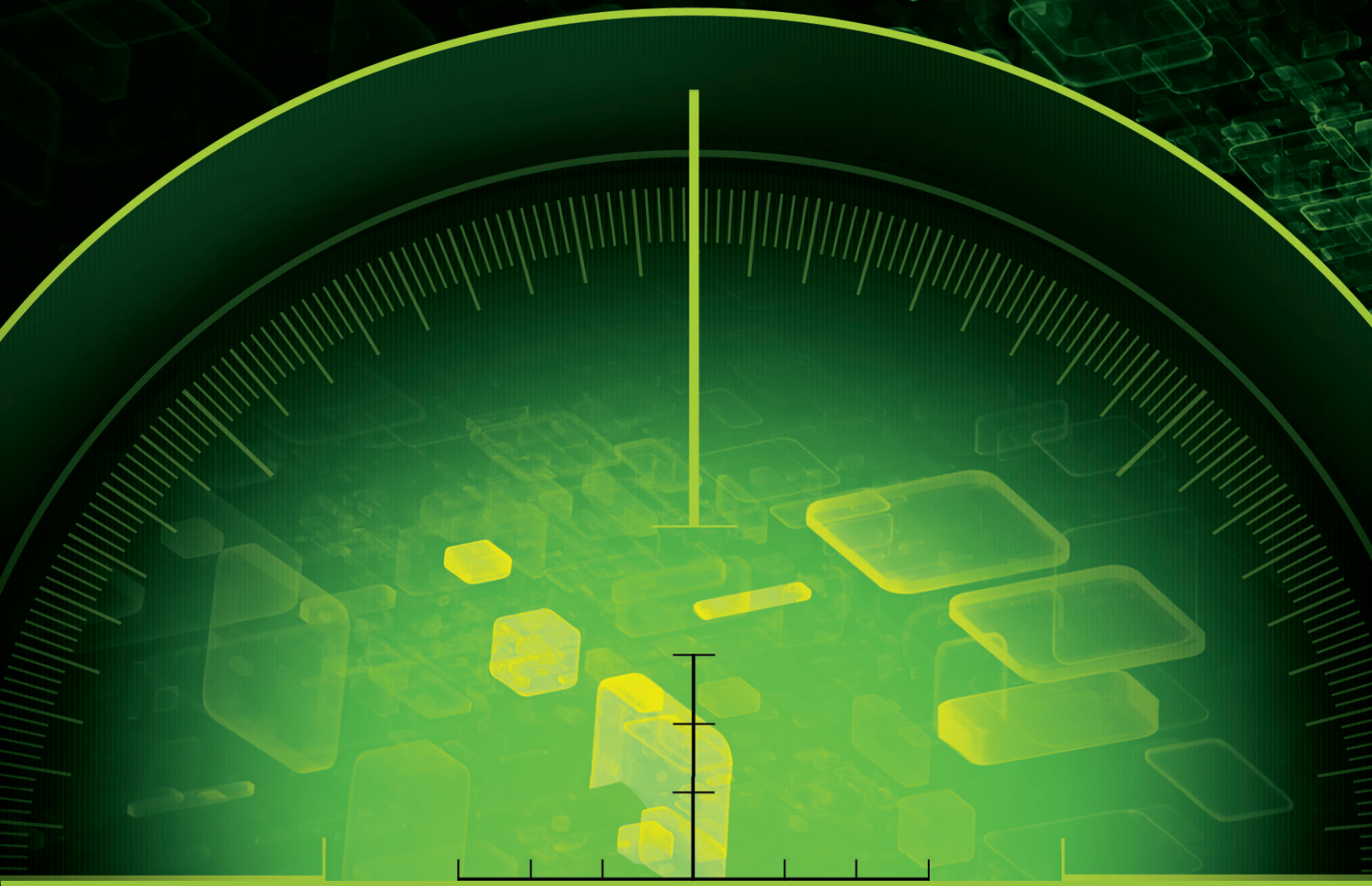
eScan™

Anti-Virus & Content Security

Malware Report

[April 2013]

