HOW HAVE THE THREATS/VULNERABILITIES FACED BY WINDOWS EVOLVED OVER TIME SINCE ITS INCEPTION?

BY: BRYANT WATKINS

NOVEMBER 30, 2023

CYSE 280

Prof. Gladden

INTRODUCTION

Over time – there are many threats and vulnerabilities faced by society that evolve over time. From the Cold War to terrorism to gun violence – the security environment has shifted over the years. That same concept very much applies to Windows Systems, as we have witnessed Windows from its infancy to now face evolving threats and vulnerabilities. This research will take an extensive look at all the major threats as well as vulnerabilities faced by Windows systems since its inception in 1985.

Since the invention of network systems there has always been constant threats and vulnerabilities. Some of the more common threats include – Ransomware, Phishing, Malware, Worms, Denial-of-Service (DoS) attacks. This research will focus specifically on the threats and vulnerabilities faced by Windows, as not all network systems face the same threats or vulnerabilities. Not only will the threats and vulnerabilities be assessed – but I will also observe the countermeasures taken by Windows as well as the effectiveness. Conclusively, I will then take the gathered information/data and utilize it to accurately project what future threats and weaknesses may be in store for Windows in the future.

Windows is widely known for its profoundly strong cybersecurity infrastructure as well as numerous safety features available on its products, but there are some incidents within its history that helps paint a picture of how Windows has navigated the dangerous security environment faced over the years. It is certainly to the vital interest of many worldwide who utilize Windows System products to have this topic addressed, with this sort of information users will better be able to make informed decisions on their technical needs based on the security environment they will be exposed to.

OVERVIEW OF THE RESEARCH/REQUIRED INFORMATION

The most critical information required during this research will likely be derived from observing some of the more damaging and debilitating malicious attacks in the history of Windows Systems. Viewing the incidents faced by Windows over the years will assist in grasping a true understanding of what type of attacks have taken place, their frequency, and just as importantly, how exactly Windows responded in both short term and long term. The required information will also allow me to make inferences, assessments, appropriate visuals, and eventually projections or predictions on what is to come in the security environment of Windows.

More critical information needed also includes information on the assailants regarding motive and method of attack. It is incredibly imperative that assailants be taken into consideration, as a scenario where an actor commits multiple attacks over time would prove very note worthy in predicting future incidents if said individuals have failed to be held accountable for their actions. The motive will also give great insight, even if malicious cyber-attacks have been committed by different actors at every instance – the motive matters greatly should I observe a pattern in the motivations inspiring these attacks if it likely to continue being the same motivation for the foreseeable future.

Statistics will also play a crucial role in the conducted research. Statistics will play the largest role in my predicting/projecting of the future. I will better be able to accurately make informed estimations as a derivative of the statistics on malicious cyber-attacks. The numbers related to incidents, such as possibility and/or success rate, will showcase any major trends that will determine what precisely may be faced Window systems for the years to come.

METHODOLOGY

The questions to be addressed pertain to the evolution of the threats and vulnerabilities concerning Windows Systems since its founding in the 1980's, as well as what the security environment may entail going forward. To answer said questions I will mainly be looking to inform myself about the biggest and most consequential malicious attacks that have ever plagued Windows. No research can or should be conducted on malicious attacks against Windows Systems without first establishing which attacks have proven most devastating and influential in the shaping of Window's security environment from past to present and beyond. Establishing the most impactful attacks allows one to begin focusing research efforts on said attacks.

