A Review of Cybercrime Caused by Computer Viruses and Worms

Kelsey Gallo

Department of Information Technology, Trident Technical College

CRJ 233: Cyber Crimes and the Law

Pr. Shawn Livingston

December 1, 2024

Abstract

Computer and internet technology development has resulted in attackers harnessing the potential of cybercrime to attain their goals. Cybercrime is often carried out using malware, a kind of software utilized for malicious purposes such as data theft or system damage, and which remains an important focus for cybersecurity professionals today. The primary recommendations for avoiding the prospect of disruption from these attacks since their rise have changed over time from legislative and social cooperation (e.g. expanded laws covering computer crime and international conventions) to technological considerations (such as implementing antivirus software, hardening systems, and looking for other possible attack vectors). This project will especially focus on notable attacks throughout history that used malware such as viruses and worms, including Iloveyou, Melissa, and Shamoon.

A Review of Cybercrime Caused by Computer Viruses and Worms

I. Introduction

Human beings have been dependent on computer technology for decades. The ease of use and access that computer devices offer make them in favor for data storage and communication with others, but also liable to be hacked or tampered with by malicious users. Since the initial developments of computer technology, hackers and criminals have relied on malware, prevalently in the forms of viruses and worms, to impair other users' computer hardware or data while reaping great financial rewards. Academic writers throughout the years have agreed that malware-driven cybercrime is a serious threat that must be addressed through cybersecurity policies and programs. The recommendations that these writers have offered to counter cyberattacks have ranged from legislative and societal collaboration to technological defenses with a greater understanding of computer operations over time. This project will explore a brief history of malware impacts on computer systems, notable cyber incidents involving viruses and worms, the legal issues raised by perceived cybercrimes, and suggestions for protection from cybercrimes and attacks provided by scholars since the year 2000.

II. A Brief Overview

Alenezi et al. (2020) outline five phases through which malware in general has evolved to the present day. The earliest phase, lasting until 1991, was populated by "basic worms and viruses" whose payloads were largely temporary computer crashes due to exhaustion of system resources. The intent of these programs was originally not to damage systems or steal data, but more often, to discover security flaws, such as those present in the early MS-DOS system. Many viruses during this time did not attempt to operate stealthily, and frequently displayed an image or message on the recipient's screen (Alenezi et al., 2020, p. 327).

In the second phase (1992-1999), hackers began to be drawn to the Microsoft Windows system, which was gaining popularity, for its ease of use and many functions (Alenezi et al., 2020, p. 328). Along with the creation of the modern Internet, Windows allowed for a wider availability of malware and the opportunity to misuse tools such as the Macro language to create malicious code. This era also saw an increased variety of propagation methods, namely email attachments and Microsoft Word documents. It was in the third phase (2000-2008), however, that cybercriminals produced large monetary damages (sometimes amounting to billions of dollars) with their malware and were prosecuted for doing so. The fact that these attackers wanted to destroy systems and gain profit was clearer, as they took advantage of more frequented forms of digital media like websites and multimedia files. The bulk of media attention (and academic research that can likely be found) dates to this period, probably because of the serious criminal potential that was posed by such rapidly growing technology at the time.

The fourth phase (2010-2016) was described by Alenezi et al. as the rise of rootkits and ransomware. While these kinds of malware are beyond the scope of this project, this phase is notable in that it placed the topic of cybersecurity in the spotlight, driving companies to invest more time and finances in building a strong cyberdefense for their assets. The fifth and current phase (since 2017) is known for "specially crafted malware" created largely for cyberespionage by national forces and government agencies. It made governments more alert for sophisticated attacks, especially those deemed "advanced persistent threats (APTs)" (Alenezi et al., 2020, pp. 330-331).

III. Notable Incidents

The first instance of malware is thought to be a worm called the Creeper worm, which was created by Robert H. Thomas in 1971 and could travel across systems (Alenezi et al., 2020, p. 327). However, the Elk Cloner, which Rich Skrenta wrote in 1982, could be considered the first “proto-virus.” It was the first to spread across personal computers (PCs) via removable storage media, specifically, the floppy disk. Around this time, computer scientist Fred Cohen developed a well-known definition for the phrase “computer virus”: “a program that can ‘infect’ other programs by modifying them to include a possibly evolved copy of itself” (Bhargava et al., 2022, p. 39).

