“Windows System Security Vulnerabilities”

CYSE 280 – Windows Systems Management and Security

Cyber Security Program - Professor Malik A. Gladden

Helen Bramow, MA - #01187330

Nov. 29, 2022

Windows System Security Vulnerabilities

This paper focuses on Microsoft ("MS") Operating Systems and other MS products, in terms of their known vulnerabilities. The research offers explanations why MS is a well-known target often of hackers, and why they are often successful. "*Nearly 50% of hackers say they compromised Windows systems more than any other within the past year*." (Woollacott, 2018) Some of the reasons include the market share, i.e., MS market share is about 60%, and also the various older versions of software used that are unsupported, or are unpatched. ("How Many Computers Use Microsoft In the World", 2022) There is a note on how many enterprise or business entities are using older software also. Additionally, there are articles stating the number of MS vulnerabilities for certain years, and some of the reasons for those vulnerabilities. There is a comparison of different versions of MS products, for instance: MS Office 97 – 2016, and another comparison of Android, Apple and MS Windows 10, Windows Server 2016 and Windows Servicer 2019 vulnerabilities for 2020. There is also a list of the top 10 Windows vulnerabilities for 2021. Then, there are some solutions or resolutions to cut back on the vulnerability problem. These include: updating the system, ensuring updates are completed, and even purchasing a new subscription. There is also a suggestion that business need to: budget for updated software, schedule vulnerability testing, and track which software versions departments are using and when the necessary updates are completed for patches to be effective on older software. These are responsibilities that businesses need to take seriously and put security measures in place. Still, there is another solution altogether: to change over to Linux OS. Linux is free, and has many advantages over MS products overall, so it could be a viable alternative for users unwilling or unable to afforded updated products.

Windows Systems Security Vulnerabilities

Introduction

Microsoft ("MS") products are used by more than 1.5 billion people around the world – by all means it is considered one of the largest software companies on earth. As of 2014, MS's market share was at 24%, but MS Office worldwide has about a 60% market share. MS also has enterprise software (business software) market share of 83%. ("How Many Computers Use Microsoft In the World", 2022) [see: Table 1 – MS Products] These are very large numbers, and part of the reason issues stand out because they affect so many users worldwide, both for businesses and personal computer too.

MS Market Share and Vulnerabilities

MS vulnerabilities matter because their market share is huge, and that has an effect from a cyber security perspective. For instance, this OS is on more than 1 billion computers, so it is vital in the IT cyber security area to know where the vulnerabilities are, and how devastating they are. Vulnerabilities are like open doors, and with that many open doors, there is a great amount of risk. Many of these vulnerabilities result from running older versions, unsupported, and even from not installing either patches or doing system updates. So, companies who are running MS should have a procedure for risk assessment and a schedule for vulnerability scans. However, there are also other options listed below.

MS OS market share also makes it a very big temptation for hackers, who would rather attack a large source of data operations (and users) like MS OS and/or Windows, versus Linux or even Apple MACs. There is just so much more data to be stolen, or held at ransom, and more dollars at stake as well – things that are definitely appealing to most thieves and hackers. ("How Many Computers Use Microsoft In the World", 2022) [see: Table 1 – MS Products]

Table 1 - Popularity of MS Products – [statistics from June, 2022] ("How Many Computers Use Microsoft In the World", 2022), and (Kaelin, 2017) – Chart by H. Bramow 11/16/22

	Desktop	Windows 10	MS Office	MS Products	Windows
World users		150 million+	60%	1.5 billion+	Over 130 million
Active users			100 million+		Over 80 billion
US users	75%				
Businesses				70%	70%
Downloads		30 million+			
Market Share			60% global		
Old Versions of MS Office			83% enterprises		

In reviewing the 2022 statistics it shows that 70% of businesses overall utilize MS products too, and businesses are a much more likely target because their data is worth more to hackers. There are also other reasons why hackers would prefer Windows over Linux, having to do with the setup of the OS and permissions, that are listed below.

