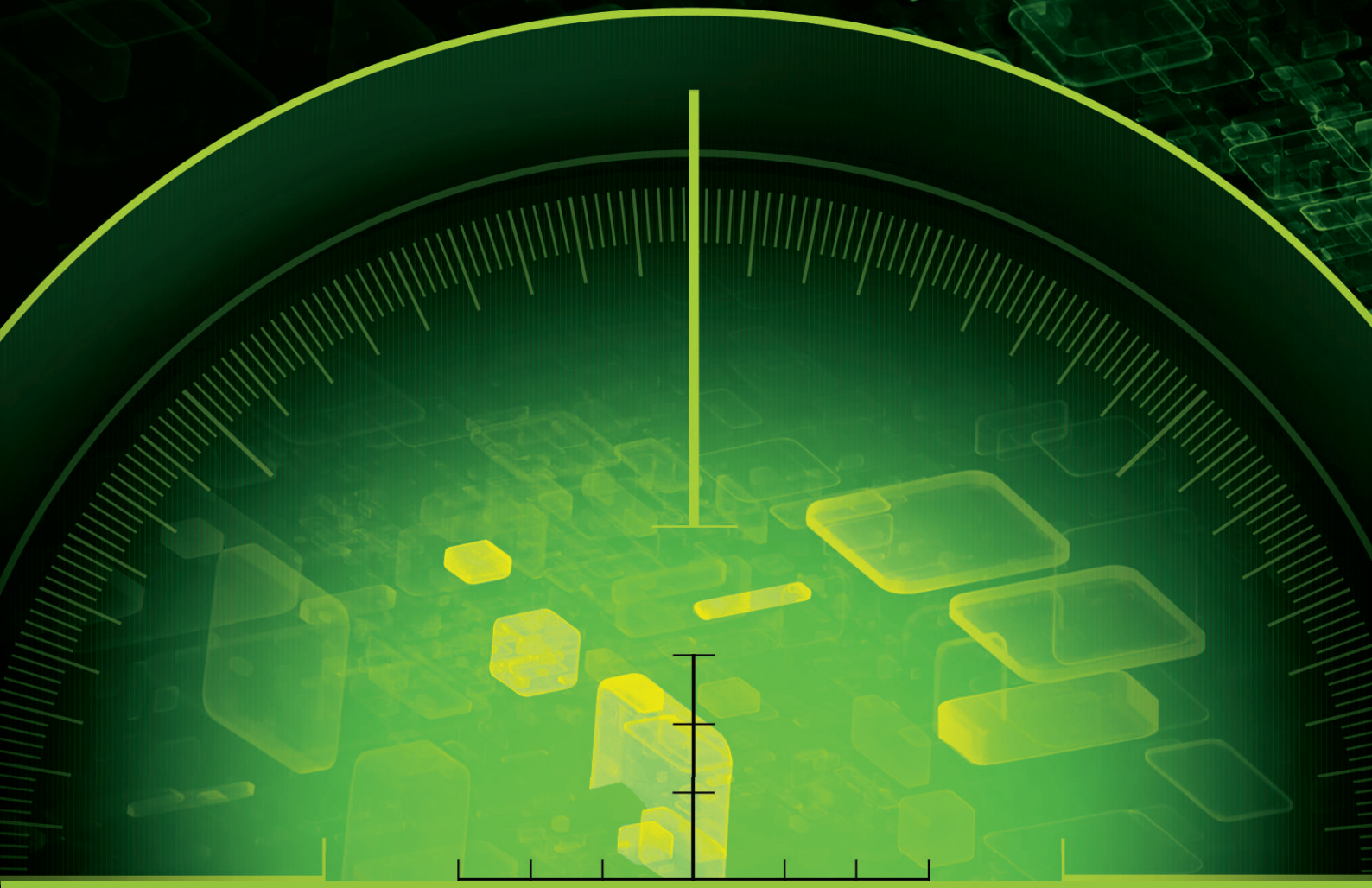
eScan™

Anti-Virus & Content Security

Malware Report

[May 2013]

