‘e Scan

Anti-Virus

Linux The Unknown Truth

eScan for

Linux: The Unknown Truth

In this rapidly growing base of server platforms, Linux has seen a rise in popularity as a server platform for corporations. The aim of this paper is to give you a basic insight of the growing threat to businesses that depend on a multi-platform network.

Linux for Business Platforms

Linux has come a long way as an operating system, ever since its inception in 1991. The main reason for its wide acceptance is mainly due to its open source rules, allowing large and medium sized organizations make customized applications for personal as well as official use. Linux is no longer used by just a handful of users – it is being adopted and has gained popularity amongst large corporations. And unlike its predecessors, the ever changing platform and with the adoption of management tools, support and services offered by distributors such as Mandrake, Debian, Red Hat, SUSE has made this open source OS more accessible to businesses. Linux has by far proved to be more than a popular commercial asset for corporations and is being increasingly used on servers for mainstream applications which include email, web, file and print sharing.

We have seen a wide acceptance of Linux as a server side platform on enterprises and will continue to grow over the next few years. That's not all, this open source operating system is also seeing potential growth on desktops and laptops, which basically also draws preference towards a multi-platform (Linux with Windows on clients) solution for most organizations. Now, from a security perspective, Linux has been considered as hard to use but a safer and more secure platform than Windows. Nevertheless, with the growing number of users and with Linux being widely accepted amongst corporate, government and education services it does come with its own set of flaws.

Ever Increasing Threat to Organizations

When in a multi-platform solution the chances of spreading an infection are high. In an unprotected Linux environment viruses based on Windows can hide and spread across the organization when two systems interact. Spreading of malicious code to and from Linux based systems can take place via mail and web protocols and also via network shares such as Samba and NFS. However, infecting other companies can not only damage the organizations reputation but can also bring up legal issues.

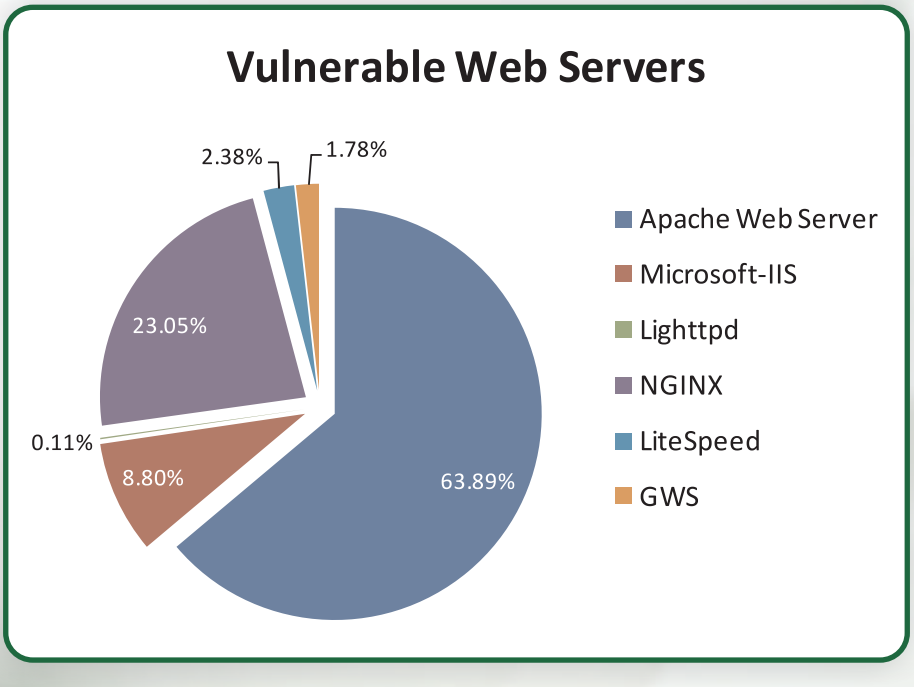
With a majority of viruses, worms, Trojans and spyware targeted mostly towards Microsoft's Windows OS, the main area of concern is the overall susceptibility of Linux to malware. The main reason for Microsoft to be the focus of targets is due to its market dominance and with Linux continuing to grow as a mainstream operating system, it will only be a matter of time before it becomes the point of focus for malware coders. With a wealth of information available on the web and with its open source code structure, Linux will slowly witness an increase in web based attacks.

Linux Malware

Vulnerabilities on any platform are liable to exploitation. This is increasingly true as virus writers, spammers and cybercriminals join forces to steal data and money from unsuspecting businesses through spyware, phishing and similar attacks. Vendor based security patches to eliminate system vulnerabilities have become a priority to be published for UNIX systems as they are for Windows. The need for patching basically states that the Linux operating systems do exhibit vulnerabilities. These can be – and have been – exploited.

So the risk of infection on Linux platforms is not to be ignored. The relatively low number of viruses, Trojans, worms and spyware attacks on Linux environments does not define a cybercriminal's inability to create viruses for the Linux operating system but instead

it reflects on the majority of Windows based users.
Many consider Linux to be dependable, easy to use and secure as an operating system but most are oblivious to the fact that Linux is also susceptible to malware infection. It is vital to remember that no operating system is tough enough to withstand a virus attack. With that said, just a single infection is enough to bring down the whole network.
In addition, a large proportion of Apache web servers are hosted on Linux (or some flavor of UNIX). Increasingly, these servers are being targeted by malware writers as a means of placing malicious code on legitimate websites. As shown below, 63.89% of Apache Web Server's were vulnerable to web based attacks as compared to just 8.8% for Microsoft-IIS. What people don't seem to realize is the growing threat to Linux machines. Here is the comparison you need to understand – What Linux is to servers is what Windows is to PCs – this basically defines the total number of Linux servers deployed in comparison to the number of Windows PC.



Linux: The Unknown Truth

Given below are a list of viruses that created havoc on Linux machines:

Linux/Slapper belongs to a family of worms which makes use of an OpenSSL buffer overflow exploit. Each varient of this worm targets vulnerable installations of the Apache Web server on the Linux operating system – this would include platforms such as SuSe, Mandrake, RedHat, SlackWare and Debian. The worm is also capable of conducting a range of Distributed Denial of Service (DDoS) attacks.

Win32/Lindose is the first cross-platform based virus to infect both Windows and Linux executable files. Once infected it searches for all files in the current directory and infects all executable files in Windows and Linux ELF files.

Linux/Lion is a worm that can create multiple backdoors by replacing critical system files. The worm is also capable of exporting passwords and system critical information to malware coders.

About eScan

eScan the world's first Real-time Anti-Virus and Content Security software adesktops and servers is developed and marketed by MicroWorld. It is powered by innovative and futuristic technologies, such as MWL technology, DIRC technology, NILP technology, and sophisticated Anti-Virus Heuristic Algorithms that not only provides protection from current threats, but also provides proactive protection against evolving threats. eScan provides 24x7 free remote support facility, integrated in the software to help customers to get their malware related issues resolved in the fastest possible time-frame. It has achieved several certifications and awards from some of the most prestigious testing bodies, notable among them being Virus Bulletin, AV-Comparatives, West Coast Labs (Checkmark), ICSA, and PCSL labs. Combining the power of various technologies, eScan provides Multilevel Real-time Protection to Computers and Networks.

For more information, visit www.escanav.com

Linux: The Unknown Truth

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