

Information Security

Prepared by Dr. Ahmed Omar

IT373

Information Security

Lecture 5



Malicious Software & Countermeasures

Lecture 5

IT373

Information Security

Prepared by
Dr. Ahmed Omar

Agenda

- ❑ Introduction to Malicious Software (Malware)
- ❑ Understanding the Attacker
- ❑ Classification of Malicious Software
- ❑ The Malware Attack Lifecycle
- ❑ Countermeasures: Detection, Recovery, and Prevention

Introduction to Malicious Software

What is Malware?

Malware (malicious software) is any program intentionally designed to:

- ☐ Cause damage to computer systems
- ☐ Disrupt operations
- ☐ Gain unauthorized access
- ☐ Steal sensitive data

Introduction to Malicious Software

Why Malware Detection Matters

Prevents financial losses

Protects sensitive personal and business data

Maintains operational continuity

Preserves privacy and security

Introduction to Malicious Software

Evolution of Malware

- **1970s-80s:** First experimental self-replicating programs
- **1990s:** Rise of viruses and worms
- **2000s:** Financial motivation, targeted attacks
- **2010s-Present:** Ransomware, APTs, AI-driven threats

Notable Malware Attacks

☐ **WannaCry (2017)**

Ransomware that affected 200,000+ computers in 150 countries. Exploited EternalBlue vulnerability. Impacted NHS, FedEx, and many others.

☐ **SolarWinds (2020)**

Supply chain attack that compromised software updates. Affected thousands of organizations including US government agencies.

Malware Trends

☐ **AI-Driven Malware:**

Using AI to create more sophisticated, adaptive threats

☐ **Multi-Extortion Ransomware:**

Combining encryption with data theft and leak threats

☐ **Fileless Attacks**

Operating in memory to avoid detection

☐ **Supply Chain Targeting**

Compromising software distribution channels

☐ **Cloud-Native Malware:**

Specifically designed to exploit cloud environments

Signs of **Malware Infection**



A **slow computer** that slows down internet speed and software applications



A **sudden loss of disk space** could be a result of malware on the hard drive



Frequent **device/machine crashes or freezes** during normal use



A **swell in internet activity** that does not correlate with user behavior



A ton of **pop-up, new toolbars, extensions** or **fraudulent websites**



An **overworked system** due to malware taking up valuable resources

What Motivates Malware Creators?

- ❑ **Financial Gain:**

The primary motivation – ransomware, banking trojans, cryptojacking, and data theft for profit.

- ❑ **Espionage:**

Nation-states and corporate spies stealing intellectual property, trade secrets, and strategic information.

- ❑ **Disruption/Sabotage:**

Causing chaos, damaging systems, or disrupting operations for political, ideological, or competitive reasons.

- ❑ **Hacktivism:**

Promoting political or social causes through cyber attacks.

- ❑ **Personal Challenges:**

Some create malware to prove technical skills or for recognition in hacker communities.



Types of Malware



Classification Overview

☐ Propagation Method

How malware spreads from one system to another, utilizing various techniques to infect multiple systems.

☐ Behavior

What the malware does once inside a system, including its activities, functions, and impact on the infected device.

☐ Purpose / Goal

The attacker's objective behind deploying the malware, such as financial gain, data theft, or system disruption.

Propagation Method

❑ Propagation method refers to how malware spreads from one system to another, utilizing various techniques to infect multiple systems.

-  **Email attachments and phishing links**
-  **Network-based vulnerability exploitation**
-  **Shared network resources and directories**
-  **Browser "drive-by" downloads**
-  **Peer-to-peer (P2P) file sharing networks**
-  **Removable media (USB drives, external hard drives)**

Propagation Countermeasures

Preventing Malware Spread

- Network segmentation to limit lateral movement
- Email filtering to block malicious attachments and links
- Web filtering to prevent access to malicious websites
- Regular patching of systems and applications
- User education on recognizing phishing attempts
- USB port control and removable media policies
- Properly configured firewalls and intrusion prevention

Behavior

❑ Behavior refers to what the malware does once inside a system, including its activities, functions, and impact on the infected device.



Creating backdoors for remote access



Encrypting files and demanding ransom



Monitoring user activity and stealing data



Downloading additional malicious software



Establishing communication with C2 servers



Disabling security software and protections

Behavior Countermeasures

Detecting & Mitigating Malicious Behavior

- ☐ Antivirus/anti-malware with real-time protection
- ☐ Behavioral analysis to detect suspicious activities
- ☐ Endpoint Detection and Response (EDR) solutions
- ☐ Sandboxing to safely analyze suspicious files
- ☐ Application whitelisting to prevent unauthorized execution
- ☐ Principle of least privilege to limit malware impact
- ☐ File integrity monitoring to detect unauthorized changes

Purpose / Goal

❑ **The purpose or goal of malware defines the attacker's objective behind deploying the malicious software.**

 **Data theft - stealing personal information, credentials, or sensitive data**

 **Financial gain - demanding ransom or stealing banking information**

 **Remote control - gaining unauthorized access to compromised systems**

 **Disruption/Damage - causing system instability or data corruption**

 **Espionage - covertly monitoring activities and collecting intelligence**

 **Spreading further malware - distributing more malicious software**

Purpose Countermeasures

Data Theft Protection

- ✓ Data encryption at rest and in transit
- ✓ Data Loss Prevention (DLP) solutions