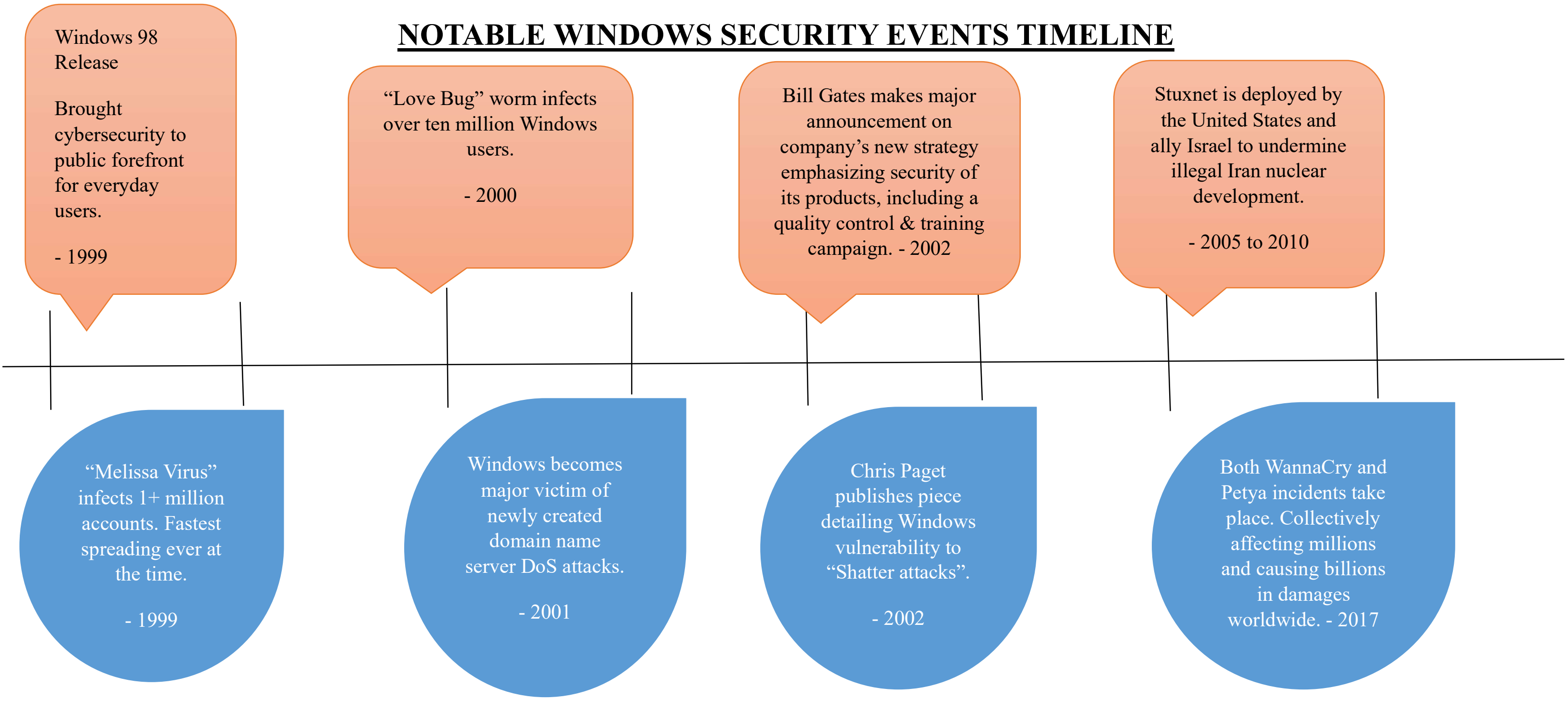
Then the research efforts shift to the frequency of major attacks. The frequency of attacks is another major pillar to the eventual conclusion to be reached. For the purposes of this research – attacks that are more frequent will be seen as a graver threat to Windows then less frequents, even if the less frequent attacks are more devastating in a vacuum. It is imperative, when studying the history of attacks against Windows, to have a keen eye for observable patterns of behavior amongst bad actors. The clearest pattern of behavior to be observed of bad actors is the number of occurrences of specific types of attacks over the past few decades.

The final pillar of the research to be conducted is to analyze and assess what steps Windows has taken in effort to combat past, present, and future cyber threats to its security environment. Assessment of Windows' actions is needed to specifically determine just how effective their mitigation techniques have been, as well as pondering its ability to effectively deter behavior in the future based on their incident response procedures. Swift, adequate, and effective mitigation and incident response techniques will lend greater confidence in Windows' ability to safeguard its vital infrastructure and interests for the near future.

Tools/Resources/Results

Charts and graphs will prove most consequential in the observation and analysis of the statistics pertinent to the history and future of Windows’ security environment. Statistical visuals that will be utilized in this research provide great benefit due to the ability of charts and graphs to organize numerical data into formats easier to comprehend. The organizational manner of the presented data will allow said information to be communicated to readers in an effective manner, allowing one to observe key points of data.

NOTABLE WINDOWS SECURITY EVENTS TIMELINE



Windows 98 Release

Brought cybersecurity to public forefront for everyday users.

