Intrusion Detection and Prevention Systems and Malware

CS-3113: PRINCIPLES OF CYBER SECURITY

BENJAMIN R. ANDERSON

Definitions

From the *Certified Information Systems Security Professional Official Study Guide, Ninth Edition* by Chapple, Stewart, and Gibson (OSG):

- ***Intrusion****: Occurs when an attacker can bypass or thwart security mechanisms and access an organization's resources*
- ***Intrusion Detection****: A specific form of monitoring that monitors events (often in real time) to detect abnormal activity indicating a potential incident or intrusion*
- ***Intrusion Detection System (IDS)****: Automates the inspection of logs and real-time system events to detect intrusion attempts and system failures.*
- ***Intrusion Prevention System (IPS)****: Includes all the capabilities of an IDS but can also take additional steps to stop or prevent intrusions. If desired, administrators can disable an IPS's extra features, essentially causing it to function as an IDS.*
    - Note*: Because an IPS includes detection capabilities, you will often see them referred to as intrusion detection and prevention systems (IDPSs)*

Definitions

From the *Certified Information Systems Security Professional Official Study Guide, Ninth Edition* by Chapple, Stewart, and Gibson (OSG):

- ***Knowledge-Based Detection****: The most common method of detection is knowledge-based detection (also called signature-based detection or pattern-matching detection). It uses a database of known attacks developed by the IDS vendor.*
- ***Behavior-Based Detection****: Also called statistical intrusion detection, anomaly detection, and heuristics-based detection). Behavior-based detection starts by creating a baseline of normal activities and events on the system. Once it has accumulated enough baseline data to determine normal activity, it can detect abnormal activity that may indicate a malicious intrusion or event.*

Definitions

From the *Certified Information Systems Security Professional Official Study Guide, Ninth Edition* by Chapple, Stewart, and Gibson (OSG):

- ***True Positive:*** *An incident occurs and is detected*
- ***False Negative:*** *An incident occurs and is not detected*
- ***False Positive:*** *An incident is detected but did not occur*
- ***True Negative:*** *An incident does not occur and is not detected*

	Detected	**Not Detected**
Incident Occurred	True Positive	False Negative
No Incident	False Positive	True Negative

Note: These are critical definitions to know.

Definitions

From the *Certified Information Systems Security Professional Official Study Guide, Ninth Edition* by Chapple, Stewart, and Gibson (OSG):

- ***Passive Response:*** *Notifications can be sent to administrators in different ways such as via email or text messages. In some cases, the alert can generate a report detailing the activity leading up to the event, and logs are available for administrators to get more information if needed.*
  - Note*: Network operations centers (NOCs) have central monitoring screens viewable by everyone in the main support center.*
- ***Active Response****: Can modify the environment using several different methods. Typical responses include modifying firewall ACLs to block traffic based on ports, protocols, and source addresses, and even disabling all communications over specific cable segments. For example, if an IDS detects a SYN flood attack from a single IP address, the IDS can change the ACL to block all traffic from this IP address.*

Definitions

From the *Certified Information Systems Security Professional Official Study Guide, Ninth Edition* by Chapple, Stewart, and Gibson (OSG):

- ***Host-Based IDS (HIDS):*** *An HIDS monitors activity* ***on a single computer****, including process calls and information recorded in system, application, security, and host-based firewall logs. It can often examine events in more detail than an NIDS can, and it can pin-point specific files compromised by an attack.*
- ***Network-Based IDS (NIDS)****: An NIDS monitors and* ***evaluates network activity*** *to detect attacks or event anomalies. A single NIDS can monitor a large network by using remote sensors to collect data at key network locations that send data to a central management console such as a security information and event management (SIEM) system.*
- ***Security Information and Event Management (SIEM)****: These tools provide centralized logging and real-time analysis of events occurring on systems throughout an organization. They include agents installed on remote systems that monitor for specific events known as alarm triggers. When the trigger occurs, the agents report the event back to the central monitoring software.*

Definitions

From the *Certified Information Systems Security Professional Official Study Guide, Ninth Edition* by Chapple, Stewart, and Gibson (OSG):