Financial Gain Countermeasures

- ✓ Immutable backups for ransomware protection
- ✓ Banking security tools and transaction monitoring

Espionage Prevention

- ✓ Network traffic analysis and anomaly detection
- ✓ Advanced Persistent Threat (APT) protection

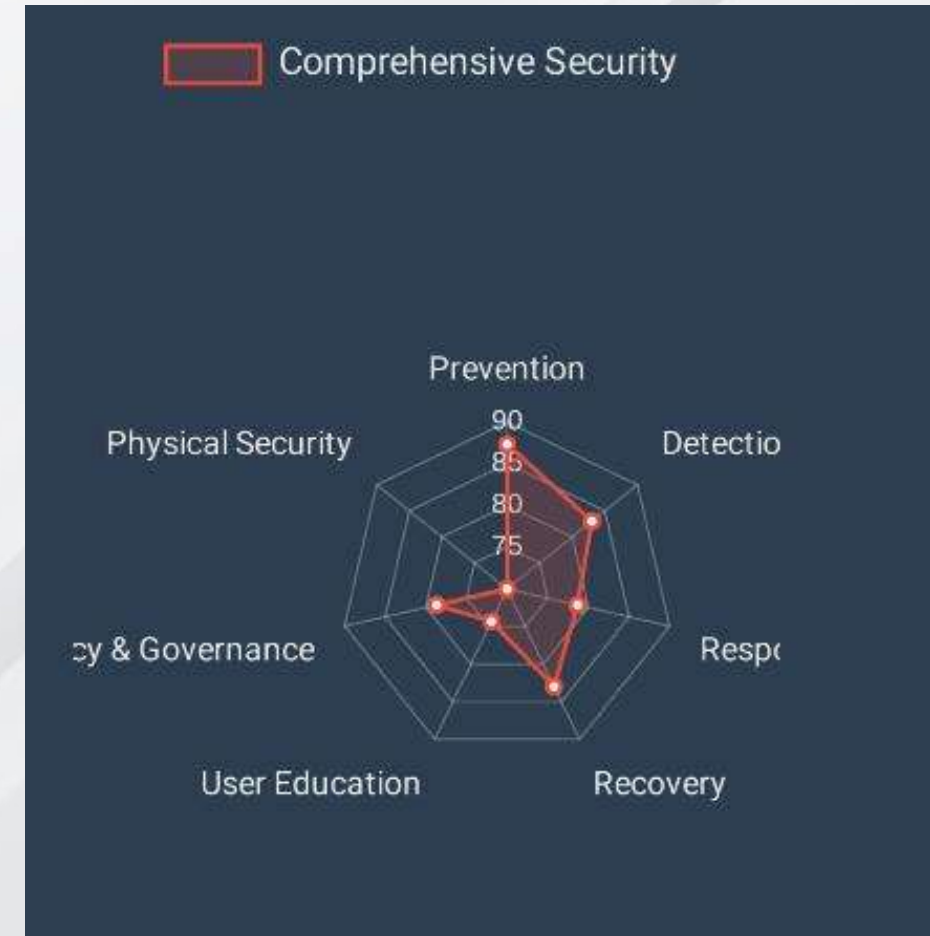
Disruption/Damage Mitigation

- ✓ Business continuity and disaster recovery planning
- ✓ System redundancy and high availability solutions

General Countermeasures

•Defense in Depth Strategy

Implementing multiple layers of security controls throughout the IT environment ensures that if one layer fails, others are in place to prevent or limit the impact of a malware attack.

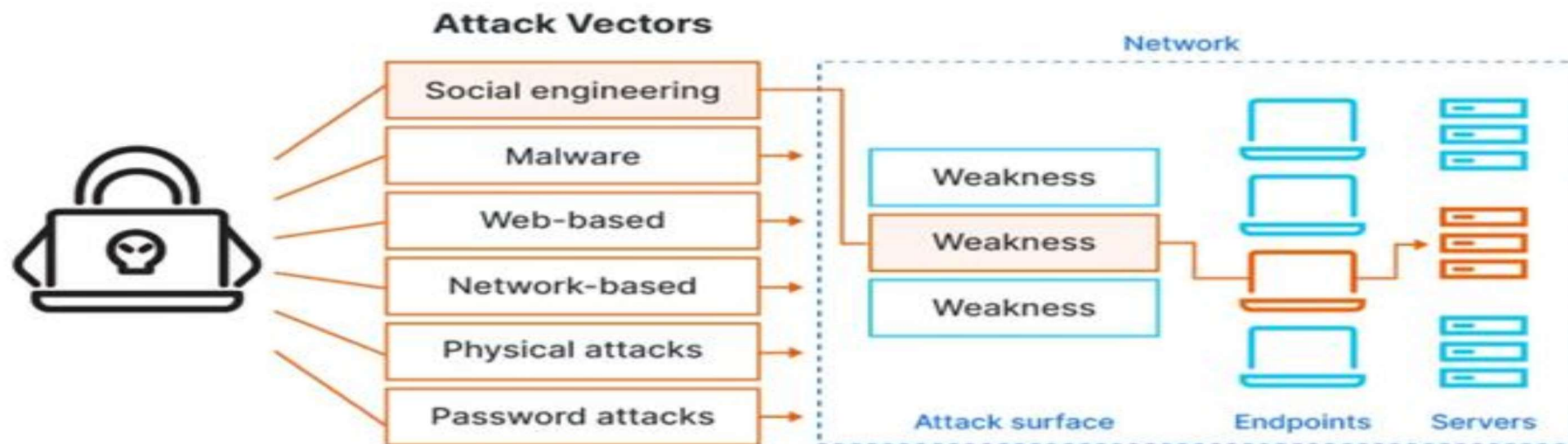


How Malware Starts: Infection Vectors

• Stages of a Malware Attack:

- **Delivery:** Initial transmission to target system (email, website, USB)
- **Execution:** Malware activates on the system (user click, exploit)
- **Persistence:** Ensures survival after reboot (registry keys, scheduled tasks)
- **Propagation:** Optional spreading to other systems
- **Payload Execution:** Performs malicious action (encryption, data theft)

How Malware Starts: Infection Vectors



Phishing: The Primary Gateway

Why Phishing Is So Effective

Human Psychology: Exploits **trust**, **curiosity**, **fear**, or **urgency** to bypass technical defenses

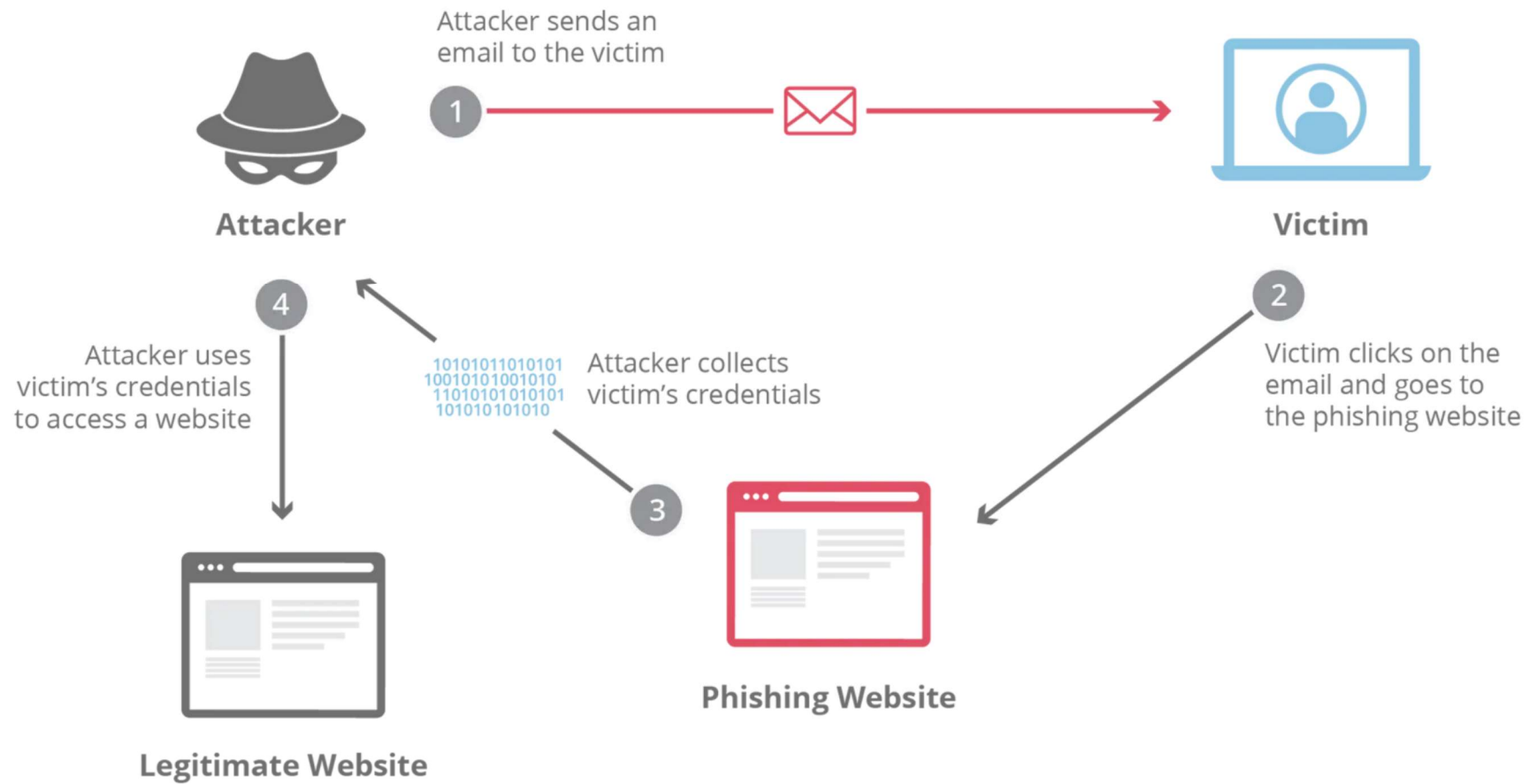
➤ **Types of Phishing:**

- ☐ Spear Phishing: Targeted attacks customized for specific individuals
- ☐ Business Email Compromise: Impersonating executives or partners
- ☐ Clone Phishing: Duplicating legitimate communications

