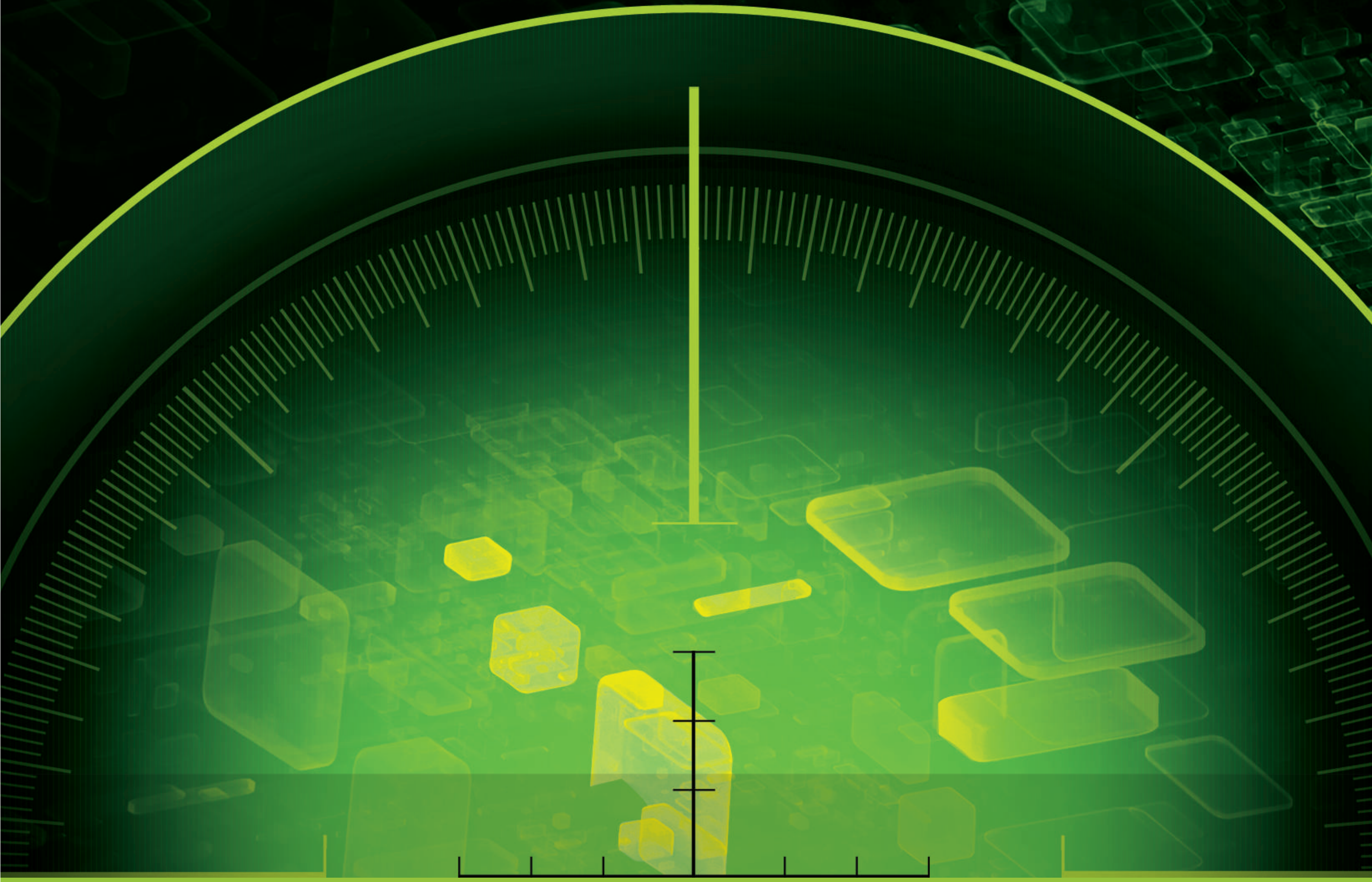
'eScan™

Anti-Virus & Content Security

Malware Report

[July 2013]

