BAIT1093 Introduction to Computer Security

Chapter 2: Malicious Software

Topics

2.1 Classification of Malware

2.1.1 Imprison – Ransomware, Cryptomalware

2.1.2 Launch – Virus (File-based Virus/Fileless Virus, Worm, Bot)

2.1.3 Snoop – Sypware, Keylogger

2.1.4 Deceive – PUP, Trojan, RAT

2.1.5 Evade – Backdoor, Logic Bomb, Rootkits

2.2 Countermeasures to Prevent Malware Attack

2.1 Classification of Malware [1]

- In a legal setting, a "**computer contaminant**" is defined as any set of computer instructions that is designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or network without the intent or permission of the owner of the information, computer system, or network.
- This legal definition is the basis for the definition of the cybersecurity word **malware (malicious software),** which is software that enters a computer system without the user's knowledge or consent and then performs an unwanted and harmful action.

2.1 Classification of Malware [1]

- Malware is continually evolving to avoid detection by improved security measures.
- According to one report, the number of new malware releases every month exceeds 20 million, and the total malware in existence is approaching 900 million instances.
- One attempt at classifying the diverse types of malware can be to examine the primary action that the malware performs and then group those together with similar actions. These malware actions used for groupings are **imprison, launch, snoop, deceive, and evade**.

2.1.1 Imprison [1]

- The type of malware attempts to take away the freedom of users to do whatever they want on their computer is called imprison.
- The type of malware that imprisons are ransomware and cryptomalware.

2.1.1 Imprison [1]

Ransomware

- Largest-growing types of malware.
- Prevents a user's endpoint devices from properly and fully functioning until a fee/ransom is paid.
- Takes away a user's freedom from freely using their computer until the ransom is transacted.
- Embeds itself onto the computer in such a way that it cannot be bypassed, and even rebooting causes the ransomware to launch again

2.1.1 Imprison [1]

Ransomware

- Became widespread around 2010. This earliest ransomware displays a screen and prevents the user from accessing the computer's resources (called blocker ransomware). The screen contains instructions that pretends to be from a reputable third party, giving a "valid" reason for blocking the user's computer.

2.1.1 Imprison [1]

Ransomware

Source: Symantec Security Response

Figure 3-1 Blocker ransomware message

2.1.1 Imprison [1]

Ransomware

Figure 3-2 Ransomware computer infection

2.1.1 Imprison [1]

Ransomware

- Ransomware continues to be a serious threat to users. Threat actors have now shifted their sights to state and local governments that typically have weaker security. In 2019, two-thirds of ransomware attacks targeted state and local governments; to date, more than 350 of these governments have been the victims of successful attacks.

2.1.1 Imprison [1]

Cryptomalware

- In recent years, a more malicious form of ransomware has arisen. Instead of just blocking users from accessing the computer, it encrypts all the files on the device so that none of them can be opened. This is called cryptomalware.

2.1.1 Imprison [1]

Cryptomalware

- A screen appears telling the victims that their files are now encrypted, and a fee must be paid to receive a key to unlock them. In addition, threat actors have increased the urgency for payment: the cost for the key to unlock the cryptomalware increases every few hours or days.
- On some occasions, the threat actors claim that a growing number of the encrypted user files will be deleted until the ransom is paid; if the ransom is not paid promptly, the key to unlock the files can never be purchased.

2.1.1 Imprison [1]

Cryptomalware

Figure 3-3 Cryptomalware message

2.1.1 Imprison [1]

Cryptomalware

- In addition to encrypting files on the user's local hard drive, new variants of cryptomalware encrypt all files on any network or attached device connected to that computer.
- This includes secondary hard disk drives, USB hard drives, network-attached storage devices, network servers, and even cloud-based data repositories.
- Thus, if a user's computer in an enterprise is infected with cryptomalware, potentially all files for the enterprise—and not just those on one computer—can be locked.

2.1.2 Launch [1]

- Infects a computer to launch attacks on other computers.
- Example: virus, worm, bot

2.1.2 Launch [1]

Virus

- 2 types of viruses: a file-based virus and a fileless virus
- File-Based Virus
  - Malicious computer code that is attached to a file.
  - There is about 50 different Microsoft Windows file types that can be infected with a virus.

Table 3-1 Windows file types that can be infected

File extension	Description
DOCX or XLSX	Microsoft Office user documents
EXE	Executable program file
MSI	Microsoft installer file
MSP	Windows installer patch file
SCR	Windows screen saver
CPL	Windows Control Panel file
MSC	Microsoft Management Console file
WSF	Windows script file
PS1	Windows PowerShell script

2.1.2 Launch [1]

Virus

- File-Based Virus
  - Reproduces itself on the same computer, meaning it replicates itself or an evolved copy of itself without any human intervention.
  - Early viruses were relatively straightforward in how they infected files. One basic type of infection is the appender infection. The virus first attaches or appends itself to the end of the infected file. It then inserts at the beginning of the file a jump instruction that points to the end of the file, which is the beginning of the virus code. When the program is launched, the jump instruction redirects control to the virus.

2.1.2 Launch [1]

Virus

- File-Based Virus
  - However, these types of viruses could be detected by virus scanners relatively easily.

