Microsoft Malware Mayhem: Tracing the Evolution of Cyber Attacks

Diana Y Solorzano

CYSE 280 - Windows Systems Management and Security

Professor Malik A. Gladden

Final Research Paper

April 11, 2024

Malware is malicious code intended to invade a system for malicious purposes. It can be used for stealing data, spying, and even corrupting systems but malware does not invade systems without assistance. Malware can also use different products and tools to disguise itself while attempting to get delivered to the target machine and can be used with trojans, viruses, worms, and many more. Microsoft has become a dominant organization in the tech community and its products are now used by millions of people worldwide, making their users and products desirable targets. Through the years, cybercriminals have developed more ways to incorporate Microsoft products into their malware by identifying and exploiting their vulnerabilities. Having an in-depth understanding of the development of malware using Microsoft products is needed so individuals and organizations can better protect their systems. My research will focus on the history behind malware developments and Microsoft products, the damages and effects these types of malware have had, and how users can better protect themselves.

The development of Microsoft products, which encompasses core MS-DOS operating systems, advanced Windows operating systems, and Office Suite, accurately represents the substantial technological revolution over the years. MS-DOS was introduced in the early 1980s, becoming the stepping stone for Microsoft's dominance over the personal computer industry. Its programming interfaces that lacked sophistication provided a simple and sensible service to its users. Later Windows editions introduced GUIs and other features that provided more sophisticated and user-friendly software. The Office Suite, a combination of Word, PowerPoint, Outlook, and many more applications has gradually become one of the leaders in increasing productivity by becoming an essential tool in different ecosystems.

Analyzing and understanding the influencers behind malware over time reveals how they have influenced the evolution of malware and the creativity behind it. Malware, which initially consisted of viruses and worms, mainly disrupts computer systems and either stole data or damages the system. In its early stages, malware mainly focused on what it could take from the hardware itself and mainly focused on damaging the hardware alone. Early malware was transferred through infected floppy disks, intending to target primarily rudimentary networks aiming at OS system bugs as MS-DOS (Saengphaibul, 2022). As time and technology progressed, malware was becoming more agile and advanced, including Trojan horses, botnets, ransomware, etc. Today new and advanced malware types are more complex and integrate social engineering, polymorphism, and zero-day exploits. The new level of complexity has allowed malware to successfully maneuver network systems without being detected by security systems.

Understanding the historical context of both Microsoft products and the evolution of malware is essential to gaining a deep insight into the current malware threats we face today. The interplay between software development and malware advancements showcases an endless game of defense and offense, so cybersecurity professionals are constantly trying to prevent and stop attacks while cybercriminals continuously build on previous malware and incorporate new exploits to create more complex and undetectable malware. Holistic analysis of malware development history identifies the driving forces behind malware creators and their capability, helping to construct a more efficient threat response system. In the same manner, having cybercriminals exploit vulnerabilities in Microsoft products has set a pace for developing better software architectures that incorporate security at every process.

Overall, the history of malware in Microsoft programs has had a powerful influence on the current scope of cybersecurity. Uncovering the evolutionary paths of the two organisms will allow us to better understand real-time risks and the most appropriate responses. Using historical information technology, organizations could benefit by developing security systems that will be able to deter, minimize, and protect against the continuous risk of malware attacks.

Reflecting on just the past 10 years, we can see that some of the most memorable and devastating malware attacks have targeted and exploited Microsoft products' vulnerabilities, resulting in substantial service disruption and financial losses for the victims. To specify, WannaCry Ransomware (2017), NotPetya (2017), and Emotet (2014-present) have been some of the most significant malware attacks that have targeted Microsoft products.

WannaCry Ransomware (2017)

The WannaCry ransomware peaked in May of 2017 when the malicious virus had caused massive damage in 150 countries, and more than 100,000 computers had been infected (Gharuf & Kristensen, 2019). As for the techniques this malware used, one of the most notable was the EternalBlue SMB vulnerability that targeted Microsoft operating systems, which was developed by the US National Security Agency (NSA) and later released by the Shadow Brokers. WannaCry is an encrypted file extension that was able to effectively prevent proper computer operations from performing and required the victims to pay a ransom in Bitcoin to receive the decryption key.

