"YOSH TADQIQOTCHI"
ilmiy elektron jurnali

Vebsayt: http://2ndsun.uz/index.php/yt

WINDOWS SECURITY IN THE WORLD OF SPREAD VULNERABILITIES

Giyosiddin Abdumalikov

Student at Asia Pacific University of Technology & Innovation

INFO:

Qabul qilindi: 31.01.2022
Ko'rib chiqildi: 02.02.2022
Chop etildi: 02.02.2022

Keywords: Windows security; Vulnerability; Threat; Windows Defender; CIA; Virus

ABSTRACT

Windows operating system (afterward OS) is prevalently utilized by a vast number of users across the globe, however, not everyone takes of the security features of the system when they are using it. This leads to being compromised of personal or confidential data if proper security actions are not implemented, thus being able to face loss of money and property will occur in no time. This paper will discuss some of the popular threats, attacks to the Windows 10 machines, and superior countermeasures will be also provided against them.

Introduction

Technology has dramatically advanced with high velocity, and admittedly, there is not almost any field that it has entered across the world. It would be quite fair to discuss computer security first before talking about the main topic which is a Windows operating system. Computer security is defined as the level of security provided to a system of information in order to meet the appropriate goals of maintaining the integrity, availability, and confidentiality of system pieces (they can contain hardware and data including software, firmware) (Stallings, Brown, Bauer & Howard, 2012). Here are the objectives of computer security: confidentiality, integrity, and availability.

Confidentiality

The basic security purpose of confidentiality is to secure information by ensuring that only those who are authorized to use it can do so, while everyone else is barred. Organizational plans and tactics, for example, must be kept secret, with only those allowed to see them permitted to do so. If other people who aren't intended to be looking at this information find out about it, the material's secret is threatened. Every purpose of the organization is jeopardized when data is collected unlawfully. Confidentiality guarantees that information is secured throughout all phases of its lifecycle:

- Who has access to private information? (Authorization)
- What is done with the sensitive information (Processing)
- How private data is stored on computers (Storage)
- How sensitive information is sent around (Transmission)

By taking better control over these actions with sensitive data, the likelihood of the data being leaked to persons who are not allowed to access the data is limited. (Singh, 2022)

Integrity

The fundamentals of preserving integrity are the dependability and accuracy of systems and data. Because the information is no longer accurate and thus no longer reliable, the value of information and the systems that use it is diminished.

The integrity of information could be brought into doubt in several ways, including the following:

- human error
- data corruption
- malicious activities

To guarantee the integrity of the information and systems involved, these actions that potentially compromise their integrity must be limited (Singh, 2022).

Availability

If the people and systems who need information do not have access to it, it is useless. The availability of information can be compromised if (Singh, 2022):

- Access to information is no longer possible.
- The levels of information accessibility change
- Data is not protected from disruption.

The abovementioned objectives not only belong to computer security but also apply to operating system security. It indicates the tactics or procedures utilized to provide splendid protection to the operating system from different threats such as viruses or malware, remote hacker attacks with the purpose of intrusion, and worms. Operating system security refers to any preventative-control mechanisms that safeguard any system assets that might be stolen, changed, or destroyed if OS security is broken ("Operating System Security - javatpoint", 2022).

Now it is time to talk about a Windows OS or operating system developed by Microsoft Inc. It is system software that oversees, manages, and organizes all elements of the desktop display. In a computer system, hardware and software need a bridge in terms of communication and here OS comes in handy.

It is in charge of assigning memory addresses to data and different applications. During data processing processes, OS controls a variety of computer-related items or information assets such as files and programs, input/output devices, and computer memory. Defects and mistakes of hardware and software are inspected with the aid of OS. (Ogunbanwo, Lateef & G.O., 2016).

According to the Statcounter website, the most used operating system is Windows with 77.93%. (Figure 1) (Dunkerley & Tumbarello, 2020)

Figure 1. The market share of Operating Systems around the World

It is better to have a look at the current adoption of the various Windows operating systems. The following Statcounter screenshot depicts the usage of the current desktop version of Windows across the world today. (Figure 2) (Dunkerley & Tumbarello, 2020)

Figure 2. The market share of Windows versions

Since Windows 10 is currently a dominant operating system across the globe even though Windows 11 is released, however, it is not utilized widely yet. Therefore, it would be reasonable to discuss Windows 10 security in-depth, including its features, potential attacks, vulnerabilities, and better practices to establish superior security. Windows 10 was launched on 29th July 2015, to replace Windows 8. There is no doubt that it was the most secure version of Windows, however, Windows 11 is overweight. Windows 10 is the company's most powerful operating system that can be virus-resistant to date. When compared to prior editions of Windows, Microsoft has introduced a number of protection methods in Windows 10 to protect the Confidentiality, Integrity, and Availability of the system.

