# Malicious Code and Activity - Mitigation Methods

Carl Lochstampfor Jr.

Department of Cybersecurity, Old Dominion University,

CYSE 300 – Introduction to Cybersecurity

October 19, 2025

## Instructions:

1. Describe some actions or techniques that can be used to mitigate or stop the impacts of malicious applications. Are some of these methods more effective than others?

2. Provide an example of a cyber-attack that resulted from the execution of malicious code. There are plenty of examples that can be queried from the Internet.

**Malicious Code and Activity - Mitigation Methods**

## Actions to Mitigate Malicious Applications & the Effectiveness of Mitigation Methods

Organizations and individuals have an armory of techniques and tools for fighting against malicious software propagation and unauthorized access to their sensitive data, creating a "defense-in-depth" war plan to meet the needs of that individual or organization (Aidan et al., 2017; Kara et al., 2022; Sandbu, 2022). According to NIST, a layered defense that combines technical, administrative, and recovery methods yields the best protection (Cichonski et al., 2012; Nieles et al., 2017; Cawthra et al., 2020). However, there is no "cookie-cutter" or "one-size-fits-all" defense against malicious entities and unauthorized access to sensitive data from threat actors. Individuals and organizations must assess their needs within their respective environments and industries when developing and implementing overlapping proactive and reactive cyber defense policies, techniques, and technologies.

Second, to mitigate and close potential vulnerabilities, it is important for all users to promptly and routinely patch their operating systems and software applications when developers and manufacturers release new firmware updates. Otherwise, users will fall victim to attacks such as the EternalBlue SMB exploit. Patch management provides essential baselines for large organizations, but it cannot prevent zero-day exploits and attacks.

Third, users should create and maintain regular data backups, adhering to the 3-2-1 strategy (three copies, two media types, one offsite). Though a reactive strategy, users want to ensure they can swiftly recover their data should a computer network be compromised. Backing up sensitive data and network configurations helps protect data integrity. It provides users with a "clean slate" option to combat specific types of malicious attacks and code, such as ransomware, thereby avoiding the need to pay the ransom to RaaS (aka, Ransomware as a Service). Additionally, it is

more time-efficient, cost-effective, and more straightforward in the long term to restore computer networks and systems from recent backups then seek other options like third-party assistance.

Fourth, user training is crucial for reducing human error within organizations, as it is a leading cause of most malicious infections, even in those that are heavily guarded and secure. User training can include quarterly phishing simulations and monetary incentives for employee participation to reduce further infection risks.

Fifth, Windows OS contains many native, technical malware tools and applications to help keep data confidential and tamper-free: applications include Windows Defender for real-time protection, AppLocker to block unauthorized apps from being automatically downloaded or opened without explicit administrator permission, and GPOs to disable risky or potentially dangerous features like macros or disabling open and unnecessary ports (i.e., Telnet, port 23). Organizations can also use the vendor-neutral monitoring tool, Event Logs. Endpoint Detection and Response (EDR) solutions that utilize and audit event logs help identify indicators of an attack, enabling early detection and containment (sometimes preventing zero-day exploits and attacks). Attack indicators can include anomalies like unusual login activity, suspicious network traffic, unauthorized file changes, security software tampering, and abnormal system resource usage. Lastly, organizations can collect and organize data to build “attacker profiles” for later use, enabling them to adapt their cyber defense strategies against new incoming attacks.

## Example of a Cyber-Attack

The 2017 NotPetya cyber-attack used the Windows OS EternalBlue exploit to self-propagate (Rhysider, 2019; McDonald et al., 2022). Cyber attackers compromised the M.E. Doc software update infrastructure to distribute wiper malware. The NotPetya malware works first by modifying and encrypting the Master Boot Record (MBR) of a Windows operating system (OS),

not just the Master Boot Table (MFT). It also writes its code to the MBR and then performs full-disk encryption. The malware behaves similarly to standard ransomware, but the final results are identical to wiper malware because the malware does not create or provide the victims with the decryption key to gain access to their encrypted data. Thus, the malware permanently locked out its victims from accessing their data, crippling systems and rendering them effectively "useless." The 2017 NotPetya cyber-attack initially targeted Ukrainian government, corporate, and citizen computer networks; however, the attack quickly spread throughout the globe to other organizations and caused billions of dollars in damage.

# References

Aidan, J. S., Verma, H. K., & Awasthi, L. K. (2017). Comprehensive Survey on Petya Ransomware Attack. In 2017 International Conference on Next Generation Computing and Information Systems (ICNGCIS) (pp. 122-125). IEEE. https://ieeexplore.ieee.org/document/8520323/

Cawthra, J., Ekstrom, M., Lusty, L., & Sexton, J., & Sweetnam, J. (2020, December). Data integrity: Detecting and responding to ransomware and other destructive events (NIST SP 1800-26B, Vol. B: Approach, architecture, and security characteristics) [Cybersecurity practice guide]. National Cybersecurity Center of Excellence, National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.1800-26

Cichonski, P. R., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide (NIST Special Publication 800-61 Rev. 2). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r2

Jack, Rhysider (Host). (2019, October 8). NotPetya (No. 54) [Audio podcast episode]. In DarkNet Diaries. https://darknetdiaries.com/episode/54

Kara, I., & Aydos, M. (2022). The rise of ransomware: Forensic analysis for Windows based ransomware attacks. Expert Systems With Applications, 190, 116198. https://www.sciencedirect.com/science/article/pii/S0957417421015141

McDonald, G., Papadopoulos, P., Pitropakis, N., Ahmad, J., & Buchanan, W. J. (2022). Ransomware: Analysing the impact on Windows Active Directory domain services. Sensors, 22(3), 953. https://www.researchgate.net/publication/358119298_Ransomware_Analysing_the_Impact_on_Windows_Active_Directory_Domain_Services

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). An introduction to information security (NIST Special Publication 800-12, Revision 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-12r1; https://csrc.nist.gov/pubs/sp/800/12/r1/final

Sandbu, M. (2022). Windows ransomware detection and protection. Packt