Module 1: IT and Security Principles

Frank Asamoah

MBA| MSC | BSC | CEH | Security + | CYSA+|CISM |CASP+| GCP Architect

@kingphranky

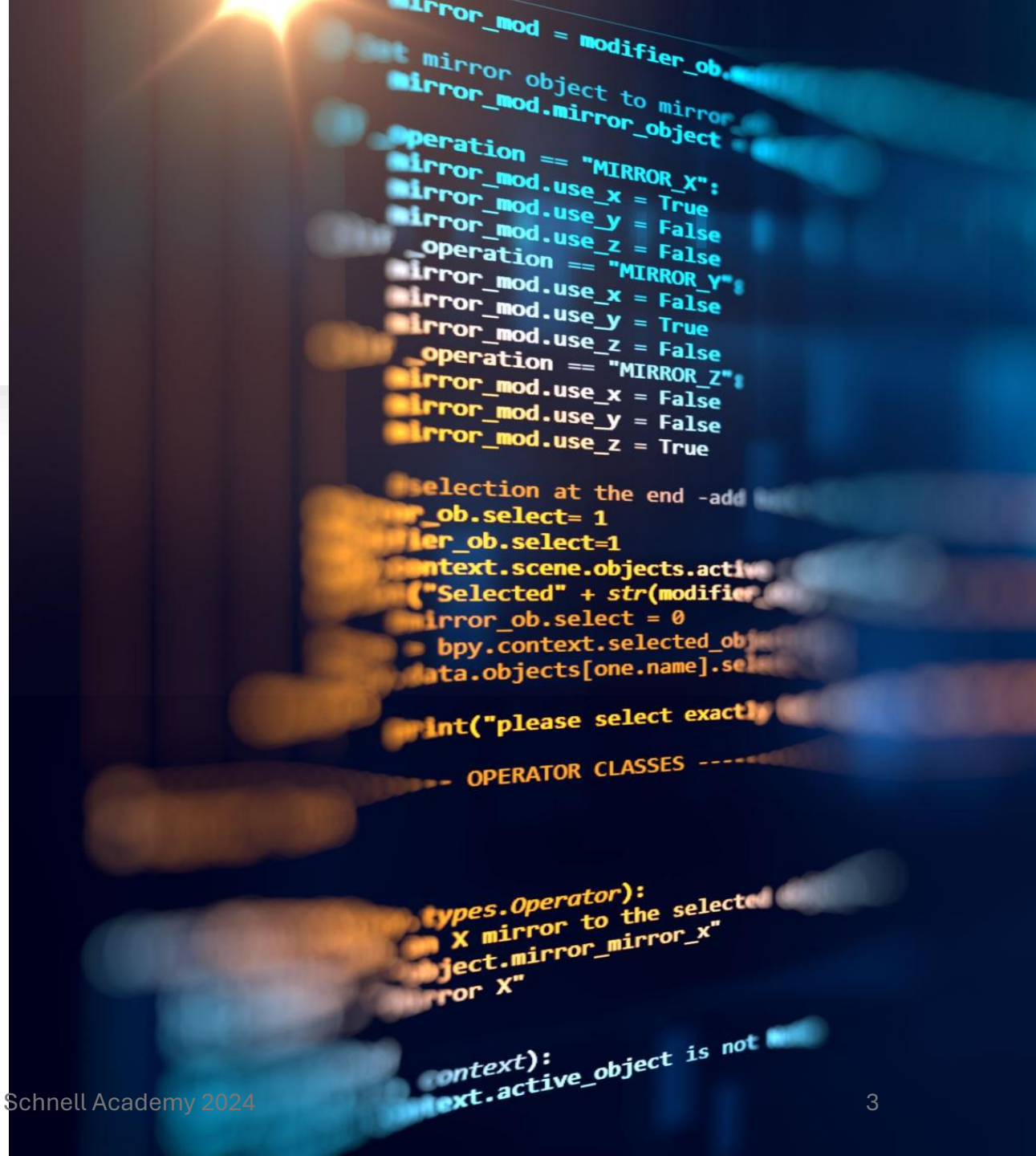
https://www.linkedin.com/in/frank-asamoah


Malware
Understanding Types, Distribution, and Prevention of Malware

Overview of Malware

Definition: Malware (malicious software) is designed to damage, steal data, or disrupt operations.

•Importance: Understanding malware is crucial to protect systems from cyber threats.



