‘e Scan

Malware Report

(April 2012)

E-mail: marketing@escanav.com

Web site: www.escanav.com

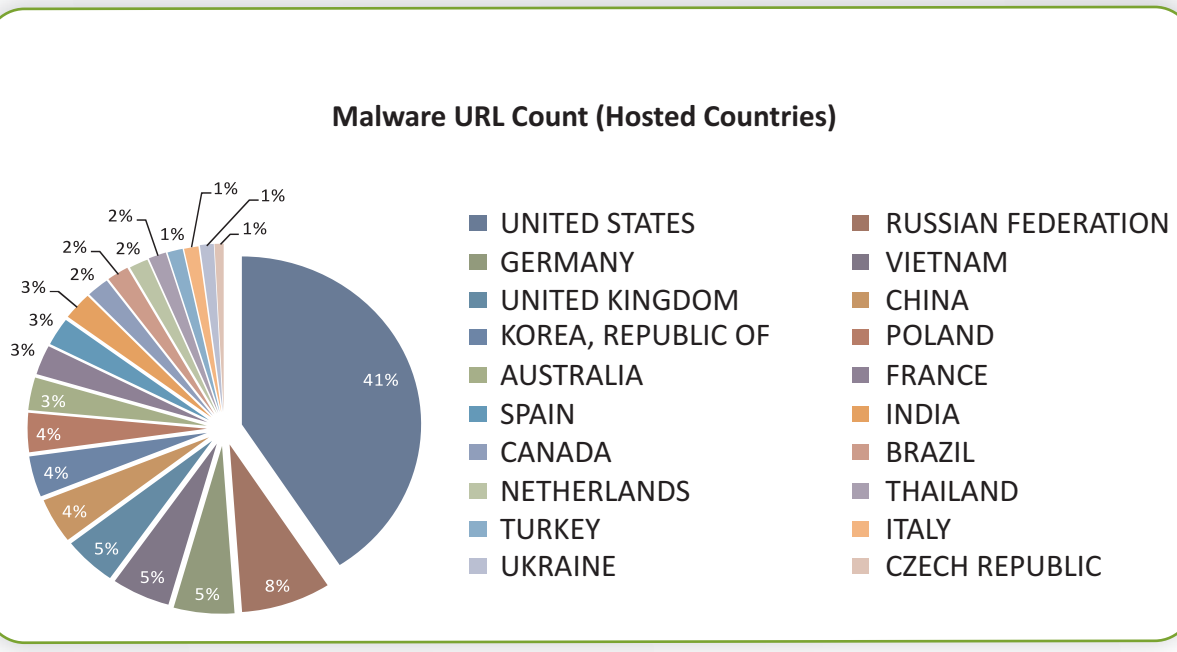
INDEX

Malware Report

Cyber crime has always been a growing concern for online users and it's only going to get bigger. April has been one of the most trending months – both in terms of technology and malware infection.

On the positive aspect we are beginning to see a transition in the way data is accessed and stored. With Google entering the cloud with its all new and revamped 'Cloud Drive' we will be witnessing a change in the way documents and files are accessed and stored. That doesn't change the fact that Google was always a cloud based concept and it definitely isn't the first to have implemented the concept of 'Keep Everything, Share Everything' with Google Drive. We have SugarSync, Dropbox, iCloud, Box, Carbonite and Mozy – to name a few, which are also cloud based and come with 5GB of storage space (selected few). The million dollar question here is – 'Would you consider your documents to be safe and secure on a drive that's beyond your reach?' 'Would you consider saving confidential documents on the Cloud?'

As far as storing confidential information is concerned, public clouds are a big no to come by as data stores. And storing them on Google Drive can severely cause major security implications. For now let's keep aside the various security loopholes concerned with public cloud services and just peek into a section of Google's policy. According to Google their policy states that "Google reserves the right to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute content uploaded to their services." Preceded by a statement that states "You retain ownership of any intellectual property rights that you hold in that content. In short, what belongs to you stays yours." The fact that Google's policy itself states to host, store, reproduce and modify should stop businesses from uploading private and confidential data. Moreover, policies should be defined by IT admins that would help prevent users from accessing public clouds.