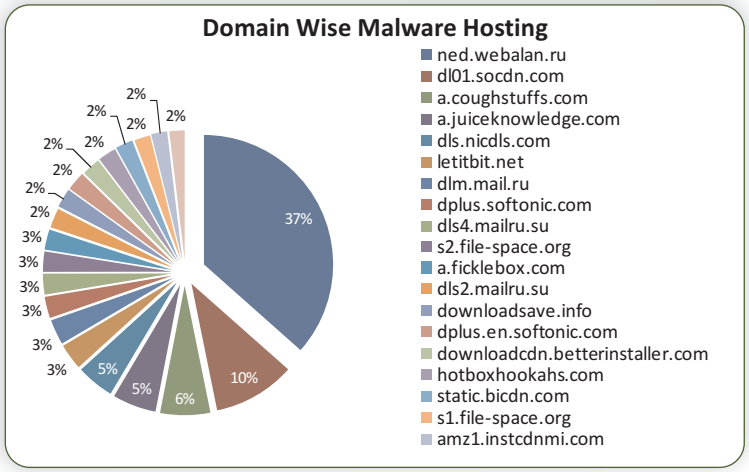


sales@escanav.com

www.escanav.com

Malware Report - April 2013

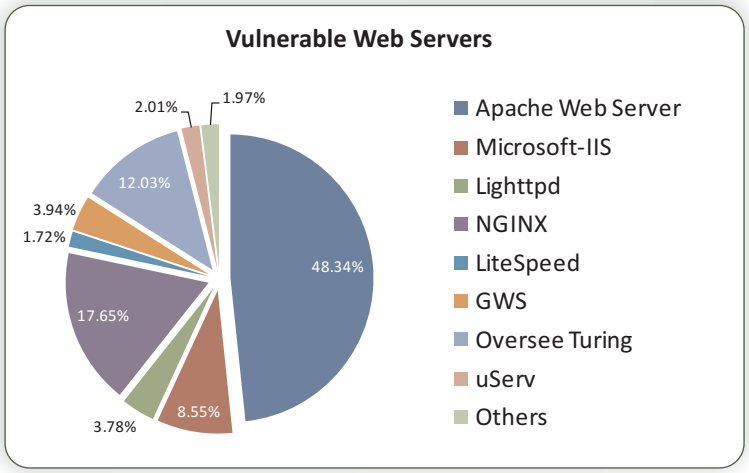
An ongoing widespread attack has been recently discovered that forces sites running three of the Internet's most popular web server push malware exploits on visitors.



A malicious backdoor (Linux/Cdorked.A) was being used behind the attack and is said to have infected at least 400 web servers where 50 of them come under Alexa's 100,000 ranking. The backdoor infects sites running on Apache, NGINX and Lighttpd web servers and are said to have exposed over 100,000 end users. However, the actual number of users infected is said to be much higher.

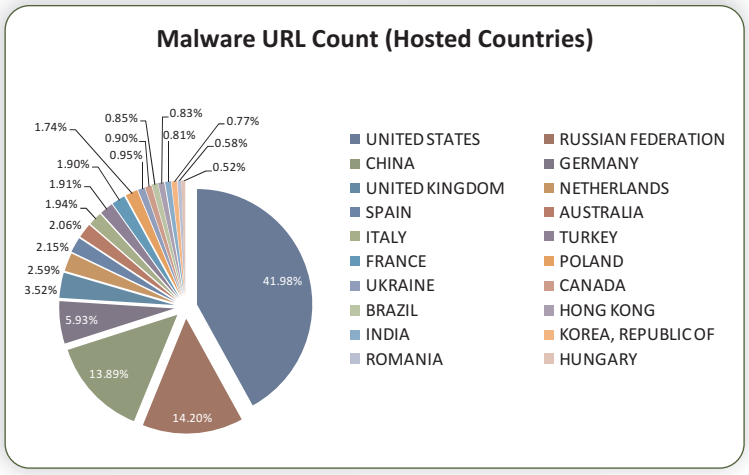
This sort of attack is also the first time where we have seen different web servers being attacked. In other words the attacker is willing to create a backdoor for Apache, Lighttpd and NGINX. Stealthy, streamlined and sophisticated the people behind the malware follow a streamlined distribution mechanism for getting malware onto end users PC.

The malware 'Cdorked' was known to infect sites running on Apache, which is by far the most popular Web server application. According to statistics, Apache and NGINX come in as the most sought after web server applications which totals to a close 48.34 percent and 17.65 percent respectively. However, Lighttpd, a web server designed for speed, comes in at just 3.78 percent. Meebo, YouTube and Wikimedia are a few that currently make use of Lighttpd. The susceptibility of NGINX got highlighted only after an update that patches a remote code-execution vulnerability was issued by its maintainers. However, there is zero evidence that the related vulnerability is related to the Cdorked infection.