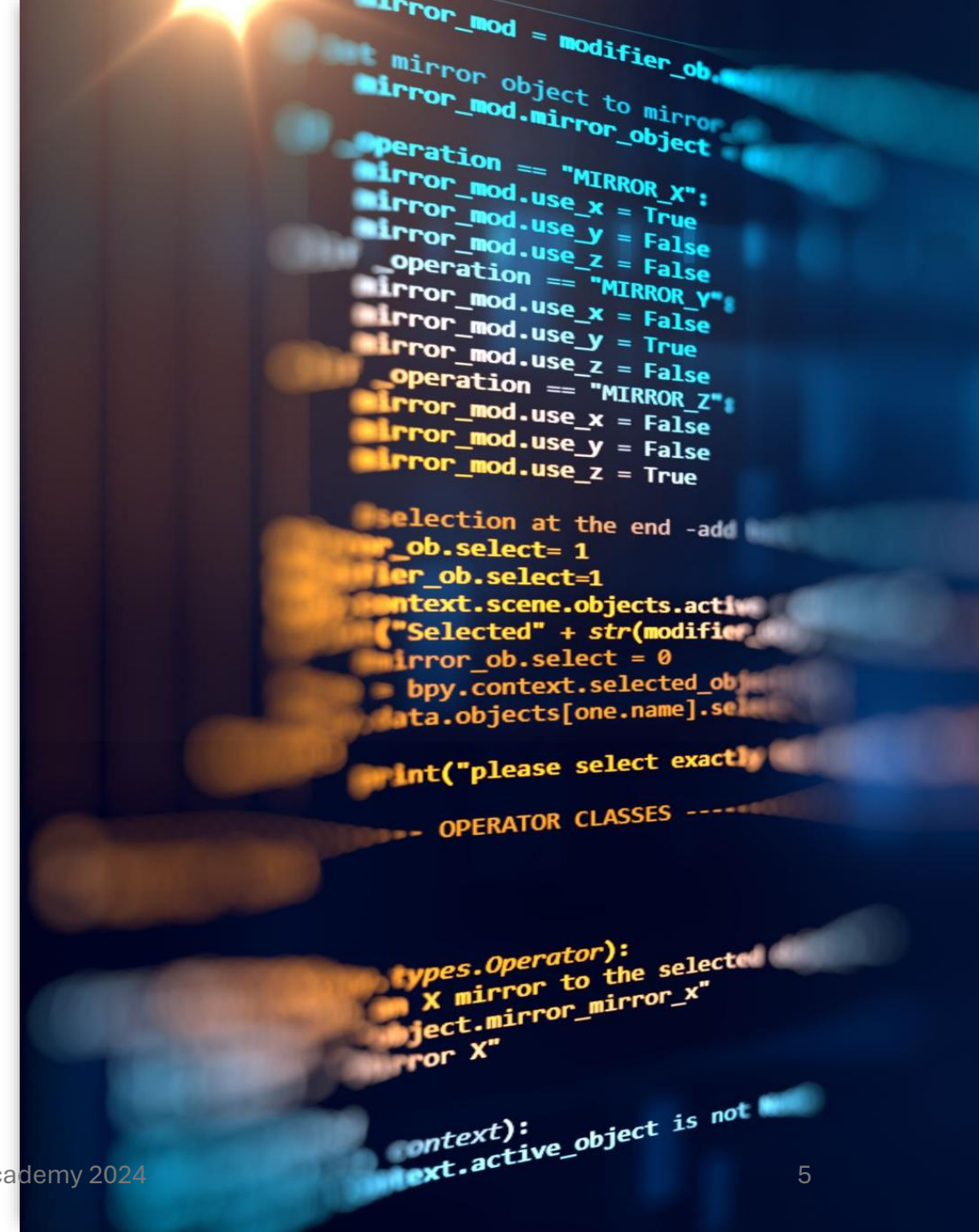
Types of Malware

Overview of common malware types with examples to illustrate their effects.

Brief mention of viruses, worms, trojans, ransomware, spyware, adware, and rootkits.

Viruses

- **Definition**: Malicious code that attaches to files, spreading when executed.
- **Characteristics**: Requires user action to activate.
- **Example**: The ILOVEYOU virus (2000), which spread through email attachments.



Worms

Definition: Standalone malware that replicates itself across networks.

•**Characteristics**: Spreads without user interaction by exploiting software vulnerabilities.

•**Example**: The Morris Worm (1988), which caused early internet disruption.

Trojans

Definition: Malware disguised as legitimate software, tricking users into installing it.

•**Characteristics**: Does not replicate but can open backdoors for other malware.

•**Example**: Emotet Trojan, known for banking fraud and malware delivery.

Ransomware

Definition: Malware that encrypts data, demanding ransom for decryption.

•**Characteristics**: Often spread via phishing emails or malicious downloads.