- ***Sandboxing:*** *Provides a security boundary for applications and prevents the application from interacting with other applications. Antimalware applications use sandboxing techniques to test unknown applications.*
- ***Logging:*** *The process of recording information about events to a log file or database. Logging captures events, changes, messages, and other data describing activities on a system. Logs will commonly record details such as what happened, when it happened, where it happened, who did it, and sometimes how it happened.*
- The main types of logs are:
  - Security Logs
  - System Logs
  - Application Logs
  - Firewall Logs
  - Proxy Logs
  - Change Logs

Definitions

From the *Certified Information Systems Security Professional Official Study Guide, Ninth Edition* by Chapple, Stewart, and Gibson (OSG):

- ***Security Logs:*** *Security logs record access to resources such as files, folders, printers, and so on. For example, they can record when a user accessed, modified, or deleted a file.*
- ***System Logs:*** *System logs record system events such as when a system starts or stops, when services start or stop, or when service attributes are modified. If attackers are able to shut down a system and reboot it with a CD or USB flash drive, they can steal data from the system without any record of the data access.*
- ***Application Logs:*** *There logs record information for specific applications. Application developers choose what to record in the application logs.*
- ***Firewall Logs:*** *Can record events related to any traffic that reaches a firewall. This includes traffic that the firewall allows and traffic that the firewall blocks.*
- ***Proxy Logs:*** *Improve internet access performance for users and can control what websites users can visit. Proxy*
- ***Change Logs:*** *Record change requests, approvals, and actual changes to a system as part of an overall change management process.*

Definitions

From the *Certified Information Systems Security Professional Official Study Guide, Ninth Edition* by Chapple, Stewart, and Gibson (OSG):

- ***Audit Trails:*** *Records created when information about events and occurrences is stored in one or more databases or log files. They provide a record of system activity and can reconstruct activity leading up to and during security events.*
- ***Monitoring****: The process of reviewing information logs, looking for something specific.*
- ***Log Analysis:*** *A detailed and systematic form of monitoring in which the logged information is analyzed for trends and patterns as well as abnormal, unauthorized, illegal, and policy-violating activities. Log analysis isn't necessarily in response to an incident but instead a periodic task, which can detect potential issues.*

Definitions

From the *Certified Information Systems Security Professional Official Study Guide, Ninth Edition* by Chapple, Stewart, and Gibson (OSG):

- ***Security Orchestration, Automation, and Response (SOAR):*** *Refers to a group of technologies that allow organizations to response to some incidents automatically.*

SOAR systems often use playbooks and runbooks:

- ***Playbook****: A document or checklist that defines how to verify an incident. Additionally, it gives details on the response.*
  - *A playbook for a SYN flood attack would list the same actions security administrators take to verify a SYN flood is under way. It would also list the steps administrators take after verifying it is a SYN flood attack*
- ***Runbook****: Implements the playbook data into an automated tool.*
  - For example, it would identify how an IDPS would detect a SYN flood
    - Ex: Number of SYNs and number of completed TCP handshakes
  - It would then respond in a specific way
    - Ex: Start recycling half-open TCP connections (oldest first) – it should only take a few seconds to complete the TCP handshake, so any connections that are older than that are probably spoofed packets

IDS and IPS

That completes definitions – for now

One key thing to note: A network-based IPS (NIPS) must be in-line of the network path in order to ***prevent*** an attack

- A NIPS that is out-of-band may be able to alter firewall rules, or system behavior to stop an attack from continuing, but it can’t prevent the beginning of the attack
    - Some attacks only require a single packet to execute
    - This means an out-of-band NIPS cannot prevent it
- However, being in-line can be done logically instead of physically
    - For example, a mail server may receive incoming email but not process it until it send it through the NIPS – or any other analysis engine
    - So, while the NIPS may not be on the physical network path, it is on the logical network path, and can prevent the attacks

Detection Strategies

Knowledge-based strategy:

- This is based on signatures
- For example, it could identify that a packet that had a “jndi:ldap” or “jndi:rmi” is probably a Log4Shell attack

Behavior-based strategy has two general approaches: Anomalies and abnormal behavior

