

**Windows Management and Cybersecurity: Latest Security Threats and Mitigation
Strategies**

Brandon M. Burke

Old Dominion University

CYSE 280: Windows System Management and Security

Professor Gladden

April 11, 2024

Abstract

In today's interconnected digital landscape, Windows systems play a pivotal role in organizations, serving as the backbone for critical operations and data storage. However, this prominence also makes them prime targets for cyberattacks. In this comprehensive study, we delve into the multifaceted realm of Windows security, examining the most common types of cyber threats that specifically target Windows environments. We explore the latest security vulnerabilities that Windows systems are susceptible to, analyzing their potential impact on both the systems themselves and the sensitive data they house. Furthermore, we evaluate the effectiveness of existing mitigation strategies in safeguarding against these threats. As we peer into the future, we also delve into emerging technologies and innovative approaches for enhancing Windows security, ensuring a robust defense against ever-evolving cyber risks.

Keywords: Windows systems, Windows security, cyber threats, vulnerabilities, mitigation strategies, emerging technologies

Windows Management and Cybersecurity: A Comprehensive Study of the Latest Security Threats and Mitigation Strategies

In an increasingly digitized world, computers wield significant influence over the market. From personal laptops and smartphones to fridges and stoves connected to the internet, technology permeates our daily lives, shaping how we work, communicate, and even cook our meals. The seamless integration of digital devices into our routines underscores the transformative power of technology in the modern era. Windows, an operating system developed by Microsoft, dominates a substantial portion of the computer landscape. Approximately 70% of computers worldwide run on some version of Windows, making it a cornerstone of the digital ecosystem. Its user-friendly interface, compatibility with a wide range of software, and extensive market presence contribute to its enduring popularity. However, this widespread adoption comes with a caveat: Windows is also the most targeted operating system. Its popularity makes it an attractive target for cybercriminals seeking vulnerabilities to exploit. This paper explores the most common types of cyberattacks targeting Windows systems, identifies the latest security threats faced by these systems, analyzes their impact on both the systems and the stored data, evaluates existing mitigation strategies, and delves into emerging technologies for enhancing Windows security.

Most Common Types of Cyberattacks

The most common cyberattacks that are conducted on Windows operating systems are malware infections, distributed denial-of-service, and phishing. According to Cloudflare, malware is “a portmanteau from the words malicious and software, which can refer to viruses, worms, trojans, ransomware, spyware, adware, and other types of harmful software” (*What is Malware?* 2024). Out of this list, the most common type of malware is called ransomware.

Ransomware is a malicious software that encrypts files on a victim's computer, rendering them inaccessible until a ransom is paid to the attacker. Unlike routine file encryption for security, ransomware leaves the decryption key in the hands of the hacker, preventing users from accessing their files. In a typical attack, the hacker demands payment to decrypt the files, with ransoms ranging from hundreds of dollars for individuals to millions for corporations. Some variants even threaten to delete files after a specific time, pressuring victims to pay swiftly. Additionally, certain ransomware strains steal copies of data, threatening to release them if payment is refused. Large companies and government agencies storing sensitive data are particularly vulnerable. Although paying the ransom offers no guarantee of file decryption, it is possible cybercriminals will honor their promises to maintain their reputation (Pachhala et al., 2021). One prominent example of ransomware being widespread was WannaCry in May 2017. The ransomware would spread through networks just as a standalone worm program. It would exploit a vulnerability called Eternal Blue in Microsoft's server message block (SMB) protocol to gain access to the system. Simultaneously, the ransomware used its worm-like capability to spread to other computers on the same network. Once a computer was infected by WannaCry, the ransomware would encrypt the files and demand a ransom of \$300 to \$600 in bitcoin (*What is WannaCry Ransomware?* 2024). Eventually, this ransomware would be stopped with a built-in kill switch, but not without leaving billions of dollars in damages.

Another attack on Windows computers is a DDOS attack. A DDOS attack is "is a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic" (*What is a Distributed Denial-of-Service (DDos) Attack?* 2024). Windows computers are particularly susceptible to this type of attack, as more than half of all computers worldwide are

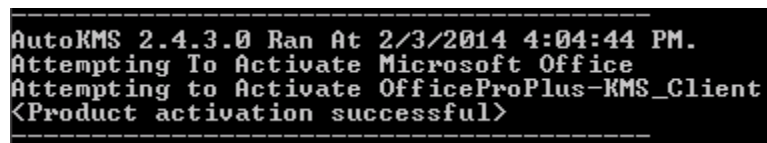
Windows-based. Cybercriminals will often use hundreds to thousands of computers that they compromised or rented to send Internet traffic to a particular machine running a service available to the public. With gigabytes of Internet traffic coming in at once, it causes the machine to run significantly slow or crash, resulting in a denial of service for administrators and potential customers. Tools such as HPing3 or GoldenEye can be used to accomplish this in an easy and short time frame.

