Understanding and Analyzing Malicious Activity

A High School Introduction to Cybersecurity Threats

Cybersecurity Fundamentals

March 8, 2025

Understanding Cybersecurity Threats: An Introduction

- Cybersecurity threats are intentional actions designed to compromise digital systems and information.
- **Malicious activity** refers to any action intended to harm, disrupt, or gain unauthorized access to computer systems.
- Almost 80% of organizations experienced at least one successful cyber attack in the past year.
- Understanding different types of threats is the first step in effective defense.
- This presentation covers the major categories of cybersecurity threats and how to identify them.

The Importance of Recognizing Malicious Activity

Why Detection Matters

Early detection of threats can significantly reduce damage and recovery costs.

- The average data breach costs organizations over $4 million in damages and recovery.
- **Threat indicators** are observable evidence that an attack may be in progress.
- Most successful attacks show warning signs before major damage occurs:
  - Unusual network traffic patterns
  - Unexpected system behavior
  - Anomalous login activities
  - Suspicious file modifications
- Building a "security mindset" helps protect both organizations and individuals.

Key Threat Categories in the Digital World

Category	Examples
Malware	Ransomware, Trojans, Viruses
Physical	Brute force, RFID cloning
Network	DDoS, DNS attacks, Wireless
Application	Injection, Buffer overflow
Cryptographic	Downgrade, Collision attacks

- Each category exploits different vulnerabilities within digital systems.
- Attackers often combine multiple attack vectors for maximum impact.
- Defenses must address all categories to be effective.

Example

In 2017, the WannaCry ransomware attack affected over 200,000 computers across 150 countries, showing how quickly digital threats can spread globally.

Basic Concepts in Threat Identification

The Security Triad

Confidentiality, **Integrity**, and **Availability** form the core principles of information security.

- **Threat actors** are individuals or groups who initiate attacks:
  - Nation-states
  - Cybercriminals
  - Hacktivists
  - Insiders
- **Attack vectors** are pathways used to gain unauthorized access.
- **Vulnerabilities** are weaknesses that can be exploited.
- **Indicators of compromise (IoCs)** are evidence that an attack has occurred.

Ransomware: When Your Data Is Held Hostage

- **Ransomware** is malicious software that encrypts victim's files and demands payment for the decryption key.
- Common infection vectors include:
  - Phishing emails with malicious attachments
  - Drive-by downloads from compromised websites
  - Exploiting unpatched security vulnerabilities
- Modern ransomware employs strong encryption that makes recovery without the key virtually impossible.
- Attackers typically demand payment in cryptocurrency to maintain anonymity.

Prevention Focus

Regular backups stored offline are one of the best defenses against ransomware attacks.

Trojans: Deceptive Packages with Hidden Dangers

Trojan Type	Primary Function
Banking	Steal financial credentials
RAT	Remote Access/Control
Downloader	Install additional malware
Backdoor	Create persistent access
Spyware	Monitor user activity

- **Trojan horses** are malware disguised as legitimate software to trick users into installation.
- Unlike viruses, Trojans do not self-replicate but rely on user deception.
- They're often distributed through social engineering tactics that exploit trust.

Example

Michael Scott downloaded what he thought was a free screen saver, but it was actually a Trojan that gave hackers access to Dunder Mifflin's customer database.

Worms: Self-Replicating Digital Threats

Key Characteristic

The defining feature of worms is their ability to spread automatically without user interaction.

- **Computer worms** are standalone malware that replicate and spread across networks without requiring host files.
- Worms exploit network vulnerabilities to propagate rather than attaching to programs.
- Impact of worm infections:
  - Network bandwidth consumption
  - System resource depletion
  - Service disruption
  - Delivery of secondary payloads
- The rapid spread makes worms particularly dangerous for large organizations.

Spyware: When Someone Is Watching

- **Spyware** is malicious software designed to gather information without the user's knowledge.
- Common information targets:
  - Browsing history
  - Login credentials
  - Financial details
  - Personal messages
- Often remains hidden while monitoring activity.

Warning Signs

- System slowdowns
- Unexpected pop-ups
- Browser changes
- Strange network activity
- Battery drain (mobile)

Bloatware: Resource Drain and Hidden Risks

- **Bloatware** refers to unwanted software that consumes excessive system resources while providing limited value.
- While not always malicious, bloatware can contain hidden components that compromise security.
- Common sources of bloatware:
  - Pre-installed on new devices
  - Bundled with other software downloads
  - Adware installations
  - Trial software that remains after expiration
- Some bloatware collects user data for advertising purposes without clear disclosure.