- Anomalous behavior (anomalies) are activities that are known to be bad
  - Trying to telnet into a Domain Controller
  - Remote access request from Russia
- Abnormal behavior are activities that a user generally doesn’t do
  - Multiple logins at 3:00 am
  - However, one user’s anomalies may be another user’s normal behavior – a global company may have offices in sensitive countries that log into the corporate LAN

Detection Strategies

There are several approaches to identifying malicious behavior:

- ***User Profiling***: The user's pattern of behavior is observed and established over a period of time. Each user tends to use certain commands more than others, routinely access the same files, login at certain times and at specific frequencies, and executes the same programs.
- ***Intruder Profiling***: Intruder profiling attempts to define the actions that an intruder will take when unauthorized access is obtained.
    - For example: when an intruder first gains access, the action often taken is to check to see who else is on, examine files and directories, etc…
    - ***One of these is search for a file named "password" or "passwords"***
- ***Human Signature Analysis***: This is used to verify the user is who they claim to be, and often using typing patterns. (Speed, accuracy, time between keystrokes, etc.)
- ***Action-based (attack "signatures"):*** Action-based techniques look for specific activities or actions (known as attack signatures) that are indicative of intrusive activity
    - For example: a user attempts to exploit known security holes

False Positive Paradox

From Wikipedia:

- *https://en.wikipedia.org/wiki/Base_rate_fallacy#False_positive_paradox*
- *An example of the base rate fallacy is the false positive paradox. This paradox describes situations where there are more false positive test results than true positives. For example, if a facial recognition camera can identify wanted criminals 99% accurately, but analyzes 10,000 people a day, the high accuracy is outweighed by the number of tests, and the program's list of criminals will likely have far more false positives than true.*
- In this case, at 99% accuracy, there would be 100 false positives a day – which would look just like a true positive and have to be investigated
- When scaled up to millions of people or interactions, 99% is unworkable

In the 2013 Target breach, the IDS did alert on the malware – however, it was just one alert out of thousands the system produced each day and was lost in the chaos

The ultimate challenge with an IDS is making sure you detect as many attacks as you can (minimize false negatives), while keeping the number of false positives manageable

Snort

From the Snort website:

- *Snort is the foremost Open Source Intrusion Prevention System (IPS) in the world. Snort IPS uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generates alerts for users.*
- *Snort can be deployed inline to stop these packets, as well. Snort has three primary uses: As a packet sniffer like tcpdump, as a packet logger — which is useful for network traffic debugging, or it can be used as a full-blown network intrusion prevention system. Snort can be downloaded and configured for personal and business use alike.*
- https://www.snort.org/

Snort Rules

A sample snort rule follows:

- The text up to the first parenthesis is the rule header and the section enclosed in parenthesis is the rule options.

```
alert tcp any any ->
192.168.1.0/24 111 \ (content:" |
00 01 86 a5| "; msg: "mountd
access";)
```

- In this rule an alert including the message "mountd access" will be generated if a tcp packet is:
- ***Received from***:
  - Any IP address using any port
- ***Going to***:
  - Any address in the range 192.168.1.0-255 (/24 signifies the entire range) ***and*** on port 111
- ***With the binary contents***:
  - |00 01 86 a5| (represented here in hexadecimal).

For more information regarding Snort rules, you can consult:

Snort documentation:

- http://manual-snort-org.s3-website-us-east-1.amazonaws.com/

Infosec Institute article:

- https://resources.infosecinstitute.com/topic/snort-rules-workshop-part-one/

Honeypots and Honeynets

Honeypots and Honeynets are the computer/network version of a mousetrap

- The system is there, and looks interesting, so it draws in the attacker
- However, the system isn't used for normal operations, so anyone accessing it is probably an attacker
- This allows an attacker to be identified, monitored, and their behavior analyzed

One major project in this area is the Honeynet Project:

- *The Honeynet Project is a leading international 501c3 non-profit security research organization, dedicated to investigating the latest attacks and developing open source security tools to improve Internet security. With Chapters around the world, our volunteers have contributed to fight against malware (such as Confickr), discovering new attacks and creating security tools used by businesses and government agencies all over the world.*
- https://www.honeynet.org/about/

Honeypots and Honeynets

A similar project that has been previously mentioned is the HADES project from Sandia National Labs

More information on HADES, and the efforts they take to create a realistic environment to occupy and profile an attacker can be found at the following links:

- https://ip.sandia.gov/techpdfs/HADES.pdf
- https://newsreleases.sandia.gov/misleading-hackers/

Malicious Software

Malware is simply a contraction from ***Mal***icious Soft***ware***

Refer back to Lesson 0, slides 7-9 for the definitions of various types of malware

- You will be responsible for knowing the different types of malware

Viruses

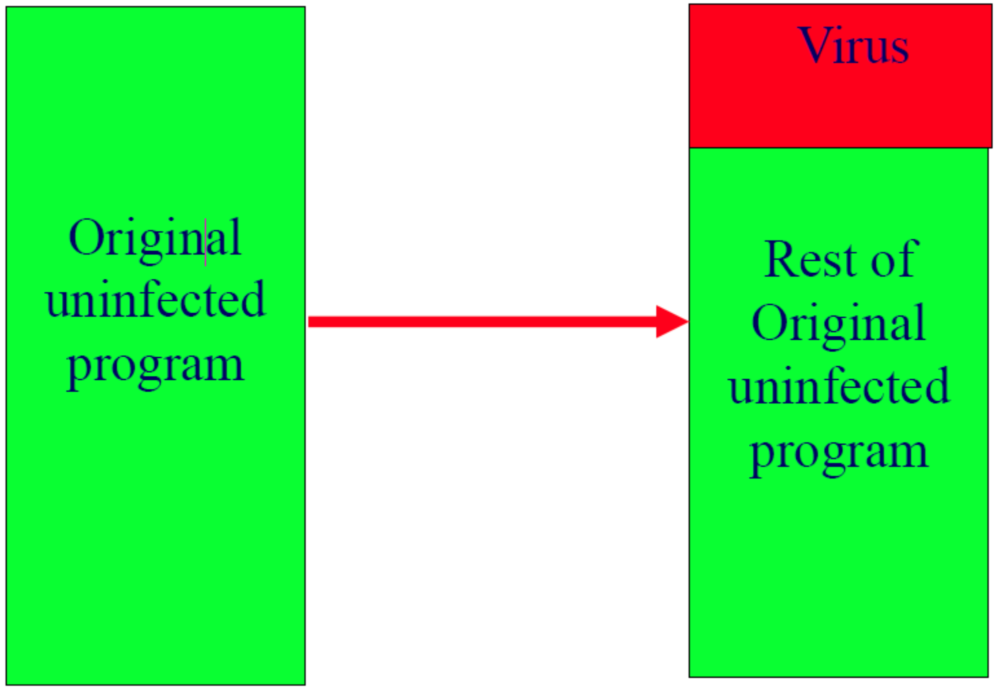
Traditionally, viruses must attach themselves to another program

They usually contain a malicious code segment which may not be immediately noticed

There are 3 major “types” of viruses:

- ***Boot***: Computer operating systems set aside a portion of each disk for code to boot the computer. Boot Viruses (or System infectors) store themselves in this area and hence are invoked whenever the disk is used to boot the system.
- ***Program***: These contaminate files that contain computer code, especially .EXE and .COM files but also .SYS and .DLL.
- ***Macro***: These viruses hide themselves in normal documents (such as Microsoft Office) and use built in macros or scripting abilities to execute
  - ***Note***: A Microsoft Office file ending with “x” such as .docx or .xlsx cannot be used to store macros – however, an Office Template file can have macros – and can also be saved with the “x” in the extension. ***Be careful what you trust!***