Phishing attacks are the most common attacks that occur, trumping malware and distributed denial-of-service attacks. According to NIST, phishing is “a technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a website, in which the perpetrator masquerades as a legitimate business or reputable person” (*Phishing* 2024). Phishing is highly effective because it relies on human error rather than computer or software errors. To achieve this, attackers will send emails, phone calls, or texts to a target individual. If the target individual interacts with one of these methods, it is possible that the attacker can convince the target to give them personal identifiable information such as emails, phone numbers, usernames, or passwords. One example of a successful phishing is the USPS phishing attack in 2020. The cybercriminals sent SMS messages that told recipients they should click a link to view important information about an upcoming USPS delivery (8 *Devastating Phishing Attack Examples and Prevention Tips* 2024). The malicious link actually took victims to various web pages designed to steal their Google account credentials. Phishing is far more common than one thinks. From the Verizon Data Breach Investigations Report, 74% of data breaches involved a human element or interaction (*Verizon Data Breach Investigations Report 2023* 2023). Although this number is down from the previous year, it shows that

phishing is the most popular and effective method for gaining access to sensitive information from company servers and databases.

Latest Security Threats and Impacts

Fully patched Windows systems are still vulnerable to countless vulnerabilities, malware, and security threats. One of the top threats as of April 2024 is HackTool:Win32/AutoKMS which was identified by Microsoft. AutoKMS is used to crack or patch unregistered copies of Microsoft's software (*Cyberthreats, Viruses, and Malware* 2024). This threat will bypass the activation license associated with Microsoft programs and will activate the products if done successfully as shown in Figure 1.



```
AutoKMS 2.4.3.0 Ran At 2/3/2014 4:04:44 PM.  
Attempting To Activate Microsoft Office  
Attempting to Activate OfficeProPlus-KMS_Client  
<Product activation successful>
```

Figure 1

The problem is when people begin the distribution of cracked or patched software that could contain malware while posing as a legitimate Microsoft product. For example, an attacker can make a malicious website advertising that Microsoft Word has an update. An unsuspecting user can view the ad, download the program, and execute it. The program will function as the normal Microsoft Word, but will have cracked or patched code or license key packaged inside. It is possible that the key or code could be malicious, giving the attacker full control over a system using the cracked software. The Pirate Bay would be a notorious website that would host cracked or patched applications. It was not uncommon that many of these applications would contain hidden malware. As mentioned previously, malware can be used to encrypt files, take control of an operating system, or exfiltrate data stored on that computer.

Another threat recognized by Microsoft is Trojan:Win32/Wacatac.B!ml. This is a trojan meaning it hides its malicious intent in other programs. Microsoft identifies it as a “threat [that] can perform a number of actions of a malicious hacker's choice on your PC” (*Cyberthreats, Viruses, and Malware* 2024). The Wacatac Trojan can be embedded in almost any software. Like the previous example used, it can be used in combination with AutoKMS. An attacker can create an ad, a user downloads the cracked software, and the user runs the software. The cracked software can contain malicious code. The attacker now has a reverse shell on the Windows system leading to a compromise of the CIA triad. These two malicious files mostly affect individual users at home and small businesses, as there is a lack of robust security policies in place. This allows the both files to infect computers with a high success rate while also maintaining persistence leading to more compromise to any network or domain a computer is connected to.

Effectiveness of Existing Mitigations

Windows computers have existing mitigations built in the operating system to prevent malicious infections or service denial that can occur from user error, exploits and vulnerabilities, or distributed denial-of-service. Most notably, Windows computers have code signing and integrity. To ensure that Windows files have not been tampered with, the Windows Code Integrity (WCI) process verifies the signature of each file in the operating system. Code signing is core to establishing the integrity of firmware, drivers, and software across the Windows platform (*Windows 11 Security Book: Powerful Security by Design* 2023). Code signing works by creating a digital signature from encrypting the hash of the file with the private key portion of a code-signing certificate and embedding the signature into the file. The code integrity process then verifies the signed file by decrypting the signature to check the integrity of the file and

confirm that it is from a reputable publisher. Although this measure does work for a majority of applications and files that are installed to Windows computers, code signing can be spoofed meaning an attacker could successfully pass WCI. A common vulnerability and exposure, CVE-2020-1464 does just this. This vulnerability allowed attackers to bypass WCI, thus smuggling malicious files onto a system. The attacker could then execute the malicious files, which compromises the availability, integrity, and confidentiality of the system (*Windows Spoofing Vulnerability* 2020). This vulnerability was exploited for two years before being patched. This shows that WCI is not effective as a standalone solution. The existence of vulnerabilities such as CVE-2020-1464 underscores the need for additional security measures beyond code signing alone. Organizations and individuals should adopt a layered security approach to protect against such threats.