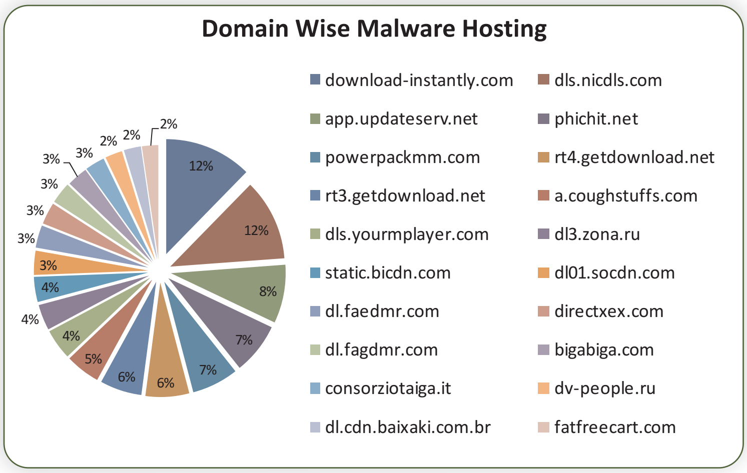


sales@escanav.com

www.escanav.com

Malware Report - July 2013

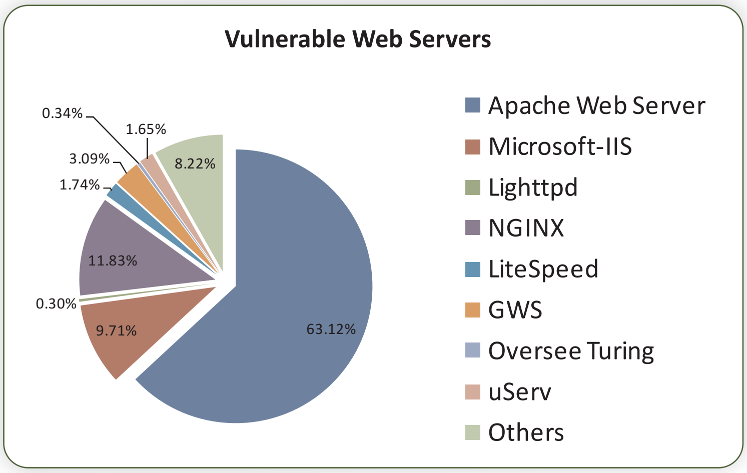
Bots are one of the most complex pieces of tool in the malware industry. They are built mainly to allow hackers to gain control over a large number of computers at any given point in time. They are then used to spread malware, send out spam and commit fraud.



The working of a bot is complex and can infect a person's PC in more ways than one. They are specifically designed to search the web for machines which are unprotected and vulnerable. A bots main purpose is to infect and report back to its command and control center. And stay hidden till they are asked to carry forth a task. In short, a bot acts like a bridge that allows hackers to control thousands of infected machines at any given point in time.

Main Purposes of Bots
Sending: Spam, Viruses, Spyware
Stealing: Credit card numbers, bank credentials, personal information
DoS: Conducting attacks against a specific target by launching Denial of Service attacks
Clickfraud: Used to boost web advertisements by automatically clicking Internet ads

Last month we had mentioned about Citadel's new variant specifically aimed at users making use of social networks, banks, and major e-commerce sites that include Amazon across France, Spain, Italy and Germany. And it was during the same month Microsoft and FBI worked in sync to disrupt more than 1400 Citadel botnets.