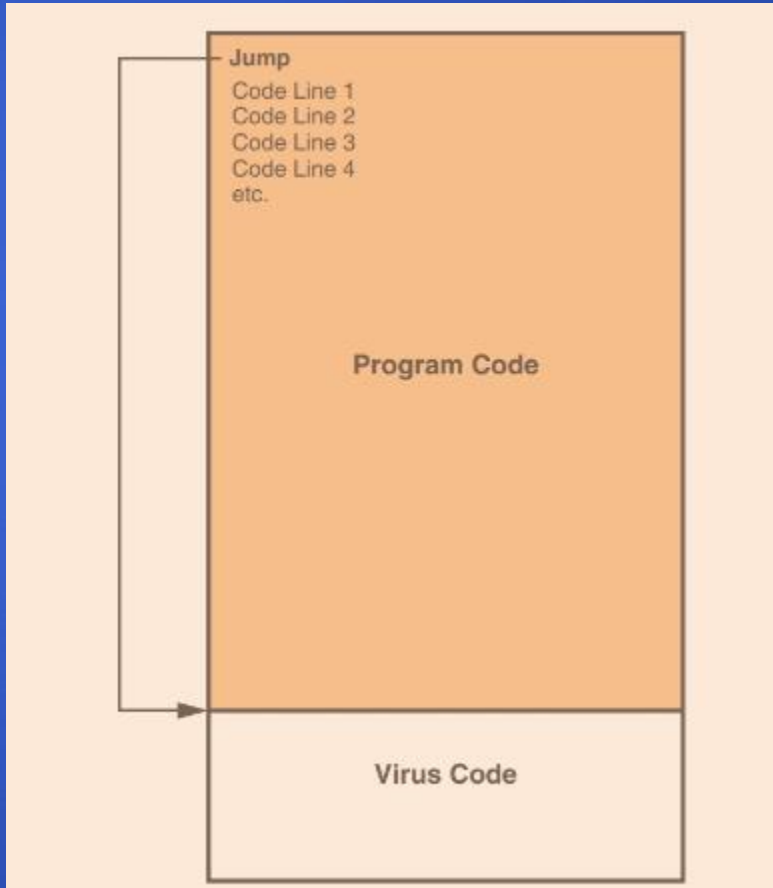


Figure 3-4 Appender infection

2.1.2 Launch [1]

Virus

- File-Based Virus
  - Later file-based viruses went to greater lengths to avoid detection; this type of virus is called an **armored file-based virus**.
  - Some of the armored virus infection techniques include the **split infection** (it split the malicious code itself into several parts and then these parts are placed at random positions throughout the program code) and the **mutation** (the virus changes its internal code to one of a set number of predefined mutations whenever it is executed).

2.1.2 Launch [1]

Virus

- File-Based Virus
  - Each time the infected program is launched or the data file is opened—either by the user or the computer's operating system (OS)—the virus first unloads a payload to perform a malicious action (such as to corrupt or delete files, prevent programs from launching, steal data to be sent to another computer, cause a computer to crash repeatedly, or turn off the computer's security settings).

2.1.2 Launch [1]

Virus

- File-Based Virus
  - Then the virus reproduces itself by inserting its code into another file, but only on the same computer. A virus can only replicate itself on the host computer where it is located; it cannot automatically spread to another computer by itself. Instead, it must rely on the actions of users to spread to other computers. other computers.

2.1.2 Launch [1]

Virus

- File-Based Virus
  - Because viruses are attached to files, they are spread when a user transfers those files to other devices. For example, a user might send an infected file as an email attachment or copy an infected file to a USB flash drive and give the drive to another user. Once the virus reaches a new computer, it begins to infect it. Thus, a virus must have two carriers: a file to which it attaches and a human to transport it to other computers.

2.1.2 Launch [1]

Virus

- Fileless Virus
  - Does not attach itself to a file.
  - Take advantage of native services and processes that are part of the OS to avoid detection and carry out its attacks.
  - These native services used in a fileless virus are called **living-off-the-land binaries (LOLBins).**

2.1.2 Launch [1]

Virus

- Fileless Virus

Table 3-2 Microsoft Windows common LOLBins

Name	Description
PowerShell	A cross-platform and open source task automation and configuration management framework
Windows Management Instrumentation (WMI)	A Microsoft standard for accessing management information about devices
.NET Framework	A free, cross-platform, open source developer platform for building different types of applications
Macro	A series of instructions that can be grouped together as a single command to automate a complex set of tasks or a repeated series of tasks, can be written by using a macro scripting language, such as Visual Basic for Applications (VBA), and is stored within the user document (such as in an Excel .xlsx workbook or Word .docx file)

2.1.2 Launch [1]

Virus

- Fileless Virus
  - the malicious code of a fileless virus is loaded directly in the computer's random access memory (RAM) through the LOLBins and then executed

2.1.2 Launch [1]

Virus

- Fileless Virus
  - Advantages of a fileless virus over a file-based virus:
    - Easy to infect
    - Extensive control
    - Persistent
    - Difficult to detect
    - Difficult to defend against

2.1.2 Launch [1]

Virus

- Fileless Virus
  - Advantages of a fileless virus over a file-based virus:
    - **Easy to infect**
      - Through a malicious webpages that the user visits.
      - Silently send a script to the victim's web browser, which invokes a scripting language such as JavaScript
      - The browser passes the instructions to a LOLBIN such as Powershell, which reads and executes commands.

2.1.2 Launch [1]

Virus

- Fileless Virus
  - Advantages of a fileless virus over a file-based virus:
    - **Extensive control**
      - Several LOLBins have extensive control and authority on a computer.
      - For example, Power-Shell has full access to the core OS of a Windows computer, so it can undermine existing security features. PowerShell can also manipulate user accounts and password protection.