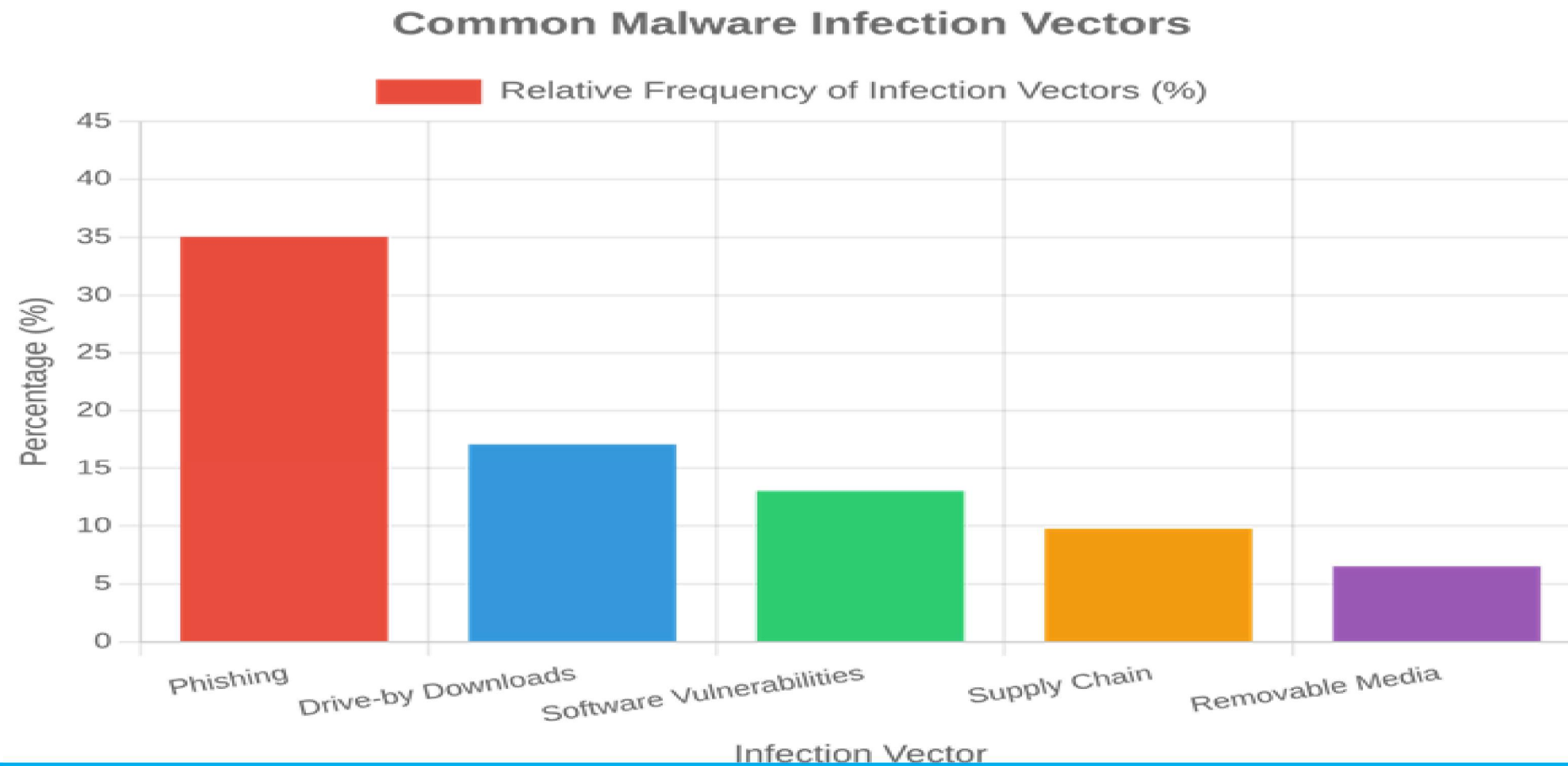
➤ **Delivery Methods:** Email (most common), SMS (smishing), voice calls (vishing), social media messages

➤ **Success Rate:** Even with training, phishing campaigns typically achieve 10-20% click rates