- 1999

“Melissa Virus” infects 1+ million accounts. Fastest spreading ever at the time.

- 1999

“Love Bug” worm infects over ten million Windows users.

- 2000

Windows becomes major victim of newly created domain name server DoS attacks.

- 2001

Bill Gates makes major announcement on company’s new strategy emphasizing security of its products, including a quality control & training campaign. - 2002

Chris Paget publishes piece detailing Windows vulnerability to “Shatter attacks”.

- 2002

Stuxnet is deployed by the United States and ally Israel to undermine illegal Iran nuclear development.

- 2005 to 2010

Both WannaCry and Petya incidents take place. Collectively affecting millions and causing billions in damages worldwide. - 2017

The above timeline showcases some of the more critical events in the history of Window systems that have helped shape the security environment for Windows from past to present. As displayed by the first notation – Windows releasing Windows 98 in 1999 was revolutionary and innovative at that time in the establishment of the cybersecurity for everyday users. Less than a couple of years from Windows 98, following a couple of incidents and vulnerability discoveries affecting millions, Bill gates then announced the enormous cybersecurity campaign he and

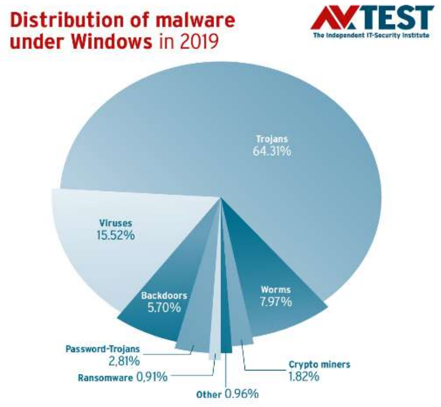
Microsoft would embark on. Given the robust nature of Windows security – there were few more major incidents, events, or crises in the past two decades save for those noted above.

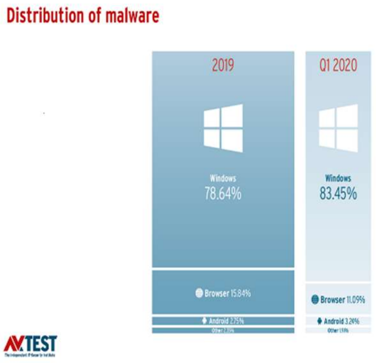
History of Common Windows Vulnerabilities

1980's	No security-conscious OS
Early 1990's	"Ping of death" attack susceptibility
Mid to late 1990's	"Black orifice" Trojan attacks
Early 2000's	Buffer flow attack susceptibility

As observed through my research and the visual representations above – many of the dangerous re-occurring vulnerabilities found in Windows systems were most problematic early in the life of Windows. Given the newness of technology and the internet at the time (1980's to early 1990's) – Windows was very much learning and trying to navigate the dangerous nature of the Information Technology field as was everyone else. With the lack of experience at the time, Windows biggest vulnerability in its early stage was the complete omission of cybersecurity centric operating systems. The lack of any security measures creates vulnerabilities for obvious reasons, access was granted to literally anybody.

The 1990's and early 2000's would prove to be the most fundamentally dynamic and revolutionary for Windows. The 1990's brought attention to vulnerabilities found among most other systems. The main attacks faced by Windows in the 1990's consisted of worms and bugs – as seen with the "Love Bug" and Melissa Virus. Other key attacks in the 1990's included Dos attacks that would simply overwhelm the system – as seen with an onslaught of Buffer overflow attacks as well as the "Ping of Death" attacks. Windows, as well as many others in the IT community, soon began to realize that even with the stringent security measures put in place in the early 2000's – users would always prove to be the weakest point in any security infrastructure.





The 21st century brought a share of different threats than earlier Windows years. The 21st century saw an increase in DoS/DDos attacks against all systems as well as the continuation and further sophistication of malware attacks. As seen with the above images – Windows has been targeted by malware far more than other systems and a large share has been Trojan. The main reason for such a discrepancy amongst the major systems in world is largely due to two reasons – Windows' wide name recognition, and numerous documented backdoors or security gaps.