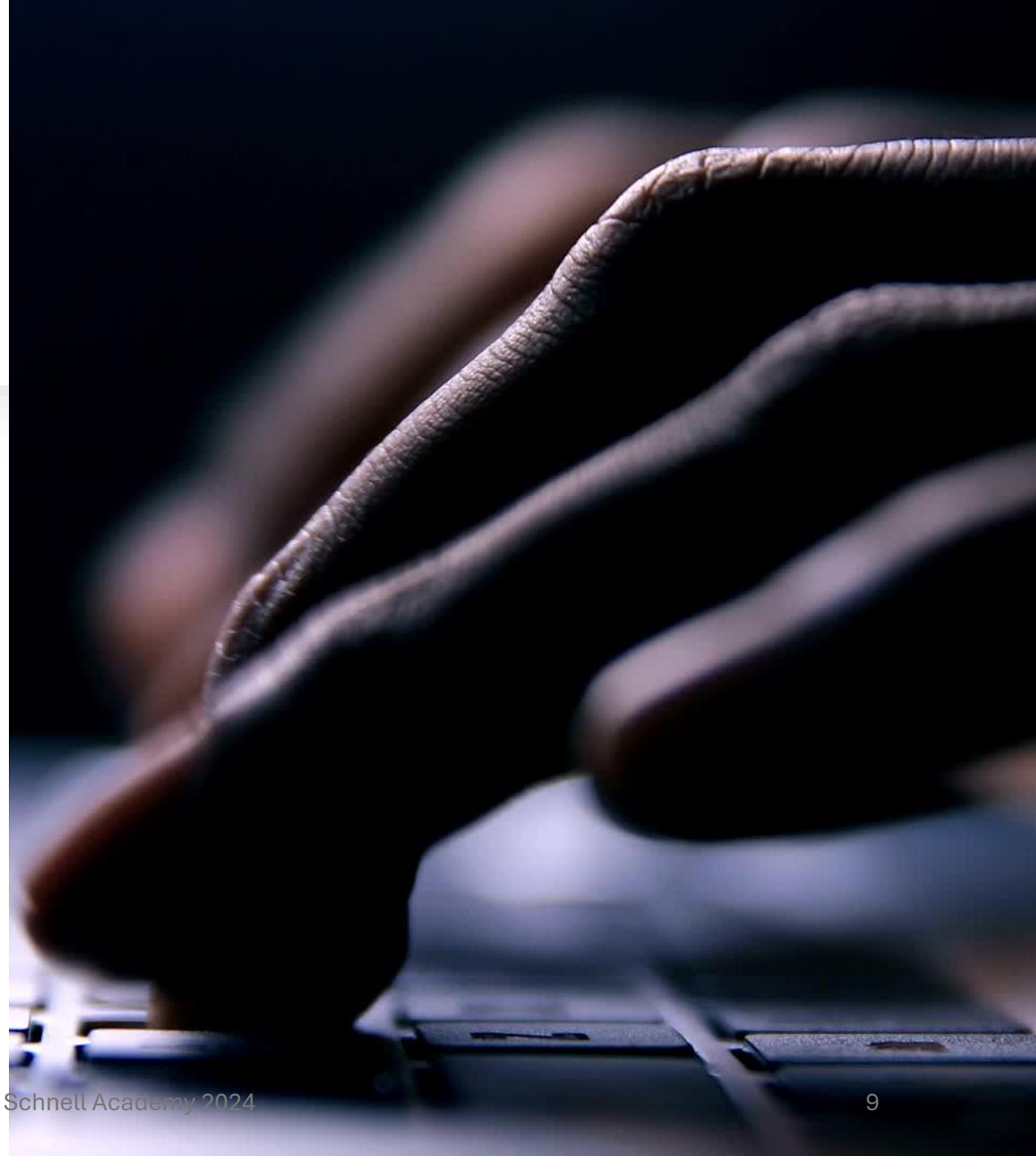
•**Example**: WannaCry Ransomware (2017), which affected healthcare systems and businesses worldwide.

Spyware

Definition: Software that secretly monitors user activities and collects data without consent.

•**Characteristics**: Used to steal sensitive information, like login credentials.

•**Example**: Keyloggers that capture keystrokes to steal passwords.



Adware

Definition: Software that displays unwanted advertisements on devices.

Characteristics: Often bundled with free software downloads.

Example: Fireball Adware, which hijacked browsers to generate ad revenue.

Rootkits

Definition: Malware that gains root-level (administrator) access while hiding its presence.

- **Characteristics**: Allows attackers control over compromised systems.

- **Example**: Stuxnet Rootkit, targeting industrial systems.

Common Malware Distribution Methods

•**Email Attachments and Phishing**: Malicious attachments and links.