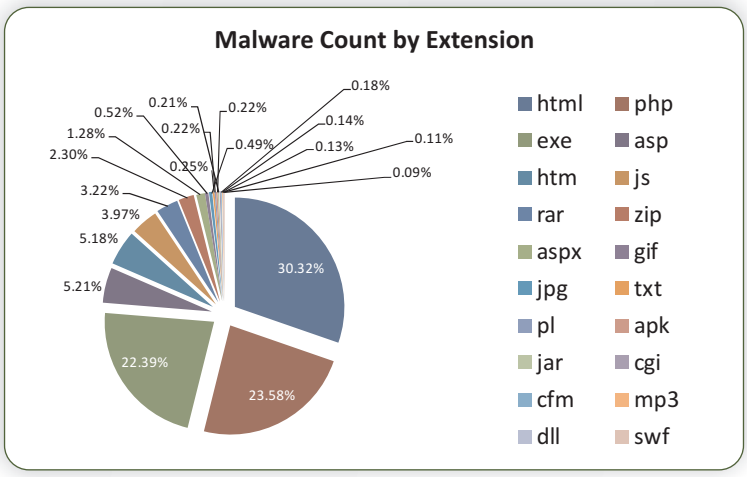
The malware has been observed to cause popular and trusted websites push exploits that attempt to install malware on users who visit compromised web pages. It does this by redirecting users to malware hosting sites which basically house the Blackhole exploit kit. In addition, the malware is extremely stealthy and can go undetected even when the target computer is being

attacked. However, those who have been attacked in recent times have been singled out. Also, the malware comes with a large number of embedded IP addresses that are blocked from being infected.



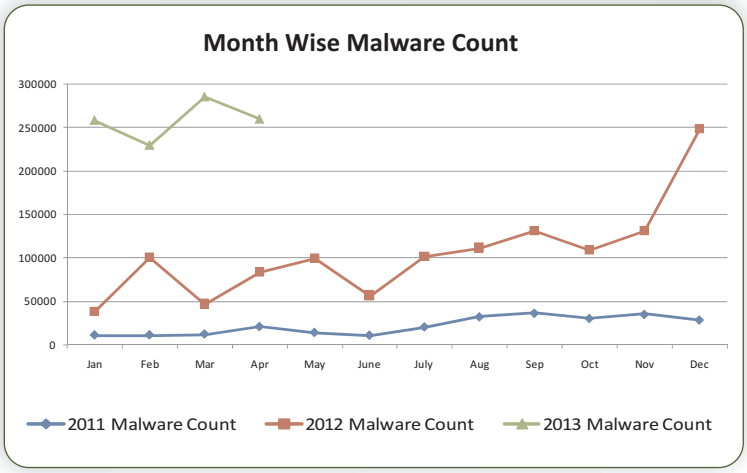
The malware is also advanced enough to differentiate between different computing platforms used by end users. Users coming from Windows based OSs are redirected to sites that host the blackhole exploit while Tablet or Smartphone users are redirected to porn sites that host malicious code. Over 70 various encrypted commands can be directed to systems that have been compromised, giving the attackers granular control that can be invoked remotely. Moreover, the malware isn't capable of spreading on its own and it also isn't programmed to exploit vulnerability in other specific software.

An exploitation such as this, suggests that malicious coders are expanding beyond traditional Microsoft based OSs. In the past, Linux based malware were not taken seriously as there used to be just a handful of them. However things have changed with time and we now see a number of web servers infected with malware. And this method is slowly growing by the number.



This month was also home to a new Trojan downloader that is not only hard to detect but is also capable of wiping its track by deleting all traces. The downloader (Win32/Nemim.gen!A), goes on to show that malware writers are progressively getting more sophisticated. The Trojan is designed to infect executable files in attached drives. By doing this it can release a special tool that is capable of stealing email based passwords, instant messaging accounts and a host of other services. The downloader is unique in many aspects as it is not only responsible in downloading the core components of the malware. It in fact remains to be a key component of the operation even after the target system has been infected.

We have also seen a growing increase in bank frauds. Over HK$9.6 million in company bank accounts were targeted by use of an email scam that tricked 13 people into revealing codes that were generated by personal security devices that help customers to conduct online transactions. The said email diverted the victims to websites that looked like the banks actual site, where the customers typed in their security code and login details.



Although HK$9.6 million was involved, only HK$2.8 million was successfully transferred to overseas accounts, which include Britain, the United States and the Czech Republic. Other transactions were interrupted when the victim's discovered what was happening before the process ended.

The attacks on eCommerce and Financial services aren't going to stop anytime soon. Attackers are targeting network infrastructures to cause collateral damage to other shared resources, so organizations must think about their different areas of vulnerability beyond website URLs.

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