Phishing: The Primary Gateway



Infection Vectors



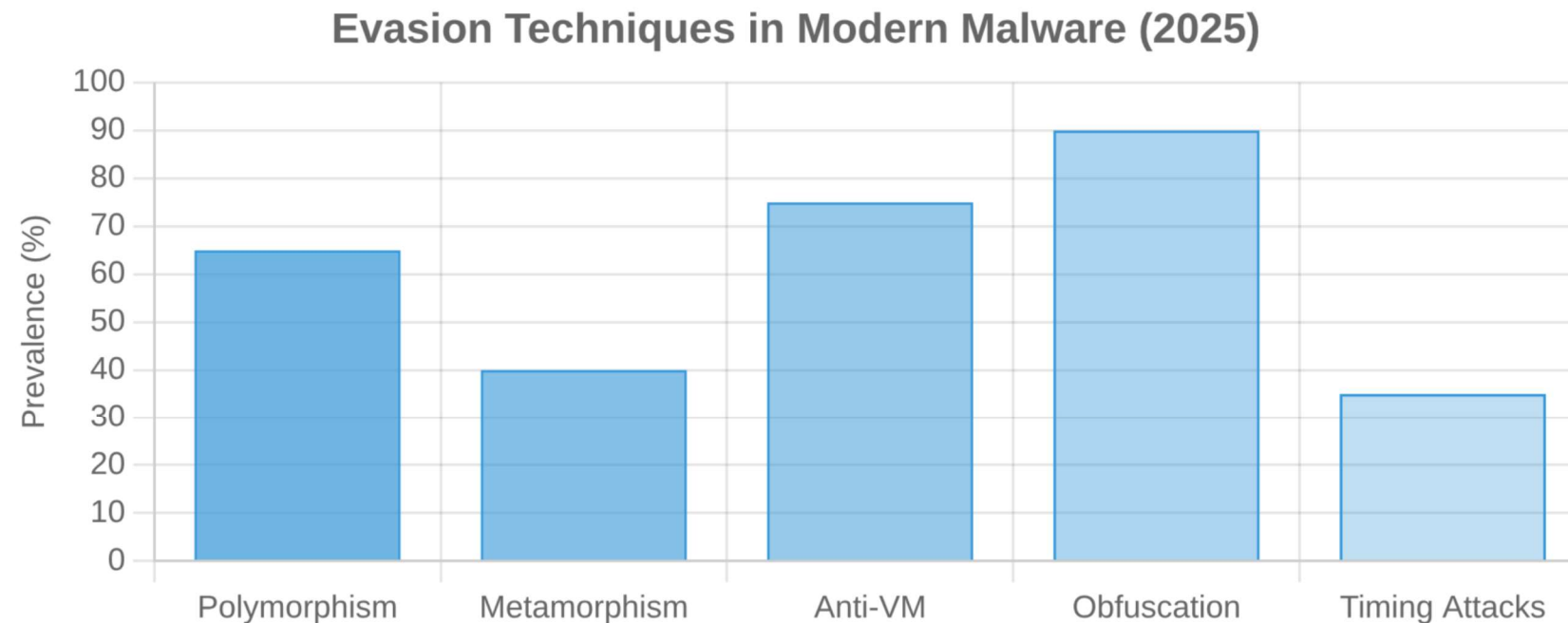
Evasion Techniques

Refer to methods used by attackers to **bypass** or **trick** security systems and remain undetected while carrying out malicious activities. The goal is to deliver an exploit, attack, or other form of malware to a target system or network without being caught by defenses like firewalls, intrusion detection systems (IDS), antivirus software, or even human analysts.

- **Polymorphism**: Changes code while maintaining functionality
- **Metamorphism**: Completely rewrites code with each replication
- **Anti-VM/Sandbox**: Detects analysis environments
- **Obfuscation**: Makes code difficult to understand
- **Timing Attacks**: Delays execution to bypass analysis

Evasion Techniques

Here's a summary of their prevalence and why they're so critical in the ongoing "cat and mouse" game between attackers and defenders

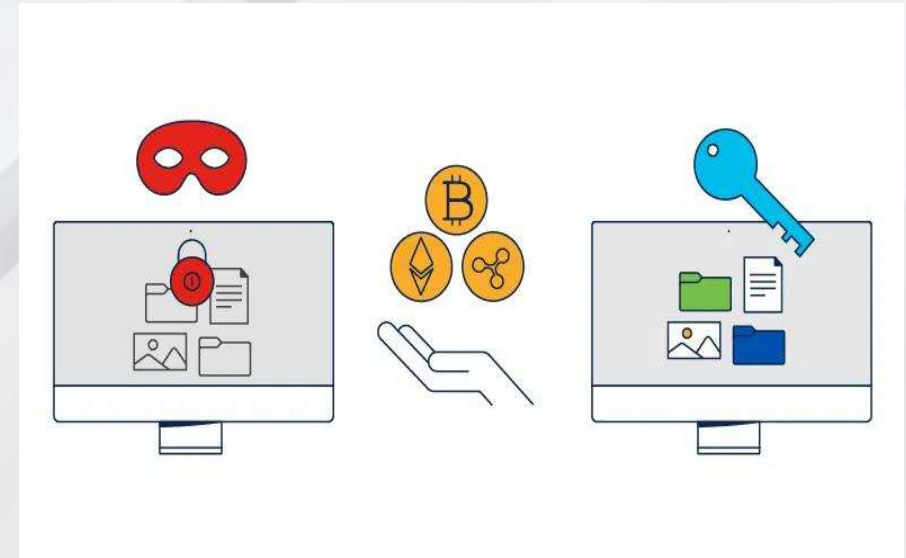


Ransomware

Malware that encrypts a victim's files and demands payment (ransom) to restore access.

Key Characteristics:

- Uses strong encryption algorithms
- Demands payment in cryptocurrency (usually Bitcoin)
- Often includes a countdown timer
- May threaten to publish stolen data (double extortion)

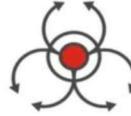


Ransomware

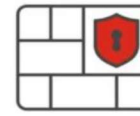
9 Tips To Reduce Ransomware Risk



Never click on
Unverified links



Scan emails for
Malware



Use firewalls &
Endpoint Protection



Only download
from trusted sites



Keep backups of
Important data



Use a VPN when
Using public wi-fi



Use security
Software



Do not use unfamiliar
USB devices



Avoid giving out
Personal Data

Trojans, Worms, and Viruses

❑ Trojans

Malware disguised as legitimate software that tricks users into installing it. Unlike viruses, trojans don't self-replicate.

