



Introduction To Malware



Copyright © www.ine.com

Topic Overview

- ▶ What Is Malware?
- ▶ Categories Of Malware

What Is Malware

▷ Malware = **Malicious Software**

“Code or software that is specifically designed to damage, disrupt, steal, or in general inflict some other "bad" or illegitimate action on data, hosts, or networks.” – cisco.com

<https://www.cisco.com/c/en/us/about/security-center/virus-differences.html>

▷ Malware is classified by:

- ▶ The ways it infects a system
- ▶ The methods used to propagate the malware

Copyright © www.ine.com



Methods of infection include; Stealing data, deleting files or data, locking files or data to make them inaccessible, corrupting files or data, or disabling entire systems.

-

Methods of propagation include; software bundled with other (legitimate) files, exploits to known OS vulnerabilities, installations as a result of user interaction with websites, email attachments, and much more.

Malware Types

Computer Virus	Worm
Mailer and Mass-Mailer Worms	Logic Bombs
Trojan Horse	Back Doors
Exploits	Downloaders
Spammers	Key Loggers
Root Kits	Ransomware

Copyright © www.ine.com



Before talking about the various solutions that one can implement on a host to protect against viruses, malware, etc we need to become aware of the various terms involved and what types of malicious software we're trying to protect against.

-

Many of these things are similar (or identical) in their intent and operation...but differ in their delivery and propagation mechanisms.



Viruses & Worms



Copyright © www.ine.com

Topic Overview

- ▶ Computer Virus – Definition
- ▶ Worms – Definition
- ▶ Mailer Worms

Viruses & Worms

▶ Computer Virus

- ▶ A malicious software that infects a host file or system area to perform undesirable outcomes such as erasing data, stealing information, or corrupting the integrity of the system. In numerous cases, these viruses multiply again to form new generations of themselves
- ▶ Typically attached to executable (.exe) files and not activated until the executable is run

▶ Worm

- ▶ Viruses that replicate themselves over the network infecting numerous vulnerable systems. In most occasions, a worm will execute malicious instructions on a remote system without user interaction
- ▶ Do not require transfer of any host programs in order to spread

Copyright © www.ine.com



To be classified as a virus or worm, malware must be able to propagate.

-

A computer virus is a type of malware that propagates by inserting a copy of itself into and becoming part of another program. Viruses spread when the software or document they are attached to is transferred from one computer to another

-

A virus depends on a host program to replicate whereas a worm propagates independently of other programs.

-

To spread, worms either exploit a vulnerability on the target system or use some kind of [social engineering](#) to trick users into executing them. A worm enters a computer through a vulnerability in the system and takes advantage of file-transport or information-transport features on the system, allowing it to travel unaided.

Mailer Worms

▷ Mailer and mass-mailer worms

- ▶ Executables that utilize fake emails to propagate themselves
- ▶ May Randomly compose the subjects and bodies of the messages from words and phrases carried in the worm's own code
- ▶ The name of the file attachment can be either random, or 'borrowed' from other files.

▷ Some examples:

- ▶ W32/Waledac.A
- ▶ Loveletter.A@mm
- ▶ W32/SKA.A@m (a.k.a. the Happy99 worm),



Copyright © www.ine.com



An example...the W32/Waledac.A email worm: The name of the email attachment is always "ecard.exe". The contents of the email try to fool you into believing you've received a Christmas greeting from a friend by having a subject line such as...

---A Christmas card from a friend
---Happy Christmas! Happy Christmas!
---and MANY many others

Once the executable is clicked on, the worm:

- saves a copy of itself to the Windows registry system
- amends the registry so the worm is run upon every system startup event.
- searches through all of your files for email addresses
- spams copies of itself from email addresses it has found
- gathers information about your computer which it encrypts and sends to one of several IP addresses

https://www.f-secure.com/v-descs/email-worm_w32_waledac_a.shtml



Bombs, Horses & Backdoors



Copyright © www.ine.com

Topic Overview

- ▶ Introduction To Logic Bombs
- ▶ Introduction To Trojan Horse Viruses
- ▶ What Are Backdoor Viruses

Logic Bombs

- A delayed-action virus (also called, “slag code”)
- Malicious code injected into a legitimate application that executes after either a pre-defined timeframe or failure of a user to respond to a program command.
- Once activated, may;
 - Display a random message
 - Delete or corrupt data
 - Have other, undesirable effects
- “Code or software containing a logic bomb may not be detected by traditional antimalware tools because they use custom code designed for a particular system and scenario; no signature exists to detect them.” - searchsecurity.techtarget.com



