Malware Protection Using Traditional Security Tools

R. ARJUNARAO[1], KURRA HARSHA KEERTHI[2]
[1] *Associate Professor, Aurora's Degree & PG College*
[2] *IGNOU*

Abstract— In today's digital world everyone is becoming (or) part of it. Digital technology has become integral part of everyone's life and is being used from day to day works such as purchase of daily needs, bill payments, etc. to complex tasks/works such as handling air traffic control. While using the technology one of the primary concerns to all is privacy, availability, security of the information stored/transmitted by using the digital technology/device. Denial of access to the information, interruption in the process while accessing any data or device/system when required by the authorised user is one of the main issues in this digital world. In digital world this type of cybercrimes can be carried out from any part of the world which is contrary to conventional crimes. Malware is one of the main threats to any individual device or organisation systems. It will have a great impact on the CIA of the information security i.e., Confidentiality, Integrity and availability as malwares compromise them. End point/user of any process is very important because maximum crimes can be avoided if the end point/end user of the process/device is cautious and this is the main concern in this project/research. This project/research is about, to know what is malware, steps to be taken by individual/organisation for mitigation, prevention and control of malware attacks. This is carried out by studying the traditional tools/methods available for End point security of any system.

Indexed Terms— Malware, detection, networks, security, ransome, infected,encryption

I. INTRODUCTION

Malware is unauthorised/malicious programmes which are prepared by programmer to harm / damaged / corrupts / deletes/ restricts access of an authorised programme/user of computers/mobile devices/PDA/electronic devices (Or) for unauthorised access to a device/data. Both personal and organisational devices can be affected by malware. It will have a great impact on the CIA of the information security i.e., Confidentiality, Integrity and availability as these programmes are compromising them.

Types of Malwares:

- VIRUS (Vital Information Resource Under Siege),
- Worms
- Trojan Horses
- Ransom ware
- Spy ware
- Ad ware
- Rouge software
- Scare ware
- Wiper
- Rootkits
- Backdoors
- Botnets

VIRUS: These are the programmes which siege the authorised access to a programme or data to an authorised user. These programmes can also replicate themselves and infect other programmes of the devices/ on networks and cause damage to the networks.

Worms: Worms are the programmes which replicate themselves and cause damage to the programmes and networks of the systems. The only difference between a virus and worm is, virus has to be executed /run by the user for the first time whereas worm doesn't need execution/run initially.

Trojan Horses: It is a programme which intent to appear to do a specific task/to be an authorised programme but the programme performs another task in the background which is not intended by the user/programmer.

Ransom ware: These are programmes which are used by hackers/cybercriminals to prevent authorised access of data/programme to the authorised user/programmer by using various programmes or encryption and demand ransom money for providing access/decryption of the data/programme.

Spyware: Spyware is a programme which is used by a user/entity/organisation to gather/collects data/information of any person/user/entity/organisation without their knowledge. It appears to be a legitimate programme but it transfers data without permission which is unauthorised.

Ad ware: Adware is a programme used for advertisement. These programmes are developed for income generation by the developers and used by the business entity for advertisement purpose and capturing the data of the user for studying the purchase patterns/interests of the user/customer and prepare user/customer profile and for the purpose of target advertisement.

Rouge ware: This is method in which a message displays on the screen such as "Your computer/pc/device is infected by malware. To Check and remove the malware Click Here". It is method to misguide the user that the device is infected by virus, insists the user to pay for a tool to remove the virus from the device and install a software/programme which is a malware on the user device and collect data/information of the device/user from the device.

Scare ware: It is a social engineering method in which the device user gets manipulated by the anti-virus sellers/ a group programmers in which the user is made to believe that the device is infected by a virus or malware and create situation to the user to feel that it is essential to buy a software or take necessary support for disinfection of the device immediately. So that the users buy'ssoftware or pay a certain amount for the necessary support for removal of infection.

Wiper: It a programme which is used to wiping out the data/information or important/necessary programmes from the device. Some wiper malware wipes out the complete information on the hard disk of the infected devices.

Rootkits: These are the programmes which provide access of a programme or data to an unauthorised user. It is also help is masking (hiding of existence) or prevent detection of unauthorised access/users.

Backdoors: It is a process to bypass or avoid normal process of the authorisation to a data/device/network and gain access of the data/device/network. All the above-mentioned types of malwares can be used thorough this process.