The other issue with MS users is the use of old, unsupported versions of MS software. These versions have various holes and gateways that are not addressed usually. Again, from Table 1, it shows that "83% of enterprises" are utilizing old forms of MS Office in particular. But, that is when reviewing simply in terms of the 'numbers,' it is definitely attractive to hackers looking for either some ransom money, data to steal, and/or some recognition for a cause. From an IT security perspective, it is all about assessing the risk, and mitigating the risk. Another thing that comes to mind is also the current laws on correcting vulnerabilities regarding timelines and notice to consumers, and government oversight also. That issue could be its own subject in another research paper! This applies to MS OS and/or Windows perhaps more than other OS companies simply because of the massive numbers involved, and even the numerous old software versions that are unsupported but still utilized by both consumers and enterprises or businesses. ("How Many Computers Use Microsoft In the World", 2022)

MS Businesses use Old MS Office Versions

In addressing any software vulnerabilities, it is necessary to also contemplate the older versions which are not subject to updates. Those updates can be very valuable in terms of protection from hackers, by closing up known gateways and by plugging holes. Although it takes years sometimes for companies to find the holes, it can take even longer to acknowledge their existence and then to publish software patches for consumers and businesses alike. MS has many different products today and is a very old system from about 20+ years ago. They consistently stop supporting their older versions of software, in lieu of supporting only the newer versions. And, what about the vulnerabilities they either don't find, or choose not to create patches for? For companies – enterprises which are businesses utilizing old MS software versions, this makes their data vulnerable to known attack sites. This is perhaps the most important reason why all companies and enterprises should update their software versions to the current version. The companywide cost is a tax write off, but the best reason to implement it is because that upfront cost will provide a future savings from not being hacked. Hence, it would also make it very worthwhile to do. It could be like an insurance policy – protection upfront for

what might occur later on down the road. In most cases, you would need to do anything further. This is what we call 'mitigating the damages.'

Another alternative for running current MS software, both businesses and for consumers alike, is to purchase or update to newer forms of MS software via subscription. Again, it would be a tax write off for companies, and the cost savings would come from greater IT security. It would still require that they keep up with the current updates though and keep the installs current. MS would benefit from consistently retaining the same customer base, and consumers and businesses might find a subscription program easier to keep current. Keeping software current is one way to avoid being the target of hackers, or at least lowers the risk.

Table 2 - https://www.techrepublic.com/article/83-of-enterprises-use-microsoft-office-but-there-is-danger-lurking-in-that-huge-number/

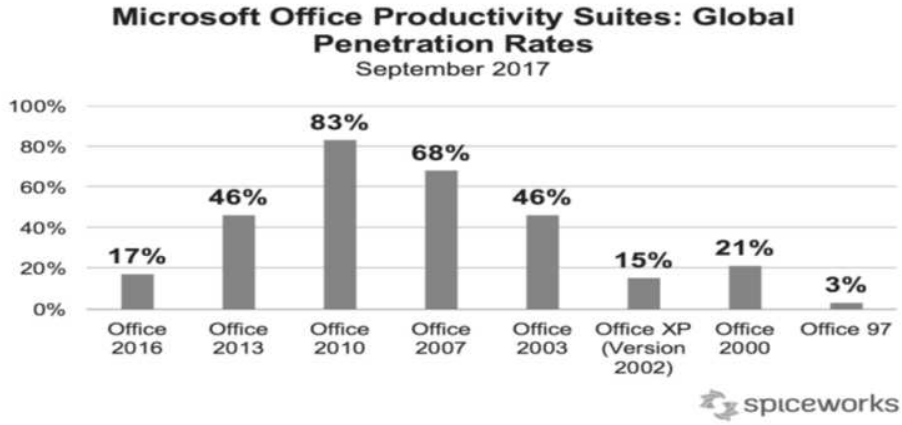
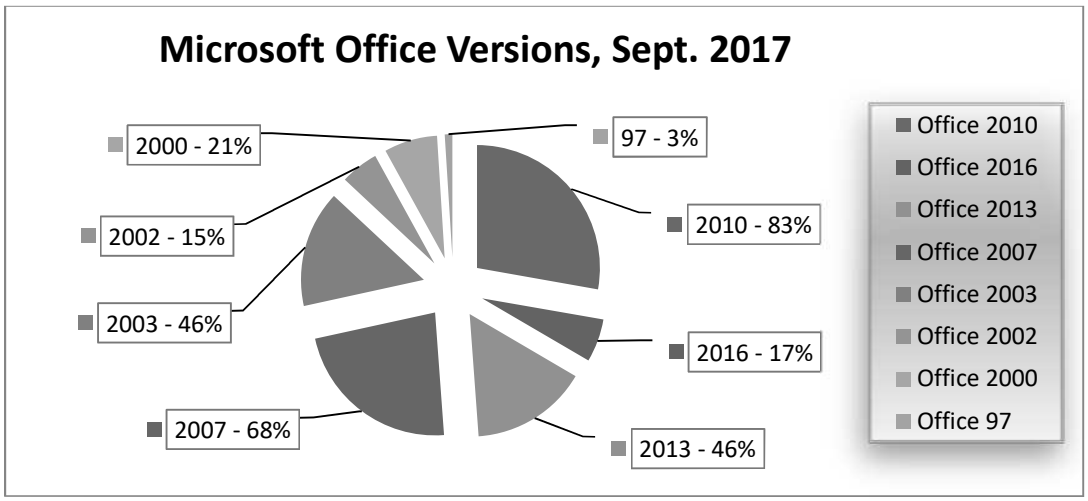