(Ramasamy & Kumar Baskaran, 2019)

Vulnerabilities of Windows

Admittedly, there are a substantial number of vulnerabilities for all versions of Windows, nevertheless, several top Windows 10 vulnerabilities are going to be discussed below owing to their popularity.

1. Win32k Elevation of Privilege Vulnerability

Through privilege escalation, a threat actor can take entire control of a Windows PC by exploiting a hole in the scrollbar part which is a Windows 10 GUI component (Tunggal, 2021).

2. Microsoft Font Driver Vulnerability

There is a remote code execution vulnerability in OpenType fonts which is handled by Windows Adobe Type Manager. As a result, attackers are able to install applications or programs, see/alter/remove information, and add new users with complete control of the system. (Tunggal, 2021)

3. .NET Framework Escalation of Privilege Vulnerability

Custom-crafted.NET applications may cause privilege escalation exploit and users are required by attackers with deception in order to run some apps first (Tunggal, 2021).

4. Re-Direct to SMB Vulnerability

All versions of Windows are infected with this vulnerability, not excluding Windows 10, and it pays close attention to a core Windows API library and communication between Windows and SMB. Malicious SMB-based servers come in handy here to be visited by users in terms of redirection, and their login details might be stolen. (Tunggal, 2021)

5. Microsoft Windows Journal Vulnerability

Once a specifically created Journal file is opened by the user, it is highly likely to allow RCE which remote code execution. Those who have fewer user privileges are not likely to be infected compared to those who have administrative rights (Tunggal, 2021).

6. Internet Explorer Vulnerabilities

One of the well-criticized web browsers, namely Internet Explorer has a myriad number of vulnerabilities. The most serious of these flaws could allow remote code execution if a user views a specially crafted webpage in Internet Explorer (Tunggal, 2021).

7. Microsoft Graphics Component Vulnerabilities

If a user opens an especially designed document or navigates to an untrusted webpage that contains embedded TrueType or OpenType fonts, a vulnerability could allow remote code execution. (Tunggal, 2021)

8. Microsoft Edge Vulnerabilities

Internet Explorer that is the old-used web browser prior to Edge was not considered as the most secure, in addition, Edge could not be secure too. Specially crafted web pages using Microsoft edge by users lead to RCE and security feature bypass exploits (Tunggal, 2021).

9. Windows 10 Mount Manager Vulnerability

By inserting a USB device into the target system, this vulnerability allows for the possible privilege escalation. This method is utilized to write a malicious binary to disk and execute the code by an attacker. (Tunggal, 2021)

Threats to Windows

As Windows 10 is one of the most widely used OS across the globe, it is considered to be one of the most wanted targets for hackers. The vast majority of attacks are conducted over the Internet with the sole purpose of personal gain by cyber thieves. The following sections discuss several of the most common forms of threats on Windows 10 (Ramasamy & Kumar Baskaran, 2019).

Malware - Malware is a general phrase that indicates potentially harmful or untrusted software and applications. It generally damages the system and disrupts the regular operation of computing equipment. By infecting a computer with malware, cybercriminals can gain illegal access to and use of system resources, steal passwords, shut down a computer, demand a ransom, and do a variety of other things. Personal data is stolen to sell or use as leverage on victims by them since they are most of the time motivated by financial gain. Here some common malware attacks such as Rootkits, Phishing, and Ransomware will be discussed (Ramasamy & Kumar Baskaran, 2019).