Botnets: It a device or group of devices which are connected to internet/network, got infected and are completely under the control of the attackers or hackers and used for denial of service or distributed denial of service attacker's or hackers. Here one individual device which is under the control of the attacker or hacker is called bot. These bots are also used to send spam mails, overload buffers in the networks, etc.

Project Category: In today's cyber world end points protection is very much important because may new applications which are user friendly are emerging daily as per the requirements of the end user in which personal data of the user and business/entity data is being shared through these applications. If these applications are not protected from cyber-attacks/ hackers/phishing/malware it affects privacy of both the user and the organisation. In case of users, it is breach/loss of the personal data and for an organisation it is loss of trust on the organisation by the users.

End point security in one of the many risk mitigation methods used by various organisations and sometimes end users for ensuring the security of the applications used by them. In case of an individualuserofanofflineapplication,forexample on a MS Word (.docx) file we can implement few security measures such as using a password, encryption of the file, etc. and after ensuring security it can be sent to another person or organisation by many means of communication such as e-mail, whatsup, etc. Coming to online applications all the security measures must be maintained by the organisation or the business entity in which one or many persons/teams are involved.

If the end points of the application are not secure enough it is a threat and risk to the organisation or the business entity. For any organisation if the device/network is infected by malware then it may lead to loss of data, wasting of manpower and working

hours, etc. In case of a business entity, it also includes loss of trust, customer, and financial crisis.

For an individual user all the security settings/policies of the device must be take care by the user himself/herself. In case of an organisation each task/role of system security is handled by an individual or various persons/groups/teams based on the requirements and size of the organisations. Systems administrators of the organisations plays a very important role in securing the devices of the organisation*s from various types of attacks/malwares. Based on the roles and responsibility of the individual or group/team the tools used by them will be decided for the security of the system. Roles and responsibilities of the all the persons who take care of system security should match with the organisational goals which have a direct impact on the output/results of and for the organisation. If the system security settings differ from organisational goals, then system administrator and organisation should investigate the issues and make necessary changes.

At the same time all the users should be educated and trained regarding the system requirements and best practices to avoid any attack to the system due to lack of knowledge. By this lot of time and efforts of the system administrator and organisation is saved due to malware /security attacks on the devices.

Today's malwares are more complicated and advanced compared to past malwares. Presently there are many tools available in open market/source which helps any individual to create malware as per individual requirements and online training videos /tutorials are available which help in getting knowledge of creating malware. By maintaining end point security, the system uptime, availability of resources to the end users will enhance and increase.

Some examples of malware attacks are:

- Directing the user to an illegitimate website which appears to be a legitimate website and gathering data of the user.
- Installing key loggers without the knowledge of the users.
- Infecting the system/device with Trojan horse so that system is not available/accessible for/by authorised users.
- Encryption of device/data and demand ransom amount of money.

II. RESEARCH METHODOLOGY

Primary Data - Various National and International standards for implementing end point security and risk management of the systems/devices. Studying and analyse end point security of the system of an organisation.

Secondary Data- Books and Web links for Understanding Malware and types of malwares, how it affects the system and steps/procedures to be followed for end point security.

III. SCOPE OF THE PROJECT

- To understand the various types of threats to the system by malware attacks.
- How these attacks take place?
- Impact of malware attack on a system and organisation.
- How to mitigate the risk caused due to malware attacks?
- Preventive steps to be taken against malware attacks.
- How to handle a malware attack and its effect on a system and the organisation?
- Provide information regarding famous malware attacks and its effect on the system and organisation.
- Provide latest guidelines issued by various organisations for prevention of malware attacks and risk management of the system.

This project is useful for persons handling the responsibilities of System and Networks Administrators, IW Teams & Auditors, System Security staff and managers, System Incident handlers and responding teams.

IV. ANALYSIS

- Malware incident prevention

For prevention of malware by a user or an organisation, first step is to identify the vulnerability,

prepare robust policy and make necessary settings for prevention of vulnerability, reduce the threats, and improve the defensive system/methods. Next step is to create awareness about the policies, vulnerabilities, threats, and defensive systems. Next is training of the user for prevention of malware incidents.

