COMPUTER VIRUSES

Sotvoldiyeva Kamola
Tashkent. Alfraganus university. student.

Annotatsion: *The article delves into the multifaceted nature of computer viruses, addressing various categories such as file infectors, boot sector viruses, macro viruses, and other common variants. It elucidates the potential ramifications of virus infiltration, shedding light on the potential for data loss, system corruption, and operational disruptions.*

Furthermore, the article outlines proactive measures for fortification against these digital perils, emphasizing the critical role of robust antivirus software, software update protocols, cautious email practices, and vigilant network defenses. By equipping readers with a deeper understanding of the nuances surrounding computer viruses and reinforcing the importance of preventive actions, the article aims to empower individuals and organizations in fortifying their digital ecosystems against these insidious threats.

With its comprehensive examination of computer viruses and its emphasis on proactive defense strategies, this article serves as an invaluable resource for anyone seeking to bolster their knowledge of cybersecurity and fortify their digital defenses.

Keywords. *Virus, dominance, computer viruses, interconnected world, operating system, interface, browser Hijacker, boot Sector Virus, direct Action Virus, Types of, Boot Sector Virus, Web Scripting Virus, infection, understanding, crucial, furthermore.*

In the era of digital dominance, computer viruses have become a significant concern for individuals and organizations alike. Understanding the nature of computer viruses, their impact, and the essential preventive measures is crucial in today's interconnected world.

There are nine main virus types, some of which could be packaged with other malware to increase the chance of infection and damage. The nine major categories for viruses on computers are:

BOOT SECTOR VIRUS

Your computer drive has a sector solely responsible for pointing to the operating system so that it can boot into the interface. A boot sector virus damages or controls the boot sector on the drive, rendering the machine unusable. Attackers usually use malicious USB devices to spread this computer virus. The virus is activated when users plug in the USB device and boot their machine.

Web Scripting Virus

Most browsers have defenses against malicious web scripts, but older, unsupported browsers have vulnerabilities allowing attackers to run code on the local device.

BROWSER HIJACKER

A computer virus that can change the settings on your browser will hijack browser favorites, the home page URL, and your search preferences and redirect you to a malicious site. The site could be a phishing site or an adware page used to steal data or make money for the attacker.

Resident Virus

A virus that can access computer memory and sit dormant until a payload is delivered is considered a resident virus. This malware may stay dormant until a specific date or time or when a user performs an action.

Direct Action Virus

When a user executes a seemingly harmless file attached to malicious code, direct-action viruses deliver a payload immediately. These computer viruses can also remain dormant until a specific action is taken or a timeframe passes.

Polymorphic Virus

Malware authors can use polymorphic code to change the program’s footprint to avoid detection. Therefore, it’s more difficult for an antivirus to detect and remove them.

File Infector Virus

To persist on a system, a threat actor uses file infector viruses to inject malicious code into critical files that run the operating system or important programs. The computer virus is activated when the system boots or the program runs.

Multipartite Virus

These malicious programs spread across a network or other systems by copying themselves or injecting code into critical computer resources.

Macro Virus

Microsoft Office files can run macros that can be used to download additional malware or run malicious code. Macro viruses deliver a payload when the file is opened and the macro runs.

Types of Computer Viruse

Computer viruses come in various forms, each designed to infiltrate systems and cause harm in different ways. Some common types include:

1. File Infectors: These viruses attach themselves to executable files and activate when the file is executed.

2. Boot Sector Viruses: They infect a computer's master boot record or disk partition table, disrupting the boot process.

3. Macro Viruses: Typically embedded in documents and spreadsheets, they exploit the macro capabilities of software applications.

Impact of Computer Viruses

The impact of computer viruses can be devastating, leading to data loss, system failures, and even financial or reputational damage. Viruses can corrupt or delete files, steal sensitive information, and render systems inoperable, causing significant disruption to personal and professional activities.

PREVENTIVE STRATEGIES

Thankfully, there are several effective strategies to protect against computer viruses:

1. Use Antivirus Software: Deploy reliable antivirus solutions with real-time scanning and threat detection capabilities.

2. Keep Software Updated: Regularly update operating systems, applications, and security patches to address known vulnerabilities.

3. Exercise Caution with Email: Be cautious of email attachments and links, as they can be common vectors for spreading viruses.

4. Enable Firewalls: Implement and configure firewalls to monitor and control incoming and outgoing network traffic.

Conclusion

As technology continues to advance, the threat of computer viruses remains ever-present. It is crucial for users to remain vigilant, stay informed about emerging threats, and implement robust security measures to safeguard their digital environments. By understanding the types of computer viruses, their impact, and the best practices for prevention, individuals and organizations can mitigate the risks posed by these malicious software entities.

The battle against computer viruses is ongoing, but with vigilance and proactive measures, it is possible to navigate the digital landscape with enhanced security.

REFERENCE :

1.Melhum, Amera I., and Susan A. Mahmood. "Parasitic Computer Viruses." Journal of Zankoy Sulaimani - Part A 4, no.

2. Henderson, Harry. Computer viruses. San Diego, Calf: Lucent Books, 2005.

3. Denning, Peter J. Computer viruses. [Moffett Field, Calif.?]: Research Institute for Advanced Computer Science, 1988.

4. Collier, Paul. Computer viruses. London: Member Services Directorate of the Institute of Chartered Accountants in England and Wales, 1991.

5. Roberts, Ralph, and Ralph Roberts. Computer viruses: A Compute! book. Edited by Stephen Levy. Greensboro, NC: Compute! Books, 1988.

8. Akhmadalieva, D. R. (2023). USING GAMIFICATION IN ENGLISH LESSONS. Mental Enlightenment Scientific-Methodological Journal, 4(03), 8-13.

9. Yusupjonova, D., & Axmadaliyeva, D. (2023). Using computer and online technologies in teaching english. Models and methods in modern science, 2(12), 151-155.

10. Jamoliddinova, M., & Axmadalieva, D. (2023). Organization of foreign language teaching in higher educational institutions and introduction of speech units for students. Development of pedagogical technologies in modern sciences, 2(11), 96-99.

11. Sevara, A., & Akhmadalieva, D. (2023). The Major Issues in Teaching and Writing of Contemporary Literature. Information Horizons: American Journal of Library and Information Science Innovation (2993-2777), 1(9), 91-95.

12. Akhmadaliyeva, D. R., & Igamberdieva, S. A. Methodology of Developing Media Competence In The Process of Teaching English to Students of Technical Higher Educational Institutions. Pindus Journal of Culture, Literature, and ELT.