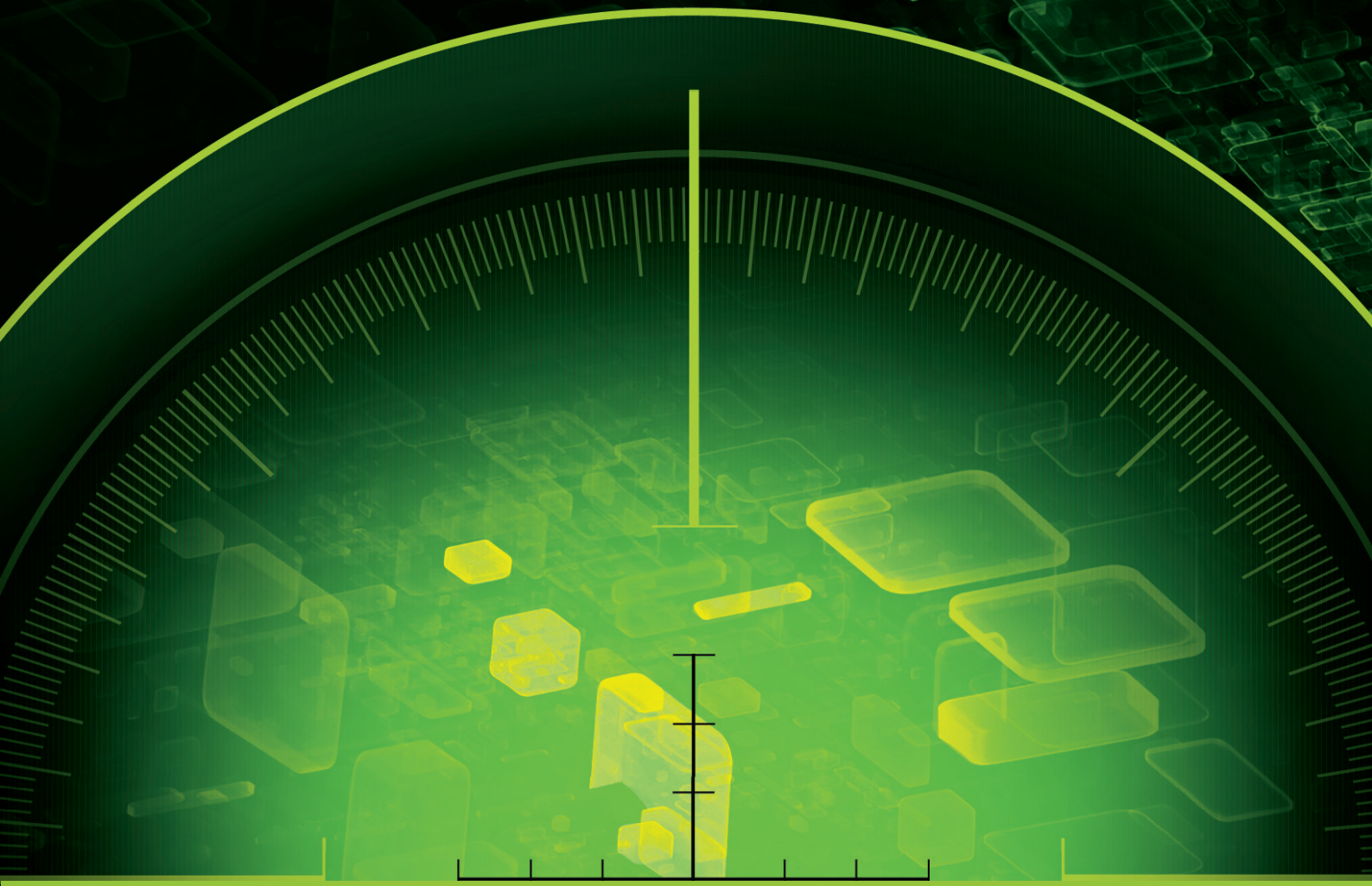
eScan™

Anti-Virus & Content Security

Malware Report

[January 2013]