User Account Control (UAC) is built into the operating system and works alongside code signing. UAC helps prevent malware from damaging a PC and enables organizations to deploy a better-managed desktop. With UAC, apps and tasks always run in the security context of a non-administrator account unless an administrator specifically authorizes administrator-level access to the system (*Windows 11 Security Book: Powerful Security by Design* 2023). This mechanism helps enhance security by preventing unauthorized changes and reducing the risk of malicious software gaining elevated privileges. Additionally, UAC can block the automatic installation of unauthorized apps and prevent inadvertent changes to system settings. In the past, UAC has been bypassed, allowing administrator level privileges to a Windows system. In 2022, UAC was bypassed on Windows 11 and Windows Server 2022 by security researcher Patrick Hoogeveen through the use of Powershell and DLL files. The script Hoogeveen made detects what version the target operating system is running and executes commands to bypass UAC

(Hoogeveen, 2022). This would allow attackers full control of a system giving them a permanent foothold until the flaw is patched. This bypass still works as of February 28, 2024. Although UAC is robust and prevents privilege escalation from malware installed on the system, it is still possible to bypass the checks put in place to gain elevated privileges on the system.

The last notable protection built into the Windows operating system is Windows Defender. Windows Defender has the following mitigations in place to protect the operating system: tamper protection, detection for indicators of compromise, and exploit protection (*Windows 11 Security Book: Powerful Security by Design* 2023). Tamper protection prevents unauthorized users and programs from modifying system files and files of other programs. This can prevent further exploitation of the system and domain connected to the computer. Windows Defender also checks for indicators of compromise. For example, an administrator can configure Defender to block the PowerShell terminal. If a program tries to launch PowerShell, Defender can alert the user and automatically block the interaction. Defender also prevents exploits such as running malicious code on the computer from installed software or from the command line. Moreover, the antivirus gets updated every 24 hours to add new signatures or unique identifiers for malware and other exploits to prevent a Windows machine from getting compromised. In the past 30 days, Windows Defender has thwarted 6,828,300 devices from malware infections related to education purposes such as school computers for students and faculty. This amounts to 80% of reported malware cases that were blocked in the last 30 days as shown in Figure 2

(*Cyberthreats, Viruses, and Malware 2024*).