The global scale of WannaCry was mind-blowing, hundreds of critical infrastructures, healthcare systems, and enterprises were experiencing ransomware attacks. This attack had an estimated cost of over ten billion dollars, including money paid towards the ransom, data recovery expenses, and productivity loss.

NotPetya (2017)

Initially disguised as ransomware, NotPetya appeared in June of 2017 as a destructive malware with a primary focus on systems in Ukraine, but it soon grew to attack systems in other countries as well. This malware attack targeted a known vulnerability in the MS Windows operating system and used the EternalBlue exploit and WannaCry to travel through as many networks as it did. Unlike typical ransomware, NotPetya did not provide the opportunity for victims to pay a ransom to retrieve their data. Instead, it randomly wrote over the existing data on the infected machines, destroying hundreds of systems and financial deficits for the affected organizations (Crosignani, Macchiavelli, & Silva, 2020). NotPetya also caused the most damage to vital industries, such as banking, energy, and transportation, which resulted in regular users not being able to do daily tasks. This attack demonstrated the power malware attacks had, resulting in power being in the wrong hands of cybercriminals and the devastating consequences that come with it.

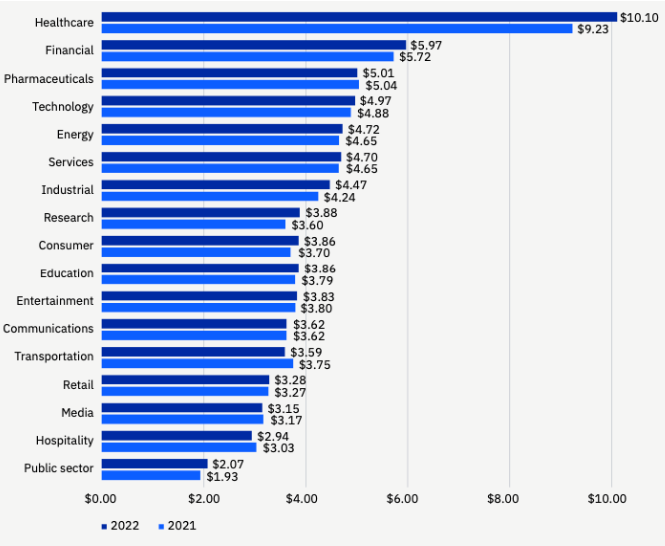
Emotet (2014-present)

Among the most successful and malicious malware is Emotet, which was discovered back in 2014 as an ordinary Trojan but quickly escalated to becoming a sophisticated Malware-as-a-Service (MAAS) platform. Emotet was able to reach its victims by using malicious email attachments, which were disguised to look like ordinary invoices for services or delivery notices. Once the malware had been executed, Emotet was able to fetch and download other payloads which included ransomware and other malware, and then import it onto the infected machine and other machines connected.

Emotet was notorious for using Microsoft Office Suite products to exploit vulnerabilities such as macros and scripting (Kuraku & Kalla, 2020). Its persistent presence and tactics allowed for this malware to be invisible and continuously bypass the defenses put in place. These significant malware attacks perfectly explain how proper cybersecurity practices and well-structured defense mechanisms are needed to reduce the risks caused by malware that targets Microsoft products.

The exploitation of Microsoft products and software by malware attacks has been nothing short of expensive. These types of attacks have the potential to cause both financial and reputational loss, not only for companies but also for individual users.

