‘e Scan

Malware Report

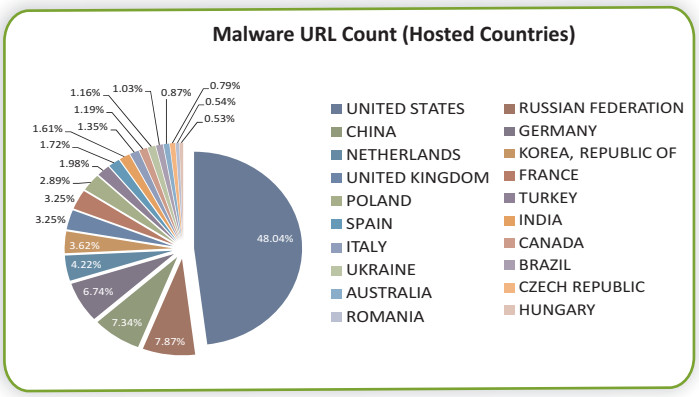
(November 2012)

E-mail: marketing@escanav.com

Web site: www.escanav.com

Malware Report - November

Another year comes to an end but not without leaving a trail of security issues and concerns. This year also saw a shift in the over trend and



distribution of malware. The rise in Smartphones have essentially turned them into a fundamental objective for cybercriminals, who have started to target these devices at a much larger scale.

Here is our take on what we expect to see in the 2013

Difficult to Detect Malware

Undetectable Malware – the perfect malware that a hacker can ask for. The method generally revolves around creating millions of mutant variants which are then scanned using a cloud based service that is home to a number of security products. Services such as these come for as little as $1 for 24 hours of unlimited usage, where hackers are allowed to test any number of malware against detection. The perpetrators then release the undetected malware variants into the World Wide Web to further infect unwary users. Cloud based services will play a major role since they will be the main point of contact for a number of malicious coders.

Exploitation of Social Networks

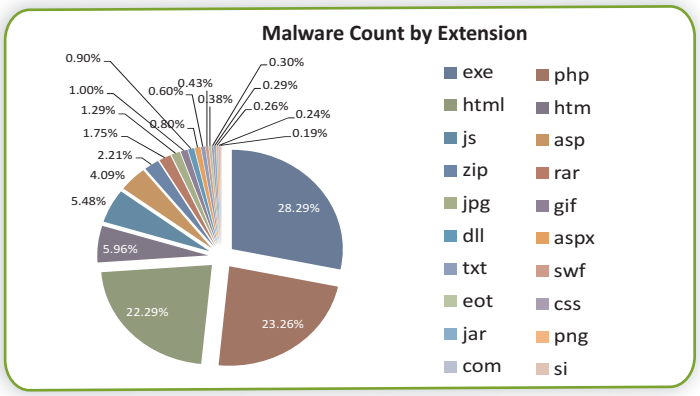
Social networks are not only considered as an excellent platform by the general public but it also comes as a perfect fit for cybercriminals. First and foremost, it can be easily used to spread spam and scams using the all famous news feed. Social networks are also considered as a launch pad to conduct attacks on unsuspecting victims – this can be achieved by impersonating as a 'Friend'. Also, more than 70% of URLs shared are shortened links, where at least 55% of the links posted lead to malware. And these are the links that users click without giving a second thought.

Use of Rootkits to Conceal Zero-Day Attacks

Operating system vulnerabilities make up for the most sought after attacks by cybercriminals. However, they are difficult to come by. To successfully exploit such vulnerabilities and to be able to go undetected, the need to conceal the malware using a rootkit is what most hackers look out for. Not only are rootkits difficult to detect but are also extremely difficult to remove as it conceals itself at hardware level. Moreover, they give Administrator level privileges to attackers and can go undetected to a general user.