Table 3 - Data: https://www.techrepublic.com/article/83-of-enterprises-use-microsoft-office-but-there-is-danger-lurking-in-that-huge-number/, Chart by H. Bramow 11/17/22



As shown in Tables 2 and 3, 83% of MS Office in business/enterprises is from 2010, which is an old, free version of MS Office. According to TechRepublic.com, these are mainly businesses with employees up to 1,000. These companies could be held liable in the case that their companies were hacked, data, especially private client data, was stolen, lost or held for ransom, since they failed to obtain a more recent copy of MS Office that is supported by MS. Although most software is useable while not having manufacturer support, it may however have unforeseen security vulnerabilities which the company may then become responsible for. That free software may exhibit the hidden cost of known, aging, vulnerabilities. And, the old software can no longer be maintained if the manufacture, MS, isn't supporting that version anymore. (Kaelin, 2017) The additional risk with employees mainly working virtually after the virus scare, is employees may get hacked on their personal computers and their personal data may also be stolen or ransomed. But, of course, virtual working has brought up other security risks, like employees opening the gateway to company's classified data anyway.

MS and Vulnerabilities

"IT security professionals admit that one in three breaches are the result of vulnerabilities that they should have already patched." (Ranger, 2019)

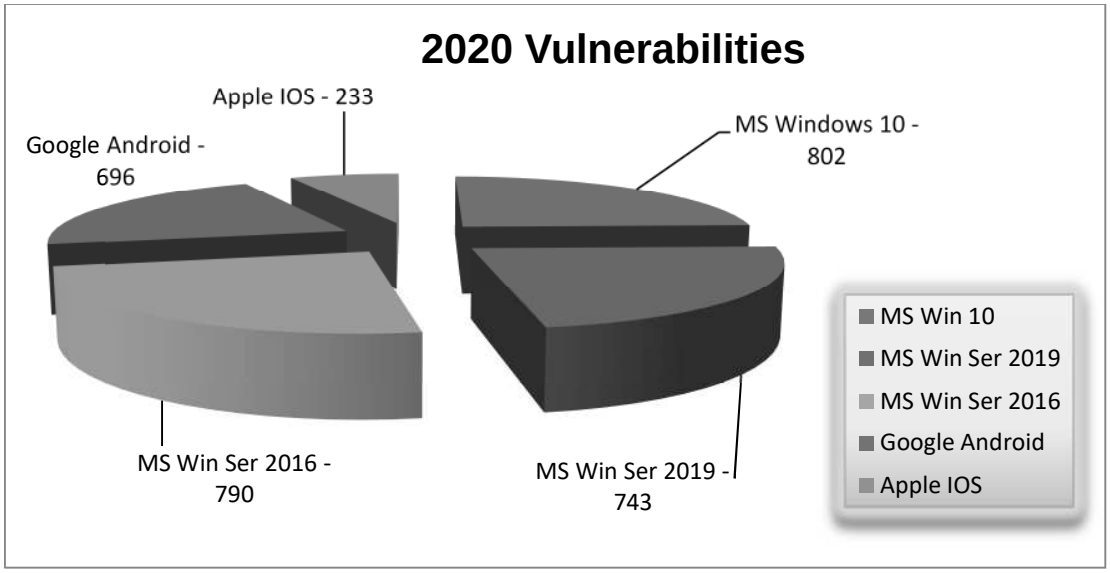
MS is not known for security, period, but is known as being a leaky system overall. Windows has many known vulnerabilities listed every year. This year, 2022 is already higher than last year for Windows 10. Since 2018, there has been from 486 – over 800 vulnerabilities per year. For 2022 so far, there are more than 361. (Microsoft Windows 10 Vulnerabilities - Security Vulnerabilities in 2022) In order to be proficient at cyber security and IT security in general, it is important to know how vulnerable an operating system (OS) is. There are a more than a few ways to do this. One way is to know the OS version and the number of vulnerabilities, and that is a good clue for 'how hackable' a system is, or rather how easy it is to hack. Overall, MS vulnerabilities in all its versions leaves it open for hacking, as well as the fact that billions of computers are running those various versions with those open doors.