- Rootkits - Rootkits are viewed as a sophisticated and hazardous sort of malware that operates in kernel mode with the privileges of the OS. Rootkits have the ability to remain undetected in a system for as long as possible. After a rootkit infection, the data that a computer informs about itself cannot be believed. The four types of rootkits are listed below.
- Firmware Rootkits: These rootkits replace the PC's firmware, allowing them to run before Windows.
- Bootkits: A more sophisticated sort of rootkit that combines rootkit functionality with the aim to damage the Master Boot Record (MBR). Bootkits are intended to load from the master boot record and remain active during the operation of the system.
- Rootkits in Kernels: By getting access to the kernel, an attacker has total control of the OS. These rootkits replace a portion of the OS kernel, allowing them to operate when the machine powers up.
- Driver Rootkits: Since the vast majority of drivers work in kernel mode, they have a right to access all crucial kernel files and can impersonate one of Windows' trusted drivers for connecting with the computer's hardware.
- Phishing – An attacker that is executing a phishing attack aims to collect personal data through emails, websites, text messages, or other types of contact that frequently seem to be from genuine organizations or persons. An attacker then utilizes the stolen data to undertake operations such as hacking, stealing the identity and money from the bank accounts, and many more. Some of the most common phishing techniques are listed here. (Ramasamy & Kumar Baskaran, 2019).

• Invoice Phishing: A hacker mails to victims saying that they have an overdue invoice from a well-known vendor or firm, with a link to check and pay the invoice.

• Payment/ Delivery Scam: Users must give a credit card number or other personal data in order for their credit card details to be updated with a well-known third-party- party vendor.

• Tax Phishing: One of the most prevalent IRS phishing emails is receiving an important email message indicating that someone sends money to the IRS.

• Downloads: Other frequent phishing deception includes an intruder sending a false email requesting the target to view or download a file, generally one that needs users to sign in.

- Ransomware – Ransomware is a form of software that encrypts files and directories, making crucial files unavailable. Its purpose is to extort money from victims in order to return the decryption key, and bitcoin is the preferable form of payment. The majority of ransomware attacks start with email attachments containing malware, or with websites that try to install ransomware by exploiting flaws in browsers and other software. When a device is infected with ransomware, the data on it is immediately encrypted using encryption techniques such as RSA or RC4. Spora, WannaCry, and Petya are examples of well-known ransomware (Ramasamy & Kumar Baskaran, 2019).

There are numerous sorts of malware such as worm, virus, adware, spyware, rootkit, backdoor, zero-day attack, trojan horse ransomware, and among other examples (Wiley, 2017). It is not wise here to give a perfect explanation for each and every one of them since several ones have been fabulously discussed. However, it would be sufficiently fair to talk little about the symptoms of malware:

- Poor system performance and it happens again when it is connected to the Internet
- Less available memory than usual
- Browser closes or stops responding and has unknown add-ins
- Computer stops responding and takes longer to start up
- File size suddenly changes and corrupted
- Unknown programs are installed
- Components of Windows no longer work, and programs cannot start (Wiley, 2017)

Countermeasures Against Cyber-Attacks

Countermeasures given by Windows 10 to avoid the above-mentioned cyber dangers are described below.

The CIA

When addressing Windows 10 security, it is vital to gather security requirements in order to protect confidentiality, integrity, and availability of the system, as well as to assure that the OS is sufficiently secure and reliable. Additionally, the most valuable assets of the system are protected with the aid of security requirements to help Microsoft. The following security properties must be met for the CIA of the system to be maintained:

- Support for Cryptography – Windows cryptographic features allow encryption and decryption including cryptographic signatures and hashing as well as public keys, credential management, and certificate validation are supported. Windows gives help cryptographic functions to applications that are in both user-mode and kernel-mode. To be able to authenticate individuals including systems and protect their data of them in transit, Windows creates and uses public-key certificates.

- Data Protection for Users – Windows 10 contains several tools that aid to protect consumer details from externally or internally unauthorized accessibility, also to avoid them having access to the data of each other. In addition, it supports VPN (a virtual private network) and other security measures to keep user data safe.
- Authentication and identification — Each Windows user must be recognized and approved in accordance with administrator-defined regulations. Windows stores user IDs, authentication details, group memberships, privilege relationships, and login permissions in account databases.
- Trusted Path for Communication – Windows 10 uses HTTPS, DTLS, and TLS to create a secure communication channel. (Ramasamy & Kumar Baskaran, 2019).

1) UEFI Secure Boot: Prior to starting the OS, the integrity of every part of the startup process is checked by it and solely reliable OS bootloaders are able to be loaded on the computer with UEFI firmware and Trusted Platform Module.

