Windows System Security Vulnerabilities

Clarence V. Kimbrell Jr.

Old Dominion University

CYSE 280: Windows System Management and Security

Professor Malik A. Gladden

April 6, 2023

Windows Systems Security Vulnerabilities

The Windows operating system has been around for nearly 40 years. Its creation dates back to 1985, featuring the first modern-day graphical user interface for IBM-compatible personal computers (Britannica, 2021). Microsoft was heavily inspired by "Lisa," which was the first GUI-based computer available for public purchase (Powell, 1991). This was revolutionary because computers before the first Windows Operating System or Lisa were based on command-line interfaces (Loshin, 2021). Users had to remember multiple varying lengths of commands to complete tasks, which was inconvenient, and it was hard to remember them without manuals present.

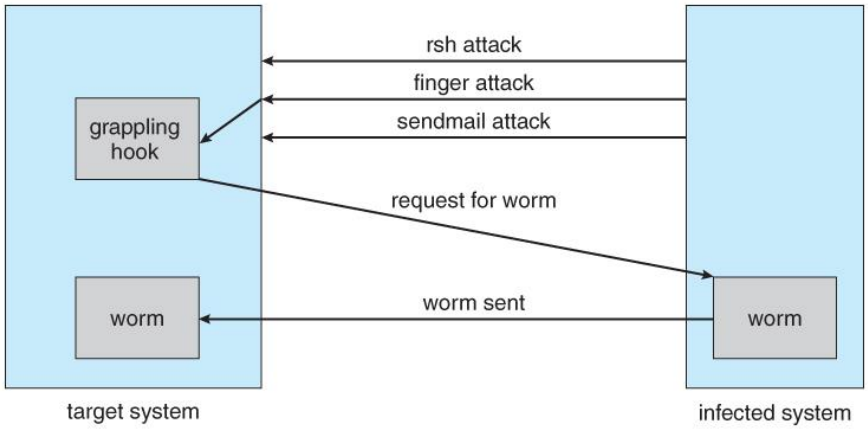
The command-line interfaces are still used today but declined in popularity after the creation of graphical interfaces. They can be seen in the fields of information technology, computer science, and cybersecurity. Every operating system administrator can complete tasks and operations using the command line. Graphical interfaces have taken control of the technology scene because they can be used by the everyday user.

Shortly after the creation of the first version of Windows, Microsoft added newer features such as file and print managers (Britannica, 2021). Then, arguably the most impactful update to the Windows operating system was in 1995 (Britannica, 2021). In that year, Microsoft released Windows 95, which had built-in internet support, including Internet Explorer (Britannica, 2021). Users were exposed to the internet, making personal computers with the Windows operating system a sought-after commodity. With all these versions of Windows, there were already security flaws and vulnerabilities that could be exploited, and more and more versions were being released. The rise of them became more apparent.

Research

Windows Worm

To understand how Windows operating systems were plagued with vulnerabilities in their earliest versions, it is best to examine the first ever to occur. The FBI labeled this the "first major attack on the internet," which was called the Morris Worm (The Morris Worm, 2018). This computer worm was launched on November 2, 1988, from a computer at the Massachusetts Institute of Technology (The Morris Worm, 2018). The Morris worm was devastating because it spread across the United States the next day (The Morris Worm, 2018). Fortunately, this was launched a year before the worldwide web was created. The FBI's website has a list of some of the most notable victims, such as Harvard, Princeton, Stanford, John Hopkins, NASA, and the Lawrence Livermore National Laboratory. This worm targeted Windows computers and all systems connected to the network.



(Famous Buffer Overruns, n.d.)

The worm was able to accomplish what it did by exploiting a backdoor in an earlier version of the email and a bug in the "finger" program (The Morris Worm, 2018). It would replicate itself on every connected computer to a network and slow its operations down until they