Examples: Zeus, Emotet, DarkComet

❑ Worms

Self-replicating malware that spreads across networks without requiring user interaction. Exploits vulnerabilities to propagate.

Examples: ILOVEYOU, Conficker, Stuxnet

Trojans, Worms, and Viruses

Viruses

- Malicious code that attaches to legitimate programs and executes when the host program runs.
- Requires user action to spread.

Examples: Melissa, CIH/Chernobyl, Sasser

Trojans, Worms, and Viruses

Feature	Trojans	Worms	Viruses
Self-replication	No	Yes	Yes
User interaction	Required	Not required	Required
Host program	Disguises as one	Independent	Requires one
Primary spread	Social engineering	Network vulnerabilities	File sharing

Spyware, Adware, and Rootkits

Spyware

Software that secretly monitors user activity and collects sensitive information without consent.

Keylogging

Screen capturing

Browser monitoring

Impact: Identity theft, financial fraud, privacy violations

Adware

Software that automatically displays unwanted advertisements and tracks browsing habits.

Pop-up ads

Browser redirects

Search hijacking

Impact: Degraded performance, privacy concerns, poor user experience

Rootkits

Stealthy software that provides persistent privileged access while actively hiding its presence.

Kernel modification

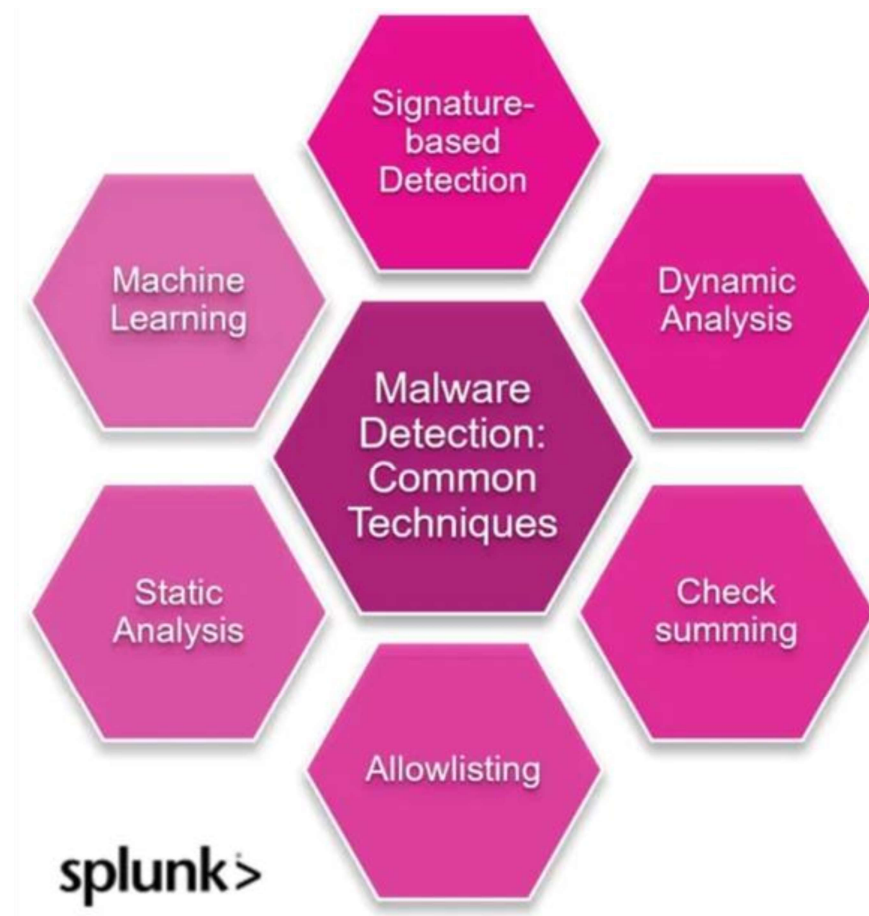
Process hiding

Backdoor creation

Impact: Complete system compromise, extremely difficult to detect and remove

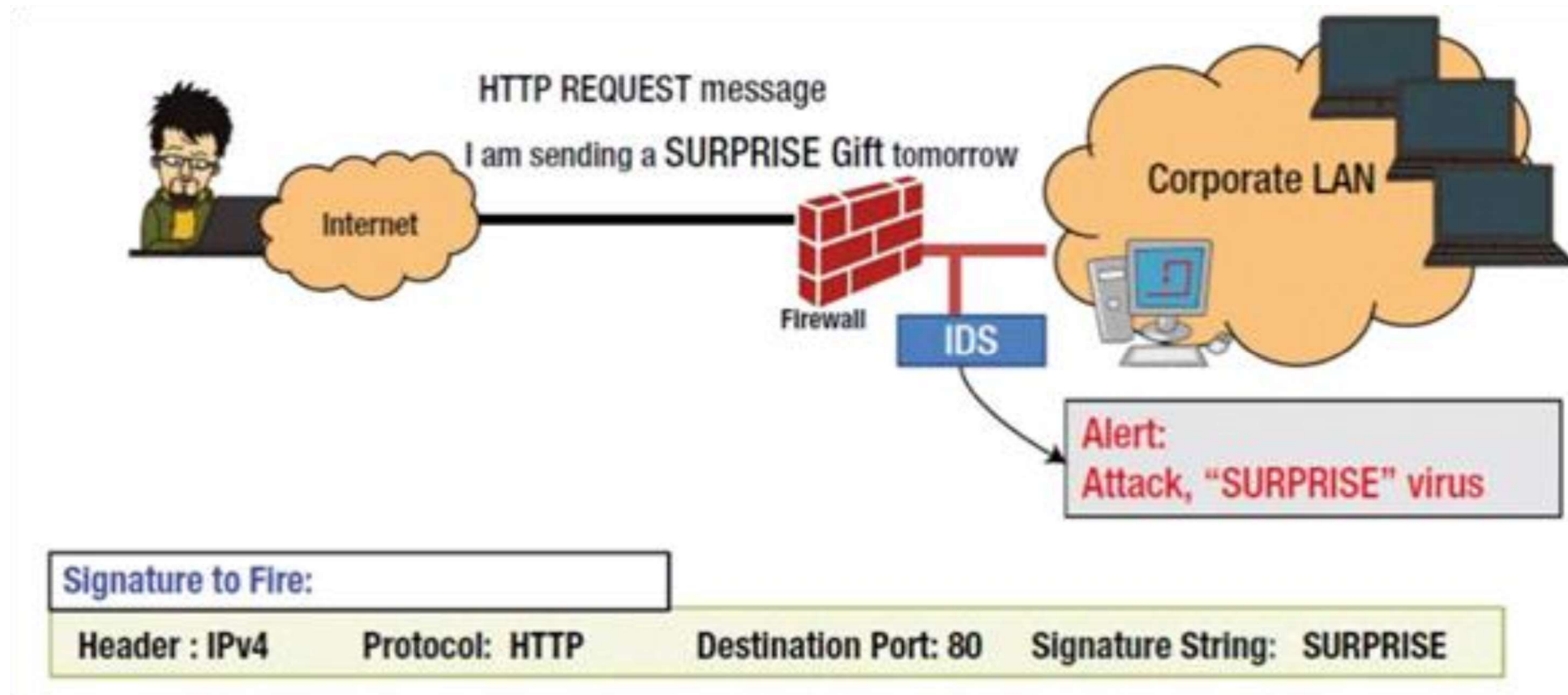
Malware Detection Overview

Malware detection is the process of identifying and preventing malicious software from compromising systems and networks.