Another way those vulnerabilities can be exploited (a common IT industry word) is by an attacker using the 'ping' command and retrieving DNS and other information on their 'targets'. Then, using MS known vulnerabilities, the attacker(s) can specifically attack targets using those any of those known vulnerabilities. (Henry, 2010) Microsoft is leaving open doors and with all the years of Microsoft products that are still on the market and unsupported, that only increases

the numbers of vulnerabilities too. As shown in Tables 2 and 3, MS Office 2010 is being utilized by many businesses still. A patch is usually fast to install, however, there is not always a patch available even though MS or the manufacture might be well aware of the problem it presents.

MS vulnerabilities had almost a 50% rise from 2019 to 2021. To be more exact, MS had vulnerabilities of 1188 published in 2020, while Google only had 950 published and Apple was much lower at 381 vulnerabilities. In comparison for 2020, the vulnerabilities were as follows: Windows 10 had 802; Windows Server 2019 had 743; and Windows Server 2016 only had 790. (Winder, 2021) They still took the prize in 2020 for number of vulnerabilities! Comparatively speaking Google's Android had 696 and Apple's IOS had 233 vulnerabilities. (Winder, 2021)

Table 4 - MS 2021 Vulnerabilities as Compared to Google/Android and Apple/IOS - Chart by H. Bramow 11/17/22; Data from **(Winder, 2021)**.



MS Windows – the Most Hacked OS

"*Nearly 50% of hackers say they compromised Windows systems more than any other within the past year*." (Woollacott, 2018) Since MS's Windows is the most used OS in the world, there are known vulnerabilities attackers will most probably use to attack their targets. As of 2021, these are the top 10 Windows vulnerabilities:

1 – the (RDP) Remote Desktop Protocol (Disclosure Info);
2 – the (RDP) Remote Desktop Protocol (DOS);
3 – Kernel Privilege Elev.;
4 – Hyper-V Privilege;

5 – Spoofing ;
6 – Print Spooler;
7 – Windows Group Policy Privilege (Elev.);
8 – Graphics Components Remote Code Exe.;
9 – TCP/IP DOS; and
10 – NetBT Info. (Pollack, 2021)

Protection of end points is one way to avoid some of these pitfalls. According to Calcom.com, many of the security breaches occur from these end points. Hardening these endpoints includes making necessary changes to both services and protocols. And, systems will require constant updating, changing, and checking them frequently because openings do 'pop up.' ("Windows 10 Solution Page.") [It is important to note that Calcom.com is talking about Windows 10 not 2010 version.]