Copyright © www.ine.com



Frequently logic bombs are used by disgruntled employees. For example, let's say a [privileged user](#) has a grudge against his company and is afraid he might soon be fired. In advance of his firing, he sets up a scheduled job that checks to see if his user account has been active during the past 90 days; if no activity is found, the scheduled job deletes a critical database. Sure enough, the user is fired, and a few months later, once his account has been inactive for 90 days, the database is deleted. In most cases this would be a visible and obvious action, but what makes a logic bomb especially insidious is that it changes its code randomly, making it more difficult to detect and more damaging to the targeted organization. - <https://searchsecurity.techtarget.com/tip/Understanding-logic-bomb-attacks-Examples-and-countermeasures>

Logic bombs are typically installed by privileged users who know what security controls need to be circumvented in order to go undetected until they detonate. The malicious code could also be included within an existing piece of software installed on a target system. A logic bomb often bypasses whitelisting or file system integrity checks because a malicious admin, usually the person responsible for a logic bomb, could tamper with or disable whitelisting and file integrity systems.

Trojan Horse

- ▶ Malware disguised as legitimate software
- ▶ Users are typically tricked via some kind of social engineering into installing the malware
 - ▶ Opening email attachments from trusted sources
 - ▶ Downloading pirated apps
- ▶ Unlike viruses and worms, Trojans are not able to self-replicate
- ▶ Sometimes engineered to provide backdoor access to infected systems or download additional malware (downloaders)



Copyright © www.ine.com



Famous Trojan that was first detected in 2014 (and still active today) is Emotet. This particular Trojan is actually capable of self-replication like a worm and is specifically engineered to obtain banking information from you.

-

In February 2018 the Emotet Trojan infected several systems in the City of Allentown, PA forcing them to shutdown many critical infrastructure networks and pay more than \$1M to clean up the problem.

<https://www.mcall.com/news/breaking/mc-nws-allentown-computer-virus-20180220-story.html>

-

A “downloader” is a piece of malware engineered to allow the download of more malware.

Backdoor Viruses

- Malware designed to provide an attacker with unauthorized access to a compromised system
- Often come pre-packaged with additional malware capabilities such as;
 - Screenshot captures
 - Keystroke logging
 - File infection
 - File encryption
- Requires user-intervention in order to be activated



Copyright © www.ine.com



Even genuine programs may have undocumented remote access features.

-

Often, backdoors are installed by other parasites like Trojans, viruses, or even spyware.



Exploits, Key Loggers, Root Kits & Ransomware



Copyright © www.ine.com

Topic Overview

- ▶ What Is An Exploit?
- ▶ Spammers, Key Loggers & Root Kits
- ▶ Ransomware

Exploits

- ▷ Unintentional holes left in software that malicious actors can use to their advantage.
- ▷ Malicious actors scan systems, looking for these holes in order to “exploit” your system.
- ▷ Exploits are classified by the type of vulnerability that can be exploited.
- ▷ Exploits are not malware, but delivery mechanisms for malware

<https://blog.malwarebytes.com/101/2017/03/what-are-exploits-and-why-you-should-care/>

Copyright © www.ine.com



Exploits are ultimately errors in the software development process that leave holes in the software’s built-in security that cybercriminals can then use to access the software and, by extension, your entire computer.

-

Types of exploits are zero-day (attacks on vulnerabilities that aren’t even known by the software developer yet), DoS and XSS (Cross-Site-Scripting in which an attacker somehow injects their own malicious code into the legitimate code of a website, such that when you open the website the attacker has access to some of your data).

Spammers, Key Loggers & Root Kits

- Spammers: Malware designed to create and distribute spam.
- Key Loggers: Malware designed to capture, and transmit, all of your keystrokes on your keyboard with the intent of obtaining passwords, PINs, etc.
- Root Kits: Malware designed to provide administrator access to your OS so it can:
 - Scan your traffic
 - Install other programs
 - Hijack computer resources
 - Enslave the computer in a botnet

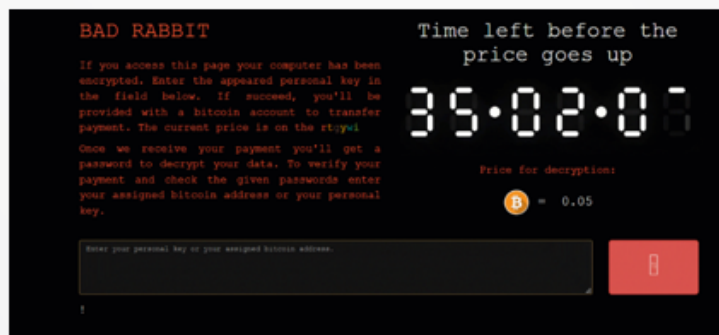


Copyright © www.ine.com

Rootkits - Once installed, it becomes possible to hide the intrusion as well as to maintain privileged access. The key is the root or administrator access. Full control over a system means that existing software can be modified, including software that might otherwise be used to detect or circumvent it. The main goal of a rootkit is concealment. It is not designed to corrupt your files or otherwise visually damage your system (like a Virus) but rather do its work completely undetected.