2.1.2 Launch [1]

Virus

- Fileless Virus
  - Advantages of a fileless virus over a file-based virus:
    - **Persistent**
      - A program that is loaded into RAM for execution will terminate once the computer is shut down or rebooted.
      - However, fileless viruses often write their script into the Windows Registry, which is a database that stores settings for the Windows OS and application programs.
      - Each time the computer is restarted or on a set schedule, the script of the fileless virus is again launched

2.1.2 Launch [1]

Virus

- Fileless Virus
  - Advantages of a fileless virus over a file-based virus:
    - **Difficult to Detect**
      - Files that are infected with a file-based virus can be scanned by an antivirus tool for detection.
      - However, because a fileless virus loads into RAM, no file can be scanned.
      - by using LOLBins, there is no evidence of other tools being used. And some LOLBins like PowerShell run in a section of system memory that cannot be queried or searched, making its activities virtually impossible to detect.

2.1.2 Launch [1]

Virus

- Fileless Virus
  - Advantages of a fileless virus over a file-based virus:
    - **Difficult to Defend Against**
      - To fully defend against a fileless virus, it would be necessary to turn off all the potential LOLBins, which would cripple the OS and cause it to not properly function.
      - These LOLBins are loaded by default when the OS starts so that any attempt to turn selected LOLBins off would already be too late.

2.1.2 Launch [1]

Worm (Network Viruses)

- Malicious program that uses a computer network to replicate.
- A worm is designed to enter a computer through the network and then take advantage of a vulnerability in an application or an OS on the host com-puter. Once the worm has exploited the vulnerability on one system, it immediately searches for another computer on the network that has the same vulnerability.

2.1.2 Launch [1]

Worm (Network Viruses)

- Early years, worms are relatively benign and designed simply to spread quickly but not corrupt the systems they infected. These worms slowed down the network by consuming all network resources due to quick replication.
- Today's worm can leave behind a payload on the systems they infect and cause harm, much like a virus.
- Actions that worms have performed include deleting files on the computer or allowing the computer to be remotely controlled by an attacker.

2.1.2 Launch [1]

Bot

- Software that allows the infected computer to be placed under the remote control of an attacker for the purpose of launching attacks.
- This infected robot computer is known as a bot or zombie.
- When hundreds, thousands, or even millions of bot computers are gathered into a logical computer network, they create a botnet under the control of a bot herder.

2.1.2 Launch [1]

Bot

Table 3-3 Uses of botnets

Type of attack	Description
Spamming	Botnets are widely recognized as the primary source of spam email. A botnet consisting of thousands of bots enables an attacker to send massive amounts of spam.
Spreading malware	Botnets can be used to spread malware and create new bots and botnets. Bots can download and execute a file sent by the attacker.
Ad fraud	Threat actors earn money by generating a high number of "clicks" on advertisements at targeted websites, using a bot to mimic the mouse clicks of a user.
Mining cryptocurrencies	Also called "cryptomining," this is a process in which transactions for various forms of cryptocurrency are verified, earning the "miner" a monetary reward. Botnets combine the resources of millions of bots for mining cryptocurrencies.

2.1.2 Launch [1]

Bot

- Infected bot computers receive instructions through a command and control (C&C) structure from the bot herders regarding which computers to attack and how.

2.1.2 Launch [1]

Bot

- There are a variety of ways for this communication to occur, including the following:
  - A bot can receive its instructions by automatically signing in to a bot-herding website where information found from the website is interpreted as commands.
  - Bots can sign in to a third-party website; bot herder not needing to have a direct affiliation with that website.
  - Commands can be sent via blogs, specially coded attack commands through posts on Twitter, or notes posted in Facebook.
  - Bot herders are increasingly using a “dead drop” C&C mechanism by setting up a Google Gmail email account and then creating a draft email message that is never sent but contains commands the bot receives when it logs in to Gmail and reads the draft. Because the email message is never sent, there is no record of the com-mands. All Gmail transmissions are protected so that outsiders cannot view them.

2.1.3 Snoop [1]

- Another category of malware “snoops” or spies on its victims.
- The two common types of snooping malware are spyware and keyloggers.

2.1.3 Snoop [1]

Spyware

- Tracking software that is deployed without the consent or control of the user.
- Spyware can secretly monitor users by collecting information without their approval through the computer's resources, including programs already installed on the computer, to collect and distribute personal or sensitive information.

2.1.3 Snoop [1]

Spyware

Table 3-4 Technologies used by spyware

Technology	Description	Impact
Automatic download software	Downloads and installs software without the user's interaction	Could install unauthorized applications
Passive tracking technologies	Gathers information about user activities without installing any software	Could collect private information such as websites a user has visited
System modifying software	Modifies or changes user configurations, such as the web browser home page or search page, default media player, or lower-level system functions	Changes configurations to settings that the user did not approve
Tracking software	Monitors user behavior or gathers information about the user, sometimes including personally identifiable or other sensitive information	Could collect personal information that can be shared widely or stolen, resulting in fraud or identity theft

2.1.3 Snoop [1]

Keylogger

- Silently captures and stores each keystroke that a user types on the computer's keyboard.
- The threat actor can then search the captured text for any useful information such as passwords, credit card numbers, or personal information.
- A keylogger can be a software program or a small hardware device.

2.1.3 Snoop [1]

Keylogger

- Software keyloggers are programs installed on the computer that silently capture sensitive information.
- However, software keyloggers, which conceal themselves so that the user cannot detect them, go far beyond capturing a user's keystrokes.
- These programs can also capture everything on the user's screen and silently turn on the computer's web camera to record images of the user.