Experts agree it is best to close up the known vulnerabilities, and patching them is ideal when they are available. MS Window users who have 'newer' old versions like: Windows 7, 8, and 8.1, can still upgrade free to Windows 10 this year for free. Windows 10 still has security risks, but at least patches are being done for it still. However, it is necessary to find all those patches, download and install them too. Then, users must keep up with the system maintenance (or system admin's must) to keep vulnerabilities at their lowest. (Tunggal, 2022)

Vulnerability Scanning

"*Windows operating systems are some of the most used as well as exploited OS around the world*." (Chauhan, 2012)

For Windows OS especially, it is important to implement a schedule for vulnerability assessments or scanning. Windows is popular and easy to navigate, and it's a popular favorite with hackers also. So, there is free software available, like Open Vulnerability Assessment System ("OpenVas"), and it can provide reliable results on exploits and vulnerabilities. OpenVas is well known and reliable, and it came into the open market from Nessus in 2005. It is better for a company to be proactive, and know where the problems are, versus suffering from a ransomware attack, data loss or some other malware. Both smaller and larger companies can save upfront on costs if they are prepared, and fix issues promptly. They can also avoid any legal issues associated with running old, unsupported software versions with known problems. But, there still needs to be a budget allocation for security, separate from IT, and a schedule of implementation, as well as the tools to do the work. (Chauhan, 2012)

Security Patches

Still, security patches are not always the remedy for vulnerabilities, like ones to Microsoft Windows Active Directory (AD). There is good reason for this according to Microsoft because attackers know where to attack and how to retrieve credentials. These credentials then give them access into the OS, and software patches will not remedy this situation. (Jungles, 2012) Hardening of the AD would be necessary to avoid these problems. But also there are also steps that would limit the damages if a hacker gains access. Some ways this can be done include: monitor AD in real time, use 2 factor or multifactor authentication (MFA), and secure admin hosts and domain controllers. (Singh, 2020)

MS Verification of Patches

MS has their own 'Microsoft Window's Update Patch Management System." But, there is some question over this system that verifies patches. If the system records the registry for a necessary patch, but the patch isn't actually installed on the system, there is a problem. According to Russ Cooper at TruSecure Corp., *the MS Windows system can be 'spoofed' into thinking a patch was done when it wasn't*. This is due to the fact that the system in most cases only relies upon registry keys, which can be spoofed. At least, or more specifically, spoofing of the registry can occur on these particular important patches:

- MS03-001 critical related to a MS Locator Serv.,
- MS03-030 – for DirectX, which is critical because it related to the buffer overflow; and
- MS03-023 – HTML, again critical for a buffer overflow. (Vijayan, 2003)

Of course, Microsoft disagreed but several experts claimed this is an ongoing issue. It is true that while installing updates, sometimes systems go down, or the OS may lose power, or something else happens that may stop the update from finishing. This, according to some experts, creates a problem. (Vijayan, 2003)

Alternatives to MS OS and MS Office

"*The clear consensus among experts is that Linux is the most secure operating system. But while it's the OS of choice for servers, enterprises deploying it on the desktop are few and far between.*" (Taylor, 2018)

After all the research and statistics on vulnerabilities, if companies and users are continuing to choose not to upgrade their OS and/or their MS Office products due to price, then there are still free, open sourced alternatives. It could be that MS products were originally sold

with the computers, and it was convenient just to keep using them. It could be that there wasn't a designated IT person to track the upgrades, installs and patches. It could just be that it was easy to ignore it until it becomes a problem. Whatever the reason, there is plenty of advanced notice today, and plenty of widespread cyber security issues publicized so that everyone, especially companies should know that it is necessary to budget for both security, vulnerability scans, and personnel to track updates and flaws. It is both a legal issue and an issue with data security, especially privacy of clients and of users too. Still, there are viable, open sourced alternatives today that also work as listed below.

Other Alternatives to MS Office

When MS was perhaps the main office software available and marketed to businesses, this might be a good choice (the upgrade option). However, it is important to note that Gates originally loaded his software onto IBM personal computers, and they were sold that way – which was a way to get lifelong business and personal customers. There were not many alternatives available at that time, but Word Perfect was one major competitor and a favorite with most law firms. This is perhaps the main reason MS came to own such a large percentage of the market share, and still does, due to its 'convenience' setting already on the equipment. However, nowadays there are many free competitors, especially with the growth of Linux products and their well-known safety record over and above anything MS has to offer.