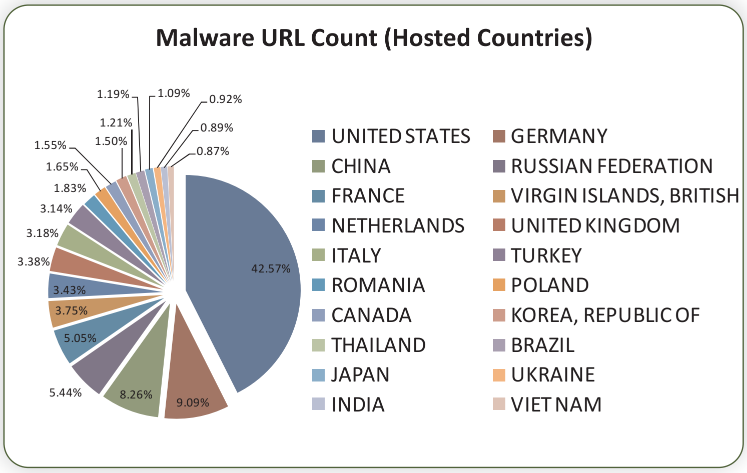


According to reports gathered by security researchers, approximately 230,000 connections were made from 20,000 infected computers in Japan. The difference in the structure of the code isn't much and it still is designed to target domestic users and six Japanese financial institutes. In addition the malware is capable of harvesting information from e-mail services such as Google, Yahoo and Microsoft.

Even with Microsoft's effort in disrupting the botnet, the malware still is quite prevalent as far as banking fraud is concerned. At any given point in time Citadel infected PCs remain connected to at least nine various remote command and control servers. As mentioned, the overall functionality remains the same, where it makes use of customized drop down menus and requests for information generated in local languages.

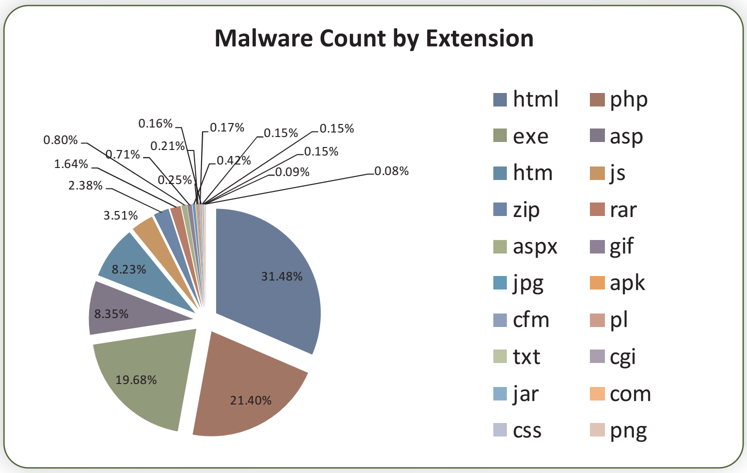
July also saw the development of a sophisticated StealRat botnet that was capable of bypassing advanced anti-spam defenses. The bot makes use of compromised websites to send out spam messages. Furthermore, the malware can be broken down into three different parts. It can be used to:

- Compromise a website to send spam
- Hack computer systems for gathering and sending spam
- Hijack websites for delivering the payload


Malware URL Count (Hosted Countries)

To remain undetected, the spam server hides behind three layers of unsuspecting victims: two hijacked websites and one infected PC. That being said, the infected PC acts as a point of contact between the spam server and the hijacked websites. And since the spam server in itself isn't sending out spam, it will seem to have originated from the infected PC. Moreover, to nullify all visibility between them the spam email in itself does not deliver the payload. A compromised website comes embedded with the link to the payload, which is usually porn or a pharmacy website, and also includes a spamming script which is coded in PHP.

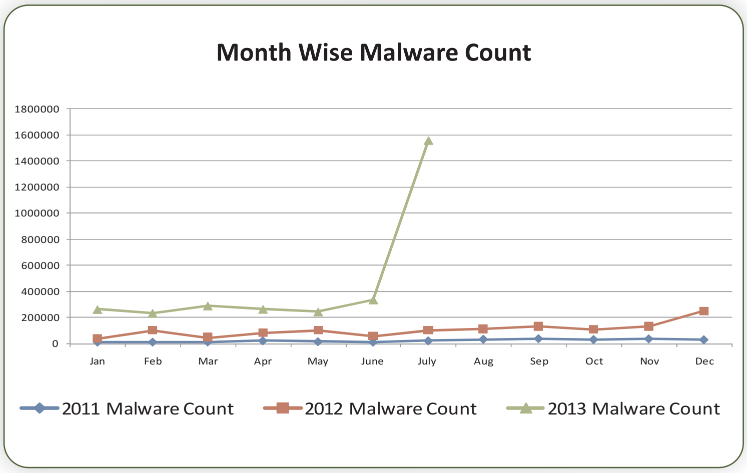
The infected PC then harvests data that it receives from the malicious spam server. The harvested data includes backup mail server, sender name, recipient address and various email templates. A hacked website will usually contain a randomly named folder with several PHP scripts.