2) Microsoft Exchange Online Protection: Different layers of filtering are utilized, and various controls are provided in terms of spam filtering for bulk mail or international spam. The emails, online storage, and files are protected against malware with the aid of it.

3) Controlled Folder Access: Ransomware is avoided from encrypting files and preserving them for money by limiting file and folder access.

4) Awareness

5) Install the most recent operating system updates (Ramasamy & Kumar Baskaran, 2019).

Additionally, while having a great number of countermeasures there, the most indispensable security setting is Windows update. It helps Windows 10 users to maintain their PCs up to date by examining a specific server. The software that resolves security holes, updates that make Windows and apps much more stable is installed by the server while solving problems with current Windows applications and provides novel features. Microsoft can host the server, or it can be set up and administered in-house using WSUS (Windows Server Update Services) (Wiley, 2017).

Moreover, the employment of a newly updated antivirus software application is the second stage in securing a computer from infection. It is also strongly suggested to install an antispyware software suite if the antivirus program does not contain an antispyware element. To find and remove malicious software, performing a comprehensive system scanning with an antivirus tool every week and a quick scan when the symptoms begin to show is crucial (Wiley, 2017).

Microsoft's Windows Defender is a piece of software in Microsoft Windows ensuring that spyware is avoided, eliminated, and quarantined by it. By identifying and uninstalling malicious programs from a system, it will serve to protect the system from notifications, poor performance, and security risks that are posed by unknown applications. There is a monitoring system which is called real-time protection that proposes anti-spyware measures once the adware is identified minimizes disruptions and helps users stay productive are all elements of Windows Defender. Windows Defender, like an antivirus program, must be kept up to date (Wiley, 2017).

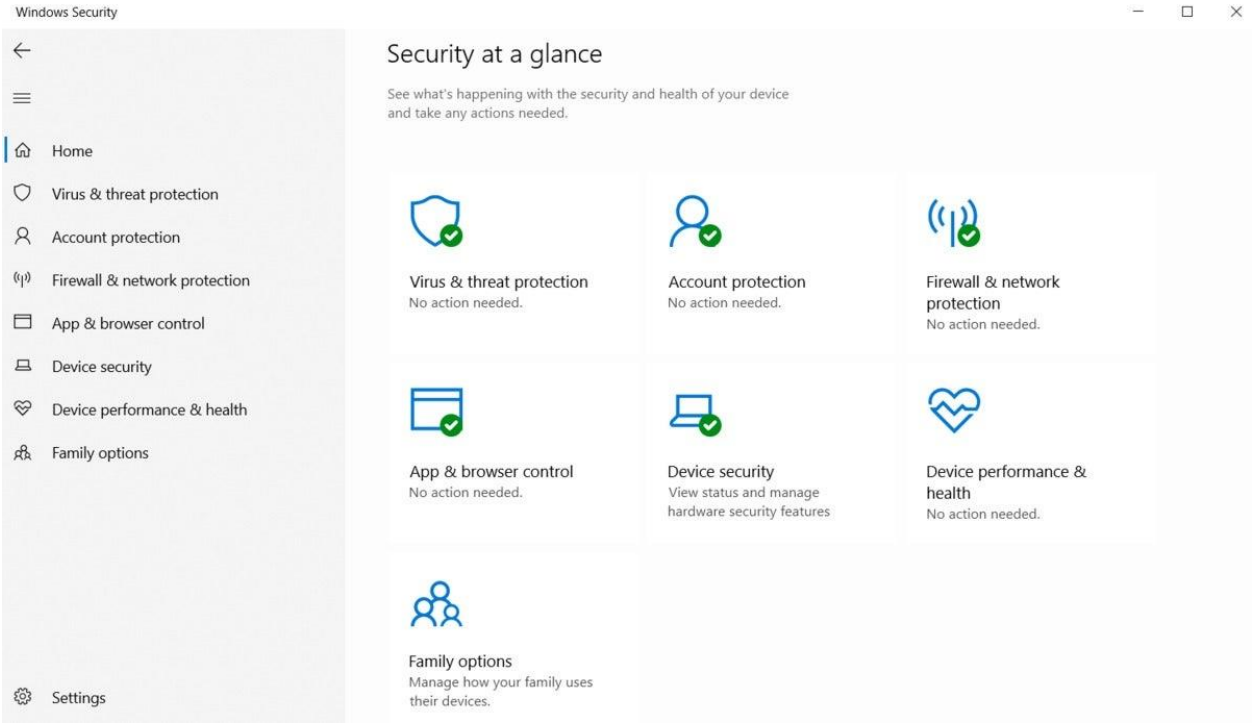

Figure 3. Windows Security ("Stay protected with Windows Security", 2022)

Windows security interface and features

It is clear that there are several sections in Windows security, and it would be better to give some tiny definitions for them.