One great alternative to MS Office is FreeOffice. It is the open sourced option from SoftMaker, and it is totally free. It is also compatible with MS Office, and comes with several programs for: spreadsheets, presentations and also word processing. It is available for: Linux, Windows, Mac, and as of 2021, it even has a programming tool too. (Öteyo, 2021) It even has a version that for $20 can be added to an Android Tablet. There is also a professional upgrade for Free Office for about $40 per year. (Ansaldo, 2018)

OS Alternatives to MS OS

Linux is a viable, free, open sourced alternative to MS OS. It has free software apps available, and LibreOffice is the well-known option for word processing. However, in recent years the quality has gone down. So, FreeOffice would be a very viable alternative. Linux OS has a lot to offer over MS OS, although unless people are into IT, they usually will be totally unaware of the advantages of Linux over MS. Also, in the past as stated above, Gates did his best to talk down about Linux because it was free and open sourced, as do most of his associates.

Still, it is a free choice, with its own security. Today, it even has some GUI (Graphic User Interface) menus versus just knowing Linux commands, which is a plus to appeal to more people. It is so small it can fit on a USB and is easily portable.

Conclusion

MS Windows and MS Office are some of the most popular software products and OS in the world, and many businesses, large and small, as well as consumers rely on them every day. They run on over a billion computers all over the world. But, they are a security risk when the software is either unsupported and/or security patches are no longer available, or are simply not being installed. Hackers know the known vulnerabilities on OS's, and there are many on MS products overall. And, due to the vast numbers of computers and businesses running MS Windows, they are a very tempting target for ransomware and malware. The massive numbers on MS Windows makes them much more tempting than Linux or Apple to hackers.

Since Windows has been running on pcs many years, and has several different products, the vulnerabilities on Windows are massive. Many users are using very outdated software, even businesses. Table 1 shows that "83% of enterprises" use older versions of MS Office. This is risky and could be costly. Companies could claim a tax write off for software updates and subscriptions so this may help make the update more affordable. They could also be held responsible if they were hacked and data was leaked or stolen, if they failed to keep their software updated.

But still another reason for vulnerabilities includes not installing security patches, and not running any sort of vulnerability scanning to verify the gaps in their OS. This put all data at risk, and companies knowingly using outdated software could be held liable for these actions also. It is important in IT security to assess the risk, and take steps to mitigate the risks. This can be done, and there should be procedures in place to ensure it is done. To start with, vulnerability scanning should be done periodically, and there are free tools available. For instance, one free scanning tool is OpenVas. Companies would benefit their IT security to know where the holes are, i.e., doors that are still open and patches not completed or installed. Companies should have a plan in place and schedule security scans, as well as a plan to update their outdated software. They could instead install all the necessary security patches in the meantime however it still would be best to budget the cost of scheduled scans, and upgrade the software too. It could greatly lower the data loss risk and help to avoid future issues too.

Another risk mitigating tool would be to update the software, or to purchase a subscription. MS now has subscriptions available however it would need to be budgeted for. However, there are also other alternatives available. There are some free alternatives to MS Office, like Word Perfect and even FreeOffice. These are comparable software packages, and FreeOffice works on MAC, Linux and MS operating systems. The Linux OS is also free and has compatible, free application software. It is GUI based now too and has LibreOffice. So, if the cost of software is a problem, there are free solutions.

In conclusion, there are many alternatives to MS OS and software, and even some which are free. There are free vulnerability scanners, and there are security patches usually available, but some tracking of those patches is necessary. Some hardening of the OS and of the AD (Active Directory) can be done also. These are basic steps to help prevent vulnerabilities and to lower the risk involved. These are things that can be practiced and budgeted for. But there is also another free OS called Linux, and other free software besides MS Office available too. Mostly, older unsupported software and OS are risky overall so some efforts should be made to enhance security to avoid data loss and problems from it.