Ransomware

- ▶ Malware designed to lock-and-encrypt an infected host's data until a ransom is paid to the attacker.
- ▶ Typically spread through Phishing emails or infected websites
- ▶ In 2017 the average ransom demand was US\$522 (Norton.com)



Copyright © www.ine.com



Shown above is a screenshot of the “Bad Rabbit” ransomware attack that hit several countries in Eastern Europe in late 2017. The attackers demanded a payment in Bitcoin of approximately \$280.



Categories Of Endpoint Protection



Copyright © www.ine.com

Topic Overview

- ▶ What Is Endpoint Protection?
- ▶ Categories Of Endpoint Protection

Endpoint Protection

- ▶ Multiple lines-of-defense should be implemented to protect your data;
 - ▶ Firewalls
 - ▶ Routers
 - ▶ Switches
 - ▶ Endpoint protection
- ▶ Endpoint protection relates to protections available on the host device (PC, Laptop, Server, Tablet, Smart Phone, etc)
- ▶ These protection methods typically take the form of software applications.

Categories Of Endpoint Protection

- ▷Antivirus
- ▷Antispyware
- ▷Malware analysis and protection
- ▷Personal Firewalls
- ▷Data & email encryption
- ▷Usage of VPNs



Antivirus & Antimalware



Copyright © www.ine.com

Topic Overview

- ▶ What Are Antivirus/Antimalware Programs?
- ▶ How Do These Programs Work?
- ▶ Examples Of Antivirus/Antimalware Programs
- ▶ Introduction To AMP For Endpoints
- ▶ Introduction To Cisco TALOS

Antivirus, Antimalware & Antispyware Software

- ▶ Within a host, the first line-of-defense should be a good antivirus/antimalware program.
- ▶ These programs detect, prevent and take action to disarm or remove malicious software from your computer
- ▶ Detection of viruses/malware done by:
 - ▶ Signature-based - for specific detection of known malware
 - ▶ Heuristic Detection – Looking at the code of files for suspicious properties
 - ▶ Behavioral-based detection - Looking for suspicious behavior as files are allowed to run

Copyright © www.ine.com



Most antivirus software uses signature-based detection. Antivirus software vendors analyze known malware, and catalog the characteristics that are used to recognize them in a signature database. Scanning files and memory for these signatures reveals the malware.

-

Heuristics can decompile software to reveal its sourcecode, and then see if any of that sourcecode matches the sourcecode of any known malware.

-

Behavioral-based: Is the file attempting to overwrite the registry? Invoke a keystroking-capturing command? Is it trying to modify another executable program?

Antivirus, Antimalware & Antispyware Software

- ▶ Antivirus/antimalware/antispyware software can be obtained freely, for a one-time fee, or on a subscription basis.
- ▶ Examples of commercial and free options include:
 - ▶ avast!
 - ▶ AVG Internet Security
 - ▶ Bitdefender Antivirus Free
 - ▶ ZoneAlarm PRO Antivirus + Firewall and ZoneAlarm Internet Security Suite
 - ▶ F-Secure Antivirus
 - ▶ Kaspersky Anti-Virus
 - ▶ McAfee Antivirus
 - ▶ Panda Antivirus
 - ▶ Sophos Antivirus
 - ▶ Norton Antivirus
 - ▶ ClamAV
 - ▶ Immunet

AMP For Endpoints

- ▶ Cisco AMP = Cisco Advanced Malware Protection
- ▶ Uses a mix of preventative engines and cloud-based intelligence updated by:
 - ▶ Cisco Talos
 - ▶ Cisco Threat Grid
- ▶ AMP for endpoints supports several Operating Systems:
 - ▶ Windows
 - ▶ Mac OS
 - ▶ iOS
 - ▶ Android
 - ▶ Linux

Copyright © www.ine.com



Cisco Talos

- ▶ “The Talos Security Intelligence and Research Group (Talos) is **made up of leading threat researchers** supported by sophisticated systems to **create threat intelligence** for Cisco products that detects, analyzes and protects against both known and emerging threats. Talos maintains the official rule sets of Snort.org, ClamAV, SenderBase.org and SpamCop.”
- ▶ “**Talos is the primary team that contributes threat information to the Cisco Collective Security Intelligence (CSI) ecosystem.** Cisco CSI is shared across multiple security solutions and provides industry-leading security protections and efficacy. In addition to threat researchers, CSI is driven by intelligence infrastructure, product and service telemetry, public and private feeds and the open source community.”