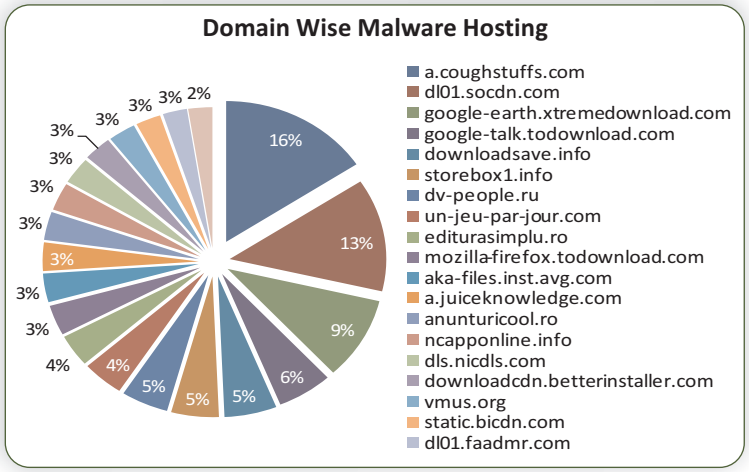


sales@escanav.com

www.escanav.com

Malware Report - May 2013

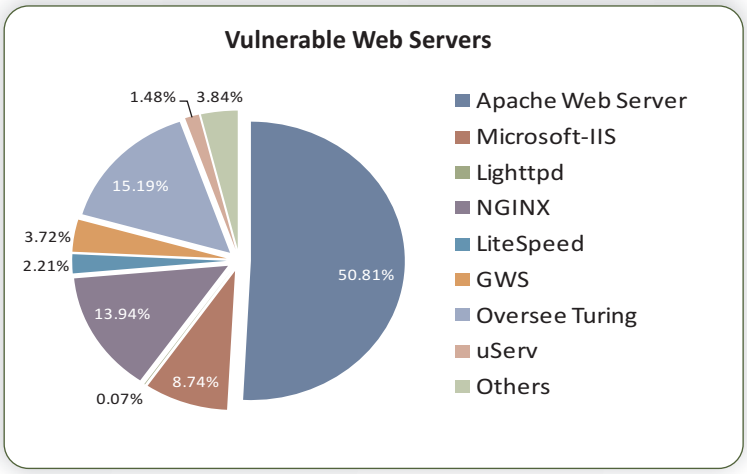
Malware – they have been around for more than a decade and have grown into the digital world. Like December last year, the month of May brought in the discovery of yet another global malware campaign hitting 350 high profile targets in 40 different countries.



The cyber espionage campaign, codenamed Operation NetTraveler, has been active since at least 2004, stealing more than 22 gigabytes of data from computers around the world. The data stolen were mostly related to space exploration, nanotechnologies, energy production, medicine and communications from government institutions, embassies, research centers, military contractors and energy industries. The researchers noted this was the same tool used to target Tibetan and Uyghur activists, two groups often targeted by Chinese hackers. It has also been noted that the APT functioned at very specific time slots which lasted from 8 to 6 under the Beijing time zone.

The malware gets its unique name from a string contained in the code: 'NetTraveler is Running!'

The functioning of the malware is also said to be connected to a group composed of 50 hackers; most of which speak native Chinese as well as some English.

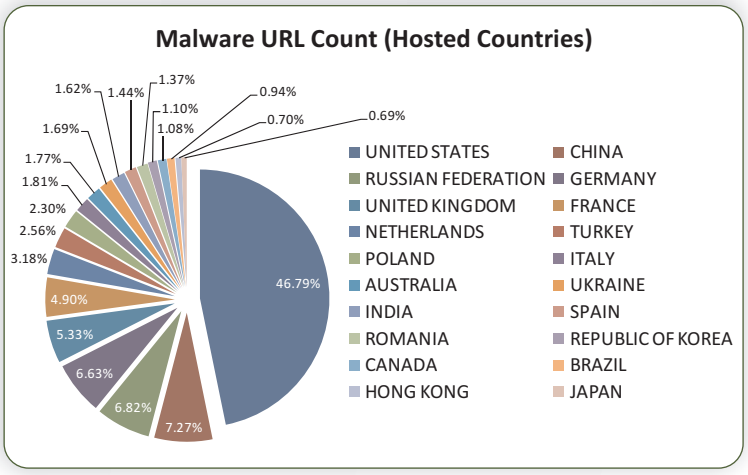


However, the complexity of the malware is nothing to write home about as NetTraveler takes advantage of already discovered exploits and resources which are easily available and downloadable online. In essence the tactics used were very basic which states that hackers without governmental support could have carried it out.