The first widespread computer malware was the Morris worm, otherwise known as the Internet worm of November 2, 1988. A graduate student named Robert Tappan Morris designed it while attempting to calculate the size of the internet. Due to a programming error, however, his malware ended up negatively affecting 15,000 computers (a large portion of the internet at the time) in 15 hours. The resulting worm exploited vulnerabilities in Unix programs such as sendmail and the weakness of passwords. It was also the first convicted breach of the Computer Fraud and Abuse Act of 1986, which made it illegal to tamper with computer systems connected with US government and financial services (Bhargava et al., 2022, pp. 39-40).

In the decade that followed, Internet users produced numerous viruses and worms that took advantage of how other users understood this new technology, such as V-sign with the Windows file system and Melissa with Microsoft Word macros. The one notable virus to have its author prosecuted during this time period is ILOVEYOU, informally known as “the love bug.” Released in 2000, the virus targeted Microsoft Outlook users by sending an email with a document attachment claiming to be a “love letter for you.” Once opened, the document used Visual Basic Scripting to encrypt or overwrite various types of computer files. The virus would then spread to all of the Outlook users listed in the victim’s contacts list. ILOVEYOU ended up attacking over 50 million computers in the span of 10 days, and many companies shut down their email servers to attempt to halt the virus's spread (Bhargava et al., 2022, p. 41; Joshi & Patil, 2013, p. 208).

After the turn of the 21st century, hackers turned to new forms of malware for attacking systems, such as ransomware, spyware, and keyloggers. Bhargava et al. (2022) assert that viruses came to worldwide prominence again after about 12 years with the Shamoon virus. Shamoon attacked network systems and devices controlled by Saudi Arabia's state-owned oil company, Aramco, in response to the Saudi government's interference throughout the Middle East. It destroyed 75% of Aramco's systems and amounted to one of the largest cyberattacks on a single organization in modern history (Bhargava et al., 2022, p. 40). A notable ransomware worm from this decade is WannaCry, which forced its way into computer systems of hospitals, banks, warehouses, and other industries in Russia, China, and the US. Suspected to originate from North Korea, it allowed the attackers to gain much profit from ransom payments using Bitcoin (Bhargava et al., 2022, p. 41; Alenezi et al., 2020, p. 330).

IV. Legal Issues Raised

Cesare (2001) observes that "When computer crimes were first recognized, they were simply encompassed by traditional crimes, the only difference being that the crime was committed with the aid of a computer" (141). The 1980s brought about unforeseen technological advances, and with them, the ability to cause legitimate physical and financial damage. Lawmakers in the United States and other countries have realized that these effects could only be possible with computer technology and recognized computer crimes as separate federal offenses (Cesare, 2001, pp. 141, 146-147). One cybercrime of note was the result of the aforementioned

Melissa virus, which racked up an estimated $80 billion worth of destruction and led to the arrest of its author (Cesare 2001, pp. 143, 147).

Scholarly commentary during the 2000s and the years shortly after has largely focused on the legal repercussions of crimes carried out with emerging malware. Namely, there have been debates on whether cybercrimes should indeed be prosecuted under their own category, and if so, what actions would warrant calling a crime a “cybercrime.” Tavani is one such proponent of considering the reality of computer activity in the legal sphere; he asserts that it is not always possible for generic laws to extend to computer crimes, necessitating the clarification of crime concepts related to computer technology (Tavani, 2000, pp. 4, 6). However, academic works have raised other issues based on the boundless nature of cyberspace. Computer programs defy international borders both in their availability and impact, making them easy to access but difficult to crack down on (Cesare, 2001, p. 137, 150). Some countries also have less developed laws on cybercrime than others; the government of the Philippines, for instance, dismissed the charges against the creator of the ILOVEYOU virus who resided there because it was less knowledgeable on the malicious nature of computer viruses (Katyal, 2001, p. 1004).