- Virus & threat protection – To assist to identify the newest threats while observing the device. Scans are run and updates are provided with this section.
- Account protection – There are some options related to sign-in and account settings. They may contain various options like Windows Hello, Pin, Password.
- Firewall & network protection – Networks and Internet connections are monitored by managing firewall settings in order to see the current status.
- App & browser control – There is reputation-based protection along with exploit protection in this section. The former is responsible for the protection of the system in terms of dangerous downloads, websites including programs, and files while the latter is in charge of protection against attacks.
- Device security – To protect the device from unwanted malware attacks by examining inbuilt security features
- Device performance & health – To ensure the system is up-to-date with the latest of the version of Windows along with maintaining it clean with the aid of the status details on performance health of the device.
- Family options – To observe children's internet behavior as well as the devices in the home ("Stay protected with Windows Security", 2022).

The following status symbols represent the level of safety:

Green indicates that there are no recommended actions at this time.

Yellow indicates that safety recommendation is available for the device.

Red indicates that something urgently needs to be addressed.

Windows Security access

To be able to access the windows security, here are the following steps:

- Start > Settings > Update & Security > Windows Security ("Stay protected with Windows Security", 2022)

Conclusion

Overall, it can be quite fair to emphasize the importance of Windows security since the majority of companies, organizations, authorities, universities, and among other examples massively utilize especially Windows operating systems at the workplace. This indicates that the threats to those systems are highly likely to be huge in number, and if proper countermeasures are not implemented in the environment, malicious attackers will obviously take advantage of them. As a result, a considerable amount of money and data will be lost due to the breach. Hence, considering these aspects of the issue, several precautions have been demonstrated against well-known attacks.

References

1. Stallings, W., Brown, L., Bauer, M., & Howard, M. (2012). *Computer security*. Upper Saddle River: Prentice-Hall.
2. Singh, J. (2022). Retrieved 24 January 2022, from https://cybersecuritykings.com/2020/06/14/what-is-cia-in-cyber-security-essential-info/
3. Operating System Security - javatpoint. (2022). Retrieved 24 January 2022, from https://www.javatpoint.com/operating-system-security
4. Ogunbanwo, A., Lateef, U., & G.O., O. (2016). *MICROSOFT WINDOWS OPERATING SYSTEM* [Ebook] (2nd ed., p. 2). Ogun State: College of Science and Information Technology, Tai Solarin University of Education, Ogun State, Nigeria. Retrieved from https://www.researchgate.net/publication/317182647_MICROSOFT_WINDOWS_OPERATING_SYSTEM
5. Tunggal, A., 2021. *How to Fix the Top 10 Windows 10 Vulnerabilities [Infographic] | UpGuard*. [online] Upguard.com. Available at: <https://www.upguard.com/blog/top-10-windows-10-security-vulnerabilities-and-how-to-fix-them#toc-1> [Accessed 26 January 2022].
6. Dunkerley, M., & Tumbarello, M. (2020). *Mastering Windows Security and Hardening* (pp. 24,25). [S.l.]: Packt Publishing.
7. Ramasamy, K., & Kumar Baskaran, V. (2019). *Security in Windows 10* [Ebook] (p. 2). Ottawa, Canada: Carleton University. Retrieved from https://www.researchgate.net/publication/342484974
8. Wiley, J. (2017). *Microsoft Official Academic Course - Security Fundamentals* (2nd ed., pp. 145,146,147). Hoboken, NJ: Microsoft.
9. Stay protected with Windows Security. (2022). Retrieved 24 January 2022, from https://support.microsoft.com/en-us/windows/stay-protected-with-windows-security-2ae0363d-0ada-c064-8b56-6a39afb6a963