The financial loss that comes with malware attacks on Microsoft products can be quite significant which may also affect their business operations. Cybercriminals almost always demand ransom payments with no guarantee of receiving a decryption key and being able to retrieve their data. Besides the costs related to data recovery, victims will have indirect expenses associated with restoring systems and potential legal fees. Businesses tend to see a larger financial loss during these attacks. When their systems get attacked, downtime can be detrimental especially if the businesses attacked are dependent on continuous operation, such as banking and healthcare. Based on the Cybersecurity Ventures report, ransomware costs on a global level will surpass $20 billion by 2021, which has substantially increased from a couple of years back, clearly highlighting the financial impact these attacks have (IBM, 2022).

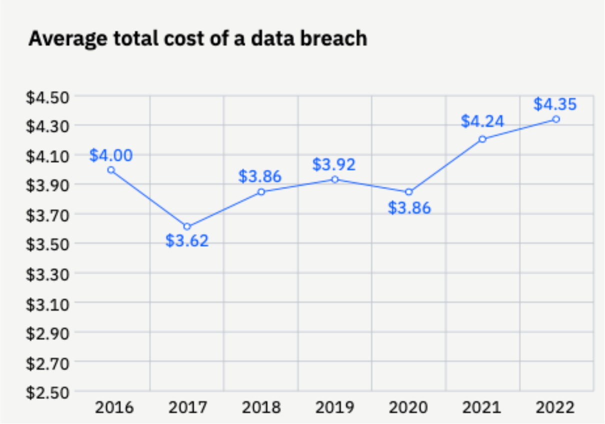


(IBM, 2022, Figure 4: Measured in USD millions).

The healthcare sector has seen the most financial loss due to malware attacks, following it are financial, pharmaceuticals, and technology. The financial sector has seen a rise of USD .25 million (4.4%) from 2021 to 2022. The industrial sector, which encompasses businesses such as manufacturing, chemical, and engineering, saw a 5.4% increase in 2022. That was an increase of USD .23 million in a single year. Only a few sectors saw a slight decrease in their average total costs: medicine, transportation, media, and hospitality.

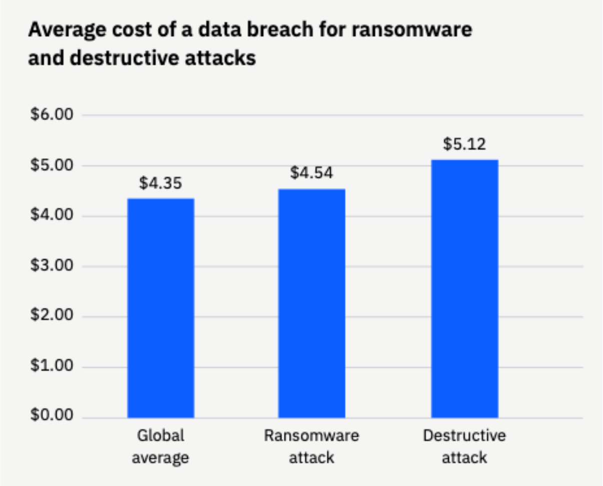
Financial loss is not the only damage these malware attacks have had on Microsoft the company. Producing products that make users vulnerable to these types of malware attacks can have a detrimental effect on their reputation, resulting in decreased confidence in Microsoft products which could ruin the company. Consumers may believe that Microsoft products are not secure and decide to try adopting a new software due to reputation damage. Furthermore, the continuous use of malware targeting Microsoft products may begin to undermine the consumer's faith in the company's ability to protect their privacy and data, influencing the market share and negatively affecting customer retention. Quick reactions to Windows targeting malware have forced the company to invest and prioritize its overall security which has been beneficial to its reputation.

Malware attacks may seriously affect end users, both individuals and organizations. System halts and data loss can lead to a disruption of normal business operations and decrease productivity. Concerning data breaches, personal data can be stolen, which may result in identity theft, financial problems, or a bad reputation for an individual or institution (Ahmed, 2022). Additionally, other factors contribute to the average total cost of a data breach which include credit monitoring services and legal services. IBM Security's study recorded that the average cost of a data breach is about USD 3.86 million, highlighting the enormous financial and operational effects of these attacks.



