‘e Scan

Malware Report

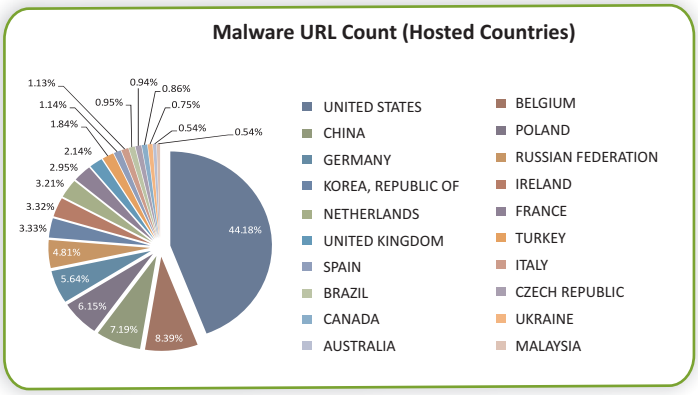
(October 2012)

E-mail: marketing@escanav.com

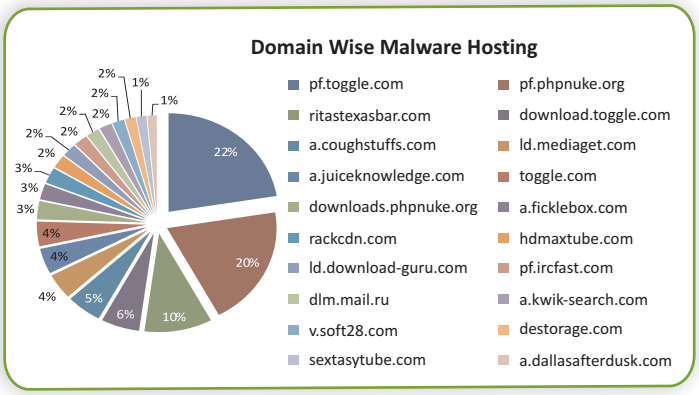
Web site: www.escanav.com

Malware Report - October

Information security is probably one of the most discerning factor that has plagued the Web. The term information security however is not anymore limited to securing data stored on desktops, laptops or servers. Smartphones are beginning to play a much larger role in the distribution of malware. In this day and age, protecting and blocking information theft has become the number one priority not only for enterprises but for users as well.

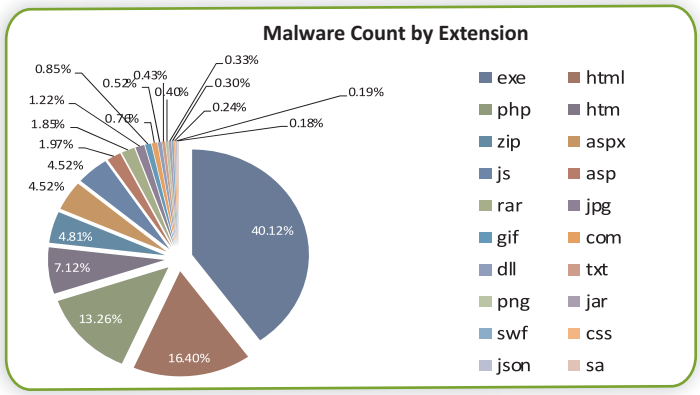


The rise in Smartphones was inevitable and with technology progressing at such pace, it won't come in as a surprise to see them replacing their desktop counterparts in the coming years. Smartphones have also made way for larger known devices such as the Tablet PC. When combined, these two devices are like a powerhouse filled with options of running and executing your daily tasks – an aspect that laptops are also designed to do but with the added weight and bulk. Now who would want to carry a device that's three times heavier and at least seven times bulkier than a Smartphone.



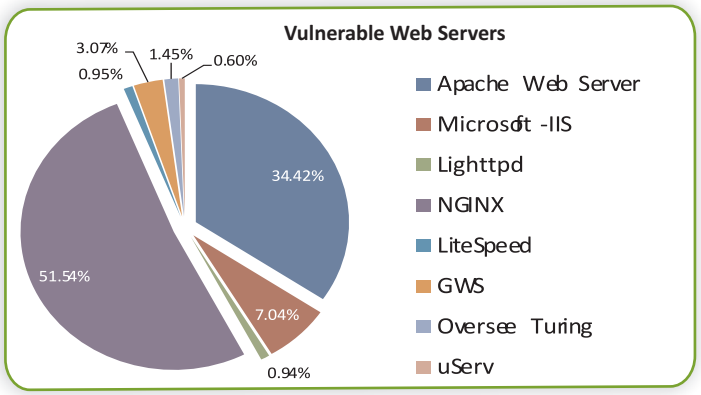
There was a time when the so called IT gurus had predicted a PC for every household. With technology progressing at such rapid pace Smartphones have eaten into the sales of both Desktop PCs and Laptops. From big brands such as Samsung, HTC, Nokia to lesser known brands – the mobile market is flooded with options that cover all price levels.