Gray Area Threat

Bloatware exists in a gray area between legitimate software and malware, making it challenging to classify and address.

Viruses: How They Infect and Spread

- **Computer viruses** are malicious programs that replicate by inserting copies into other programs.
- Require a host file and user action to spread between systems.
- Unlike worms, viruses need a "host" application and cannot propagate independently.

Virus Type	Behavior
Boot sector	Infects startup code
File infector	Attaches to executables
Macro	Uses document macros
Polymorphic	Changes its code

Example

Leslie Knope opened an email attachment about a "Parks Award," accidentally releasing a virus that replaced all documents on the Parks Department server with pictures of raccoons.

Keyloggers: Tracking Every Keystroke

Privacy Invasion

Keyloggers can capture sensitive information including passwords, credit card numbers, and private communications.

- **Keyloggers** are surveillance tools that record keystrokes made by a computer user.
- Implementation methods:
  - Software applications
  - Browser extensions
  - Hardware devices (USB or keyboard adapters)
  - Firmware modifications
- Malicious keyloggers are often installed through phishing, social engineering, or bundled with other malware.
- Modern keyloggers may also capture screenshots, monitor clipboard content, and track browsing activity.

Logic Bombs: Time-Triggered Attacks

- **Logic bombs** are malicious code segments programmed to execute when specific conditions are met.
- Common trigger conditions:

Trigger Type	Example
Temporal	Specific date/time
Logical	File presence/absence
Quantitative	Login count threshold
Environmental	Network connection status

- Often planted by insiders with programming access, making them difficult to detect.
- Logic bombs can lie dormant for extended periods before activation.
- Common payloads include data deletion, encryption, or creating backdoor access.

Detection Challenge

Because logic bombs remain inactive until their trigger condition, they often evade traditional security scanning.

Rootkits: Hidden Deep in Your System

- **Rootkits** are collections of tools designed to gain and maintain unauthorized administrator-level access.
- They operate at the lowest levels of the operating system, making detection extremely difficult.
- Rootkits can modify system files and processes to hide their presence from security software.
- They often create persistent backdoors that survive system reboots and software updates.

Type	Target
User-mode	Applications
Kernel-mode	OS core
Bootkit	Boot process
Firmware	Hardware

Stealth Threat

The primary danger of rootkits is their ability to remain undetected while enabling ongoing system compromise.

Brute Force Attacks: Breaking Down the Door

What Is a Brute Force Attack?

A systematic attempt to discover passwords or keys by trying all possible combinations until the correct one is found.

- **Brute force attacks** attempt to gain unauthorized access by systematically trying all possible combinations.
- Common targets:
  - Login credentials
  - Encryption keys
  - PIN codes
  - API keys
- Success depends on computing power and the complexity of the target password or key.
- Modern systems typically implement countermeasures like account lockouts and rate limiting.

Time to Crack

A password with complexity of:

RFID Cloning: Digital Identity Theft

- **Radio-frequency identification (RFID)** technology uses electromagnetic fields to identify and track tags attached to objects.
- **RFID cloning** involves copying data from a legitimate RFID tag to create an unauthorized duplicate.
- Common targets:

Target	Use Case
Access cards	Building entry
Credit cards	Contactless payment
Passport chips	Border control
Product tags	Inventory tracking

- Attackers can use specialized readers to capture RFID data from several feet away without physical contact.
- Cloned tags can be used to gain unauthorized physical access or make fraudulent transactions.

Example

Jim Halpert noticed his office access card worked even after he

Environmental Attacks: Exploiting Physical Vulnerabilities

Physical Security Matters

Even the strongest digital security can be compromised if physical access controls are inadequate.

- **Environmental attacks** exploit physical conditions and surroundings of computing systems.
- Categories of environmental attacks:
  - **Temperature manipulation**: Overheating or cooling systems to cause failures
  - **Power attacks**: Deliberate power surges, cutting power during critical operations
  - **Electromagnetic attacks**: Using EM radiation to interfere with or monitor devices
  - **Acoustic attacks**: Using sound to extract information from certain devices
- Social engineering often accompanies these attacks to gain initial physical access.

DDoS Attacks: Overwhelming the Target

- **Distributed Denial of Service (DDoS)** attacks aim to make online services unavailable by overwhelming them with traffic.
- Unlike regular DoS attacks, DDoS utilizes multiple compromised computer systems as attack sources.
- These attacks can generate hundreds of gigabits per second of malicious traffic.
- Common targets include websites, online services, and DNS providers.

