Study on Computer Viruses

ICTU Student 175
Thai Nguyen University of Information and Communication Technology
Thai Nguyen University, Thai Nguyen, Vietnam
student175@ictu.edu.vn

***Abstract*—This thesis provides an in-depth analysis of computer viruses, their history, types, and impacts, as well as methods for detecting and preventing them. The author also developed a Trojan program to demonstrate password theft techniques. The research highlights the challenges in virus detection and prevention, emphasizing the need for continuous updates and user awareness. The study involved collecting and analyzing relevant literature, including books, hacker manuals, and online resources. The author identified key aspects of virus behavior and provided insights into common virus types and their detection methods. However, the author acknowledged limitations in the depth of virus recognition mechanisms and the use of FTP for file transfer, which is insecure. The findings underscore the importance of continuous updates and user education in virus prevention. The author suggests that while antivirus software can help, a deeper understanding of virus behavior is necessary for effective protection.**

***Index Terms*—computer viruses, Trojan, password theft, antivirus, virus detection, virus prevention**

I. Introduction

Despite the long history of computer viruses, they remain a significant challenge for both users and IT professionals. The thesis addresses the difficulties in understanding system-level knowledge, the scarcity of relevant literature, and the complexity of virus types, which vary in their mechanisms and impacts. The author notes that system-level knowledge is often not publicly available, making it difficult for users to understand the underlying mechanisms of viruses. Additionally, the scarcity of literature on the topic limits the depth of knowledge available to researchers and practitioners. The complexity of virus types, with each virus having unique characteristics and methods of operation, further complicates the task of understanding and preventing them [1]. Published books on the methods and subject of this project provide context for this English summary [3], [4], [5], [6], [8], [9]. Published articles on the methods and subject of this project provide context for this English summary [7].

II. Methods

The study involved collecting and analyzing relevant literature, including books, hacker manuals, and online resources. The author also developed a Trojan program to demonstrate password theft techniques. The literature review covered a wide range of topics, from the history of computer viruses to the latest detection and prevention methods. The Trojan program was written in Python and used FTP to transfer stolen data, highlighting the insecurity of this method. The author used this program to simulate a real-world scenario of password theft, providing a practical example of how viruses can operate [1].

Supervisor: ICTU Teacher 115, Thai Nguyen University of Information and Communication Technology.

III. Results

The research identified key aspects of virus behavior and provided insights into common virus types and their detection methods. The author found that B-viruses and F-viruses, two major types of viruses, have distinct mechanisms of operation. B-viruses typically infect boot sectors, while F-viruses infect executable files. The author also noted that the effectiveness of antivirus software is limited by the time it takes to update virus recognition mechanisms. The use of FTP for file transfer was identified as a significant security risk, as it is an insecure protocol. The author's Trojan program successfully demonstrated the theft of passwords, highlighting the need for robust security measures [1].

IV. Discussion

The findings underscore the importance of continuous updates and user education in virus prevention. The author suggests that while antivirus software can help, a deeper understanding of virus behavior is necessary for effective protection. The limitations in the depth of virus recognition mechanisms and the use of FTP for file transfer, which is insecure, highlight the need for more advanced and secure methods of data transfer. The author also emphasizes the importance of user awareness, as many viruses exploit user ignorance to gain access to sensitive information. The study provides valuable insights into the behavior of viruses and the methods used to detect and prevent them, contributing to the broader understanding of computer security [1].

V. Conclusion

The thesis concludes that while antivirus software is useful, a comprehensive approach combining software updates, user awareness, and understanding virus behavior is essential for effective virus prevention. The author suggests that users should be educated about the risks of using insecure protocols like FTP and the importance of keeping their systems up to date. The study provides a practical example of how viruses can operate and the importance of robust security measures. The author hopes that this work will contribute to the broader understanding of computer security and the development of more effective methods for preventing and detecting viruses [1].

References

[1] ICTU Student 175, ”Study on Computer Viruses,” internal undergraduate thesis (original in Vietnamese), Thai Nguyen University of Information and Communication Technology, 2010.

[2] John Aycook, 2006, Computer viruses and Malwave

[3] Robert Slade, ”Guide to Computer Viruses,” Springer New York, 1996. ISBN 9780387946634. DOI: 10.1007/978-1-4612-2384-9.

[4] Eric Louw, Neil Duffy, ”Managing Computer Viruses,” Oxford University PressOxford, 1992. ISBN 9780198539735. DOI: 10.1093/oso/9780198539735.001.0001.

[5] David Ferbrache, ”A Pathology of Computer Viruses,” Springer London, 1992. ISBN 9783540196105. DOI: 10.1007/978-1-4471-1774-2.

[6] Robert Slade, ”Robert Slade’s Guide to Computer Viruses,” Springer New York, 1994. ISBN 9780387943114. DOI: 10.1007/978-1-4684-0227-8.

[7] Carey Nachenberg, ”Computer virus-antivirus coevolution,” Communications of the ACM, vol. 40, no. 1, pp. 46-51, 1997. DOI: 10.1145/242857.242869.

[8] J. Aycock, Computer Viruses and Malware. Springer, 2006. DOI: 10.1007/0-387-34188-9.

[9] OECD, Computer Viruses and Other Malicious Software: A Threat to the Internet Economy. OECD Publishing, 2009. DOI: 10.1787/9789264056510-en.