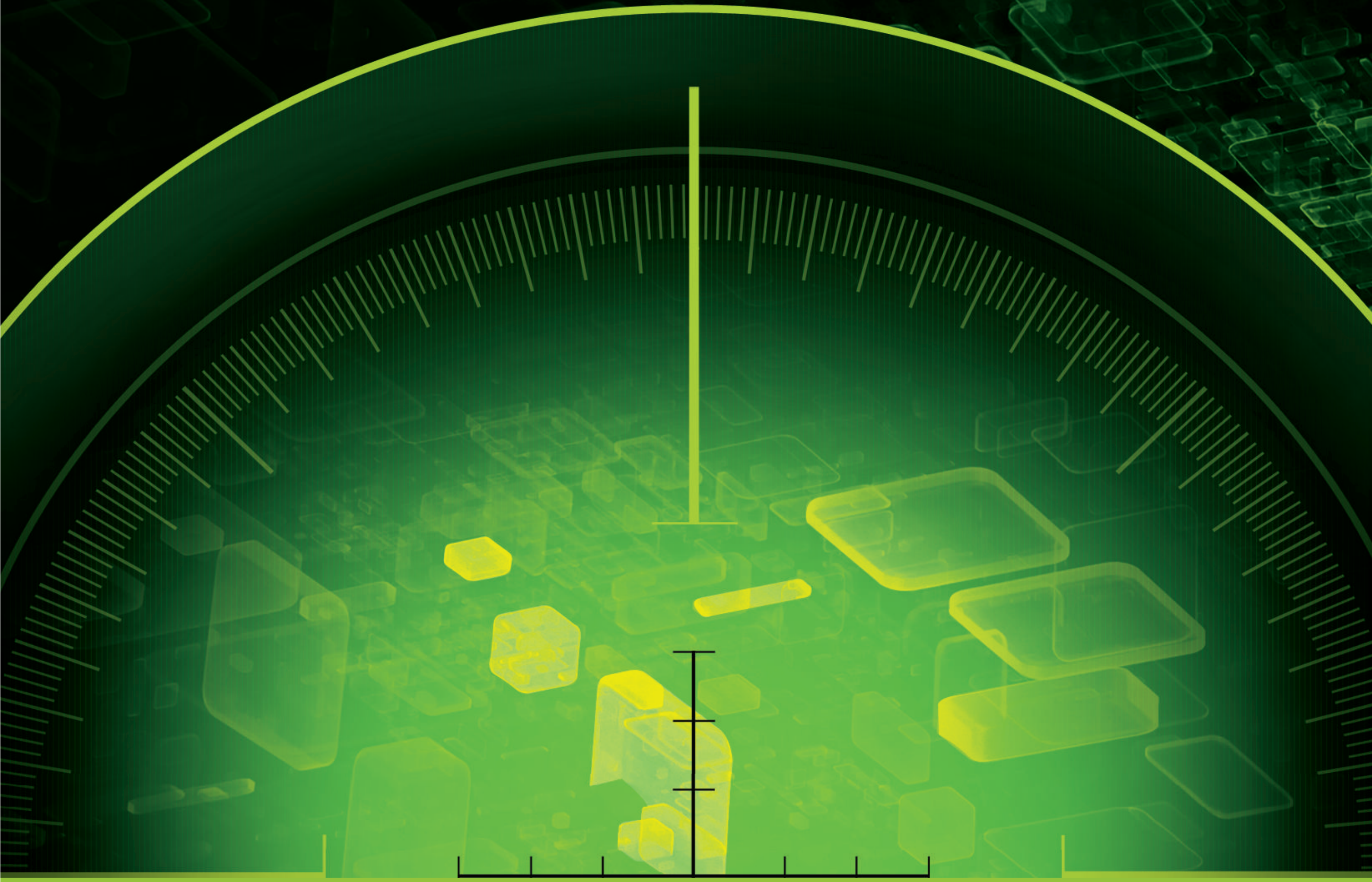
'eScan™

Anti-Virus & Content Security

Malware Report

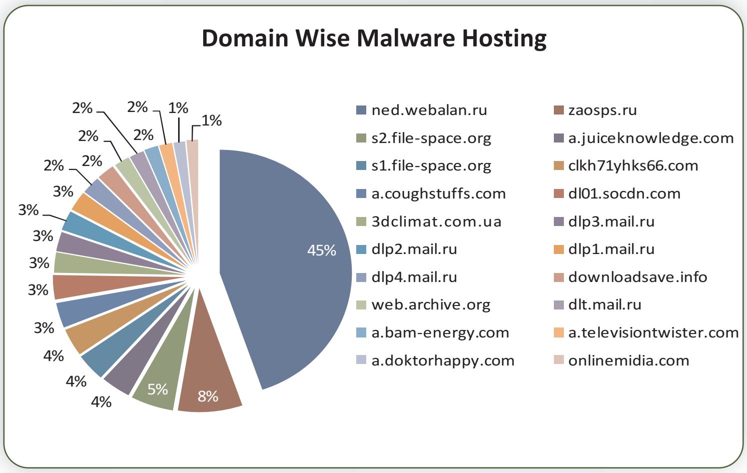
[March 2013]



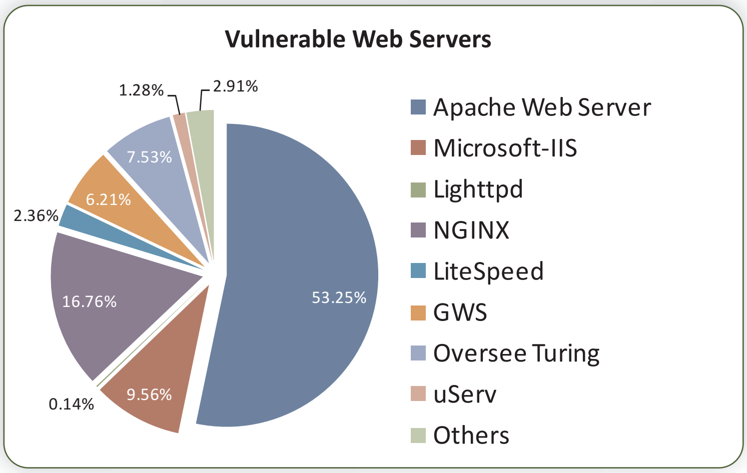
sales@escanav.com www.escanav.com

Malware Report - March 2013

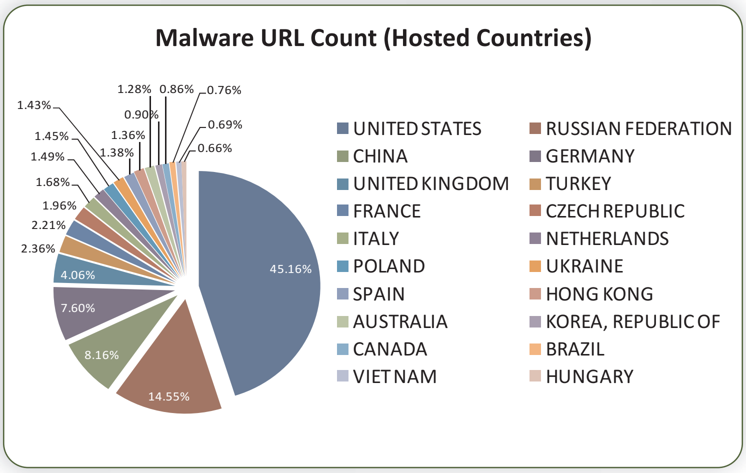
We had stated that malware will grow in terms of distribution and infection in our February based malware report. We had also emphasized on their distribution by infecting legitimate websites. The month of March in-fact saw thousands of legitimate websites serve malware to unsuspecting visitors. Linux based web servers running Apache have been targeted where the attackers gained root access through vulnerabilities found in web-based control panels.