Malware Count by Extension

Is safeguarding data turning out to be a daily struggle?
With the rise in Mobile and Windows based malware, the need for two-factor authentication and tighter security controls are beginning to be a must have for large businesses. With time, it will in fact become the only choice to safeguard critical assets of a company. Over the years we have seen companies grow to almost double its potential and with that growth we have seen them equally struggle to keep up to speed with the evolving threat landscape. The main area of concern is the fact that a number of organizations simply fail at classifying data according to their importance. While the main functionality of the IT team is to secure

company assets from falling in the wrong hands, it is the business heads that need to take responsibility to secure all that is of importance.

Moreover, in our quest to provide the best of security we have noticed employees pilfer through sensitive company data. While internal attacks have been of utmost concern, it is the web based attacks that need to be kept at bay. While a good firewall does the job in blocking in blocking external threats, the ability to breach a company's security perimeter is just a click away. One click on a wrong link or access to a malicious website is all it takes to infect the whole network.



Take the instance of news outbreaks such as the birth of the royal baby and Spain's deadly train crash. The news was covered by almost all media around the world and was the most talked about. It was also the most sought after by hackers to help spread malware. A message masquerading as news was linked to malicious software, using the birth of the royal baby as bait. Clicking on the link installs the Zbot malware, which is made to siphon off the users banking details.

The main reason to target breaking news is for the sheer number of readers they attract. Larger the number of readers larger will be the chance of spreading the infection. Any major story which covers natural disaster to peppy celebrity news is bound to become a hot target for malware based scams. And it goes without saying that natural disasters and human tragedy are bound to be followed up with fake donation sites.

If you have taken note you will realize that this month has also witnessed a massive spike in the distribution of malware. The scale at which they have risen is close to 4 times of what we noted in June and it has by far been the most active month in comparison to the previous six. It has also witnessed a rather large number of compromised Apache Web Servers which cumulates to roughly 63.12%. With that said, cyber-criminals have been making use of a number of malicious HTML (31.48%) and PHP (21.40%) based scripts to further infect web users.

The charts itself explains that spikes like these will not just remain as spikes but they will grow into something that we will be noting on a monthly basis.

Disclaimer

The above report is based on malware URL collected for the month of July, 2013 and is a representation of the growth in malware infected URLs in the span of 1 month. The domains mentioned were found infected at the time of report creation. However, the domain/site/URL might be safe now as the infection may have been removed by the host. MicroWorld Technologies Inc. is not liable to any party for any direct, indirect, special or other consequential damages caused.

All artwork and content is property of MicroWorld Technologies Inc. and cannot be used or reproduced by any person or company without the written consent of MicroWorld Technologies Inc. Any unauthorized reproduction of artwork or content is subject to legal action. The information is provided by MicroWorld Technologies Inc. without any assurance or guarantee of its correctness, be it express or implied. Neither do we make any implied affirmations regarding the negotiability, the suitability for certain purposes or the nonviolation of laws and patents.

Any concerns as to the legality of reproduction should be directed to:

The Marketing Department
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.
Web site: www.escanav.com
E-mail: marketing@escanav.com

All other trademarks, registered trademarks, company names, product names, domain names and brand names are the property of their respective owners, and MicroWorld Technologies Inc. disclaims any ownership in such third-party marks. The use of any third party trademarks, logos, or brand names is for informational purposes only, and does not imply an endorsement by MicroWorld Technologies Inc. or vice versa or that such trademark owner has authorized MicroWorld Technologies Inc. to promote its products or services.

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