GLOBAL JOURNAL OF ENGINEERING, DESIGN & TECHNOLOGY
(Published By: Global Institute for Research & Education)
www.gifre.org

TRENDS IN COMPUTER VIRUSES: A REVIEW

[1]Erick K. Rotich, *[2]Metto Kimutai S, [2]Samoei K. Daniel, & [1]Lily Siele
[1]Department of Mathematics and Computer Science, University of Eldoret, Kenya
[2]Department of Information Science, Moi University, Kenya
*Corresponding Author

Abstract

Computer use is becoming part of our lives every other day however there have been considerable threats of computer viruses in the recent past. Viruses have had adverse effects on data and programs ranging from formatting hard disks, damaging information infrastructure, suddenly restarting machines, deleting or modifying data and in some cases mild effects such as slowing down machines or producing irritating sounds. Viruses have been a major cause for worry especially with the advances in data processing, storage and movement of information technologically. Many computer users and organizations especially the computer intensive organizations have had to invest heavily in dealing with viruses particularly those organizations running the windows platform. These computer viruses have been defined by their characteristics of entry and multiplication without the user's notice as well as diverting the normal functioning of the computer. This paper seeks to define a virus and explain its related terms such as malicious software, worms, and Trojan horses. It explains vulnerabilities of operating systems in relation to viruses, it makes an observation on strengths of Linux versus Windows, outline the present state of affairs, apart from using anti-virus software, there are other procedures which can help protect against viruses which are also mentioned, the future of computer viruses and the conclusion that the Internet is serving its purpose of interconnecting computer and hence promoting distribution of viruses then makes some recommendations on viruses.

Key words: computer virus, malware, operating systems.

1. Introduction

Computer viruses are software programs that are designed and developed to interfere with normal computer operations and spread from one computer to another without the operator's knowledge.

Computer viruses fall in the family of malicious programs which are otherwise called malware. Malware also includes rootkits, spyware, worms, Trojan horses and fraudulent adware. According to O'Donnell (2012), a rootkit is a silent type of malicious software designed to hide the survival of some processes from the standard methods of detection and enables illegal access to a computer. According to Wienbar (2005), Spyware is a type of malware that gathers information about users in a computer exclusive of their awareness. The existence of spyware is concealed from the user and can be difficult to notice. Oldfield (2005) defines a worm as a malicious program that exploits security vulnerabilities to extend to new computers through network and a Trojan horse as a program that shows undisruptive characteristics but conceals its malicious capability. Viruses exploit some system vulnerabilities whether in operating systems or some application software to get illegal rights of entry, harm other programs, and do damage to user operations or user data.

Viruses in the early years did spread slowly this was because they were mostly on floppies, but the evolution of computer networks and the internet has made spread easier and more rapid. The paradox is the more connected a country or an organization is, the more vulnerable it is to viruses.

2.0 The Vulnerability of Operating Systems to Viruses

Vulnerability is a flaw which permits an attacker to decrease a system's information guarantee. Viruses use vulnerabilities in operating system and application software to gain unauthorized access, spread, and do damage.

Different operating systems have different vulnerabilities to viruses. UNIX-based operating systems such as Linux have not been affected by malware threats as compared to Microsoft Windows operating systems.

Scott (2003) attributes the small degree of virus spread in Linux to the small number of users running as a desktop operating system, the inability for malicious code to access the root and fast updates developed and released to seal Linux vulnerabilities. Scott (2003) observed that some Linux versions such as Samba or NFS servers, may keep documents in undocumented, susceptible Microsoft layout, such as Microsoft word or Excel that may contain and spread viruses. Linux mail servers for instance should run antivirus programs in order to counteract viruses prior to them showing up in the mailboxes of Outlook users.

Linux servers may also be used by malicious code exclusive of any attack against them for example where web content and scripts are inadequately controlled and used by malware to attack any guests who may access them.

2.1 General Symptoms of Viruses

The following are some symptoms of virus infections in your computer system:

- Some system files may be missing or you receive error messages on missing files.
- The computer functions as anticipated but at other times, it stops responding.
- The operating systems may not start although you may not have done any installations or modified any programs.
- The computer takes longer than expected to run an application.