Quotes courtesy of <https://blogs.cisco.com/author/talos>

Copyright © www.ine.com



AMP Dashboard

- ▶ Cisco AMP provides a central, administrator's dashboard to gain overall visibility into the health of your endpoints.
- ▶ AMP provides file and device trajectory which help to identify;
 - ▶ All affected applications, processes and systems
 - ▶ Identify "Patient Zero"
 - ▶ Identify the method and point of entry of malware



Copyright © www.ine.com



AMP continuously analyzes and records all file activity on endpoints, regardless of a file's disposition. At the first sign of malicious behavior, AMP alerts you with an indication of compromise, can automatically block the file, and show you the complete recorded history of the threat across the entire environment.



Personal Firewalls & HIPS



Copyright © www.ine.com

Topic Overview

- ▷ Differences Between Network Firewalls & Personal Firewalls
- ▷ Objectives Of Personal Firewalls
- ▷ How Do Personal Firewalls Protect You?
- ▷ Use Cases For Personal Firewalls
- ▷ What Is HIPS?
- ▷ Common HIPS Rulesets

Personal Firewalls

▷ **Network Firewalls** are typically implemented as hardware appliances.

- ▷ Placed at network security boundaries
- ▷ Designed to protect traffic to/from entire networks (subnets)

▷ **Personal Firewalls**

- ▷ Implemented as software solutions on hosts (PCs, Tablets, etc)
- ▷ Often come integrated into the Operating System
- ▷ Pervasive and consistent use across all hosts can constitute a "Distributed Firewall"
- ▷ Good solution for hosts that are mobile

Copyright © www.ine.com



A distributed firewall requires that the personal firewall policies are controlled by a centralized administration system. A distributed firewall can provide similar protection as a traditional firewall.

Personal Firewall Operation

▶ Two main objectives:

- ▶ Block unauthorized access to your computer
- ▶ Permit authorized data and communications to-and-from your computer

▶ How does it do this?

- ▶ Rules and exceptions are applied to all inbound and outbound traffic
- ▶ Rules are configurable. New rules can be added.
- ▶ Rules can vary depending on the type of network you are connected to
 - ▶ Corporate network
 - ▶ Public Network
 - ▶ Home Network



Copyright © www.ine.com

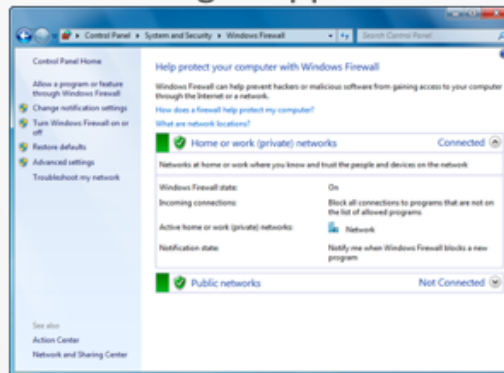


Personal Firewalls typically will ask you (when you connect to a new network) how you want to categorize that network (home, public, etc). This categorization helps it to know what set of rules to apply.

Personal Firewalls – Use Cases

► Use cases:

- Mobile Hosts
- VPNs that utilize split-tunneling
- Whitelisting and blacklisting of application traffic



Copyright © www.ine.com



Mobile Hosts: A host is protected by a network firewall as long as it resides on an inside interface of that firewall. If that host moves between networks it might be placed into a network that is vulnerable and not covered by the network firewall.

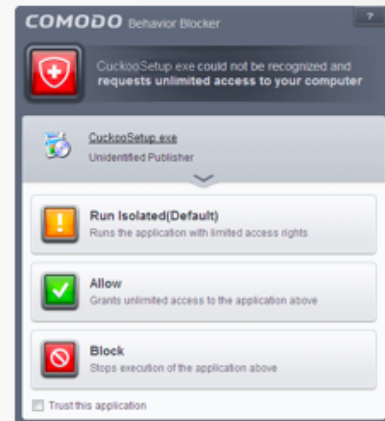
- When a VPN uses split-tunneling, a personal firewall will protect the host from attacks originating from the Internet, and protect against malicious actors on the Internet gaining access to your device...and thus gaining access to your protected VPN network.