2.1.3 Snoop [1]

Keylogger

•

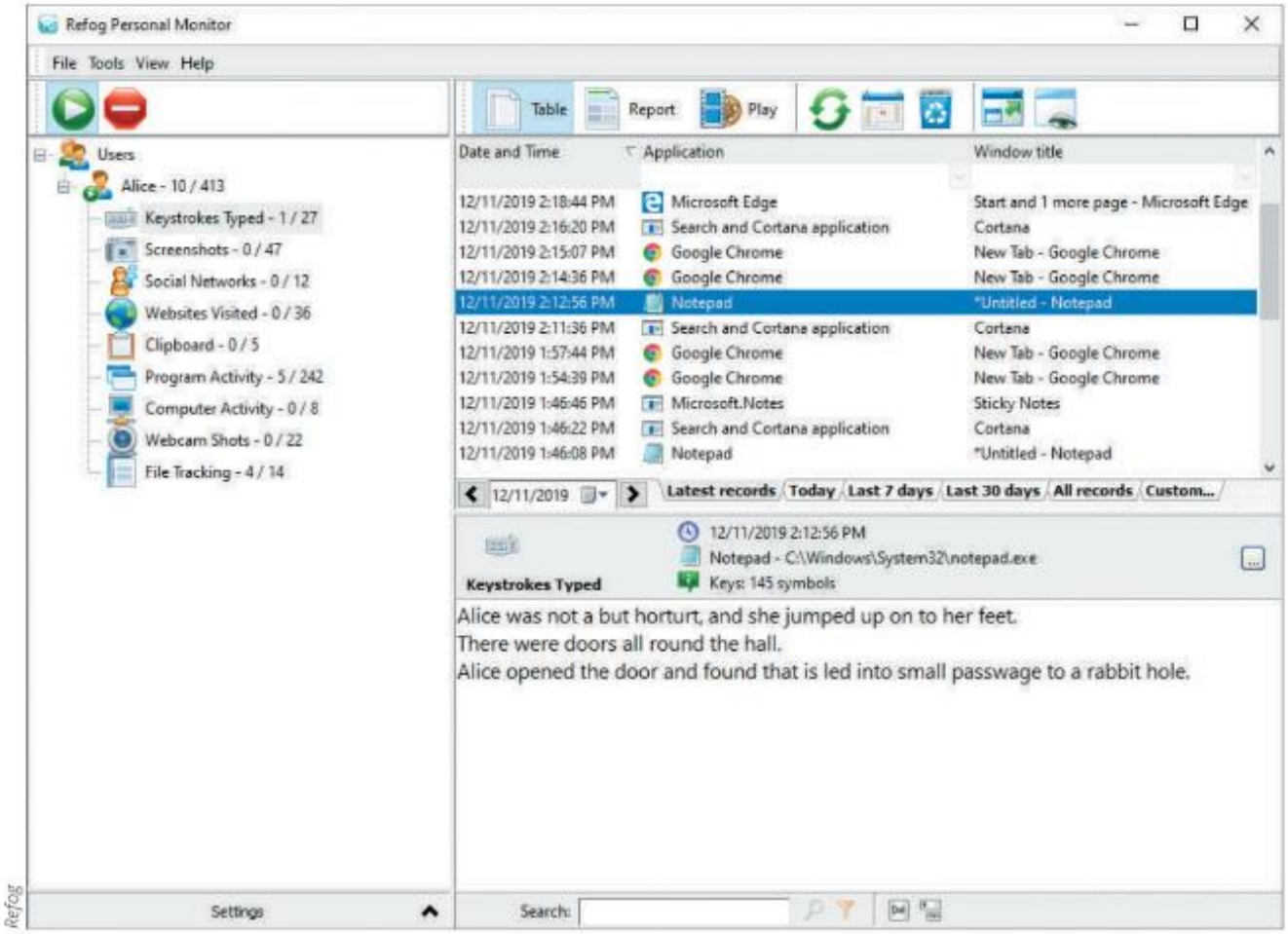


Figure 3-5 Software keylogger

2.1.3 Snoop [1]

Keylogger

- For computers that are in a public location such as a library or computer lab but are “locked down” so that no software can be installed, a hardware keylogger can be used instead.
- These keyloggers are hardware devices inserted between the computer keyboard connection and USB port.

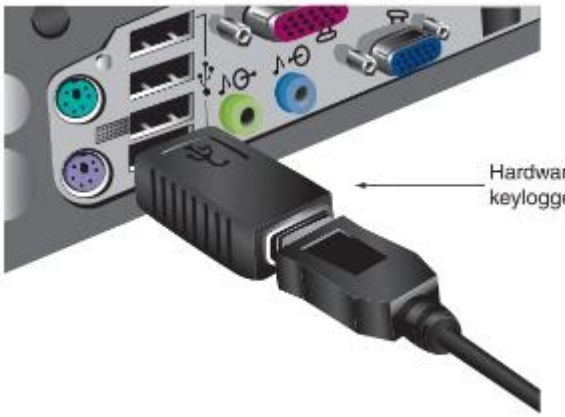


Figure 3-6 Hardware keylogger

2.1.3 Snoop [1]

Keylogger

- Because the device resembles an ordinary keyboard plug and the computer keyboard USB port is often on the back of the computer, a hardware keylogger can easily go undetected.
- In addition, the device is beyond the reach of the computer's antimalware scanning software and thus raises no alarms.
- A disadvantage of a hardware keylogger is that the threat actor must install and then later return to physically remove the device in order to access the information it has stored, each time being careful not to be detected.