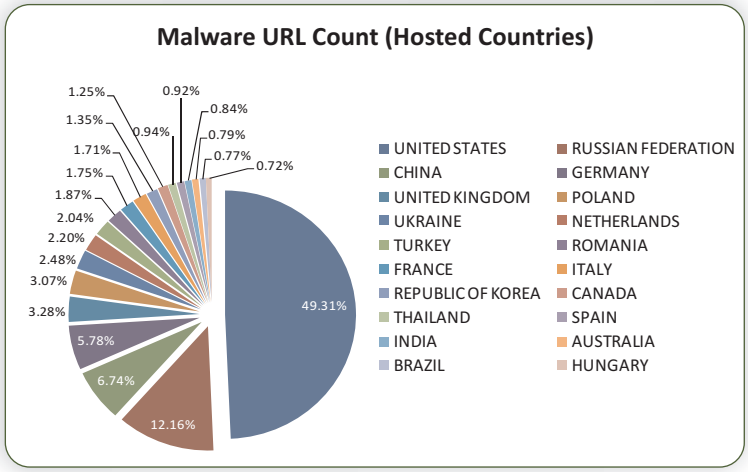


sales@escanav.com

www.escanav.com

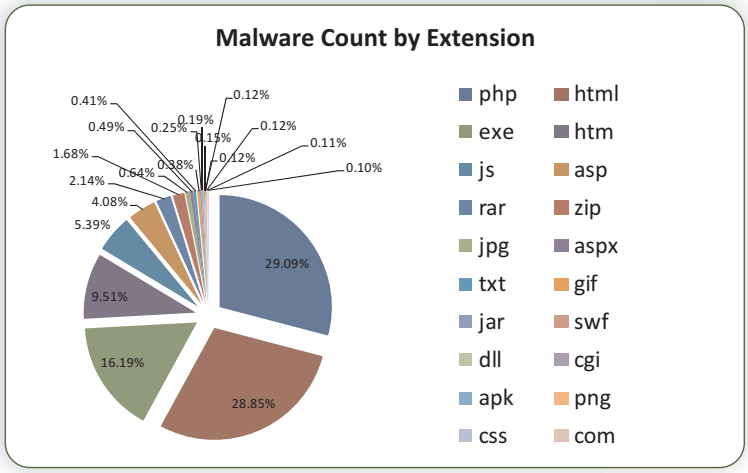
Malware Report – January 2013

It's been over a year since we last predicted about the trend in 2012. Moreover, the year that was, not only focused on the behavioral growth of malware but it has also brought about a change in the way web users are targeted. We are beginning to see an increase in strategized attacks where everything from implementation to execution are carried forth with upmost detailing. Take the recently detected Red October incident, it is considered as one of the largest and most potent attack in the history of cyber crime. A crime so huge, it paints the globe red with its victims. And like we had predicted, malware has advanced beyond what it was a few years back.

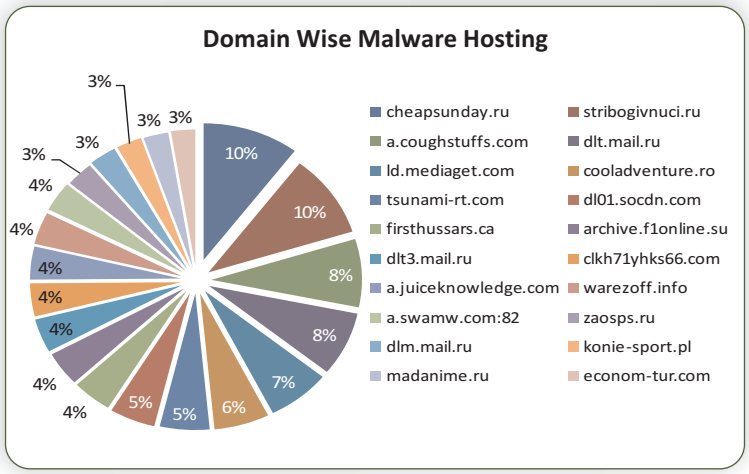


2012 has seen a number of targeted attacks which include a number of successful APT campaigns. A lot of time and research has gone into uncovering nitty gritty aspects of some of the most profound malware. This was also the year where stealth and persistence were used to a great extent to remain undetected. Moreover APT's are more than just a deployment of malware, there needs to be a continued action process that needs to be maintained and this is achieved by hooking on to legitimate applications. Having said that, ongoing APT campaigns can easily be detected using a network traffic analysis tool. To bypass such detection the need to write code at the NDIS (Network Driver Interface Specification) level is increasing significantly thus making detection difficult.

Digitally signed malware is also not new and malware which come with digital signatures are capable of hooking on to core system level applications making them near impossible to detect. The best possible explanation is that of a Rootkit. It is best defined as a stealthy type of software, often malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer. The term rootkit is a concatenation of "root" (the traditional name of the privileged account on Unix operating systems) and the word "kit" (which refers to the