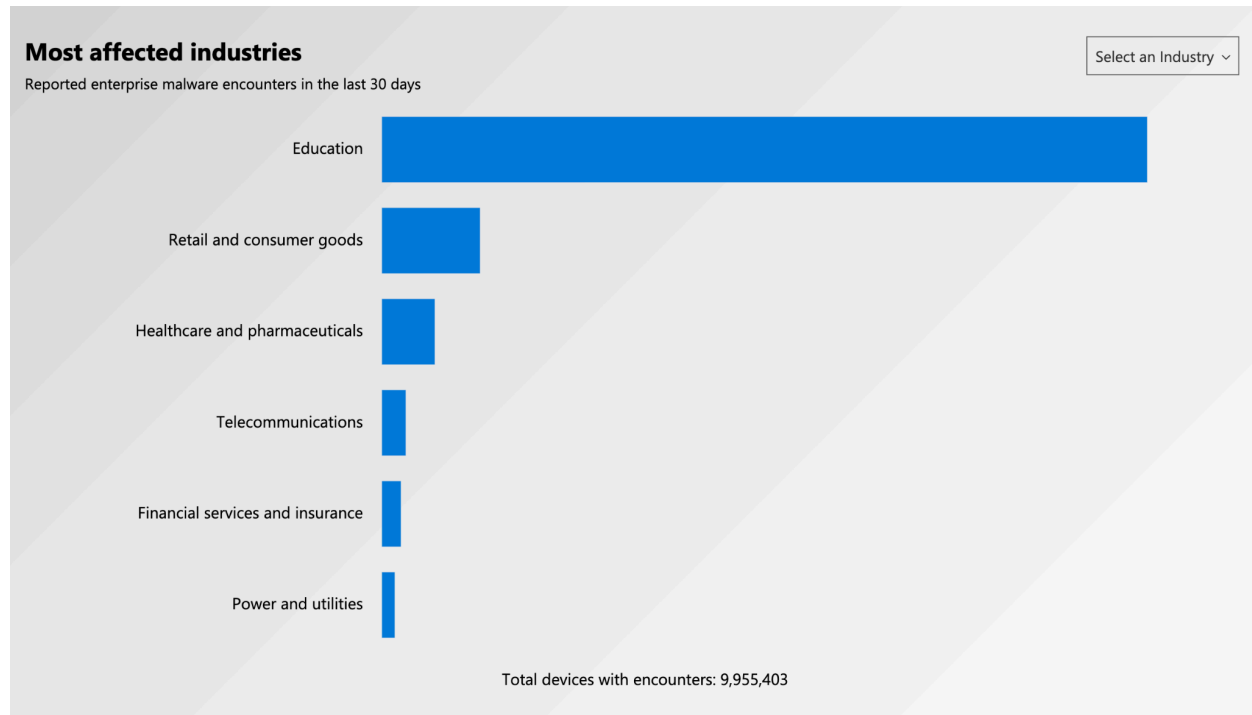


Figure 2

The only caveat of Window Defender is it has to be updated with the latest malware signatures or identifiers to prevent exploitation. Unfortunately, many organizations often do not update their software including Defender because it can cause dependency issues for other critical operations on their network. This can lead to vulnerabilities and eventual exploitation of the vulnerable network and machines, leading to data exfiltration. However, there are emerging technologies that can help prevent exploitation, vulnerabilities, and harden existing mitigations for networks and Window computers.

Emerging Technologies and Mitigations

As technology evolves, it becomes more necessary to integrate emerging technologies and mitigations into the technological infrastructure. Today, user-based authentication and password are widely used in all information systems and services from website to computer

logins. However, usernames and passwords are becoming obsolete as more and more data breaches occur, compromising user passwords. The same can be said for Windows systems, which are the most targeting operating systems. To combat the traditional usernames and passwords, passwordless authentication is starting to become more prevalent. Passwordless login is an authentication method that allows a user to gain access to an application or IT system without entering a password or answering security questions (Parmar et al., 2022). A user can accomplish this by using hardware based tokens or software based tokens to login and authenticate with a computer or server. Hardware based tokens such as a YubiKey (*Figure 3*) require a physical device to be plugged in or integrated with the computer to allow authentication. Once the device is connected to a computer such as a Windows system, the device will grant access to that specific user. This is more secure than usernames and passwords because it requires a device to be physically present to allow authentication.



Figure 3

Software based tokens or authentication applications are the most common form of passwordless logins. Software tokens enable the user to download and update a program running on their machine or mobile device, which creates tokens for the user automatically to authenticate with

(Parmar et al., 2022). Smartphones are often used to send push notifications to the user. A user then clicks on the push notification and the computer, server, or website will authenticate the user of the service. Microsoft allows this on Windows computers using the Microsoft Authenticator application to allow authentication with its services and machines. Like hardware based tokens, this is more secure because it requires the software to be present on a nearby device to authenticate with a service or machine.

Another emerging practice is zero trust framework architecture also known as ZTA. ZTA is “an approach to cybersecurity and risk management that safeguards the environment no matter where data and people reside” (Hubbard et al., 2021). In other words, zero trust is the process of not trusting any device, file, or configuration unless it is properly verified and authorized to connect, run, or implement on a system. Many organizations are starting to include this practice within their networks and end-user Windows computers. This means there will be less malware infections and less successful phishing attempts, especially against the highly targeted Windows systems. Zero trust also coincides with the principle of least privilege. Least privilege is the concept and practice of restricting access rights for users, accounts, and computing processes to only those resources absolutely required to perform legitimate functions (Miller, 2023). Like zero trust, this will prevent more malware infections, successful phishing attempts, and privilege escalation if a system is compromised, thus minimizing damage by limiting access for each user or role on a network or domain.

Lastly, the most important emerging technology, that will be forever evolving, is cybersecurity awareness training programs. \$4.35 million dollars is the average cost of a data breach globally, meaning employees and businesses are responsible for safeguarding data against malicious attacks (Grigas, 2023). A majority of compromises happen because of human

interaction, whether it is clicking on a malicious link or downloading a malicious program. It is up to organizations and companies to train employees to prevent this financial loss. However, employees often do not take this training seriously. To combat this, companies are starting to make the training into a game-like format or gamifying. Gamifying this training means turning the training into a game that employees participate in. Rewards can be added to the training game, such as a small bonus. Giving employees a small bonus will be significantly cheaper than a data breach occurring with millions of dollars on the line and loss of customer loyalty. Furthermore, employees will be more incentivized to take the training more seriously, which will decrease the odds of a data breach occurring within a company. Employers should give this training every four to six months and send out mock phishing campaigns periodically to test the employees to see what needs to be improved in the training material.