2.1.4 Deceive [1]

- Malware attempts to deceive the user and hide its true intentions.
- Software in this category includes potentially unwanted programs (PUPs), Trojans, and remote access Trojans (RATs)

2.1.4 Deceive [1]

Potentially Unwanted Program (PUP)

- Software that the user does not want on their computer.
- PUPs often become installed along with other programs and are the result of the user overlooking the default installation options on software downloads.

Figure 3-7 Default installation options

2.1.4 Deceive [1]

Potentially Unwanted Program (PUP)

- PUPs may include software that is pre-installed on a new computer or smart-phone and cannot be easily removed.
- Other examples of PUPs are advertising that obstructs content or interferes with web browsing, pop-up windows, pop-under windows, search engine hijacking, home page hijacking, toolbars with no value for the user, and settings that redirect to competitors' websites, alter search results, and replace ads on webpages.

2.1.4 Deceive [1]

Trojan

- According to ancient legend, the Greeks won the Trojan War by hiding soldiers in a large hollow wooden horse that was presented as a gift to the city of Troy. Once the horse was wheeled into the fortified city, the soldiers crept out of the horse during the night and attacked the unsuspecting defenders.

2.1.4 Deceive [1]

Trojan

- A computer Trojan is an executable program that masquerades as performing a benign activity but also does something malicious.
- For example, a user might download what is advertised as a calendar program, yet in addition to installing the calendar, it also installs malware that scans the system for credit card numbers and passwords, connects through the network to a remote system, and then transmits that information to the attacker.

2.1.4 Deceive [1]

Remote Access Trojan (RAT)

- A RAT has the basic functionality of a Trojan but also gives the threat agent unauthorized remote access to the victim's computer by using specially configured communication protocols.
- This creates an opening into the victim's computer, allowing the threat agent unrestricted access. The attacker can not only monitor what the user is doing but also change computer settings, browse and copy files, and even use the computer to access other computers connected on the network.

2.1.5 Evade [1]

- Help malware or attacks evade detection.
- This includes backdoor, logic bomb, and rootkit.

2.1.5 Evade [1]

Backdoor

- A backdoor gives access to a computer, program, or service that circumvents any normal security protections.
- Backdoors installed on a computer allow the attacker to return later and bypass security settings.

2.1.5 Evade [1]

Backdoor

- Creating a legitimate backdoor is a common practice by developers, who may need to access a program or device on a regular basis, yet do not want to be hindered by continual requests for passwords or other security approvals.
- The intent is for the backdoor to be removed once the application is finalized. However, in some instances, backdoors have been left installed, and attackers have used them to bypass security.

2.1.5 Evade [1]

Logic Bomb [1] [2]

- A logic bomb is computer code that is typically added to a legitimate program but lies dormant and evades detection until a specific logical event triggers it.
- The most common factor that logic bomb will be triggered is date/time.
- Once it is triggered, the program then deletes data or performs other malicious activities.

2.1.5 Evade [1]

Logic Bomb

- Logic bombs are difficult to detect before they are triggered. This is because logic bombs are often embedded in very large computer programs, some containing hundreds of thousands of lines of code, and a trusted employee can easily insert a few lines of computer code into a long program without anyone detecting it. In addition, these programs are not routinely scanned for containing malicious actions.

2.1.5 Evade [1]

Logic Bomb [2]

- Examples of cases related to logic bomb
  - Roger Duronio, system administrator for UBS was charged in June 2006 using logic bomb to damage the company's computer network.
  - Mittesh Das was found guilty in 2017, where he created a logic bomb deleting files in US Army Reserve payroll systems after his company lost the contract.
  - Nimesh Patel created a logic bomb to attack his former employer's servers in 2016.

2.1.5 Evade [1]

Rootkits [1]

- Malware that can hide its presence and the presence of other malware on the computer.
- It does this by accessing “lower layers” of the operating system or even using undocumented functions to make alterations.
- This enables the rootkit and any accompanying software to become undetectable by the operating system and common antimalware scanning software.

2.1.5 Evade [1]

Rootkits [2]

- A collection of tools that a hacker uses to mask his/her intrusion and obtain administrator-level access to a computer or computer network.
- The intruder installs a rootkit on a computer after first obtaining user-level access, either by exploiting a known vulnerability or cracking a password.
- Collects user IDs and passwords to other machines on the network, thus giving the hacker root or privileged access.

2.1.5 Evade [1]

Rootkits [2]

- A rootkit may consist of utilities that also do the following:
  - Monitor traffic and keystrokes
  - Create a backdoor into the system for the hacker's use
  - Alter log files
  - Attack other machines on the network
  - Alter existing system tools to circumvent detection

2.2 Countermeasures to Prevent Malware Attack

- Developing Security Policies
- Implementing Security Awareness Training
- Using App-Based Multi-Factor Authentication
- Installing Anti-Malware & Spam Filters
- Changing Default Operating System Policies
- Performing Routine Vulnerability Assessments

Note: The list shown above is not exhaustive

Source: https://purplesec.us/common-malware-types/#Prevent

2.2 Countermeasures to Prevent Malware Attack

Developing Security Policies

- Important element of companies' cyber security strategy as a road map to employees of what to do, when to do it and who gets the access to systems or information.
- Examples of security policies that may help to prevent malware attack:
  - Social Engineering Awareness Policy
  - Server Malware Protection Policy
  - Software Installation Policy
  - Removable Media Policy

Source: https://purplesec.us/common-malware-types/#Prevent

2.2 Countermeasures to Prevent Malware Attack

Developing Security Policies → 1) Social Engineering Awareness Policy

- Defines guidelines to provide awareness around the threat of social engineering and defines procedures when dealing with social engineering threats.