Viruses – Insertion Into Files

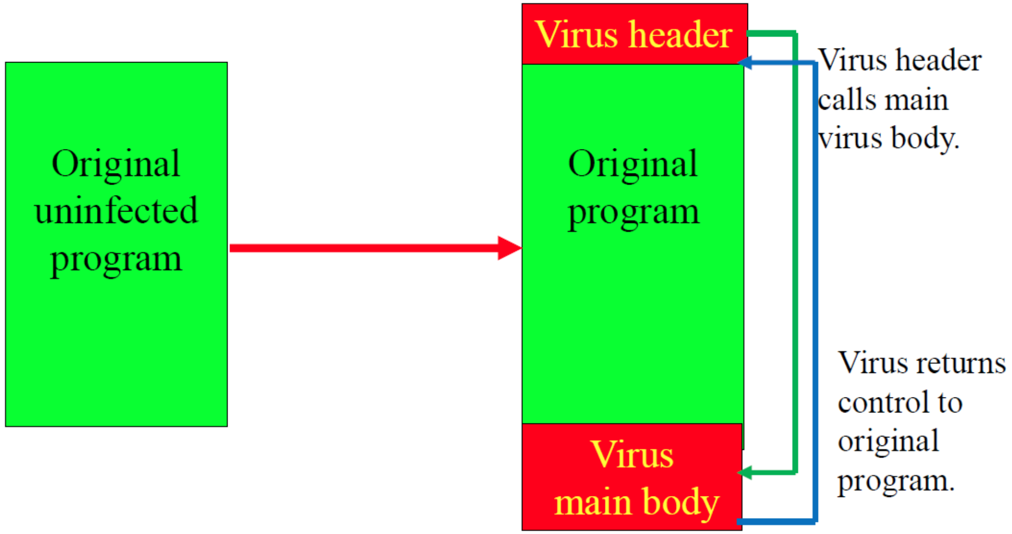


Original uninfected program

Virus

Rest of Original uninfected program

File Infection: Overwriting



Original uninfected program

Virus header

Original program

Virus main body

Virus header calls main virus body.

Virus returns control to original program.

File Infection: Appending

Slammer Worm

Read: *The Spread of the Sapphire/Slammer Worm* from CAIDA:

- https://www.caida.org/catalog/papers/2003_sapphire/

From the article:

- *The Sapphire Worm was the fastest computer worm in history. As it began spreading throughout the Internet, it doubled in size every 8.5 seconds. It infected more than 90 percent of vulnerable hosts within 10 minutes.*
- *The worm infected at least 75,000 hosts, perhaps considerably more, and caused network outages and such unforeseen consequences as canceled airline flights, interference with elections, and ATM failures. Several disassembled versions of the source code of the worm are available.*

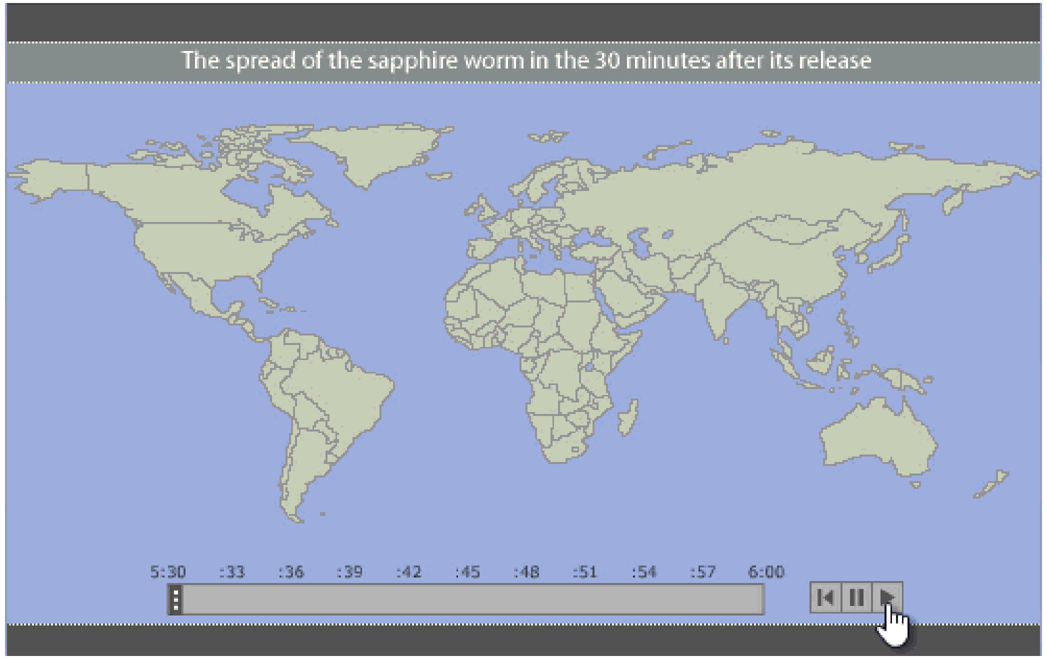
One of the problems with the flood of traffic from Slammer was that administrators could not get remote access to their systems