The files were customized and aimed at specific targets where emails containing malicious Microsoft Office documents were used for spreading the infection. As mentioned, the files were specifically customized depending on the target of the attack. These would include files

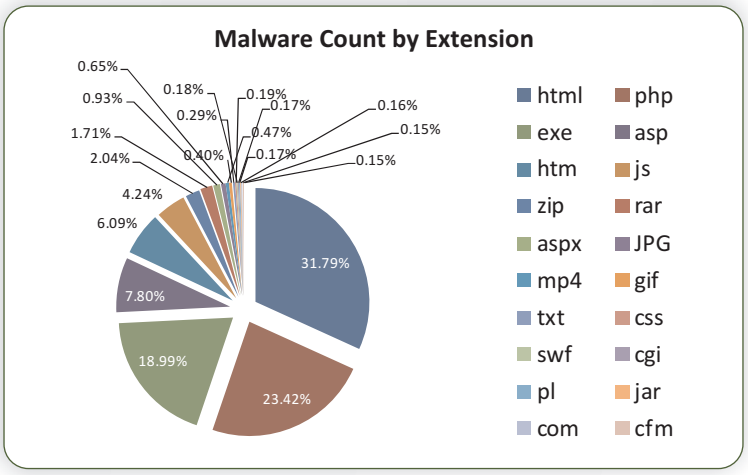
such as “Report - Asia Defense Spending Boom.doc," "His Holiness the Dalai Lama's visit to Switzerland Day 3.doc" and "Army Cyber Security Policy 2013.doc."

On execution the malware then installs itself on the victims PC, following which it starts gathering data such as documents, excel sheets and keylogs. The malware is also programmed to install a backdoor which then injects other types of malware. The victims were mostly concentrated in Mongolia, Russia, India and Kazakhstan. Six of the victims infected with NetTraveler were also victims of Red October (highly sophisticated cyber espionage campaign). However, both the APTs were different in their own way. The networking infrastructure of NetTraveler is basically designed for more distributed operations than the infrastructure designed for Red October. The code itself reveals that the hackers behind NetTraveler don't have the same level of expertise or technical talent that was shown within Red October.



Citadel Takedown

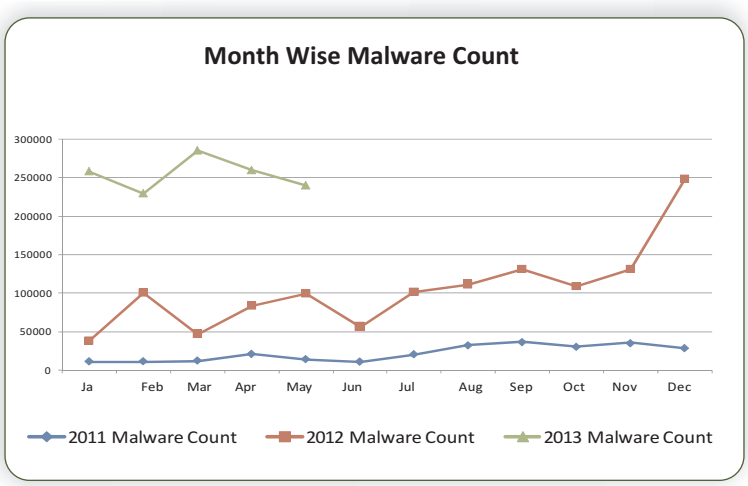
The Citadel botnet was one of the biggest cybercrime rings that was supposedly responsible for siphoning off more than $500 million from banking accounts. The malware is known to have infected over 5 million computers in a span of 18 months.



However, the malware is said to have been taken down by Microsoft, FBI and 80 other authorities from across the world.

That said, the network consisted of at least 1,400 botnets which were used to siphon off data, attack other computers and commit online crimes. With that being said, the coordinated takedown hasn't quite nullified the infrastructure but it has significantly disrupted the malware from spreading any further.

The malware was mainly spread via pirated version of Microsoft Windows. When infected the malware is capable of stealing banking credentials which is then used to siphon off money from large banking institutions like Bank of America, HSBC, Wells Fargo and financial



companies such as Paypal and American Express. The botnets were mainly located within the United States, but also in Western Europe, Hong Kong, India and Australia.

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