Source: https://purplesec.us/common-malware-types/#Prevent

2.2 Countermeasures to Prevent Malware Attack

Developing Security Policies → 2) Server Malware Protection Policy

- Outline which server systems are required to have anti-virus and/or anti-spyware applications.

Source: https://purplesec.us/common-malware-types/#Prevent

2.2 Countermeasures to Prevent Malware Attack

Developing Security Policies → 3) Software Installation Policy

- Outline the requirements around the installation of software on company computing devices.
- To minimize the risk of loss of program functionality, the exposure of sensitive information contained within the Company's computing network, the risk of introducing malware, and the legal exposure of running unlicensed software.

Source: https://purplesec.us/common-malware-types/#Prevent

2.2 Countermeasures to Prevent Malware Attack

Developing Security Policies → 4) Removable Media Policy

- to minimize the risk of loss or exposure of sensitive information maintained by the company and to reduce the risk of acquiring malware infections on computers operated by the company through infected removable media.

Source: https://purplesec.us/common-malware-types/#Prevent

2.2 Countermeasures to Prevent Malware Attack

Implementing Security Awareness Training

- It is important to conduct security awareness training among employees on a regular basis to prevent massive losses to cyber attacks.
- Awareness training involves:
  - **Baseline Testing** – to assess likelihood that a user falls for a phishing attack
  - **Training Users** – interactive content designed to educate users on the latest social engineering attacks
  - **Phishing Campaigns** – perform simulated phishing attacks
  - **Reporting Results** – stats and graphs for both training and phishing activities to demonstrate the ROI (Return on Investment)

Source: https://purplesec.us/common-malware-types/#Prevent

2.2 Countermeasures to Prevent Malware Attack

Implementing Security Awareness Training

- Educating users on considering a few simple questions before opening any attachment [2]:
  - Was this attachment expected? Attachments from people you do not know or from whom you did not expect any attachment must always be treated as potential malware.
  - Is the email specific “There are Q3 sales report that we discussed yesterday” or generic sounding emails such as “Here is your document”? Be careful with too generic sounding emails.
  - Do you have the significant doubts about the authenticity of an email attachment? When in doubt, ask technical support.

Source: https://purplesec.us/common-malware-types/#Prevent

2.2 Countermeasures to Prevent Malware Attack

Using App-Based Multi-Factor Authentication

- Although Multi-Factor Authentication (MFA) has demonstrated evidence of deterring malware attacks, it does comes with some limitations/weaknesses.
- SMS based MFA can easily be bypassed nowadays. Threat actors can capture One Time Password (OTP) and access the user's account without the owner of the account receiving any SMS from their phone.
- Users are recommended to use app-based MFA or hardware MFA (eg Yubikey)