- They had no choice but to physically go to the systems to shut them down and apply the patches
- This greatly slowed the recovery process

Slammer Worm

From: https://www.caida.org/catalog/papers/2003_sapphire/

The GIF shows just how quickly the worm spread to vulnerable hosts


The spread of the sapphire worm in the 30 minutes after its release

Advanced Virus Characteristics

As malware defenses improve, the virus writers and attackers update their techniques to evade the updated defenses

It is like a chess game where each side adapts to what the other player is doing

Some common techniques used by virus writers are:

Stealth:

- Viruses to some degree all attempt to conceal their presence in order to maximize their chance of spreading
- APTs have been known to have malware "sleep" for over a year to ensure that, if other activities are detected, they still have a way in

Polymorphism:

- Viruses that attach an evolved copy of themselves to the new host instead of making an exact copy. They "morph".
- This prevents basic malware signatures from detecting the virus – each one is slightly different

Encryption:

- Some viruses encrypt their payload. The only part "in the clear" is the decryption routine.
- Since the ciphertext payload depends on the key used, it is trivial to have every version of the virus payload to have a different signature
- Some don't even have the key for the payload – they must retrieve it from the internet. This prevents analysis of the payload, or at least makes it more difficult.

Anti-Analysis Techniques:

- An evolution of using encryption, this makes it even harder for an analyst to study the virus/malware.
- For example, before executing an encrypted or obfuscated payload, the malware may try to determine if it is running in a virtual machine or other sandboxed environment. If it is, it executes an entirely different path than normal. Or it just never tries to retrieve the decryption key.
- It can also check the system for malware analysis tools or debuggers as part of its checks.
- While this may not stop analysis of the malware, it makes it a lot harder for the analyst, giving them a larger window where their malware is effective

The Morris Worm

We discussed Robert Morris back in Lesson One

- In 1988, while a student at Cornell University, wrote an internet worm (now called “The Morris Worm”)

Read: *Morris Worm* from Wikipedia:

- https://en.wikipedia.org/wiki/Morris_worm

From the article:

- *The worm exploited several vulnerabilities to gain entry to targeted systems, including:*
  - *A hole in the debug mode of the Unix sendmail program*
  - *A buffer overflow or overrun hole in the fingerd network service*
  - *The transitive trust enabled by people setting up network logins with no password requirements via remote execution (rexec) with Remote Shell (rsh), termed rexec/rsh*
- *The worm also functioned through the exploit of weak passwords.*
- *The Internet was partitioned for several days, as regional networks disconnected from the NSFNet backbone and from each other to prevent recontamination whilst cleaning their own networks.*

Imagine the impact today if the Internet was forced to split into several, separate networks

Botnets

Read: *What is a Botnet?* by PaloAlto Networks:

- https://www.paloaltonetworks.com/cyberpedia/what-is-botnet
- You are responsible for knowing:
  - Common botnet actions (email spam, DDoS, Financial Breaches, Targeted Intrusions) and their general descriptions
  - Definitions for botnet and botherder: *A botnet (short for "robot network") is a network of computers infected by malware that are under the control of a single attacking party, known as the "bot-herder."*
  - Communication between the bots, bot-herder, and the command-and-control systems (see diagram)

