Arian Lovo
CYSE 280
04/27/2025

Strengthening Windows Security: Threats and Defenses

In todays technology driven world, securing operating systems is more crucial and important than ever. Microsoft windows, is one of the most common and widely used operating systems there is in the world, but with that title comes with a lot of attention and in turn makes it a high target candidate for hackers looking to exploit its vulnerabilities. Despite Microsoft's ongoing efforts to enhance security, Windows remains a favorite target due to its complexity and the non stop changing landscape that is cyber threats.

While Microsoft has made significant changes in strengthening its Windows security with tools and resources like Windows Defender, BitLocker, and Secure Boot, the battle against cybercriminals continues. Attacks like the WannaCry ransomware outbreak and the SolarWinds breach are examples that demonstrate just how vulnerable Windows systems can be especially when neglected or delayed.

This paper will explore common vulnerabilities within Windows OS, examine the security tools that Microsoft offers, and discuss how these defenses have been tested in the real world. By reviewing past breaches and how Windows defenses have been put to the test in real world scenarios. By reviewing past breaches and how Windows Security measures could have helped, this paper will highlight the importance of implementing layered defenses and staying ahead of emerging threats.

Windows operating systems have long been at the heart of personal and business computing. With millions of devices running Windows, it's not shocking or surprising that it attracts attention of those with ill intentions of cybercriminals. The majority of the worlds desktop market runs on Windows, so with popularity comes a lot of attention but its no

always good. This brings unwanted attention from hackers, making it very likely to be targeted. The wide usage of this operating system combined with Window's complex structure creates structure and numerous opportunities for attackers to exploit weaknesses and find vulnerabilities.

Windows has always been a major target for activity of malicious nature. Older versions of Windows XP and Windows 7, which are still used in some organizations, this creates unique obstacles and challenges as they lack modern security protocols and do not receive the most recent updates even despite the warnings for not doing so and pushing for the updating, legacy systems are still more prevalent than not, creating an ongoing vulnerability.

However, new versions of windows like 10 and 11 have made security a priority. Features like Windows Defender, BitLocker, and Secure Boot are designed to strengthen the operating systems' defenses. While these tools are a step forward, they are not without their limitations. For example, while Windows Defender has improved to be a robust tool for real time malware protection, It has its struggles against more sophisticated forms of attacks like advanced persistent threats.

Microsoft has added a variety of security features to Windows OS over the years to improve its overall defense. One key addition is Windows Defender, which provides real time protection, scanning, and cloud-based intelligence. What started as a basic anti-virus tool has now evolved into a comprehensive suite, offering protection against ransomware, phishing, and other threats.

Arian Lovo
CYSE 280
04/27/2025

Strengthening Windows Security: Threats and Defenses

In addition to Windows Defender, BitLocker is another important security feature that has become standard in new Windows Versions. BitLocker offers full disk encryption, which is critical for preventing unauthorized access to sensitive data, especially in the case of stolen devices. Encryption helps make sure that though a device is compromised and not in possession, that data will remain secure which basically acts as a safety net.

Secure Boot was introduced with windows 8 and included in later version. Secure boot works to protect against boot time malware, ensuring that only trusted software can be loaded during the boot process. This layer of protection is essential for stopping attacks that target the system when most vulnerable starting point which is when the system first powers on.

Windows also comes in built in firewall and automatic updates, which are integral for blocking malicious network traffic and ensuring that the system is up to date with the latest security updates. While great and these tools significantly improve the security of Windows their effectiveness depends on the users or organizations commitment and awareness to properly configuring and maintaining them.

While built in tools provide a good foundation for securing Windows systems also requires adherence to established frameworks and best practices. For example, NIST's SP 800-123 provides clear guidelines for securing servers and critical infrastructure, which can be applied to windows systems as well. These guidelines focus on tightening access controls, minimizing unnecessary services, and monitoring systems for unusual activity.

Implementing these principles help to reduce the attack surface of Windows systems and makes it harder for cyber threats to exploit vulnerabilities.