Source: https://purplesec.us/common-malware-types/#Prevent

2.2 Countermeasures to Prevent Malware Attack

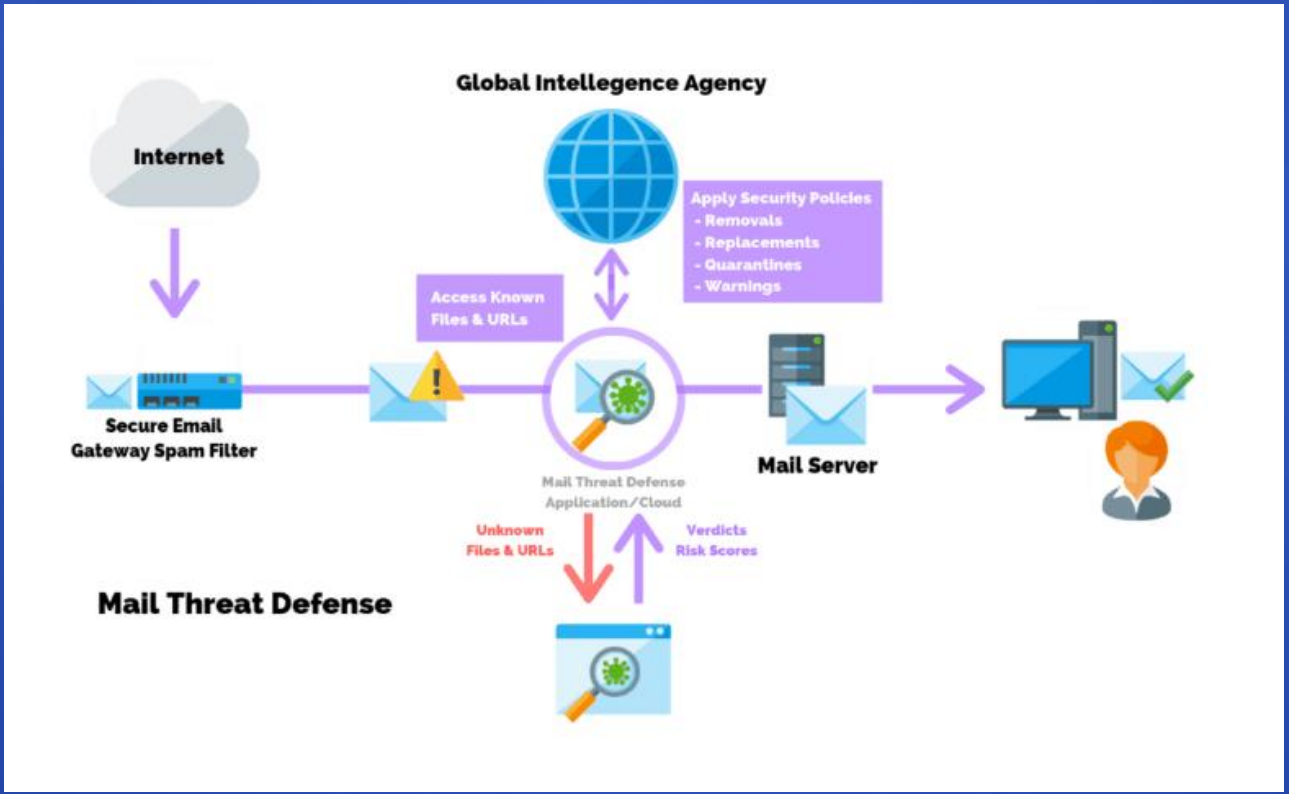
Installing Anti-Malware & Spam Filters

- Emails are the primary method for delivery malware and socially engineered attacks.
- In addition to installation of anti-malware software on end devices, it is good to install anti-malware and spam filters to mail servers as part of a defense in depth approach.
- Running up-to-date anti-malware software is a must. [2]
- If there is a need to use both host-based anti-malware and network anti-malware, it is a good practice to purchase two different vendors so that it one misses, the other is likely to catch [2]

Source: https://purplesec.us/common-malware-types/#Prevent

2.2 Countermeasures to Prevent Malware Attack

Installing Anti-Malware & Spam Filters



Source: https://purplesec.us/common-malware-types/#Prevent

2.2 Countermeasures to Prevent Malware Attack

Changing Default Operating Systems Policies

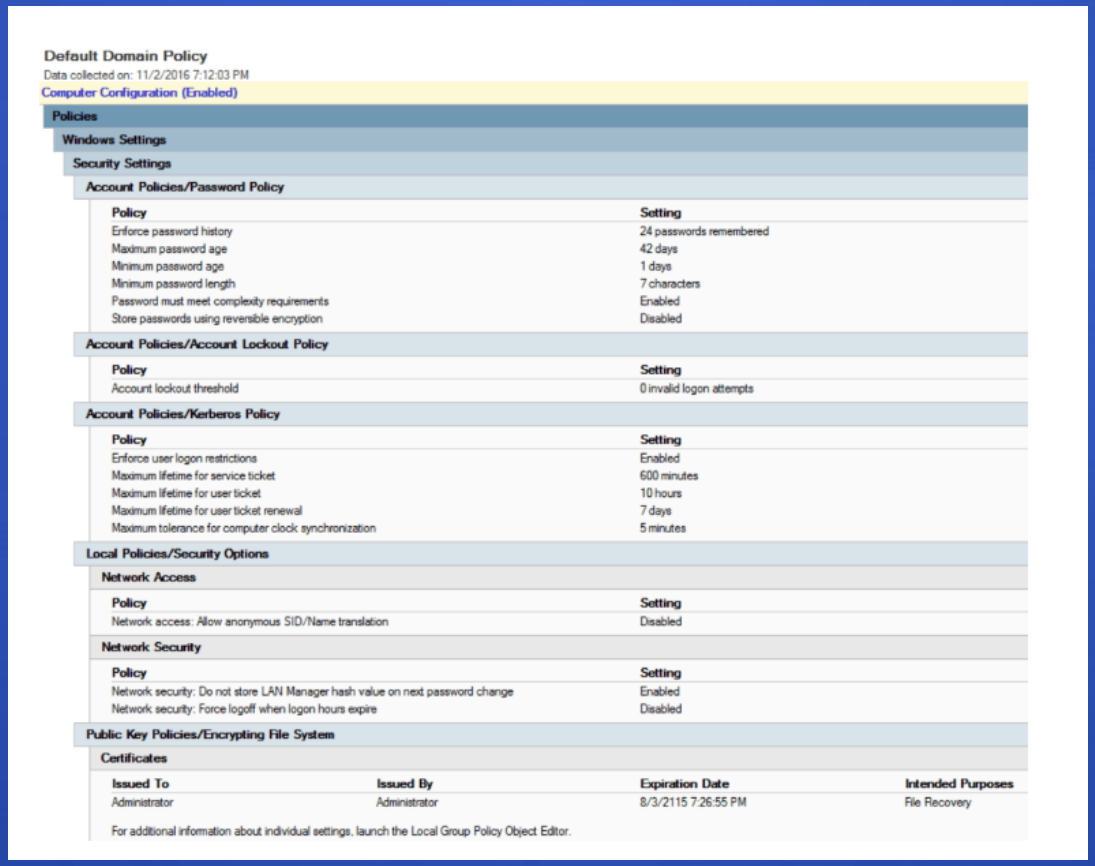
- It is recommended to improve the default security settings for operating systems.
- For example, Microsoft recommends change the password history from 10 to 24 passwords and reducing the maximum password age from 90 days to 42 days.
- Network administrator is responsible to ensure that the domain, workstations, and devices are set up to adhere to security policies within the organization.

Source: https://purplesec.us/common-malware-types/#Prevent

2.2 Countermeasures to Prevent Malware Attack

Changing Default Operating Systems Policies

•



Default Domain Policy
Data collected on: 11/2/2016 7:12:03 PM

Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Account Policies/Password Policy

Policy	Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Account Policies/Account Lockout Policy

Policy	Setting
Account lockout threshold	0 invalid logon attempts

Account Policies/Kerberos Policy

Policy	Setting
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes

Local Policies/Security Options

Network Access

Policy	Setting
Network access: Allow anonymous SID/Name translation	Disabled

Network Security

Policy	Setting
Network security: Do not store LAN Manager hash value on next password change	Enabled
Network security: Force logoff when logon hours expire	Disabled

Public Key Policies/Encrypting File System

Certificates

Issued To	Issued By	Expiration Date	Intended Purposes
Administrator	Administrator	8/3/2115 7:26:55 PM	File Recovery

For additional information about individual settings, launch the Local Group Policy Object Editor.