(IBM, 2022, Figure 1: Measured in USD millions).

In 2022, the average global total data breach cost jumped from USD .11 million to USD 4.35 million, the highest amount in the report's history. A 2.6% increase was also shown by the jump from USD 4.24 million in 2021 to USD 4.35 million in 2022 (IBM, 2022). The average total cost increased by 12.7% within the last two years reported to USD 3.86 million. Destructive attack costs averaged USD 5.12 million; a 16.3% difference from the total average of USD .77 million.



(IBM, 2022, Figure 30: Measured in USD millions).

Microsoft as a company has introduced multiple defense and security methods to prevent threats posed by malware attacks that target vulnerabilities in their products. Over the years Microsoft has focused on strategies to prevent cybercriminals from exploiting flaws in their product code. To accomplish this, Microsoft has invested in constantly running updates on their programs. These updates usually get released as ‘patches’ with the intent of correcting known errors to provide better security.

Furthermore, Microsoft has incorporated security features directly into its Windows OS and Office Suite products. The Windows security features are known as Windows Defender Antivirus and Windows Firewall. They also focus on educating end users by communicating security guidelines that can help users and organizations harden their cybersecurity defense. These guidelines include secure configuration settings, user access controls, and incident response processes.

As malware attacks continue to target Microsoft products for its wide audience, Microsoft continues to intensively create and implement new patches and security features to not fall behind. Respective countermeasures intend to address all the rapidly growing areas of threats and vulnerabilities that the threat intelligence team can receive through ongoing gathering and analysis. As a company, Microsoft continuously monitors and stays proactive to protect its products and customers from the threats of malware in today's digital world.

Understanding the evolution of malware attacks regarding Microsoft products, such as the WannaCry, NotPetya, and Emotet attacks, allows us to not only the financial and reputational loss that can be experienced but also helps explain the tug-and-pull system between malware attacks and Microsoft products. These types of malware attacks have resulted in significant financial losses for the affected users and the reputation of one of the most popular and reliable tech companies. Productivity has been disrupted as a result only adding to the list of impacts brought on by these attacks.

The dynamic character of malware attacks calls for implementing agile security systems (MSRC, 2024). Cybercriminals continue to evolve and find innovative ways to attack their targets. Hence, protection and security measures should be one of the most important concerns for users and companies. Making sure your software is up to date, cutting-edge security solutions, and establishing a culture of information security within businesses. Given the difficulty of predicting future trends, it is difficult to say whether malware attacks targeting Microsoft products will continue. Nevertheless, they will become increasingly advanced in many aspects, making them more deadly and difficult to detect. Through cooperation and assuming all technologies in the emerging sectors, collaborative efforts can greatly minimize malware attacks and aim for a safe digital world for everyone.

References

Ahmed, D. (2022, July 21). *Microsoft Office Most Exploited Software in Malware Attacks – Report*. HackREAD. https://www.hackread.com/microsoft-office-malware-attacks-exploite-flaws/

Crosignani, M., Macchiavelli, M., & Silva, A. F. (2020, July 31). *Pirates Without Borders: The Propagation of Cyberattacks Through Firms' Supply Chains*. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3664772

Ghafur, S., Kristensen, S., & Honeyford, K. (2019, October 2). *A Retrospective Impact Analysis of The WannaCry Cyberattack on the NHS*. Npj Digital Medicine. https://doi.org/10.1038/s41746-019-0161-6

IBM. (2022). Cost of a Data Breach Report 2022. https://www.ibm.com/downloads/cas/3R8N1DZJ

Kuraku, S., & Kalla, D. (2020, March 28). *Emotet Malware – A Banking Credentials Stealer*. Journal of Computer Engineering. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4402486

MSRC. (2024, January 19). *Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard*. MSRC Blog | Microsoft Security Response Center. https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/

Saengphaibul, V. (2022, March 15). *A Brief History of the Evolution of Malware*. Fortinet. https://www.fortinet.com/blog/threat-research/evolution-of-malware