IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, August 2024

A Study on the Key Applications of Malware

Dr Srinivasa Rao Kadari[1], Dr. G. Radhika[2], M. Shekar[3], R V V S Ravi Shankar[4], Ch. Madhu[5]
Babu Jagjivan Ram Government Degree College, Narayanaguda, Hyderabad, India[1,3,4,5]
Government Degree College, Khairatabad, Hyderabad, India[2]

Abstract: *Malware, a portmanteau of "malicious software," represents a significant threat in today's interconnected digital landscape. This abstract explores the multifaceted impacts of malware applications on individuals, organizations, and society at large. Types of malware include computer viruses, worms, Trojan horses, ransomware and spyware. These malicious programs steal, encrypt and delete sensitive data; alter or hijack core computing functions; and monitor end users' computer activity. malware jeopardizes individual privacy and security by surreptitiously infiltrating personal devices, often leading to identity theft, financial loss, and unauthorized access to sensitive information. Beyond personal repercussions, malware poses substantial risks to organizational integrity. It can compromise corporate networks, disrupt operations, and inflict substantial financial losses through data breaches, ransomware attacks, and intellectual property theft.*

Keywords: computer viruses, worms, Trojan horses, ransom ware , privacy, security and spyware

I. INTRODUCTION

The malware: As software designed to interfere with a computer's normal functioning, malware is a blanket term for viruses, trojans, and other destructive computer programs threat actors use to infect systems and networks in order to gain access to sensitive information .Malware, or malicious software, is any program or file that's intentionally harmful to a computer, network or server.

Malware Definition

Malware (short for “malicious software”) is a file or code, typically delivered over a network, that infects, explores, steals or conducts virtually any behavior an attacker wants. And because malware comes in so many variants, there are numerous methods to infect computer systems. Though varied in type and capabilities, malware usually has one of the following objectives:

- Provide remote control for an attacker to use an infected machine.
- Send spam from the infected machine to unsuspecting targets.
- Investigate the infected user’s local network.
- Steal sensitive data.

Malware analysis:

Malware analysis is one of the key processes in cyber security. Security analysts are regularly asked to analyze a suspicious file to check whether it is legitimate or malicious. It is important for responders because it helps them reduce false positives and understand how extensive a malware incident is.

Malware analysis is useful both for pre-incident and post-incident activity. During an incident, malware analysis gives you actionable information by identifying and classifying the malware. By documenting and identifying the malware via malware analysis, you gain a wealth of information that helps prevent future incidents.

After the incident, the information you gained from malware analysis forms part of the lessons learned. Analysts learn about patterns, methods of attack, and behavior from the newly analyzed malware that helps them devise prevention methods for other similar incidents.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, August 2024

The malware work:

A malware may explore several vulnerabilities that allow it to enter your computing environment, stay concealed, and continue to cause damage without any visible indication. For example, there might be software available which claims to do something harmless – like help to download Youtube videos. But once you install it, it sits inside your system, waiting to trigger an attack on a specific date or time.

Malware often works like a contagious infection. Once there's one harmful software installed, it opens up gateways or "backdoors" that allow other malicious software to enter your system without the requisite authentications.

Once it is installed, the malware might do one of the following:

- Try to capture personal information like financial details, credentials for online banking, etc.
- Target a corporate user to get information linked to work – this might get a malware designer/distributor access to large pools of customer data and other sensitive information.
- Simply sit in the background and slow down a system – such apps are considered as "grayware" as they pose a less severe threat than regular malware.
- Push unwanted ads to the user, earning revenues through malicious means.
- Hand over full control of your systems to a remote operator.

One of the recent malware trends is the rise of ransomware, where a remote operator blocks access to specific system functionalities until the user pays a certain amount. Let's discuss ransomware and other types of malware in detail.

Malware removal for Windows PCs

Windows is among the top operating environments hit by malware for two reasons. First, because a majority of PCs around the world use Windows, it is a convenient target for threat actors. Second, because Windows doesn't come with the same, stringent security protocol as Mac. If you've noticed a Windows system performing unusually, follow these steps to detect and remove malware:

Create a checklist of possible malware indicators

Watch out for malware indicators like:

1. A slow boot-up process
2. Unexpected pop-ups
3. Difficulty in accessing a frequently retrieved website
4. A new app on the staff menu that you don't remember downloading
5. Shrinking hard disk space without proper justification
6. Compromised hardware behavior like low-quality sound or display

A checklist like this will help you regularize malware removal and not leave it until the very last moment.

Start the PC in safe mode

Most types of malware enter, spread, and act via the internet. In safe mode, all the apps that would automatically initiate at bootup are terminated. This lets you assess genuine Windows speed and the number of apps you might be dealing with.

Also, safe mode without networking prevents the system from accessing the internet, rendering the malware powerless as you explore removal routes. There are several ways to enter the safe mode – you could either troubleshoot from settings, restart to safe mode from the sign-in screen, or switch to safe mode if you face a blank/black screen.