V. Recommended Defenses

The studied academic reports from the 2000s appear to recommend strategies of a more legislative or societal character when it comes to reducing malware’s effects, compared to the articles from the 2010s and 2020s, which provide technological solutions. Tavani, as he understood it in 2000, notes that newer technologies of the era needed to be explained in depth in order to draft laws to cover them (2000, pp. 4-5). A year later, Cesare provides suggestions for partnerships between law enforcement agencies and private organizations to maximize resources and tactics, as well as increased global cooperation, drawing from the Council of Europe’s

Convention on Cybercrime (2001, pp. 158-160, 164). Katyal (2001) proposes that law enforcement implement strategies to make Internet activity more costly if used maliciously, but accessible to all users with good intentions (pp. 1007, 1011).

Jumping to 2013, Joshi and Patil encourage users to learn about the types of viruses that are prominent today, how a virus operates, and the types of destruction that could be caused by a virus (2013, p. 209). Alenezi et al. propose utilizing artificial intelligence (AI) to help detect the new kinds of malware and attack vectors that are being introduced in the 2020s (2020, p. 331). Bhargava et al. advise computer users in 2022 to prioritize protecting data, activate antivirus software, and report incidents to security specialists (2022, p. 43). It is apparent from this research that with a better comprehension of malware operations and technology that could halt malware over time, the emphasis has shifted to continuing to learn how a virus or worm could potentially access and impact a system.

VI. Conclusion

Malware has presented a viable threat to the security of computer systems throughout their evolution, and academic sources have addressed this threat by encouraging the implementation of proactive legislation, partnerships, and digital solutions. With a greater familiarity with the effects of malware and computer-provided defenses, the recommended countermeasures have demonstrably turned from the legal sphere to the technological realm. Cybersecurity principles have gained favorability in the 2010s, and they still hold true considering that the number and types of viruses and worms that are being created are increasing today. To keep up with these advances, changes in cybersecurity laws, possible victims (e.g. smart devices), and specialized antivirus technology must be continually examined.

References

Alenezi, M. N., Alabdulrazzaq, H., Alshaher, A. A., & Alkharang, M. M. (2020). Evolution of malware threats and techniques: a review. *International Journal of Communication Networks and Information Security*, 12(3), 326-337. https://www.researchgate.net/profile/Haneen-Alabdulrazzaq/publication/349324759_Evolution_of_Malware_Threats_and_Techniques_A_Review/links/602ad0e64585158939a93934/Evolution-of-Malware-Threats-and-Techniques-A-Review.pdf.

Bhargava, P., Choudhary, R., & Gupta, A. (2022). A review study on computer virus. *World Journal of Research and Review*, 14(5), 39-44. https://www.wjrr.org/download_data/WJRR1405018.pdf.

Cesare, K. (2001). Prosecuting computer virus authors: The need for an adequate and immediate international solution. *Global Business and Development Law Journal*, *14*(1), 135-170. https://scholarlycommons.pacific.edu/cgi/viewcontent.cgi?article=1569&context=globe.

Joshi, M. J., and Patil, B. V. (2013). Computer virus: Their problems and major attacks in real life. *International Journal of P2P Network Trends and Technology*, *3*(4), 206-209. https://www.researchgate.net/profile/Dr-Bhaskar-Patil/publication/274468580_Computer_Virus_Their_Problems_Major_at-tacks_in_Real_Life/links/5683652608ae1e63f1f02394/Computer-Virus-Their-Problems-Major-at-tacks-in-Real-Life.pdf.

Katyal, N. K. (2001). Criminal law in cyberspace. *University of Pennsylvania Law Review*, *149*(4), 1003-1114. https://doi.org/10.2307/3312990.

Tavani, H. T. (2000). Defining the boundaries of computer crime: piracy, break-ins, and sabotage in cyberspace. *Computers and Society*, 30(3), 3-9. https://doi.org/10.1145/572241.572242.