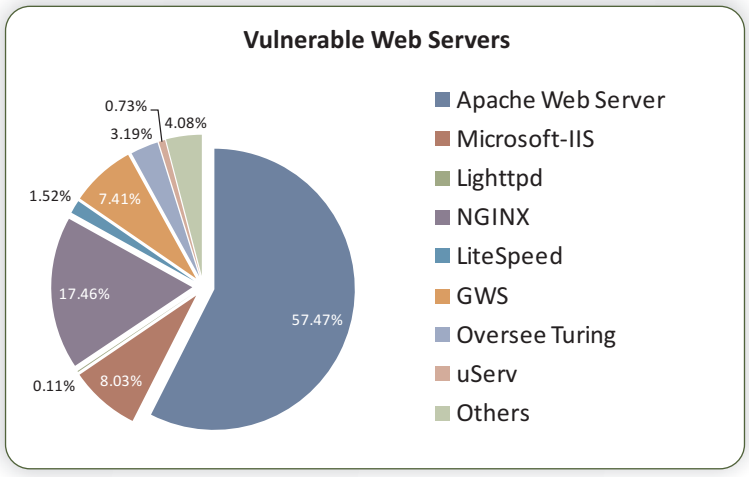


software components that implement the tool). The term "rootkit" has negative connotations through its association with malware.



Rootkit installation can be automated, or an attacker can install it once they've obtained root or Administrative access. Obtaining this access is a result of direct attack on a system (i.e. exploiting a known vulnerability, password (either by cracking, privilege escalation, or social engineering). Once installed, it becomes possible to hide the intrusion as well as to maintain privileged access. Here the key is to obtain root or Administrative rights. Full control over a system means that existing software can be modified, including software that might otherwise be used to detect or circumvent it.

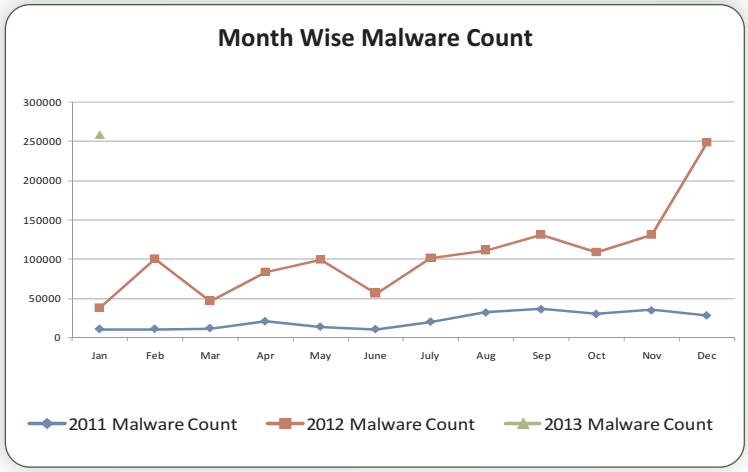
Detection methods include using an alternative and trusted operating system, behavioral-based methods, signature scanning, difference scanning, and memory dump analysis. However, in some very rare cases, removal can be difficult or practically impossible, especially when it is a kernel level rootkit; where reinstallation of the operating system may only be the available solution to the problem. On the other hand, removal of firmware rootkits may require hardware replacement or specialized equipment to remove.



Take the instance of the ZeroAccess rootkit that was discovered sometime in June 2012. Built as a complex kernel level rootkit, ZeroAccess came with the ability to enslave a victims PC by adding them to a P2P botnet. The revision that this particular rootkit has undergone represents a major shift in strategy where it basically represents a shift from Windows 32-bit kernel mode component to Windows 64-bit memory resident component (user mode). In other words, ZeroAccess no longer comes with a kernel mode component but instead it loads a DLL into services.exe and explorer.exe. Following which all functionality is performed inside the mentioned processes. The main goal of ZeroAccess remains simple: to download more malware onto the infected machine. And these basically include click fraud and spam bots. A

few other notable viruses that made it big in terms of complexity were Flame and Gauss, both specifically targeted towards Middle Eastern countries.

We are also noticing a shifting trend in malware development. Repurposed malware has been witnessing a steady growth in the last one year and so are the targets. Financial organizations have for long been a target for complex attacks. However, there has been a significant jump to other critical areas such as Government and Manufacturing. Last year also witnessed an increase (80%) in malware attacks that were basically redirects from legitimate sites. This just goes to show how modern malware is taking advantage of these trends thereby creating new challenges for IT security professionals.



The recent statistics also outline the riskiest and safest countries for encountering malware attacks. United States topped the charts with a 49.31% threat exposure rate while Russia, China Germany and the UK accounted for 12.16%, 6.74%, 5.78% and 3.28% respectively.

Hungary is currently considered as being the safest with a threat exposure rate of just .72%. Brazil, Australia, India and Spain followed with .77%, .79%, .84% and .92% respectively.

And with the growing accessibility to MaaS (Malware as a Service), 2013 will likely see tougher and highly complex malware specifically built to target various business sectors.

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