Java Based Attacks

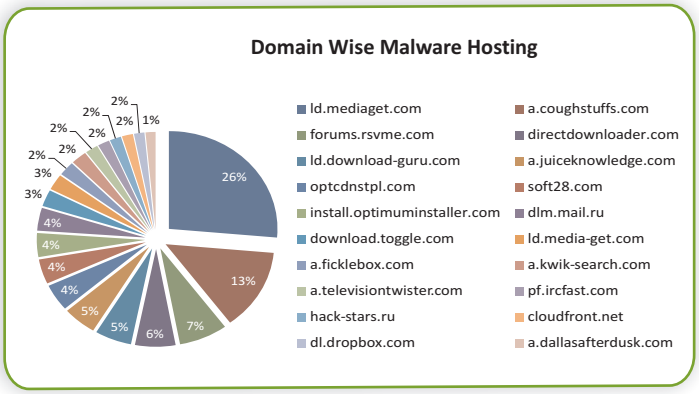
It is also seen that the malware will continue to target vulnerabilities in Java, Flash and PDF. We have and will be witnessing a continuous use of exploits specifically targeted towards Flash, PDF and Java based components. Exploiting such components will remain to be a malware coders delight as their patch process is slow in detecting and blocking multiple vulnerabilities. Moreover, by writing code in Java, hackers can attack Windows, Linux and Macs using platform independent code.



Mobile Malware

Smartphones are the new hot targets by malware writers as they are the next big thing in both communication and entertainment. Smartphone based attacks involve infecting legitimate applications. This is achieved by changing application permissions to application updates which are generally not there when the application is first installed.

Mobile devices are reshaping the way people communicate across the network and the rise in Smartphones and Tablets are giving rise to Cloud based services. With so much happening in the



Mobile segment, it goes without a doubt that targeted attacks and theft of personal information will see a definite growth in this segment. Now, since Desktops and Laptops cannot be written off completely, there will be instances where malware will be programmed to run and execute on both PCs and Smartphones/Tablets. We have seen this in the past and this trend will set new standards in the malware industry.

Mac Based Malware

The Mac malware has been the topic of discussion for most security researchers. Not only have we witnessed that the once impenetrable Mac was just a myth but the threat to this once supposedly secure OS has grown by the numbers. What seemed to be a harmless flash downloader turned out to be one of the most effective method used in infecting Mac's around the world. Distributed as a fake Flash Player update, the Flashback malware was effectively distributed using malicious websites. However, there were a number of legitimate sites used in successfully spreading the malware. For instance, Hacked WordPress blogs were being used as a platform to distribute this malware, resulting in infection in over 700,000 Mac OSs. Attacks on the Mac might be low at the moment but this is one segment that will need to be closely watched.

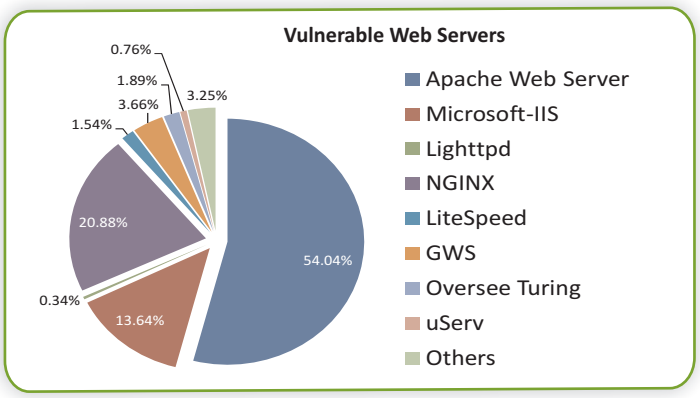
Industrial Attacks

The security industry has witnessed a significant change in the development of malware. APTs (Advanced Persistent Threats) like Stuxnet and Flame have made headlines with their complexity and methods at evading detection. It goes without saying that they are also the most difficult to detect and can go undetected for months or even years. Moreover, the overall sophistication of the attack highly depends on the security of the chosen target. For instance, if an attack can be carried out using conventional phishing and common exploit kits, the use of complex techniques such as this would not be used by adversaries.

Defending against APTs is not only tough but the tools that are used to keep such attacks at bay are often ineffective. Reason being, cybercriminals behind the creation of APTs are at constantly innovating various tactics and procedures that help circumvent security protocols and standards. Here, APTs are used with a very focused with a precise objective in mind and are financially resound, adaptive to change, resilient and patient. Here the threat will change with respect to the security deployed, until the set objectives are achieved or will withdraw if the overall cost of the operation outweighs the value of the target.