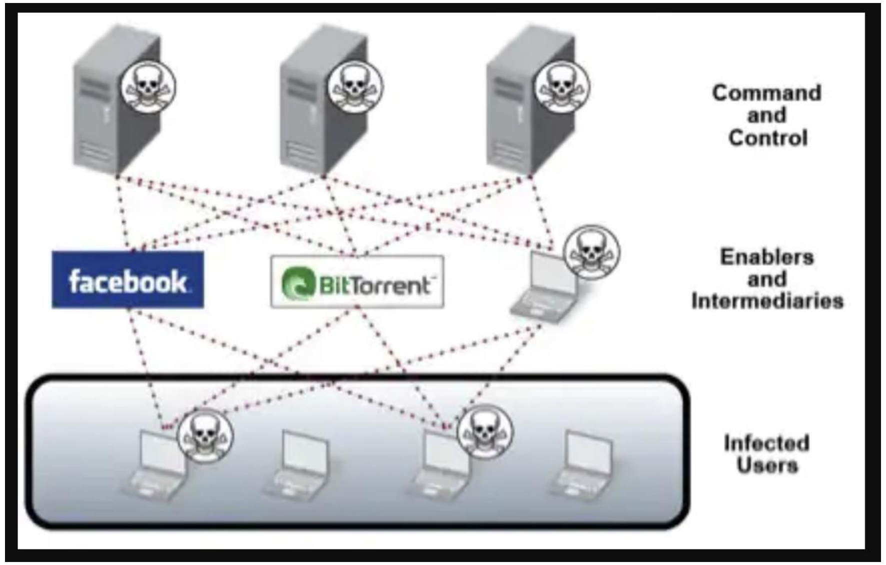


Image from: What is a Botnet? By PaloAlto Networks

Ransomware

Right now, ransomware is one of the biggest issues in cybersecurity (and probably will be for the foreseeable future)

Definition from Heimdal Security:

- *Ransomware is a type of malware that blocks users from accessing their operating system or files until a ransom is paid. It does so by locking the system's screen or encrypting the users' files.*
- https://heimdalsecurity.com/blog/ransomware/

Other than the objective, ransomware is just like any other malware

- It can use any attack vector – malicious website, email attachment, etc.
- It can use any vulnerability – once it gains control over a system, there is nothing to stop it from encrypting files
- It can use evasion techniques, or hibernate for months – this ensures it infects backups, impacting restoration operations

Ransomware

There are many variants to the ransomware attack known as single, double, and triple-ransomware (or extortionware)

- ***Single or "regular" ransomware***: Files are encrypted, and you must pay the attacker for the decryption key
- ***Double-ransomware***: On top of the single ransomware the attacker also threatens to publish private information – such as business documents and emails – unless they are paid.
  - This is a little more difficult since the attackers must exfiltrate all of the information in addition to encrypting it
- ***Triple-ransomware***: On top of the double-ransomware, the attackers threaten the organization's customers or business partners with releasing the information
  - This requires even more overhead since the information has to be analyzed to see what organizations would be impacted
  - However, since each organization is, effectively, another successful ransomware campaign – it is often worth it to the attacker