Signature-Based Detection

Uses known digital indicators (signatures) to identify malware by comparing files against a database of known threats.



Signature-Based Detection

Key Characteristics:

- ☐ Fast and resource-efficient
- ☐ High accuracy for known threats
- ☐ Requires regular signature updates
- ☐ Ineffective against zero-day or polymorphic malware

Dynamic Malware Analysis

Dynamic Malware Analysis

- ❑ Executes suspected malicious code in a controlled environment (sandbox) to observe its behavior and actions.
- ❑ **Key Advantages:**
 - Detects unknown and zero-day threats
 - Reveals actual runtime behavior
 - Identifies obfuscated or encrypted malware
 - Effective against polymorphic malware

Behavioral Analysis

- ❑ Monitors system activity to identify suspicious patterns and behaviors that may indicate malware presence.

- ❑ **Behavioral Analysis Process:**
 - Establish baseline of normal system behavior
 - Monitor for deviations from normal patterns
 - Analyze suspicious activities in context
 - Trigger alerts or automated responses

Advanced Detection Techniques

Machine Learning & AI

Uses algorithms to learn patterns from existing data and identify novel malware based on similarities to known threats.

Honeypots

Decoy systems designed to attract attackers and malware to study their techniques and gather intelligence.

- Types : Client honeypots, server honeypots, research honeypots

Advanced Detection Techniques



Heuristic Analysis

Uses rules and algorithms to detect suspicious patterns and behaviors that may indicate previously unknown malware.