Some of the biggest ever hacks or breaches against Windows systems would also occur in the 21st century. In 2017, Windows underwent immense challenges in addressing both the WannaCry Ransomware and Petya attacks. Those two attacks were methods of malware that disrupted large populations and caused billions in damages collectively. Windows addressed these incidents with patches and updates, however, many of the affected software was running on older variations of Window systems. Those efforts are not the only taken by Windows to enhance security, others of note include - Data Protection Application Interface (DPAPI), Credential Manager, User Account Control (UAC), Windows Defender, to name a few.

CONCLUSIONS

Much of the success in avoiding major breaches and incidents over the decades is a complete attestation to Windows' (Microsoft) immense security efforts first initiated by Bill Gates in the early 2000's. Users over the years have been given a plethora of security updates and enhancements. There have been some incidents and vulnerabilities in the 21st century, however, that of course are concerning and bring in to focus the challenges in continually fortifying Window's security environment. My extensive research has certainly led me to reach a conclusion on how the security environment may look for Windows going forward.

It is incredibly apparent that malware is, and will continue to be, the gravest threat to the fortified security environment of Windows. The numbers are startling, not only is malware the more prominent threat – but Windows systems specifically are more prone to these attacks than other systems by far. While Windows has made changes and advancements in its security posture towards malware, which can be seen in their action following Petya and WannaCry. Windows would provide users with cloud-delivered protection updates, made updates to their signature definition packages, and install kill switches to combat the malware.

Windows still has more work to do to combat a surging malware threat faced going forward. Given the unforeseen and fast-paced nature of malware – security updates should be made necessary to the functioning of Windows software. Windows also must uphold and expand stringent authentication, as well as encryption, methods utilized by users. Microsoft should also implement a robust campaign to educate and train its users, no security measures put in place can ever sufficiently counter poor or unsafe practices by users. No system is perfect or absolute, but if Windows builds upon some of its most advanced measures so far, as well as expand upon them, with some of the suggestions above - then they will be in better position to combat the ongoing spike in malware threats.

References

Palmer, Michael J. Hands-on Microsoft Windows Server 2016. 2nd ed., Cengage Learning, 2018.

Ciampa, Mark D. CompTIA Security+: Guide to Network Security Fundamentals. Cengage,

2022.

Patrizio, Andy. "Microsoft Issues Fixes for Non-Supported Versions of Windows Server: Critical Vulnerability Force Microsoft to Patch Versions of Windows Server and Desktops that are Long Out of Support." Network World (Online) (2019)ProQuest. Web. 13 Sep. 2023.

Gilmour, Tristan. "A Brief History of Windows Vulnerabilities: The Evolution of Threats and Security." Infosecurity Magazine, 3 Apr. 2023, www.infosecurity-magazine.com/blogs/history-of-windows-vulnerabilities/.

"From Windows 1 to Windows 10: 29 Years of Windows Evolution." Edited by Betsy Reed, The Guardian, Guardian News and Media, 2 Oct. 2014, www.theguardian.com/technology/2014/oct/02/from-windows-1-to-windows-10-29-years-of-windows-evolution.

"Cybersecurity History: Hacking & Data Breaches." Monroe College, www.monroecollege.edu/news/cybersecurity-history-hacking-data-breaches. Accessed 11 Sept. 2023.

Cohen, Jason. "Windows Computers Were Targets of 83% of All Malware Attacks in Q1 2020." *PCMAG*, PCMag, 28 Aug. 2020, www.pcmag.com/news/windows-computers-account-for-83-of-all-malware-attacks-in-q1-2020.

Gilmour, Tristan. "A Brief History of Windows Vulnerabilities: The Evolution of Threats and Security." *Infosecurity Magazine*, 3 Apr. 2023, www.infosecurity-magazine.com/blogs/history-of-windows-vulnerabilities/.

Townsened, Caleb. "A Brief and Incomplete History of Cybersecurity." *United States Cybersecurity Magazine*, 2 Nov. 2020, www.uscybersecurity.net/history/.

Belding, Greg. "Windows OS Security Brief History." *Infosec*, 15 Oct. 2019, resources.infosecinstitute.com/topics/operating-system-security/windows-os-security-brief-history/?gad_source=1&gclid=CjwKCAiAmZGrBhAnEiwAo9qHiVzdNRpxLnM4zL3F3iNRHWaOhDnqYj5lj6Y6Ato0VPQI2MzlYX6xxBoCnMIQAvD_BwE.