- The user may receive out-of-memory error messages even when the system has adequate Random Access Memory (RAM).
- When new images appear on the desktop that you did not create or put there.
- Whenever there are some strange sounds which are unexpected.
- A program vanishes from the computer although you did not remove the program.
- The computer may keep restarting unexpectedly.
- Computer programs may stop acting in response frequently.
- Computer hard disk partitions disappear.
- The computer may also crash.
- The computer may come to a halt when you try to use Microsoft Office objects.
- Whenever you cannot start or run the Windows Task Manager.
- When antivirus software detects the presence of a computer virus.
- Disk drives and disks may be inaccessible to users.
- There is a twofold extension on documents you lately opened such as .doc.exe
- An antivirus program is disabled for no reason. Additionally, the antivirus program cannot be restarted.
- Viruses corrupt data and makes changes to the data in applications.

2.2 Current Trends of Viruses

There is a new spot of anxiety in viruses which was first identified in 2007 of cross-platform malware. This has been greatly inspired by the attractiveness of cross-platform computer applications. This was brought to the forefront of malware awareness by the circulation of an OpenOffice.org virus named badbunny. Smith S (2007) of Symantec comments on this cross-platform viruses that scripting platforms, extensibility, plug-ins, ActiveX can be used.

There is a trend in Linux to malware that deceives the user to install a malicious software. This is often referred to as social engineering for example in 2009 a malicious screensaver called the waterfall was exposed which included a script to run some attack to deny users some services.

Another trend in current technologies is Software as a Service (SAAS) where software vendors provide support and maintenance on daily basis as they are running operations through web based servers.

Eschelbeck G (2012) proposes that the future is expected to have a lot of sophisticated viruses which are web-borne, and even have wider applications on mobile and smart devices. The quick adoption of cloud computing is also expected to open new avenues to virus challenges.

In future viruses may not be limited to computers since there is spread use of microchips to support human health and biometric features, there may be newer versions of viruses which will affect these chips as argued by Warwick (2004). It is also expected that viruses will be able to spread far and wide especially when powerful processors find their way into household electronic appliances such as Televisions and microwaves.

Malicious code or viruses can be used in future as a cyber weapon to penetrate a country's dangerous information infrastructure or for intelligence reason to spoil the infrastructure. The results may be:-

- Destroying critical control systems such as those used in airports.
- Damaging the national telecommunication systems infrastructure.
- Demolish financial information systems used in banking.
- Shutting down the control systems used in electrical distribution.
- Shutting down control systems used in oil refineries and gas transmission systems and
- Getting access to the dam control systems, which may result in floods

3.0 Solutions

Apart from using anti-virus software, there are other procedures which can help protect against viruses some of which include:-

- Running scheduled, updated virus scan software on all computers within the organization at least once a week.
- Keeping software patches updated with some updates such as windows systems updates which can be downloaded from vendors' websites.
- Permit only approved software to run on your institution so that unaccepted programs are not run. This involves revoking installation privileges from users so that they may not install any programs.
- Practice minimum privileges to users such that they only have access to what they need to carry out their day to day businesses especially on servers.
- Occasionally run vulnerability scanners from both inside and outside your network to find computers with vulnerabilities so you will know which ones need patched.
- Antivirus corporations should create software that averts cyber threats and involve policies which are government-backed to curb criminals involved in cyber-crime of creating and distributing viruses to make money from selling antivirus programs.
- It is advisable to save some applications like Word documents as RTF files and Excel spreadsheets as CSV files whereby these formats don't accommodate macros; hence they can't spread document viruses.
- Registering to an alert service that can caution you about new viruses and offer their identities that will facilitate your anti-virus software to notice and deter them.
- It is advisable to maintain detached networks for those computers that are linked to the internet and those that are not. This reduces the risk that clients will download infected files and spread them in the main network.
- The use of intrusion detectors and firewalls will assist to admit only authorized data to the organization and flow back to the internet.

- Configurations of the internet browsers for security such as disabling Java or ActiveX applets and cookies or request to be cautioned that such code is running.
- Users should be advised to make regular backups for all data and programs such that if the systems are infected, it is possible to restore any lost programs and data.
- Formatting the computer's hard drive is a harder option of removing viruses this involves reinstalling the operating system and all programs from original media.
- Current trends suggest an intelligent approach, which is a merger of an adaptive genetic algorithm and evolving classification functions to detect malware in dual stack especially for IPv4/IPv6 networks.