Focus: Suspicious API calls, unusual code structures, obfuscation techniques



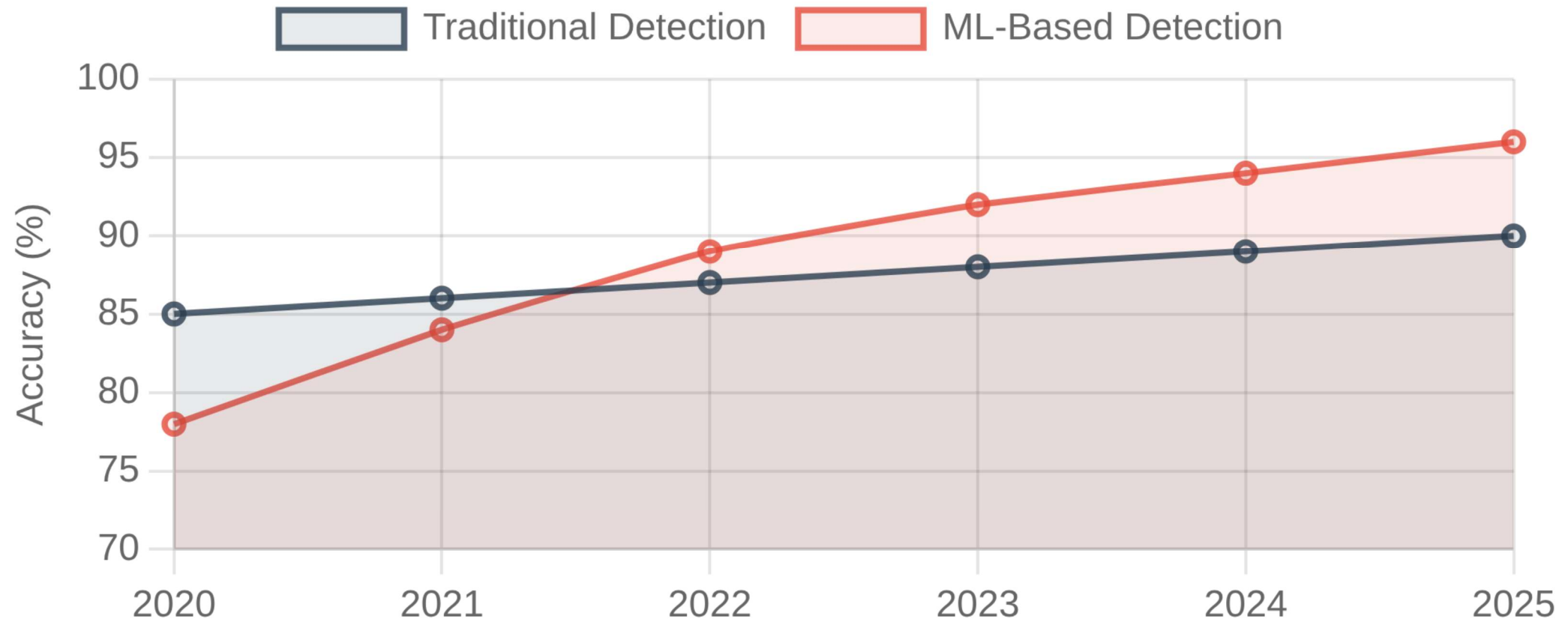
Network Traffic Analysis

Monitors network communications to identify suspicious patterns, command and control traffic, and data exfiltration.

- Methods : Deep packet inspection, flow analysis, DNS monitoring

Detection Techniques

Detection Accuracy Improvement Over Time



Malware Restoration and Recovery

1. Isolation & Containment

Disconnect infected systems from network

Block malicious indicators (IPs, domains)

2. Eradication

Use specialized removal tools

System reinstallation (wipe and reload)

3. Data Restoration

Restore from clean, verified backups

Implement system hardening measures

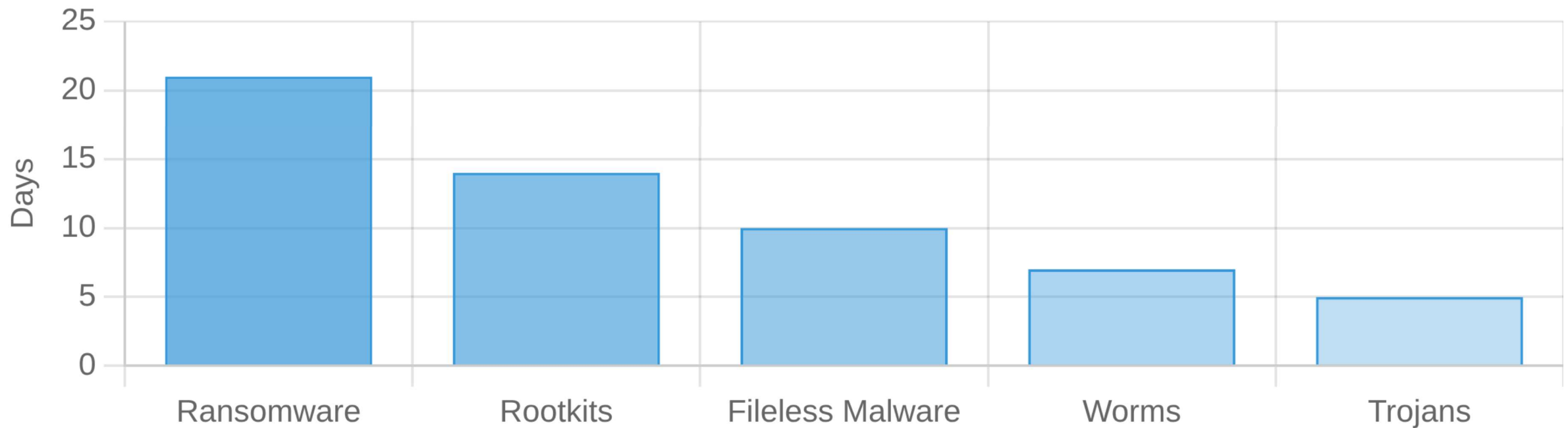
4. Post-Incident Analysis

Conduct root cause analysis

Update security policies and procedures

Recovery Time by Malware Type

Average Recovery Time by Malware Type (2025)



Summary

- ✓ **What is Malware?**
- ✓ **Evolution and Motivations**
- ✓ **Malware Classification and Types**
- ✓ **Attack Lifecycle and Infection Vectors**
- ✓ **Detection, Countermeasures, and Recovery**



Thank You

