







INDEX	
Malware Report	1
Anonymous OS	1
Duqu Rises	2
The Growth of MaaS (Malware as a Service)	2
Our Offices	5







Anti-Virus

Malware Report

Predicting future threats can be a hit or a miss for any security research organization. It certainly is interesting to wear our prediction hats and predict about what might happen in the coming days or months, but the question to ask is – how much do threats really change each year? The last 12 months have brought in a great deal of change in the overall behavior of malware, but can they really be considered as evolution or revolution of malware or probably a mix of both. With the progress in time we have in fact seen great changes/developments in the field of mobile malware, social

media, client side exploitation, hacktivism and targeted attacks. The following growth is just a tip of things to come and many of these changes will continue to influence the threat landscape for years to come.

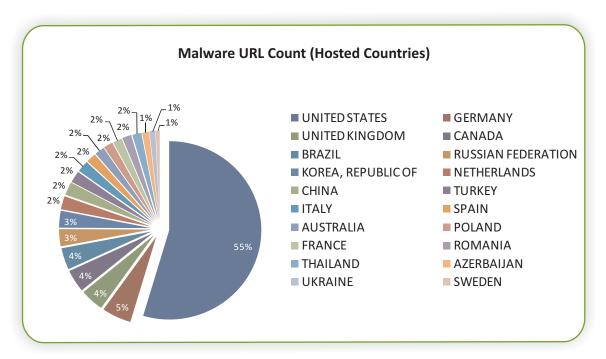
From fake OSs to resurfacing of Duqu to the sudden growth of malicious services such as MaaS (Malware as a Service), March has been a rather busy and growing month in terms of malware related news.

•••••

Anonymous OS

The release of the 'Anonymous OS' saw a lot of hits last month with downloads touching a few thousands within minutes of its launch. Wrapped in malware, the OS did more harm than good to anyone who installed it. This itself shows the depths to which cybercriminals will go to compromise users. The creation of the OS itself suggests a shift from DDoS attacks and social networks to more involved software based effort. The deal

here is to ask yourself as to why would anyone want to put their trust on an unknown OS which also happens to be created by a bunch of unknown people. The OS doesn't come as a threat to the average person or to even office workers. The only people who might be impacted by it are those who are foolish enough to knowingly install unknown software onto their PC.





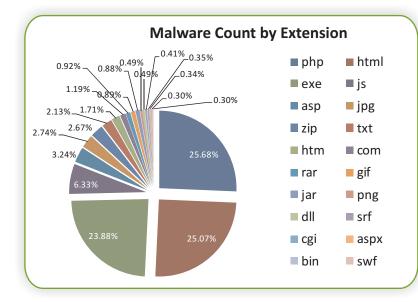




Anti-Virus

Duqu Rises

After several months of sabbatical, the creators of Duqu have recompiled one of the Trojan's components sometime in late February. The new malware comes with a modified system driver which is responsible for decrypting the rest of the



already downloaded package, which it then loads into the memory of the PC. The new driver now comes with a newly compiled date – Feb 23, 2012 while the previous driver comes with a recompiled date pointing to Oct 17, 2011. While the overall functionality of the driver remains the same, the change basically marks an effort made to slip past security software and Duqu sniffing tools such as the open source Duqu Detection Toolkit – created by the Laboratory of Cryptography and System Security (CrySys) at the Budapest University of Technology and Economics last November.

With an extremely low number of infections Dugu comes in as a malware specifically designed for data exfiltration. This particular malware comes with no payload and is built with just one motive – to gather and send back information to its command and control centers. Studies show that attacks are mainly carried out on power plants, oil refineries and pipelines. It goes without saying that Dugu is an ongoing work in progress and since the nature of the malware is more target specific, it is highly likely that the new system driver has been recompiled for a new victim. This also means that the creators have also come up with new and different techniques to bypass certain security measures and in most cases have a new zero-day.

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 (laaS). Now, add a new one and we have Malware as a Service that 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



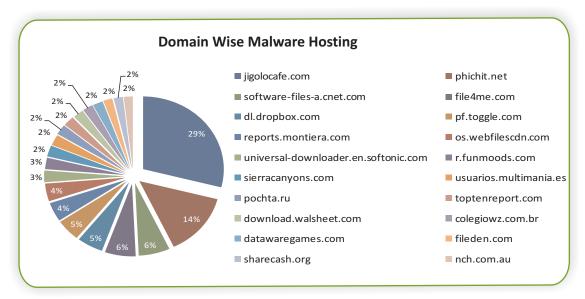
.....





Anti-Virus

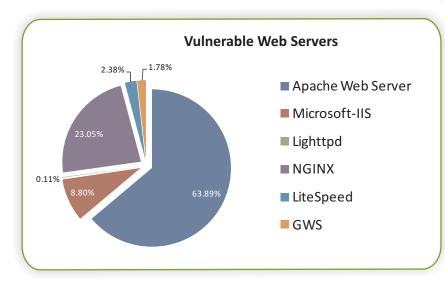
companies, the project based on the Citadel model brings in a whole new service via a customer-relationship management model. The said project has lifecycle of the product is what these malware creators excel at – from design, to release to after sales support - each stage is implemented in every detail with



care attention. What we have here is a new level of design that caters to complex solutions which highly scalable and effective. The complexity of such a design itself shows the need for high s k i l l e d (malware) programmers behind such

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 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 favor of online crime. What most fail to understand is the fact that no company, no matter how big, are 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.







Anti-Virus

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

The above stated model isn't just relevant to the Citadel malware but is essentially applicable to all kinds of malware from the moment the source code is exposed. Malware developers can then use this platform to feed in improvements to meet business needs. This itself shows how critical this transition can be for the malware business community. If and when successful a model such as this can speed up the process in malware creation and can also rope in a large amount of revenue for malware developers.

According to online statistics, a basic

Month Wise Malware Count

100000

80000

40000

Jan Feb Mar Apr May June July Aug Sep Oct Nov Dec

2011 Malware Count

2012 Malware Count

Citadel package which would include a bot builder and a botnet administration panel retails for \$2,399 along with a monthly rent of \$125. However, innovative and premium features are sold separately as add-ons. Among these is a software module (\$395) which basically allows botmasters to sign up for services which automatically updates the bot malware to evade the latest antivirus signature. Each update costs an extra \$15.

However, if we look at a broader aspect of this model, the development could benefit discreet government agencies towards strategical recruitment of hackers who work closely in the development of malware. A platform such as this will bring about an ease when it comes to searching for hackers with high skill sets. The outcome, a coherent team that can be potentially lethal especially when the development is more focused on the creation of a cyber weapon.

The famous 'Tilded' platform used in the development of the infamous Stuxnet and Duqu malware goes on to prove the previously stated argument.

The question to ask here is: what are the chances of a community being built that will solely be dedicated to the development and enhancement of malware? Seems similar to a malware run

business? Kind of, but cannot be considered as a mirror image. A development model run by a discreet government body is more target specific and focused.

Such scenarios are not new since the inception of Stuxnet followed by Duqu. It is therefore important to remain vigilant as we will be witnessing a significant growth in the cyber crime industry. There is no stopping the rise in web threats. The only thing we (Government/Private sectors, Individuals) can do is to implement strategic actions to contain the threat.







Disclaimer

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

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

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

ndia:

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

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

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