Discussion and Conclusions

In conclusion, the pervasive influence of technology in our digitized world is evident through the seamless integration of digital devices into our daily routines. Windows, as a dominant operating system, plays a crucial role in this landscape, powering most computers globally. Its user-friendly interface, compatibility with diverse software, and widespread adoption contribute to its enduring popularity. However, this ubiquity also makes it a prime target for cybercriminals. There are many malware types such as ransomware becoming more popular, denial of services attacks to bring down large or small businesses and their computational power, and phishing attacks which facilitate a majority of data breaches that occur worldwide. New threats are always emerging targeting Windows and companies or services that have weak security policies in place to prevent these attacks. Existing and emerging mitigations and technologies help mitigate this concern and are becoming more successful at defending

against these attacks and threats. As we navigate this digital era, understanding the common cyberattacks targeting Windows systems, staying informed about the latest security threats, and exploring innovative technologies for enhancing Windows security remain essential endeavors for securing information systems and the data it holds.

References

8 Devastating Phishing Attack Examples and Prevention Tips. BlueVoyant. (2024).

<https://www.bluevoyant.com/knowledge-center/8-devastating-phishing-attack-examples-and-prevention-tips>

Cyberthreats, Viruses, and Malware. Microsoft. (2024).

<https://www.microsoft.com/en-us/wdsi/threats>

Grigas, L. (2023, August 30). *What is Cybersecurity Awareness Training?*. NordPass.

<https://nordpass.com/blog/cybersecurity-awareness-training/>

Hoogeveen, P. (2022, June 8). *User Account Control Bypass For Windows 11 & Windows Server 2022*. SecJuice. <https://www.secjuice.com/multi-win-uac-bypass-x0xr00t/>

Hubbard, T., Steinhoff, J. C., Wong, S., & Klimavicz, J. F. (2021). Zero Trust in a Virtual

Cybersecurity World. *Journal of Government Financial Management*, 70(2), 12–19.

<https://doi.org/https://www.proquest.com/openview/30c22f6430bce1b543c850b3963373b7/1?pq-origsite=gscholar&cbl=26015>

Miller, M. (2023, June 13). *What Is Least Privilege & Why Do You Need It?*. BeyondTrust.

<https://www.beyondtrust.com/blog/entry/what-is-least-privilege>

Pachhala, N., Jothilakshmi, S., & Battula, B. P. (2021). *A Comprehensive Survey on*

Identification of Malware Types and Malware Classification using Machine Learning Techniques. IEEE Explore. <https://ieeexplore.ieee.org/abstract/document/9591763/>

Parmar, V., Sanghvi, H. A., Patel, R. H., & Pandya, A. S. (2022). *A Comprehensive Study on Passwordless Authentication*. IEEE Explore.

<https://ieeexplore.ieee.org/document/9760934/>

Phishing. NIST Computer Security Resource Center. (2024).

<https://csrc.nist.gov/glossary/term/phishing>

Verizon Data Breach Investigations Report 2023. Verizon. (2023).

[https://www.phishingbox.com/downloads/Verizon-Data-Breach-Investigations-Report-D
BIR-2023.pdf](https://www.phishingbox.com/downloads/Verizon-Data-Breach-Investigations-Report-D
BIR-2023.pdf)

What is a Distributed Denial-of-Service (DDoS) Attack?. Cloudflare. (2024a).

<https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/>

What is Malware?. Cloudflare. (2024b).

<https://www.cloudflare.com/learning/ddos/glossary/malware/>

What is WannaCry Ransomware?. Kaspersky. (2024, March 21).

<https://usa.kaspersky.com/resource-center/threats/ransomware-wannacry>

Windows 11 Security Book: Powerful Security by Design. Microsoft. (2023, September).

[https://www.microsoft.com/content/dam/microsoft/final/en-us/microsoft-brand/document
s/MSFT-Windows11-Security-book_Sept2023.pdf](https://www.microsoft.com/content/dam/microsoft/final/en-us/microsoft-brand/document
s/MSFT-Windows11-Security-book_Sept2023.pdf)

Windows Spoofing Vulnerability. Microsoft. (2020, August 11).

<https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-1464>