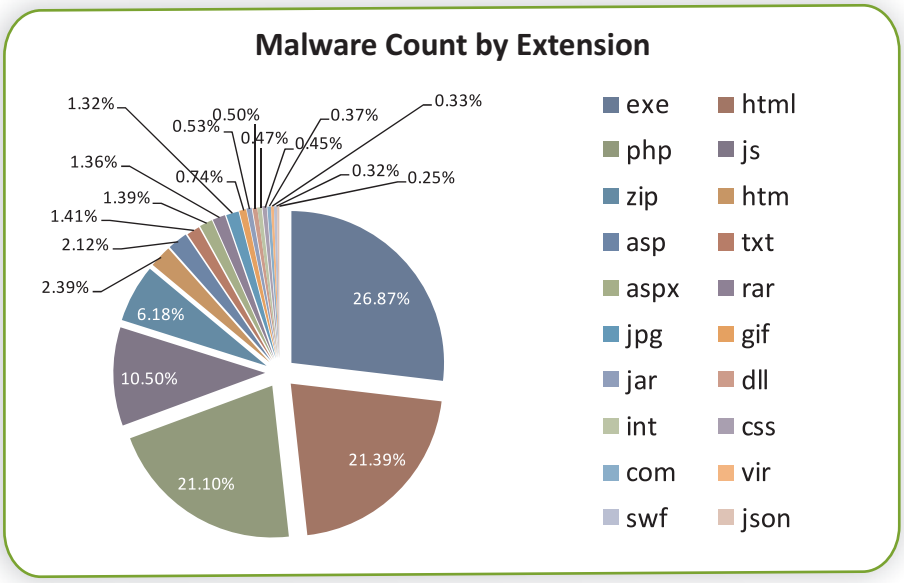
As mentioned, data security should be the utmost concern for cloud providers – be it for enterprise based users or end users. Again, customer education plays a very important role. According to statistics it is seen that small and medium businesses are simply putting their data in the hands of third 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.

Bring Your Own Device (BYOD)

Another growing concern to businesses is the rising trend towards BYOD (Bring Your Own Device), as this movement is blurring the lines between work & personal life. However, the benefits might be plenty but there are security concerns that need to be addressed.

For starters, BYOD generally tend to shift the cost of hardware to users. So with the employee bearing the cost for hardware and related services, companies tend to save a lot of money. The second significant difference is employee satisfaction. Employees have invested in laptops and Smartphone's for a reason and these are the devices they prefer to use more often than being limited to laptops and mobile devices issued by the company. In addition, the devices honed by employees are far more superior than the devices issued by the IT department – in return organizations get the benefit of the latest features and capabilities. Employees also tend to have a faster upgrade cycle than the painfully slow upgrades most organizations have.



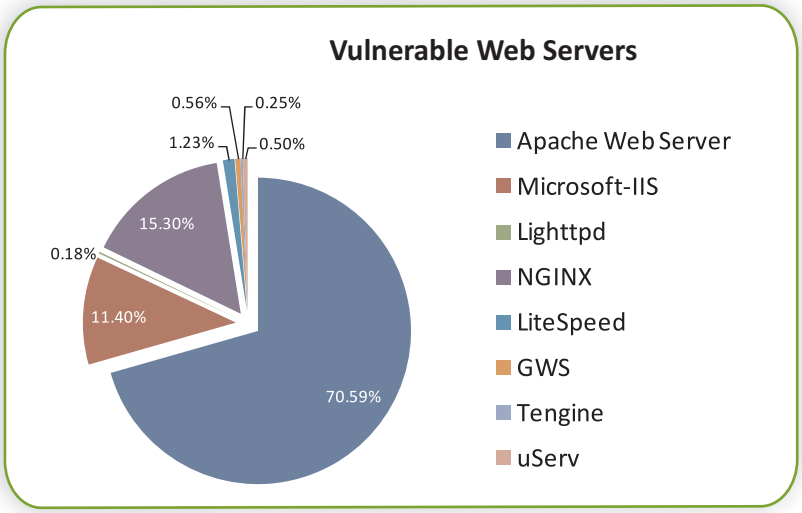
Concerns

Implementing BYOD programs aren't a bed of roses for organizations as companies lose much of the control over hardware. There are major issues to look into as well.

For instance, company issued devices come with predefined security policies that are actively managed and updated by the IT department – A more widely accepted policy that helps differentiate between what's acceptable and what's not.So when implementing BYOD companies

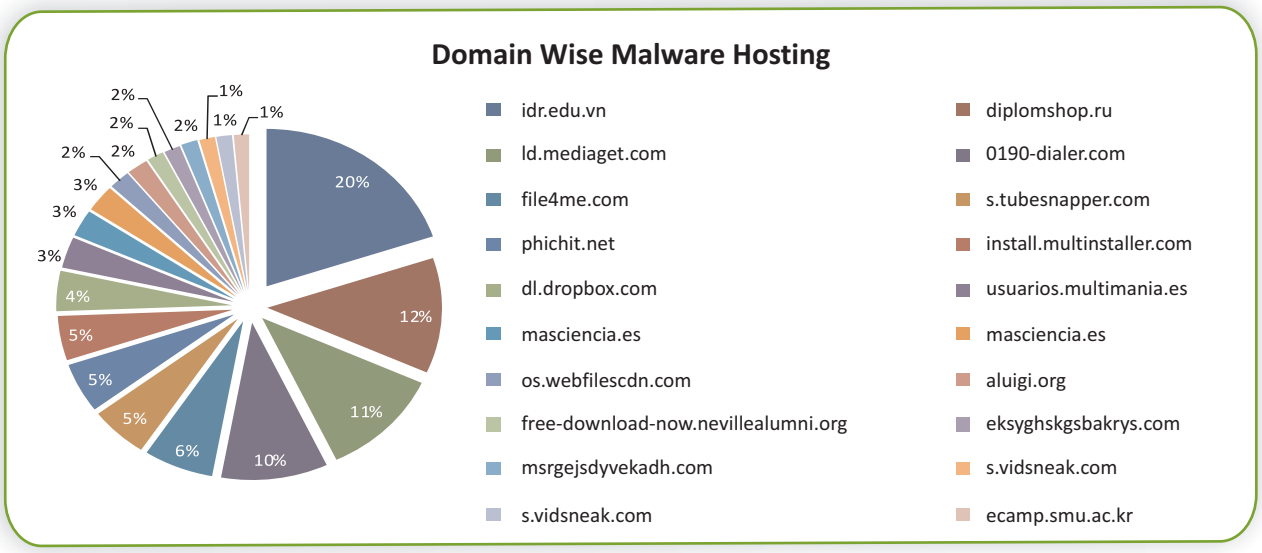
should outline the key aspects which basically state the way devices are or need to be deployed. In addition companies should make it mandatory to implement company-issued security tools as a rule towards allowing personal devices when connecting to company resources.