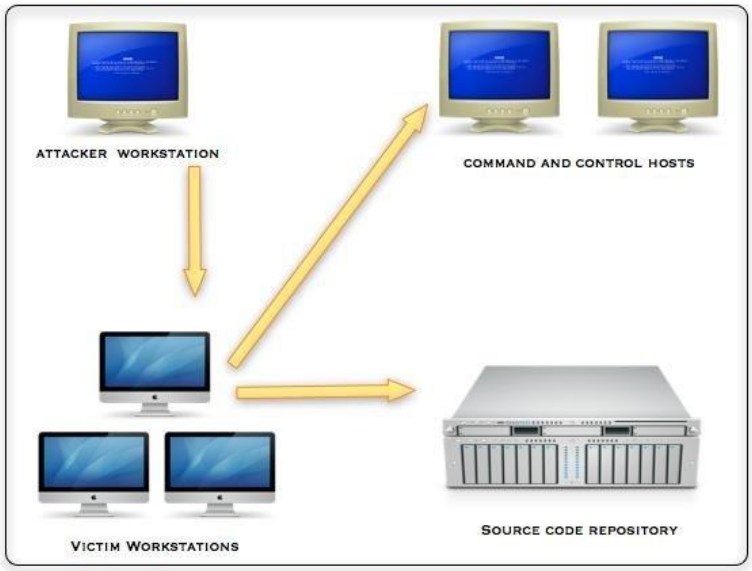
stagnated (Cohen, 2021). It caused operations to slow down so much that many places disconnected their computers and waited for a fix. Unknown to many, this was not an easy fix because it used many vulnerabilities in Windows systems. Eventually, Microsoft released a security patch called MS88-066 (Microsoft Security Response Center, n.d.). This patch targeted the finger daemon that was exploited in the launch of the Morris worm (The Morris Worm, 2018). This was only the beginning for Windows, and it showed what to expect when rolling out more updates from there on out.

Windows Zero-Day Vulnerabilities

When a new Windows update or version is released, it may contain zero-day vulnerabilities. Kaspersky, a cybersecurity company, defines zero-day as "a software vulnerability discovered by attackers before the vendor has become aware of it." This can be catastrophic because since there is no patch for it, it will likely succeed (What is a Zero-day Attack?, n.d.). Two more definitions need to be understood with the previous one, and those are zero-day exploits and zero-day attacks. A zero-day exploit is a method attackers use to hack systems with unknown vulnerabilities (What is a Zero-day Attack?, n.d.). Then there are zero-day attacks, which are the use of a zero-day exploit to cause damage to a system (What is a Zero-day Attack?, n.d.).

One infamous zero-day attack was named Operation Aurora, which was conducted on Windows 7 systems. The hackers targeted many high-profile companies in 2009 and 2010, such as Adobe Systems, Symantec, and Yahoo (Rosenberg, 2017). The attackers' main objective from Operation Aurora was to gain unauthorized access to those companies' systems and install malware. Once the hackers were in the systems, they modified source code repositories to steal

information and trade secrets (Rosenberg, 2017). It is said that the source code management systems were not well-defended at this time (Rosenberg, 2017).



(Binde, et al., 2011)

The hackers used a spear-phishing campaign to target employees of these companies and gain access to the IT systems (Everything You, 2016). Spear phishing is similar to traditional phishing, but it is towards a specific target or a small group of targets. Typically, due to their role in a company or their authorization access. This was a success, and many employee computers were compromised without them knowing, which led to the malware in the email targeting the source code management systems (Rosenberg, 2017).

Microsoft's response to this zero-day vulnerability was quick because of the potential threat this imposed on all companies involved in the attack. Microsoft issued an update to the current version of Windows 7 named "Microsoft Security Advisory 979352" (Dressman, 2010). This patch targeted the vulnerability in Internet Explorer that could allow for remote code

execution (Dressman, 2010). Windows releases patches for Windows computers often, and it is important to stay up to date with them, or you could fall victim to an attack similar to this.

Windows Spyware

Spyware has been a growing issue since 1995 (What is Spyware, n.d.). Windows systems are susceptible to spyware due to several reasons, with one of the largest factors being the user's unawareness of its presence. Spyware is particularly tricky to handle, as it remains undetectable, much like a Trojan horse. Some common signs of spyware installed on a system include links taking the user to different locations, popup displays when not browsing, and antivirus scans, even if not purchased (What is Spyware, n.d.). Spyware is dangerous because it tracks information, including emails, passwords, downloads, searches, and keystrokes (Stouffer, 2021). Nearly any information generated on an individual's computer is tracked, which can be used against the individual or sold off to other hackers.

What if the spyware was sophisticated enough to target government agencies, consultants, and organizations? This is what occurred in 2020, with the SolarWinds attack (Abrams, 2020). This spyware attack targeted supply chains and companies using a program named SolarWinds, which allowed hackers to gain access to classified data and move around the network undetected (Abrams, 2020). The SolarWinds attack remained undetected for months, allowing hackers to obtain vast amounts of information (Abrams, 2020). Hackers exploited a vulnerability using spyware on Windows 10 systems. Once inside a Windows 10 system running SolarWinds, the hackers began to install more malware to acquire additional information.