References

"How Many Computers Use Microsoft In the World". (2022, Jun. 14). Retrieved Sep. 14, 2022, from Knologist: https://knologist.com/how-many-computers-use-microsoft-in-the-world/

"Windows 10 Solution Page.". (n.d.). Retrieved Nov. 1, 2022, from Calcom software: https://www.calcomsoftware.com/windows-10-solution-page/

Ansaldo, M. (2018, Sep. 24). *"FreeOffice 2018 Review."l*. Retrieved Nov. 20, 2022, from PCWworld: https://www.pcworld.com/article/402582/freeoffice-2018-review.html

Chauhan, S. (2012, Sep. 14). *"Windows Vulnerability Assessment."*. Retrieved Nov. 17, 2022, from Resources - Infosec Institute: https://resources.infosecinstitute.com/topic/windows-vulnerability-assessment/

Henry, J. (2010, Dec.). *"Reducing the Threat of State-to-State Cyber Attack Against Critical Infrastructure through International Norms and Agreements".* Retrieved Sep. 18, 2022, from CISSM - Center for International and Security Studies at Maryland: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://drum.lib.umd.edu/bitstream/handle/1903/15621/reducing_the_threat_of_statetostate_cyber_attack_against_critical_infrastructure__120910.pdf?sequence=1&isAllowed=y

Jungles, P. S. (2012). *"Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft Techniques"*. Retrieved Sep. 18, 2022, from Microsoft: https://www.microsoft.com/en-us/download/details.aspx?id=36036

Kaelin, M. W. (2017, Nov. 7). *"83% of Enterprises Use Microsoft Office But There is Danger Lurking in that Huge Number."*. Retrieved Nov. 16, 2022, from Tech Republic: https://www.techrepublic.com/article/83-of-enterprises-use-microsoft-office-but-there-is-danger-lurking-in-that-huge-number/

Microsoft Windows 10 Vulnerabilities - Security Vulnerabilities in 2022. (n.d.). Retrieved Sep. 14, 2022, from Stackwatch: https://stack.watch/product/microsoft/windows-10/

Öteyo, K. (2021, Nov. 11). *"Instal and Use FreeOffice on Uubuntu Linux."*. Retrieved Nov. 20, 2022, from Computing for Geeks: https://computingforgeeks.com/install-and-use-freeoffice-on-ubuntu-linux/

Pollack, K. (2021, Oct. 26). *"Windows 10 Most Critical Vulnerabilities for 2021"*. Retrieved Sep. 18, 2022, from CalCom: https://www.calcomsoftware.com/windows-10-vulnerability/

Ranger, S. (2019, Jun. 4). *https://"Cybersecurity: One in Three Breaches are Caused by Unpatched Vulnerabilities."*. Retrieved Nov. 17, 2022, from ZDnet: https://www.zdnet.com/article/cybersecurity-one-in-three-breaches-are-caused-by-unpatched-vulnerabilities/

Singh, A. (2020, Jun. 22). *"How to Ensure Your Active Directory is Secure."*. Retrieved Nov. 20, 2022, from Lepide: https://www.lepide.com/blog/how-to-ensure-your-active-directory-is-secure/

Taylor, D. (2018, Feb. 6). *"Why Linux is Better than Windows or Macos for Security."*. Retrieved Nov. 20, 2022, from Computer World: https://www.computerworld.com/article/3252823/why-linux-is-better-than-windows-or-macos-for-security.html

Tunggal, A. T. (2022, May 11). *https://www.up"Top 10 Windows 10 Security Vvulnerabilities and How to Fix Them."*. Retrieved Nov. 5, 2022, from Upguard: https://www.upguard.com/blog/top-10-windows-10-security-vulnerabilities-and-how-to-fix-them

Vijayan, J. (2003, Aug. 14). *"Microsoft Patch Process Called Into Question"*. Retrieved Sep. 18, 2022, from Computer World: https://www.computerworld.com/article/2571606/microsoft-patch-process-called-into-question.html

Winder, D. (2021, Jun. 19). *https://www.forbes.com/sites/daveywinder/2021"New Windows 10 Security Shock as 1000 Vulnerabilities Revealed."*. Retrieved Nov. 3, 2022, from Forbes: https://www.forbes.com/sites/daveywinder/2021/06/19/new-windows-10-security-shock-as-1000-vulnerabilities-revealed/?sh=7eb90da436b9

Woollacott, E. (2018, Sep. 18). *"Windows of Opportunity Microsoft OS Remains the Most Lucrative Target for Hackers."*. Retrieved Nov. 16, 2022, from Port Swigger: https://portswigger.net/daily-swig/windows-of-opportunity-microsoft-os-remains-the-most-lucrative-target-for-hackers