You are responsible for knowing these definitions

Double Ransomware Attack Sequence

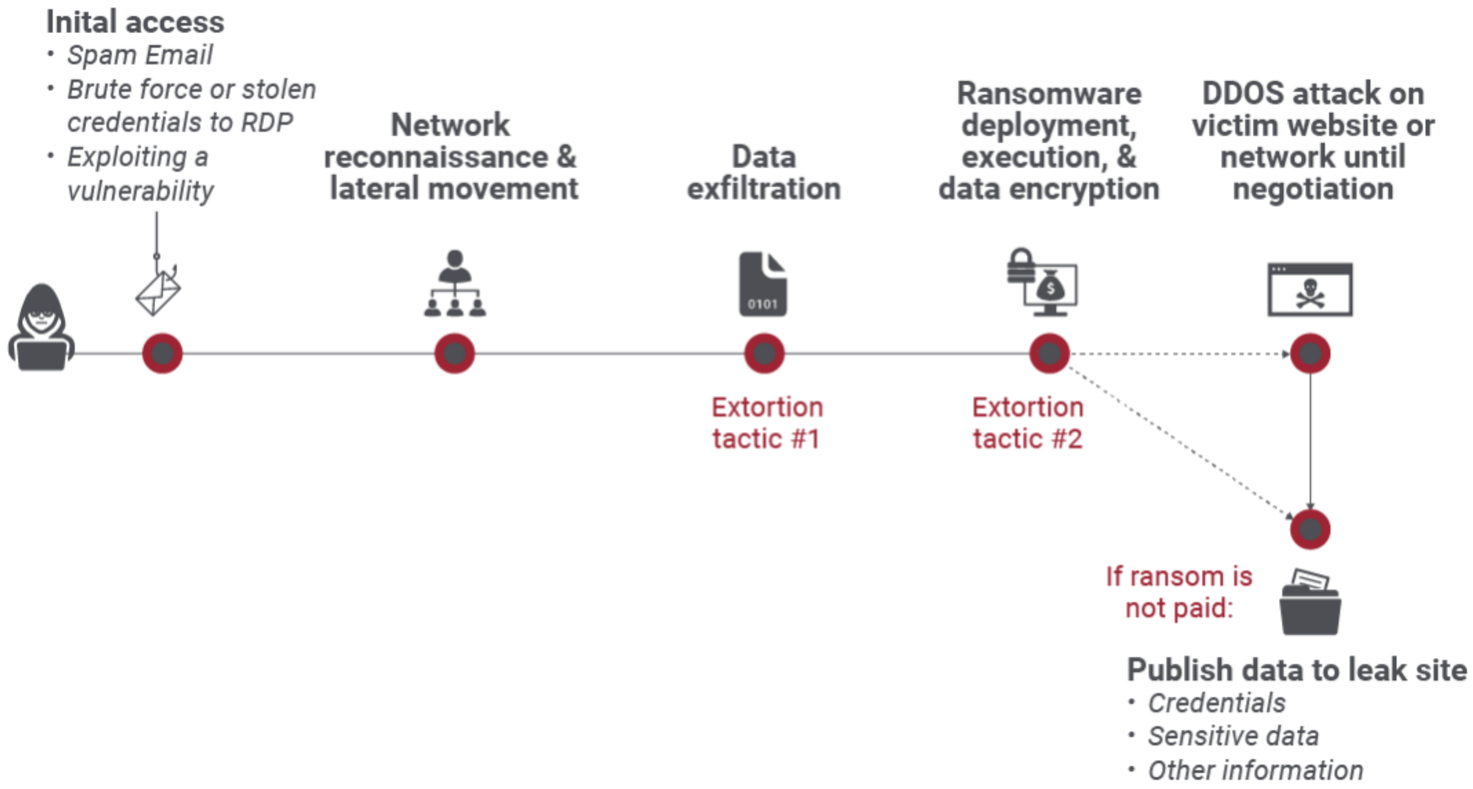

Inital access
• Spam Email
• Brute force or stolen credentials to RDP
• Exploiting a vulnerability
Network reconnaissance & lateral movement
Data exfiltration
0101
Ransomware deployment, execution, & data encryption
DDOS attack on victim website or network until negotiation
Extortion tactic #1
Extortion tactic #2
If ransom is not paid:
Publish data to leak site
• Credentials
• Sensitive data
• Other information

Image from: What is Double Extortion Ransomware? By Zscaler: https://www.zscaler.com/resources/security-terms-glossary/what-is-double-extortion-ransomware

Major Ransomware Variants

Read: *Ransomware: Notable Software Packages* by Wikipedia:

- https://en.wikipedia.org/wiki/Ransomware#Notable_software_packages
- Focus on: WannaCry, Petya (and NotPetya), DarkSide, and Ransomware-as-a-Service (RaaS)
- You should know:
  - WannaCry used the EternalBlue exploit vector allegedly leaked by the NSA
  - A Petya variant was used in cyberattacks on Ukraine
  - DarkSide involved Colonial Pipeline
  - RaaS is associated with the group Revil

Given the importance of ransomware in the threat landscape today, I encourage you to read all of the articles referenced in these slides – and follow the links for the specific ransomware packages that I listed above

Protecting Against Ransomware

The #1 protection against ransomware:

- Make sure you have offline backups of your critical information and assets – ***and can restore them***
- Online backups can be affected by sync processes – but a ***clean*** offline backup is protected
  - Just make sure you physically protect it
  - Also make sure you can restore from the backup

Here is an article with some best practices on protecting an organization from ransomware:

- *15 ways to protect your company from Ransomware attacks* by Red Level:
- https://redlevelgroup.com/ransomware-attacks-are-on-the-rise-15-ways-to-protect-your-company/
- Note that their first item is: *Back up your data, system images, and configurations, regularly test them, and keep the backups offline.*

CISA also has a ransomware guide: https://www.cisa.gov/stopransomware/ransomware-guide

- Their first item is: *It is critical to maintain offline, encrypted backups of data and to regularly test your backups.*