Optimize disk space before running a malware scan

This step ensures that your system has the maximum amount of resources as it hunts for malware. Search for the Disk Cleanup utility on Windows from the search bar on the bottom of your desktop. You can clear temporary files that are taking up disk space from this utility.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, August 2024

Scan your system for malware

There are two ways to do this. You can use a third-party provided antivirus or cyber security solution to analyze your system for traces of malware. Alternatively, you can use Windows' built-in utility called virus and threat protection. Typically, it runs in the background, checking for different types of malware at regular intervals – but you can also choose the Quick Scan option for an on-demand check.

Decide on your malware removal action

Once the scan reveals malware, you have three options: do nothing, send it to quarantine, or delete the file altogether. The decision will depend on the nature of the file, and the severity of the attack. For instance, a pure virus attack can be tackled only via deletion, as the host is already infected. But for other types of malware like adware, you might want to keep it in quarantine.

Malware harmful actions:

- **Data exfiltration**. Data exfiltration is a common objective of malware. During data exfiltration, once a system is infected with malware, threat actors can steal sensitive information stored on the system, such as emails, passwords, intellectual property, financial information and login credentials. Data exfiltration can result in monetary or reputational damage to individuals and organizations.
- **Service disruption**. Malware can disrupt services in several ways. For example, it can lock up computers and make them unusable or hold them hostage for financial gain by performing a ransomware attack. Malware can also target critical infrastructure, such as power grids, healthcare facilities or transportation systems to cause service disruptions.
- **Data espionage**. A type of malware known as spyware performs data espionage by spying on users. Typically, hackers use key loggers to record keystrokes, access web cameras and microphones and capture screenshots.
- **Identity theft.** Malware can be used to steal personal data which can be used to impersonate victims, commit fraud or gain access to additional resources. According to the IBM X-Force Threat Intelligence Index 2024, there was a 71% rise in cyberattacks using stolen identities in 2023 compared to the previous year.
- **Stealing resources**. Malware can use stolen system resources to send spam emails, operate botnets and run cryptomining software, also known as *cryptojacking*.
- **System damage**. Certain types of malware, such as computer worms, can damage devices by corrupting the system files, deleting data or changing system settings. This damage can lead to an unstable or unusable system.

Types of Malware:

Types of malware include computer viruses, worms, Trojan horses, ransomware and spyware. These malicious programs steal, encrypt and delete sensitive data; alter or hijack core computing functions; and monitor end users' computer activity.

- **Viruses** – A Virus is a malicious executable code attached to another executable file. The virus spreads when an infected file is passed from system to system. Viruses can be harmless or they can modify or delete data. Opening a file can trigger a virus. Once a program virus is active, it will infect other programs on the computer.
- **Worms** – Worms replicate themselves on the system, attaching themselves to different files and looking for pathways between computers, such as computer network that shares common file storage areas. Worms usually slow down networks. A virus needs a host program to run but worms can run by themselves. After a worm affects a host, it is able to spread very quickly over the network.
- **Trojan horse** – A Trojan horse is malware that carries out malicious operations under the appearance of a desired operation such as playing an online game. A Trojan horse varies from a virus because the Trojan binds itself to non-executable files, such as image files, and audio files.
- **Adware** – It displays unwanted ads and pop-ups on the computer. It comes along with software downloads and packages. It generates revenue for the software distributer by displaying ads.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, August 2024

- **Ransom ware** – Ransom ware grasps a computer system or the data it contains until the victim makes a payment. Ransom ware encrypts data in the computer with a key that is unknown to the user. The user has to pay a ransom (price) to the criminals to retrieve data. Once the amount is paid the victim can resume using his/her system
- **Spyware** – Its purpose is to steal private information from a computer system for a third party. Spyware collects information and sends it to the hacker.
- **Logic Bombs –** A logic bomb is a malicious program that uses a trigger to activate the malicious code. The logic bomb remains non-functioning until that trigger event happens. Once triggered, a logic bomb implements a malicious code that causes harm to a computer. Cyber security specialists recently discovered logic bombs that attack and destroy the hardware components in a workstation or server including the cooling fans, hard drives, and power supplies. The logic bomb overdrives these devices until they overheat or fail.
- **Root kits –** A root kit modifies the OS to make a backdoor. Attackers then use the backdoor to access the computer distantly. Most root kits take advantage of software vulnerabilities to modify system files.
- **Backdoors –** A backdoor bypasses the usual authentication used to access a system. The purpose of the backdoor is to grant cyber criminals future access to the system even if the organization fixes the original vulnerability used to attack the system.
- **Key loggers** – Key logger records everything the user types on his/her computer system to obtain passwords and other sensitive information and send them to the source of the key logging program.

Types of Malware Attacks

Malware attacks are any type of malicious software designed to cause harm or damage to a computer, server, client or computer network and/or infrastructure without end-user knowledge.

Cyber attackers create, use and sell malware for many different reasons, but it is most frequently used to steal personal, financial or business information. While their motivations vary, cyber attackers nearly always focus their tactics, techniques and procedures (TTPs) on gaining access to privileged credentials and accounts to carry out their mission.

Malware also uses a variety of methods to spread itself to other computer systems beyond an initial attack vector. Malware attack definitions can include:

Email attachments containing malicious code can be opened, and therefore executed by unsuspecting users. If those emails are forwarded, the malware can spread even deeper into an organization, further compromising a network.