Mobile devices are reshaping the way people communicate across the network. Close to 30% of adults in India gather news using a mobile device while the recent Olympic event attracted over 40% of mobile users. Growth wise also, Mobile apps are seeing 100% revenue per year. On the tablet front, 80% of iPad users used the tablet for browsing the web. In addition over 600-million users used the mobile platform to log into Facebook. Mobile users in China have surpassed desktop users and we are going to witness this globally in the coming years. Mobile Internet users in China have also grown by 192% since 2010.



Smartphones and Tablets are also giving rise to Cloud based storages which basically allow users to store data as well as personal information. Till date the use of Cloud based services have attracted a limited number of users. This will however change in the next couple of years as the number of service providers are slowly increasing by the numbers. We have seen Google's Cloud Drive, SugarSync, Dropbox, iCloud, Box, Carbonite and Mozy cater to the needs of Smartphone users. The freedom that phones

provide – Smartphones in this case – are nothing like what they were 5 years back. They give you



direct access and control over emails, files, photographs, document editors, etc. More so, they even allow users to connect remotely to their laptops or desktops, which can either be at home or office.

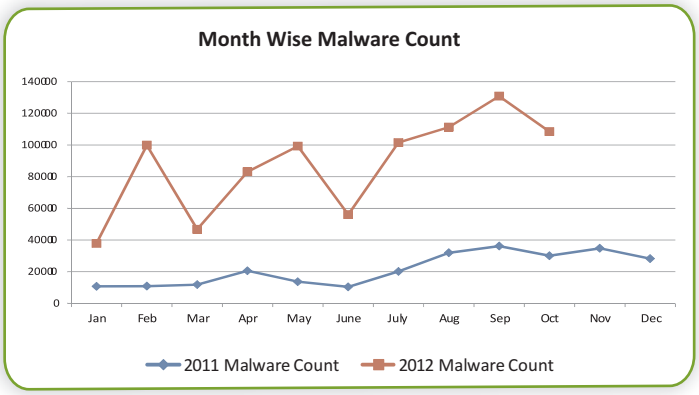
With so much happening in the Smartphone & Tablet segment, it goes without a doubt that targeted attacks and theft of personal information will see a definite growth with regard to this segment. Now, since Desktops and Laptops cannot be written off completely, there will be instances where malware will 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.

The Android Operating System attracts over 75% of most Smartphones which also makes it the most sought after target by malware writers. As recent as two months, there have been close to 200,000 suspicious programs posted in various app stores. Google Play itself has been home to embedded malware. Instances where rogue apps pose as legitimate applications have been growing by the numbers and users fail to make the difference between a legitimate app and malicious app.

In the last three months there have been records of over 35,000 rogue applications that are made to gather information on the user. With that being said, users need to understand the importance of giving access rights to an application when requested. Well over 95% of most Android users overlook the need to check the type of permission an app asks for before installation. The use of an Anti-Virus is also limited to just 15% of most Android users. In other words, 85% are still unaware of the dangers a Smartphone is likely to bring.

On the positive side, users who stick to Google's very own app store are less likely to get infected by malware, as the company is quick in taking down malicious applications (such as the ones that take more information than required). However they do run the risk of leaking sensitive data as a number of apps are made to send back user related information (mainly used for marketing purposes). The biggest problem at hand is the use of third party or independent app stores. With China leading the charts, there are many who use this as a gateway to download apps that are otherwise payable on Google Play.

There has also been evidence of the growth of Chinese hackers who are more focussed on various Indian military agencies and the Tibetan human-rights group. The apps currently under development can be made to siphon off



information and install addition components on the phone. A number of targeted attacks are currently focussed on various governments and companies, while 20% are targeted towards non-governmental and non-business organizations.

With more and more people switching over to Smartphones, there will be a definite increase in the use of cloud services – be it for enterprises or end users. Again, customer education plays a very important role. According to statistics it is seen

that small and medium businesses are simply putting their data in the hands of third parties without taking note of the security being implemented. Over 75% of organizations are making use of at least one of the many cloud based service but a mere 30% ensure that the data held by external providers are being encrypted. Therefore it makes it essential for private cloud providers to do a minimum of three things:

- Be clear about their prospects and their approach to security. State what options are available to adopt, without compromising security in the process.
- Communicate in standardized language and classify the various security risks and solutions, thus allowing companies to compare different providers easily when making purchasing decisions.
- Educate end-users on what they need to look for technically & commercially to ensure data security when migrating to a cloud-based solution.

'e Scan
Anti-Virus
& Content Security

Disclaimer

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

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