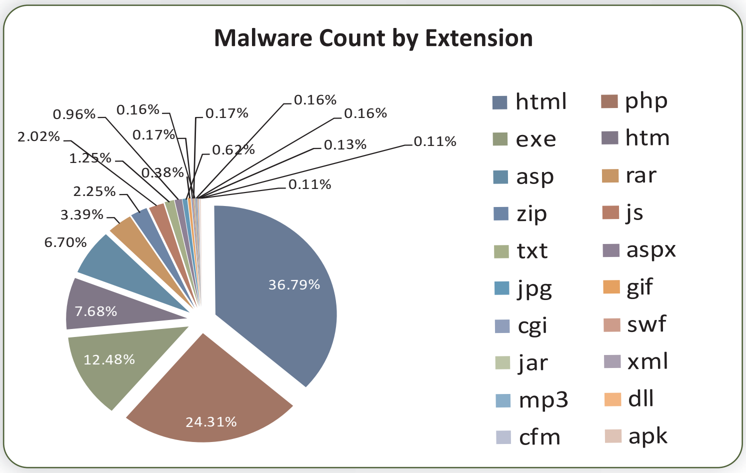
The Apache web server is also one of the most targeted systems on the web. March itself has recorded a total of 53.25% vulnerable Apache servers making it one the highest targeted servers on the web. This is made possible since servers, in all probability, are the last to get patched by IT administrators. In addition to this, the total number of vulnerable Microsoft-IIS and NGINX servers stood at 9.56% and 16.76% respectively.



We are also beginning to see social networking, such as Facebook, being used to market banking Trojans. Recently discovered by researchers at RSA, the malware up on sale was a customized botnet control panel programmed to work with the banking Trojan ZeuS. ZeuS first came in as a highly specialized malware, designed to steal online banking and customer credentials. This particular malware was modified, re-packaged and was being sold on Facebook for immediate use. Alternatively, interested buyers were also given the option to lease the botnet. He/she can then collect user details and also execute DDoS (Distributed Denial of Service) attacks.

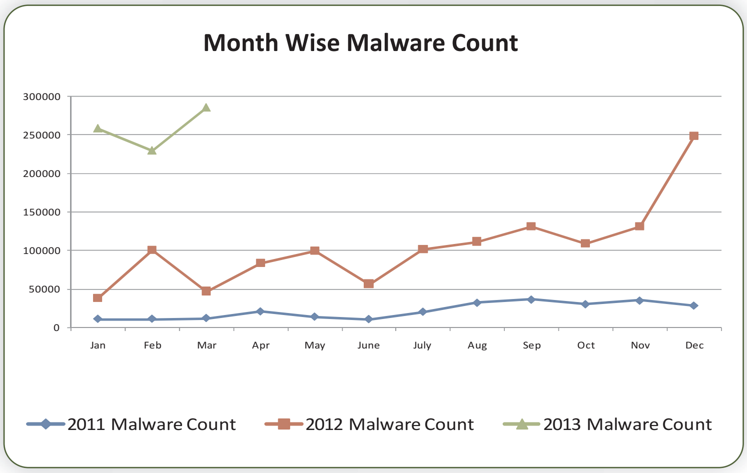


Most developers and malicious coders would prefer an underground forum to distribute their malware. This sudden switch to bring it out to public only goes to show that cybercriminals are beginning to experiment with the idea of marketing it on a much larger scale since underground forums by and large are only accessible to a handful of buyers.


Malware Count by Extension

The intention behind this sudden move is still unknown and is viewed as an extremely daring move. Having said that, implementation of using such a method is highly unlikely since the chances of getting caught are high. This was probably an initial test that was used to check the total number of hits a public account would generate in comparison to a lesser known underground forum.

In a sudden turn of events, the malware industry is beginning to target more and more Point of Sale systems. Known as vSkimmer, the malware is designed to infect Windows based computers that have payment card readers attached. The malware is capable of gathering information about the OS with its version number, language, hostname, username and also comes with a GUID identifier. The information gathered is then sent back to the C&C server which is supposedly used to keep a tab on all infected machines. The basic functionality of the malware is to extract Track 2 data. It does this by reading the data of a particular process associated with the card reader. While this might not seem harmful to the general reader, we need to know that the information recovered from Track 2 data can be used to clone the card. The malware however is not capable of reading cards that follow the EMV standard or in other words that come with a Chip and Pin. vSkimmer is also capable of working offline and it achieves this by saving a log file of all transactions carried out. It then sends the required file once the connection is established or waits for a USB device with volume name KARTOXA007 to be connected.


Month Wise Malware Count

Like we mentioned, malware will continue to grow in complexity and cybercriminals will always find ways to spread malware across all domains and networks. It is therefore important to remain vigilant as we will be witnessing a significant growth in the cyber crime industry. There is no stopping the rise in web threats. The only thing we (Government/Private sectors, Individuals) can do is to implement strategic actions to contain the threat.

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