Layer	**Attack Type**
Network	ICMP Flood
Transport	SYN Flood
Session	SSL Abuse
Application	HTTP Flood

Amplified & Reflected DDoS: Multiplying the Impact

Amplification Factor

Some reflection techniques can multiply the attacker's traffic by factors of 50x or more.

- **Amplified DDoS attacks** exploit protocols that return larger responses than the initial request.
- **Reflected attacks** bounce traffic off third-party servers to hide the attacker's identity.
- Common protocols exploited:

Protocol	**Amplification Factor**
DNS	28-54x
NTP	556-1,337x
SSDP	30x
Memcached	10,000-51,000x

- These attacks are particularly dangerous because they require minimal resources from the attacker.

DNS Attacks: Compromising the Internet's Directory

- The **Domain Name System (DNS)** translates human-readable domain names into IP addresses.
- Common DNS attack types:
  - **DNS cache poisoning**: Inserts fraudulent records into DNS resolvers
  - **DNS tunneling**: Abuses DNS protocols to exfiltrate data
  - **DNS hijacking**: Modifies DNS settings to redirect users
  - **DNS amplification**: Uses DNS servers for DDoS attacks
- These attacks can be difficult to detect because DNS traffic is typically trusted by network security systems.

Example

Ron Swanson typed "www.parksandrec.gov" into his browser but was redirected to a fake government website that asked for his credentials. The IT department later discovered the office DNS settings had been hijacked.

Wireless Network Vulnerabilities

Convenience vs. Security

The ease of access that makes wireless networks convenient also creates unique security challenges.

- Common wireless attack vectors:

Attack Type	**Description**
Evil Twin	Rogue access points mimicking legitimate netw
WPA/WPA2 Cracking	Breaking wireless encryption using captured ha
Jamming	Using radio interference to disrupt communicat
Wardriving	Scanning for vulnerable networks from a vehicle
Packet Sniffing	Capturing and analyzing unencrypted wireless t

On-Path Attacks: The Digital Eavesdropper

- **On-path attacks** (or **man in the middle**) occur when an attacker secretly relays and possibly alters communications between two parties.
- The victims believe they are communicating directly with each other, unaware of the attacker in between.
- These attacks can be used to intercept data, steal credentials, or manipulate transactions.

- Common vectors:
  - ARP spoofing
  - DNS spoofing
  - Evil twin Wi-Fi
  - SSL stripping
  - BGP hijacking

Sender	Attacker	Receiver
Thinks they're sending to receiver	Intercepts & modifies	Thinks they're receiving from sender

Credential Replay: Using Stolen Authentication

- **Credential replay attacks** involve capturing authentication data and reusing it to gain unauthorized access.
- These attacks don't require knowing the actual password, only the authentication tokens or hashes.
- Common targets:
  - Authentication cookies
  - Session tokens
  - Kerberos tickets
  - OAuth tokens
  - NTLM hashes
- Attackers typically capture credentials using network sniffers, on-path attacks, or malware.

Modern Challenge

Even with strong passwords, replay attacks can succeed if the authentication protocol itself doesn't prevent reuse.

Malicious Code in Network Traffic

- Network traffic can be manipulated to deliver **malicious code** directly to target systems.
- Delivery mechanisms:

Method	Description
Code injection	Inserting code into legitimate web traffic
Malvertising	Malicious code embedded in online ads
Drive-by downloads	Silent downloads from compromised sites
Traffic manipulation	Altering packets in transit to add malicious c

- Network-level exploits may target vulnerabilities in how systems process network packets.
- Content filtering and deep packet inspection can help identify and block malicious code in transit.

Example

While using the office Wi-Fi, Pam Beesly noticed strange redirects when browsing. IT discovered malicious JavaScript was being injected into web pages as they passed through a compromised router.

Injection Attacks: Exploiting Input Vulnerabilities

OWASP Top Threat

Injection attacks consistently rank among the most dangerous web application security risks in the OWASP Top Ten.