File servers, such as those based on common Internet file system (SMB/CIFS) and network file system (NFS), can enable malware to spread quickly as users access and download infected files.

File-sharing software can allow malware to replicate itself onto removable media and then on to computer systems and networks.

Peer to peer (P2P) file sharing can introduce malware by sharing files as seemingly harmless as music or pictures.

Remotely exploitable vulnerabilities can enable a hacker to access systems regardless of geographic location with little or no need for involvement by a computer user.

Recent some Examples of Malware Attacks:

Here are just a few of the many types of malware cyber attackers use to target sensitive data:

- **Pony malware** is the most commonly used malware for stealing passwords and credentials. It is sometimes referred to as Pony Stealer, Pony Loader or FareIT. Pony malware targets Windows machines and collects information about the system and the users connected to it. It can be used to download other malware or to steal credentials and send them to the command and control server.
- **Loki, or Loki-Bot,** is an information-stealing malware that targets credentials and passwords across approximately 80 programs, including all known browsers, email clients, remote control programs and file sharing programs. It has been used by cyber attackers since 2016 and continues to be a popular method for stealing credentials and accessing personal data.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, August 2024

- **Krypton Stealer** first appeared in early 2019 and is sold on foreign forums as malware-as-a-service (MaaS) for just $100 in crypto currency. It targets Windows machines running version 7 and above and steals credentials without the need for admin permissions. The malware also targets credit card numbers and other sensitive data stored in browsers, such as browsing history, auto-completion, download lists, cookies and search history.
- **Triton malware** crippled operations at a critical infrastructure facility in the Middle East in 2017 in one of the first recorded malware attacks of its kind. The malware is named after the system it targets – Triconex safety instrumented system (SIS) controllers. These systems are used to shut down operations in nuclear facilities, oil and gas plants in the event of a problem, such as equipment failure, explosions or fire. The Triton malware is designed to disable these failsafe mechanisms, which could lead to physical attacks on critical infrastructure .

II. CONCLUSION

The impact of malware applications transcends mere technical disruptions, influencing economic, social, and political realms. Understanding these multifaceted impacts is essential for devising proactive strategies to safeguard digital ecosystems and mitigate the far-reaching threats posed by malware in today's interconnected world. By adopting a collaborative and proactive approach, stakeholders can collectively strive towards a more secure and resilient digital future. Malware attacks are any type of malicious software designed to cause harm or damage to a computer, server, client or computer network and/or infrastructure without end-user knowledge.

REFERENCES

[1]. https://www.geeksforgeeks.org/malware-and-its-types.
[2]. https://www.techtarget.com/searchsecurity/definition/malware
[3]. https://www.paloaltonetworks.com/cyberpedia/what-is-malware
[4]. https://www.cyberark.com/what-is/malware/
[5]. ENISA Threat landscape for ransomware attacks, July 2022, [online access: 24.08.2022], https://www.enisa.europa.eu/publications/enisa-threat-landscape- for-ransomware-attacks
[6]. Fahmy M., Sharshar A., Magdy S., Maglaque R., Analyzing ProxyShell-related Incidents via Trend Micro Managed XDR, Trend Micro, November 2021, [online access: 31.10.2022], https://www.trendmicro.com/pl_pl/research/21/k/analyzing-proxyshell-related- incidents-via-trend-micro managed-x.html
[7]. Giandomenico A., IoT botnets reach new threshold in Q2 of 2019, TechTarget, August 2019, [online access:30.08.2022]..
[8]. https://intezer.com/blog/malware-analysis/the-role-of-malware-analysis-in-cybersecurity/.
[9]. https://www.spiceworks.com/it-security/endpoint-security/articles/what-is-malware-types-removal/
[10]. 10.https://www.techtarget.com/searchsecurity/definition/malware
[11]. https://perception-point.io/guides/malware/malware-detection-7-methods-and-security-solutions-that-use-them/
[12]. https://www.sciencedirect.com/topics/engineering/malware
[13]. A. V. Aho and M. J. Corasick. Efficient string matching: An aid to bibliographic search. Communications of the ACM, 18(6):333–340, June 1975.
[14]. I. Arce and E. Levy. An analysis of the Slapper worm. IEEE Security and Privacy Magazine, Jan.-Feb. 2003.
[15]. Paul Barford and Vinod Yegneswaran. An inside look at botnets. In Mihai Christodorescu, Somesh Jha, Douglas Maughan, Dawn Song, and Cliff Wang, editors, Malware Detection, volume 27 of Advances in Information Security, chapter 8. Springer, 2007.
[16]. David Brumley, Cody Hartwig, Zhenkai Liang, James Newsome, Dawn Song, and Heng Yin. Automatically identifying trigger-based behaviour in malware. In Wenke Lee, Cliff Wang, and David Dagon, editors, Botnet Detection, volume 36 of Advances in Information Security, pages 65–88. Springer, 2008.
[17]. H. Choi and H. Lee. Identifying botnets by capturing group activities in DNS traffic. Journal of Computer Networks, 56:20–33, 2011.