- Personal firewalls have the ability to permit and deny traffic based on the application, regardless of the protocols and ports.

HIPS

▶ Host Intrusion Prevention Systems

- ▶ Software packages that monitor a single host for suspicious activity by analyzing events occurring within that host.
- ▶ Malware can be difficult to spot purely based on signatures.
- ▶ HIPS Objective: To stop malware by monitoring the behavior of the code.



Copyright © www.ine.com



Unlike a personal firewall that only determines if inbound/outbound traffic is allowed or denied...a HIPS solution will watch the behavior of applications to see if they are trying to do something suspicious.

-

The normal method of a HIPS is runtime detection. It intercepts actions when they occur, but some HIPS also offer pre-execution detection. This means that the nature of an executable is analyzed before it runs, to check for suspicious behavior.

HIPS Rulesets

▶ HIPS is typically configured to pause the activity of suspected code, and prompt the user for a decision, based on configured rulesets such as:

- ▶ Should new code be allowed to take control of other programs?
- ▶ Should new code be allowed to modify registry keys?
- ▶ Should new code be allowed to terminate existing programs?
- ▶ Should new code be allowed to install drivers?
- ▶ And much more



Email & Data Encryption



Copyright © www.ine.com

Topic Overview

- ▶ The Two Phases Of Securing Email Transactions
- ▶ Email Encryption Techniques
- ▶ Encrypting Data At Rest

Email Encryption

▶ Implementing email encryption involves two phases of encryption

▶ Encryption of data-in-motion

- ▶ Securing the connection to the email server
- ▶ Encrypting transmitted and received emails

▶ Encryption of data-at-rest

- ▶ Encrypting locally-stored emails
- ▶ Encrypting locally-stored data that will be attached to emails

Email Encryption Techniques

- ▶ **Securing the connection to the email server**
 - ▶ Utilize HTTPS when connecting to web-based email services
 - ▶ Utilize SSL/TLS for local email services such as Microsoft Outlook
- ▶ **Encrypting emails-in-transit**
 - ▶ Pretty Good Privacy (PGP)
 - ▶ GNU Privacy Guard (GnuPG)
 - ▶ Secure/Multipurpose Internet Mail Extensions (S/MIME)
 - ▶ Web-based encryption e-mail service like Sendinc or JumbleMe
- ▶ **All email encryption methods require creation of Public/Private encryption keys and exchange of the Public key with your email peers (sometimes via Digital Certificates).**

Encrypting Data-At-Rest

- ▶ If an endpoint is stolen, data on the hard drive can be scanned to identify sensitive information.
- ▶ This data should be encrypted
- ▶ Some Operating Systems natively support HDD/SSD encryption such as Mac OS
- ▶ Other Operating Systems require downloading and using special encryption software.
 - ▶ BitLocker
 - ▶ TrueCrypt
 - ▶ Credant
 - ▶ VeraCrypt and others

Copyright © www.ine.com



Since 2018, Mac laptops have included a special chip called the T2, and SSD (Solid State Drive) controller that (among other things) automatically encrypts all files on your drive with AES-256 encryption.

Macs also have a feature called FileVault which adds password-protection to your encrypted computer. Thanks to the new SSD controller, the T2 automatically encrypts your drive regardless of whether you have FileVault on or not. Apple recommends that you do enable it, however, for added security. Without FileVault, your encrypted SSDs will automatically mount and decrypt without a password when connected to your Mac.



VPNs On Endpoints



Copyright © www.ine.com

Topic Overview

- ▶ Categories Of VPNs
- ▶ Site-To-Site VPNs
- ▶ Remote-Access VPNs

Utilizing VPNs

- ▶ Data-in-motion can be protected by sending it through VPNs.
- ▶ VPN = Virtual Private Network
- ▶ Different types of VPNs exist, some of which are designed to provide confidentiality, and some don't;

Copyright © www.ine.com



VPN technologies that don't include built-in confidentiality (i.e. encryption) are primarily used to tunnel data/protocols across networks that normally wouldn't support that data/protocol in its native format. Or to ensure the separation of paths (that data streams from Company-A will never accidentally end up on Company-B's network).

Categorizing VPNs

▷ Site-to-site VPNs

- ▶ Typically implemented on network infrastructure devices as the VPN endpoints (Routers or Firewalls)
- ▶ Used to establish VPN tunnels between two or more organizations
- ▶ Transparent to end users

▷ Remote-access VPNs

- ▶ Enable end users to securely connect to remote, corporate resources when working-from-home, traveling, etc.
- ▶ May require special software on the end user device (if using IPsec) or could be browser-based (if using SSL/TLS)