- **Injection attacks** occur when untrusted data is sent to an interpreter as part of a command or query.
- Common injection types:
  - SQL injection
  - Command injection
  - LDAP injection
  - XSS (Cross-Site Scripting)

SQL Injection Example

Intended: `SELECT * FROM users WHERE username = 'input1' AND password = 'input2'`

Malicious input1: `admin' --`

Resulting query: `SELECT * FROM users WHERE username = 'admin'`

Buffer Overflows: When Memory Fails

- **Buffer overflow** attacks occur when a program writes data beyond the allocated memory buffer.
- These vulnerabilities arise from poor programming practices and inadequate input validation.
- Successful exploitation can lead to:
  - System crashes
  - Data corruption
  - Arbitrary code execution
  - Privilege escalation

Protection Methods

- ASLR
- DEP/NX
- Stack canaries
- Bounds checking
- Safe libraries

Low-Level Vulnerability

Buffer overflows exploit how computers manage memory, making them particularly dangerous but also more difficult to execute.

Replay Attacks on Applications

Not Just Network Traffic

Application-level replay differs from network replay by targeting specific application functions rather than authentication alone.

- **Application replay attacks** involve capturing valid data transmissions and retransmitting them to trick an application.
- Attack scenarios and targets:

Target	Attack Scenario
Financial transactions	Duplicating money transfers
API requests	Replaying authorized API calls
Authentication sequences	Reusing login credentials
Session management	Hijacking user sessions

- Successful attacks can lead to transaction duplication, session hijacking, or privilege escalation.

Privilege Escalation: Gaining Unauthorized Access

- **Privilege escalation** involves gaining elevated access to resources that should be protected.
- Two primary types:
  - **Vertical**: Gaining higher permission levels
  - **Horizontal**: Accessing resources of peers
- Attackers often chain multiple vulnerabilities to achieve full system compromise.

Common Vectors

- Misconfigured permissions
- Unpatched vulnerabilities
- Default credentials
- Application flaws
- Token manipulation
- Path traversal

Forgery Attacks: Digital Counterfeiting

Types of Forgery

Forgery attacks can target requests, responses, or the underlying identities used in digital systems.

Attack Type	**Description**
Cross-site request forgery (CSRF)	Tricks users into submitting unwanted requests
Server-side request forgery (SSRF)	Forces server to make unauthorized internal requests
Cookie forgery	Creates/modifies cookies to impersonate users
Email forgery	Manipulates email headers to fake message origins

Directory Traversal: Escaping the Sandbox

Also Known As

Directory traversal is sometimes called the "dot-dot-slash" attack, referring to the "../" sequence used to navigate directories.

- **Directory traversal** attacks exploit insufficient security validation to access files outside intended directories.
- Attackers use path manipulation techniques like "../" sequences to navigate the file system.
- Common targets include web servers, file upload functions, and content management systems.

Example Attack String

```
../../etc/passwd
..
..
windows
system32
```

Downgrade & Collision Attacks: Weakening Encryption

- **Downgrade attacks** force systems to use weaker encryption protocols than they normally would.
- These attacks exploit backward compatibility features to use deprecated, less secure algorithms.
- Notable examples:
  - POODLE (SSL 3.0)
  - FREAK (Export-grade RSA)
  - Logjam (Weak DH parameters)

- **Collision attacks** identify different inputs that produce the same cryptographic hash value.
- When successful, collision attacks can be used to:
  - Forge digital signatures
  - Bypass integrity checks
  - Create malicious duplicates
  - Break certificate validation

Cryptographic Aging

Encryption algorithms that were once considered secure can become vulnerable over time as computing power increases

Birthday Attacks: Probability in Cryptography

- **Birthday attacks** are named after the birthday paradox in probability theory.
- The paradox shows that in a group of just 23 people, there's a 50% chance two share a birthday.
- Similarly, finding a collision in an n-bit hash function requires approximately $2^{n/2}$ attempts, not 2^n.
- This makes finding collisions much easier than would be intuitively expected.

Hash Size	Security Level
128-bit	2^{64} operations
160-bit	2^{80} operations
256-bit	2^{128} operations
512-bit	2^{256} operations

Practical Implication

Hash functions used for security applications must be significantly

Password Spraying: Casting a Wide Net

Why It Works

Password spraying evades account lockout mechanisms by trying just a few common passwords against many accounts rather than many passwords against one account.

- **Password spraying** is a brute force technique that attempts a small number of commonly used passwords against many accounts.
- Attack methodology:
  1. Gather a list of valid usernames or email addresses
  2. Select a small set of commonly used passwords
  3. Try each password against all accounts before moving to the next password
  4. Space attempts to avoid triggering lockout policies
- Surprisingly effective due to password reuse and predictable password patterns.
- Mitigation requires strong password policies, MFA, and monitoring for multiple failed login attempts across different