In lieu to the above mentioned concerns, there are also a number of compliance and ownership issues as far as data is concerned. Compliance such as PCI DSS, HIPAA or GLBA have certain requirements that need to be addressed when securing specific data. Companies need to adhere to the rules laid down by compliance authorities even if the data is on the laptop owned by the employee. Again, in the event an employee resigns retrieving data owned by the company can be an issue. To curb such discrepancies, policies need to be placed which basically defines how the required data will be retrieved from the employee's laptop or even his/her Smartphone.



A Growing Concern for Mac Users

News that has really taken the bite off most security analysts is the sudden focus on the Mac community. An estimated 800,000 Mac users are said to have been infected and part of a massive bot network – all thanks to the Flashback Trojan. The detected version of this Trojan is said to be more of a drive-by-download threat and therefore doesn't require any interaction by the user. The threat is said to work when the user visits a malicious or compromised website. And this is exactly



why drive-by-downloads are considered as one of the leading tools in spreading malware.

What are the odds of success for a drive-by-download?

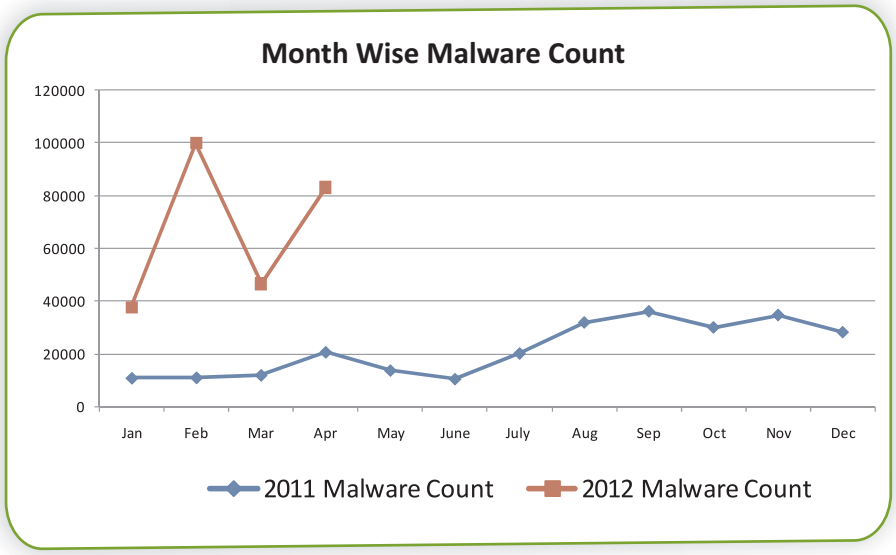
The numbers speak for itself – if 800,000 infected Macs don't spell success for you then we don't know what will. The main issue that lies here is the very fact that Mac users have been conditioned to believe that the Mac OS is virtually impenetrable. This brings us to believe that fewer number of users have an antivirus installed to help protect their Mac OS. It is also seen that Mac users are twice more likely to click links than a Windows based user.

However, the fault doesn't lie in Apple or its Operating System. The main vulnerability was in Java but users and the rightful owners need to understand that the increasing success of the Mac OS will bring in more attention from malware writers. Mac users will also witness an increase in drive-by-downloads particularly the ones that are Flash and Java based.

How much is the Malware worth?

With Flashback being the largest targeted malware campaign the total net worth shouldn't come as a surprise. Over $10,000 a day is said to be pocketed by the malware authors. The malware is specifically crafted to sniff out search queries made on Google, following which it redirects users to a page that of the attackers choosing – where revenue is generated through clicks. In other words, when an infected user clicks on a Google advertisement, the malware analyses the request and substitutes the advertisement with its own.

The total number of Macs infected with the Flashback malware is said to have decreased over time but still remains to be threat that should bring about a concern to the Mac community.



Disclaimer

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