The policies created should be based on the vulnerabilities and its implementation should protect system from getting infected by malware and ensure control prevent measures against spreading of malware. These policies should also include multi layers of malware prevent systems/methods which cover all methods of malware attacks. Specify roles and responsibilities to individuals for better implementation of the policies which helps in prevent some common types of malware attacks and quick identification of any breach which have occurred due to any new technologies or methods.

While preparing policies for malware prevention organisations should consider past, present, and future(speculative) methods/types of attacks, working environment of both host and user of the systems/applications, which helps in minimisation of effects on the system due to attacks. Even after implementing all types of defensive systems, taking all necessary steps for prevention of malware attacks, systems may get effected by malware attacks, no one can ensure that system will never be infected by any malware.

After implementing all the policies and procedures for prevention of malwares, awareness and training programmes should be implemented in regular intervals so that the individuals who are responsible for implementation of preventive measure and normal user, non-technical staff are updated about latest threats, attacks, technologies, methods, etc. in malware attacks. The efficiency of the organisation depends on how fast or quickly the organisation recovery from the damage caused by the malware attack, minimum damaged cause due to the preventive steps taken.

- Policy

The policies implemented should help in prevention of malware attack, prevent easy access for attacker or attack, toughen the system security. Some of the common policies are:

- Lengthy and complex passwords
- Scanning of the attachments in e-mails before downloading.
- Scanning network data
- Removing permissions to use removable devices and personal devices on the systems.
- Prevent installation of unauthorised software and remove unused software.
- Auditing of systems remotely and physically at regular intervals.
- Setup monitors for any unauthorised access.
- Installation of anti-virus, anti-spy ware software and establishing strong firewalls so that unintended information is not entering into the system.
- Limited access as per roles and responsibilities, decentralised authority of various roles such as user creation, password change, handling login timings, take backups, software installation, etc.
- Maintain Log of systems and monitoring every system of the organisation.
- Regular backups, restore points, disk clean ups, defragmentation.

- Awareness

Creating awareness is very important in any organisation. Initially awareness is to be created to all the users about polices and necessary preventive measures to get protected from malware. All these awareness should be as per the requirement of the organisation functions. Common practices suggested to the user in the awareness programmes are:

- Not to open e-mails from unknown sources.
- Not to download any attachments without scanning.
- Not to install applications from an untrusted source.
- Not to click on files with .bat, .vbs,.exe, etc. attached to mails, and from untrusted sources.
- Not to disable protection applications (anti-virus, anti-spy ware), firewalls.
- Not to host untrusted application on administrative accounts.
- Not to allow untrusted pop-up windows.

- Vulnerability Mitigation

An attacker uses vulnerabilities in the system to infect the systems, i.e., vulnerabilities in Operating system, services, and applications. Vulnerabilities are to be removed to avoid attacks one method for this is patch update of the OS, services, and applications. Even after updating the patches attackers use new methods to intrude into the system and infect the system. So, it is to be ensured the patches updated are done regularly.

Another important method to minimise vulnerability is to give minimum privileges/rights to the users. As for any installation or change of system settings administrative rights are required if the privilege is allotted to only a specified or minimum users it helps in reduce the chances to malware incidents. If this method is implemented even if any malware incident takes place, it affects is minimised due to lack of privileges. In any organisation the system security configurations must implement system hardening policies and settings to prevent malware attacks. Some of the steps to mitigate vulnerabilities are:

- Disable or remove are all user not in use.
- Rename or changing default usernames and passwords.
- Disable services which are not required by the systems.
- Setting login timings for the system and users.
- Physical Security to the systems.
- Regular defragmentation of hard disk.
- Disable auto-run of scripts.
- Ensure file sharing is done through a verified and pre decided method and avoid/discourage unsecured methods of file sharing.
- Enable alerts/notifications when unusual data flow of data through networks, applications or services are enabled or disabled.
- Regular updating firewall setting, anti-virus, and anti-spyware.

Anti-virus is the one of the common methods used to control and mitigate malware by an individual user or organisations. Anti-virus scans all the mails, files, boot records and scans real-time activities for any suspicious activities. Scanning of system's at regularly intervals for malware identification. Scanning of any removable devices when connected to the system.