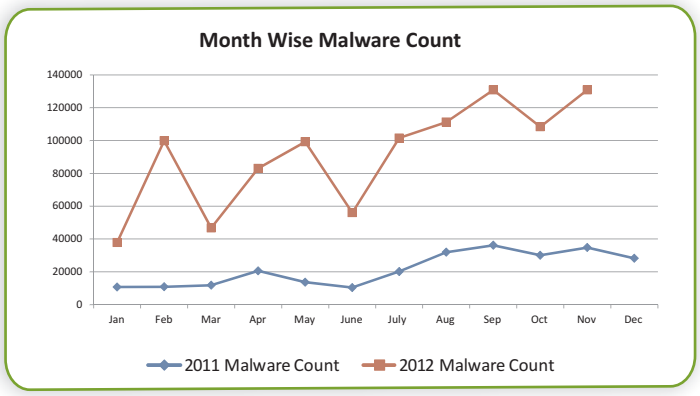
The Growth of MaaS (Malware as a Service)

In a spate of things to come, the cloud has given birth to a number of services. We have Software as



a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Now, add a new one and we have Malware as a Service (MaaS), which is slowly seeing a rise in the malware industry. The Internet has become a source for free or low-cost malware that is easily customizable to meet every hacker's need. Malware as a Service significantly reduces the skill set needed by a cybercriminal to launch automated attacks. The result is a shift in attacks from large corporations to smaller companies.

Take the example of Citadel – based on the ZeuS source code, this particular malware model aims to provide better support to its customer base while at the same time it allows cybercriminals to customize the Trojan according to their needs and command and control infrastructure. Going even a step further, malware authors have developed an



online platform where customers can request features, report bugs and even contribute modules. Moreover, this new development also comes in as an indication of a trend in malware evolution.

Just like many legitimate software companies, the project based on the Citadel model brings in a whole new service via a customer-relationship management model. The said project has already led to the creation of various modules which further adds better encryption, video/screen capture and methods of avoiding detection -- some of which that are coded by Citadel developers, other by the project's customers.

What's amazing is the conceptualization of MaaS. Just like large corporations a huge amount of detailing has gone into the creation of such a service. The lifecycle of the product is what these malware creators excel at – from design to release to after sales support - each stage is implemented in every detail with care and attention. What we have here is a new level of design that caters to complex solutions which is highly scalable and effective. The complexity of such a design itself shows the need for high skilled (malware) programmers behind such projects.

However, an important factor to note is the crime organizations financial and geographic growth has shown little slowdown over the years. This basically boils down to the lack of awareness towards most web based threats along with the constriction of preventive measures have played in favour of online crime. What most fail to understand is the fact that no company, no matter how big, are not immune to attacks.

Now coming back to the topic, what's interesting is the sale and support offered by this channel, which more often than not resemble the workings of a legal demand and supply chain. And as previously mentioned, analysis and enhancement of the product are done by submission of bug reports using an online platform. In addition, bug reports are also collected from various underground sites. This drastic change has in-fact further helped them market and sell their products.

Given below are the main services offered using Citadel's platform:

- An online network for customers such as the Citadel CRM Store. This allows users to be an active player in the malware product development lifecycle
- Reporting of bugs and other Software related errors
- A discreet platform meant for Code Sharing. Each client can share various modules and software code with one other thereby creating new modules or improvements
- Promotion of public proposals for software improvements along with the addition of new features
- Various communication channels which would include instant messengers and jabber channels

It goes without a doubt that the continued advancement in malware will keep researchers and anti-malware vendors busy in the coming months and end users will need to be vigilant while going online to reduce the chances of an infection.

Disclaimer

The above report is based on malware URL collected for the month of November, 2012 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.

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

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

Brasil:
eScan Brasil Ltda
Rua Augusta, 1836 - 7o Andar
CEP 01412-000 - São Paulo - SP
Brasil.

Tel: +55 11 4063 6500

E-mail: vendas@escanbr.com.br
Web site: www.escanbr.com.br