4.0 Conclusion

Though roughly all of the operating systems have an inbuilt protective guard to keep virus away, they rely on the working capability of the user how he will manage to keep off exposure to viruses with its assistance. Of the operating systems Linux is more stable against viruses than any other operating system including windows.

Antivirus software are a group of codes used to fill a gap in your system’s defenses which exposes it to viruses some people have laid claim that this vulnerabilities are due to the negligence of software merchants who are reluctant to advance their resources to correct some existing classes of vulnerabilities.

Viruses have a lot of negative effects which apart from loss of data, speed or confidence in the technology, they damage your credibility. If a virus sends itself from your workstation or institution to your clients or business partners, they may decline to do trade with you, or claim compensation. This causes embarrassment.

The problem of new viruses is often depicted as a continuous struggle between virus developers (who keep innovating) and the antivirus industry players, who try to keep up. Viruses and worms are flourishing because computers have vulnerabilities that can be abused. The Internet is also simply serving its purpose of interconnecting computer and hence allows or promotes distribution.

There is an argument that software vendors should be held financially liable for damages that arise from the security vulnerabilities in their software products. There is guess is that responsibility would increase motivation to write and sell more secure software, a solution that would result in a less inviting environment for viruses and worms. So far, software vendors have managed to acknowledge their role but avoid accountability. As understanding of the computer virus trouble is bound to increase, trends in virus occurrence will become more apparent.

5.0 Recommendations

Training on how to protect users against viruses would be the most effective model of dealing with viruses. Users should therefore be trained to reduce the exposure they do to their systems both in the internet and removable devices. This involves knowing where and who to report to once an incidence is detected.

There is need to develop security policies and make them part of human resource recruitment. This will make users more responsible and aware of their obligations as they interact with computer networks which are the main source of computer viruses.

Continued use of anti-virus software within organizations and at home is still the option to use as long as new models have not been developed to deal with viruses.

There is need to design and develop automatic monitoring techniques, we hope to obtain enough information about individual behavior to be able to predict and to influence the future course of computer virus trends within organizations and throughout the world.

Those companies developing anti-virus solutions should invest on more research and develop solutions for the next generation of virus protection tools.

Reference

1. Paul Oldfield (2004), Viruses and spam what you need to know. Sophos Plc
2. Wienbar, Sharon (2005), The Spyware Inferno. America Online & The National Cyber Security Alliance.
3. Waqar Ahmad (2003) Computer Viruses as a Threat to Home Users International Journal of Electrical & Computer Sciences King Abdul Aziz University Jeddah. Saudi Arabia.
4. Panda Security (2012),Microsoft Security Intelligence Report, Consumer Reports. Published Available online on http://www.statisticbrain.com/computer-virus-statistics
5. Andy O'Donnell (2012) What Is A Rootkit? Available Online http://netsecurity.about.com/od/frequentlyaskedquestions/f/faq_rootkit.htm
6. Eschelbeck Gerhard (2012) Security Threat Report 2012. available on http://www.sophos.com/en-us/security-news-trends/reports/security-threat-report/html-01.aspx retrieved on 20th march 2011
7. Thomas M. Chen (2011), Trends in Viruses and Worms. The Internet Protocol Journal - Volume 6, Number 3. Southern Methodist University. Available on http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_6-3/virus_trends.html
8. Granneman, Scott (2003). "Linux vs. Windows Viruses". Available http://www.theregister.co.uk/2003/10/06/linux_vs_windows_viruses Retrieved 20th march 2012.
9. Jo Best (2004) Could future computer viruses infect humans? Available on http://www.silicon.com/technology/networks/2004/11/12/could-future-computer-viruses-infect-humans.
10. Zahri Yunos and Ahmad Nasir Mohd Zin (2003) FUTURE CYBER WEAPONS National ICT Security and Emergency Response Centre (NISER) available http://www.cybersecurity.my/data/content_files/13/73.pdf. Viewed on 20th march 2011
11. Online resource http://en.wikipedia.org/wiki/Computer_virus viewed on 20th march 2011
12. Online resource http://support.microsoft.com viewed on 20th march 2011
13. Online resource http://en.wikipedia.org/wiki/Rootkit viewed on 20th march 2011
14. Online resource http://en.wikipedia.org/wiki/Vulnerability_computing viewed on 20th march 2011