Future Scope and Enhancement of the project

Cyber-security threats and attacks are emerging, evolving and expanding rapidly in new ways and forms with new development in programming, technologies, and tools. Attacks are from simple type of worms which are self-replicative to complex network attacks (DDOS). All ethical hackers are doing their best to prevent cyber-security attacks. They are also using various anti-virus, anti-spyware, dedicated firewalls, and security tools to prevent these attacks. Even after all this measures there are incident happening, various teams are studying and analysing the incidents but there are gaps which are not visible to the analysers.

End point security is one of the methods which helps is prevention of malware attacks and this project is about what these end point security methods are and how they help in prevention of malware attacks. The future technologies which provide end point security protection against attacks are:

- End point Detection and Response (EDR)
- Extended Detection and Response (XDR)
- Managed Detection and Response (MDR)

End Point Detection and Response (EDR)
Primary focus of EDR is to detect advanced/latest threats which can escape legacy/regular security application/tools which protect the systems from attacks. In this process the end point can be any device connected to the network or IoT. It helps in ensuring the security of the information on the device. Detect contaminated files which are breach to the security of the system. Identify all know threats and take necessary prevent actions. Real-time monitoring of network's for any unusual/malicious activities which are not detected for a longer period.

As maximum breach of the security is initiated at the End points EDR play a very important role for providing insight into actual activities undergoing on an endpoint, also identify and resolve any threat. EDR integrates with platforms such as security information and event management (SIEM).
Some applications for EDR are-
https://www.heimdalsecurity.com/enterprise-security/endpoint-detection-and-response-edr-sofware

https://www.bitdefender.com/bussiness/solutions/endpoint-security.html
https://www.sophos.com/es-es/products/endpoint-antivirus
https://www.vmware.com/products/endpoint-detection-and-response.html
https://www.crowdstrike.com/products/endpoint-security/falcon-insight-edr/
https://www.watchguard.com/wgrd-products/endpoint-protection-detection-response

- Extended Detection and Response (XDR)

Extended detection and response (XDR) is a method for enhanced threat detection and response of an endpoints/networks/cloud services which can investigate data sources of non-isolated silos. XDR uses heuristics, analytics, modelling, and automation to collate and investigate the data increasing the results/output compared to regular security tools by reducing the time taken for investigating. It helps various entities for enhanced protection to their data and operations/functioning.

XDR provides threat identification and security to multi-domains simultaneously, event analysis is based on threats, prioritize the data reliability, and take necessary steps for prevention of threats and reduce chances of system getting affected by threats. Provides improved UI with centralised dashboards. It is cost effective for the entities with maximum protection to the system/devices.
Some applications for XDR are-
https://www.sophos.com/es-es/products/endpoint-antivirus
https://www.crowdstrike.com/products/endpoint-security/falcon-xdr/
https://www.cynet.com/platform/
https://www.trellix.com/en-us/platform/xdr.html
https://www.cybereason.com/platform/xdr
https://www.eset.com/int/business/solutions/xdr-extended-detection-and-response/

Managed Detection and Response

MDR is a service which manages the benefits of EDR and XDR, if not used requires a cyber-security expert for setting up a security program for the entity/organisation. It simplifies the tedious process in analysing telemetry data. MDR helps in differentiate false alerts and real threats to the systems.

MDR provides peace of mind to the business entities as it manages various services provided by EDR & XDR. MDR is easily accessible and cost effective. MDR analyses large quantity events and identify genuine threats, alter cyber security activities, and prioritize the issues. Monitor the network, minimise the threats by identifying vulnerabilities and clearing them, identify live/active threats and minimize damage and recovery time. Helps to repair, restore, and remediate cyber security incidents. Some applications for MDR are-
https://www.sentinelone.com/global-services/vigilance-respond-pro/
https://www.crowdstrike.com/products/managed-services/falcon-complete/
https://www.checkpoint.com/solutions/mdr-services/
https://www.securityhq.com/services/managed-detection-and-response/
https://www.rapid7.com/services/managed-services/managed-detection-and-response-services/
https://www.esentire.com/what-we-do/esentire-managed-detection-and-response
https://expel.com/buy/managed-detection-response

REFERENCES

[1] McAfee Endpoint Security
[2] Check Point Endpoint Security Datasheet
[3] (PDF) Malware in Computer Systems: Problems and Solutions (researchgate.net)
[4] Guide to Malware Incident Prevention and Handling for Desktops and Laptops (nist.gov)