Source: https://purplesec.us/common-malware-types/#Prevent

2.2 Countermeasures to Prevent Malware Attack

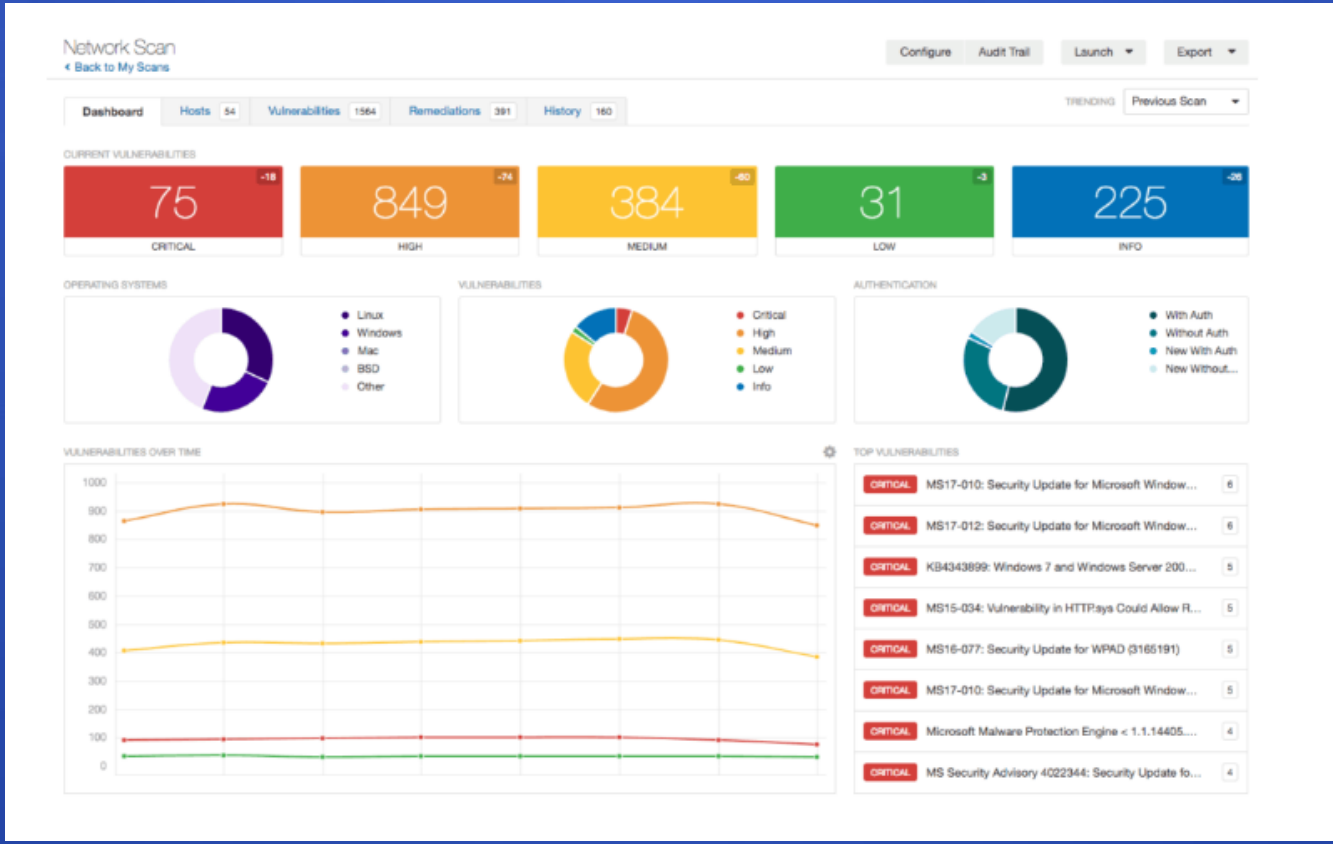
Perform Routine Vulnerability Assessments

- Performing routine network vulnerability scans help to identify known vulnerabilities, lack of security controls, and common misconfigurations.
- Scanners like Nessus are used to scan ports, analyze protocols, and map a network.
- This provides network administrators with detailed information about which hosts on a network are running what services.
- Most scanners will display the information collected in a dashboard listing each vulnerability found and its severity.

Source: https://purplesec.us/common-malware-types/#Prevent

2.2 Countermeasures to Prevent Malware Attack

Perform Routine Vulnerability Assessments



Source: https://purplesec.us/common-malware-types/#Prevent

2.2 Countermeasures to Prevent Malware Attack

Perform Routine Vulnerability Assessments

- In addition to providing the raw scan results, most vulnerability scanning services include an assessment report consisting of a remediation plan to resolve at risk systems.
- Organizations may also wish to implement a patch management program. The main purpose of patch management is to continuously identify, prioritize, remediate, and report on security vulnerabilities in systems.

Source: https://purplesec.us/common-malware-types/#Prevent

Main References

[1] Mark Ciampa. 2022. CompTIA Security+ Guide To Network Security Fundamentals. Cengage Learning.
[2] Easttom, Chuck. 2020. Computer Security Fundamentals. 4th ed. Pearson