(Solar Winds Cyber Attack, n.d.)

Microsoft had to release several patches to clean up the aftermath caused by the SolarWinds attack. One of the most notable patches was named CVE-2021-1647. This patch includes a fix for the vulnerability that was exploited in Windows Defender in the SolarWinds attack (Microsoft Defender, 2021). The SolarWinds attack was a significant breach that highlighted the vulnerabilities of the supply chain and revealed the need for better security measures within Windows 10 and supply chain management to prevent more attacks like this from occurring in the future.

Conclusion

The Windows operating system has been around for nearly 40 years, and with its various versions, it's far from perfect. These imperfections create issues, as discussed above, such as worms, zero-day exploits, and spyware. As the Windows operating system continues to evolve, the number of possible exploits that need patching will increase. Although Microsoft works quickly and efficiently to correct these issues, in some cases, it may be too late, as evidenced by numerous cyber-attacks. Therefore, individuals need to update their systems and applications

regularly. The same applies to agencies, organizations, and businesses. Failure to do so could potentially make them the next target in the never-ending cyber war.

References

Abrams, L. (2021, January 21). *The SolarWinds cyberattack: The Hack, the victims, and what we know*. BleepingComputer. Retrieved April 6, 2023, from https://www.bleepingcomputer.com/news/security/the-solarwinds-cyberattack-the-hack-the-victims-and-what-we-know/

Binde, Beth & McRee, Russ & Oconnor, Terrence. (2011). Assessing Outbound Traffic to Uncover Advanced Persistent Threat. 10.13140/RG.2.2.16401.07520.

Dressman, M. (2010, January 21). *Microsoft Security advisory 979352*. Microsoft Learn. Retrieved April 6, 2023, from https://learn.microsoft.com/en-us/security-updates/securityadvisories/2010/979352

Editors, B. T. (2021, March 31). *Microsoft windows*. Encyclopædia Britannica. Retrieved April 6, 2023, from https://www.britannica.com/technology/Microsoft-Windows

Famous Buffer Overruns . Department of Computer Science, University of Toronto. (n.d.). Retrieved April 6, 2023, from http://www.cs.toronto.edu/~arnold/347/17f/lectures/knowYourInputs/

Kaspersky, E. (2022, March 9). *What is a zero-day attack? - definition and explanation*. usa.kaspersky.com. Retrieved April 6, 2023, from https://usa.kaspersky.com/resource-center/definitions/zero-day-exploit

Loshin, P., & Gillis, A. S. (2021, December 3). *What is a command-line interface (CLI)?* SearchWindowsServer. Retrieved April 6, 2023, from https://www.techtarget.com/searchwindowsserver/definition/command-line-interface-CLI

Microsoft Defender Remote Code Execution Vulnerability. Security Update Guide - Microsoft Security Response Center. (2021, January 15). Retrieved April 6, 2023, from https://msrc.microsoft.com/update-guide/en-us/vulnerability/CVE-2021-1647#revisions

Microsoft Security Response Center. (n.d.). Security Bulletin MS88-066 - Critical. Retrieved from https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/1988/ms88-066

Powell, A. (1997, December 19). *Web 101: A history of the GUI*. Wired. Retrieved April 6, 2023, from https://www.wired.com/1997/12/web-101-a-history-of-the-gui/

Rosenberg, J. (2017). *Operation aurora*. Operation Aurora - an overview | ScienceDirect Topics. Retrieved April 6, 2023, from https://www.sciencedirect.com/topics/computer-science/operation-aurora

Solarwinds cyberattack. Splunk. (n.d.). Retrieved April 6, 2023, from https://www.splunk.com/en_us/surge/solarwinds-cyberattack-response.html

Stouffer, C. (2021, December 13). *Types of ransomware to recognize + ransomware protection tips*. Official Site. Retrieved April 6, 2023, from https://us.norton.com/blog/malware/spyware#

What is spyware?: Juniper Networks Us. Juniper Networks. (n.d.). Retrieved April 6, 2023, from https://www.juniper.net/us/en/research-topics/what-is-

spyware.html#:~:text=A%20Brief%20History%20of%20Spyware,of%20the%20%E2%80%9Cspyware%E2%80%9D%20term.