•**Drive-by Downloads**: Unintended downloads on compromised sites.

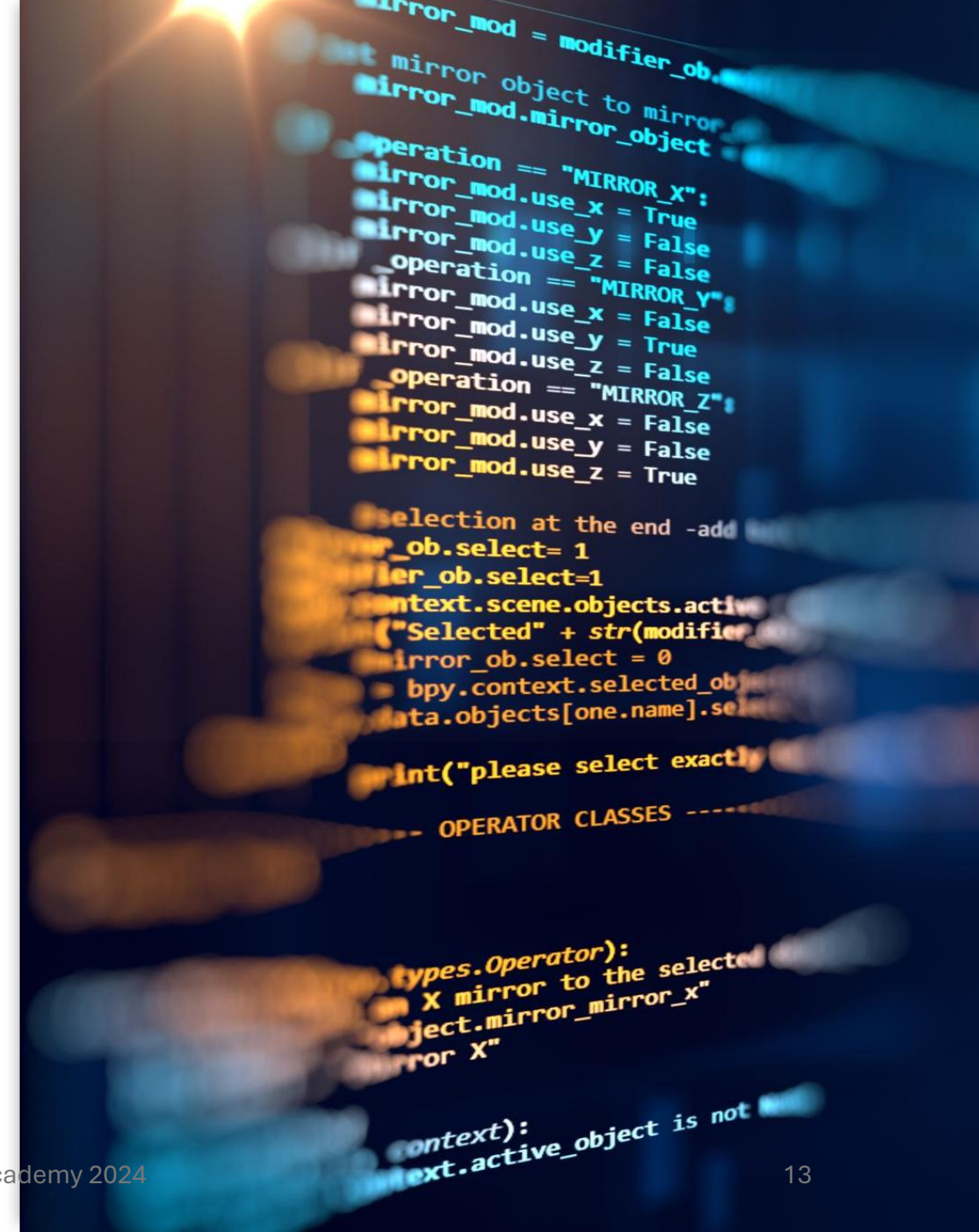
•**Malicious Advertisements (Malvertising)**: Ads redirecting to infected sites.

•**Removable Media**: Infected USB drives and external hard drives.

•**Exploiting Vulnerabilities**: Malware using unpatched software weaknesses.

Signs of Malware Infection

- **Unusual System Behavior**: Slowdowns, crashes, unknown programs.
- **Pop-up Ads**: Excessive pop-ups outside browsers.
- **Unauthorized Changes**: Altered settings or files.
- **Missing Files**: Files disappearing or encrypted.
- **Unusual Network Activity**: High bandwidth usage.



Prevention and Mitigation Strategies

Install and Update Antivirus: Regular updates to antivirus software.

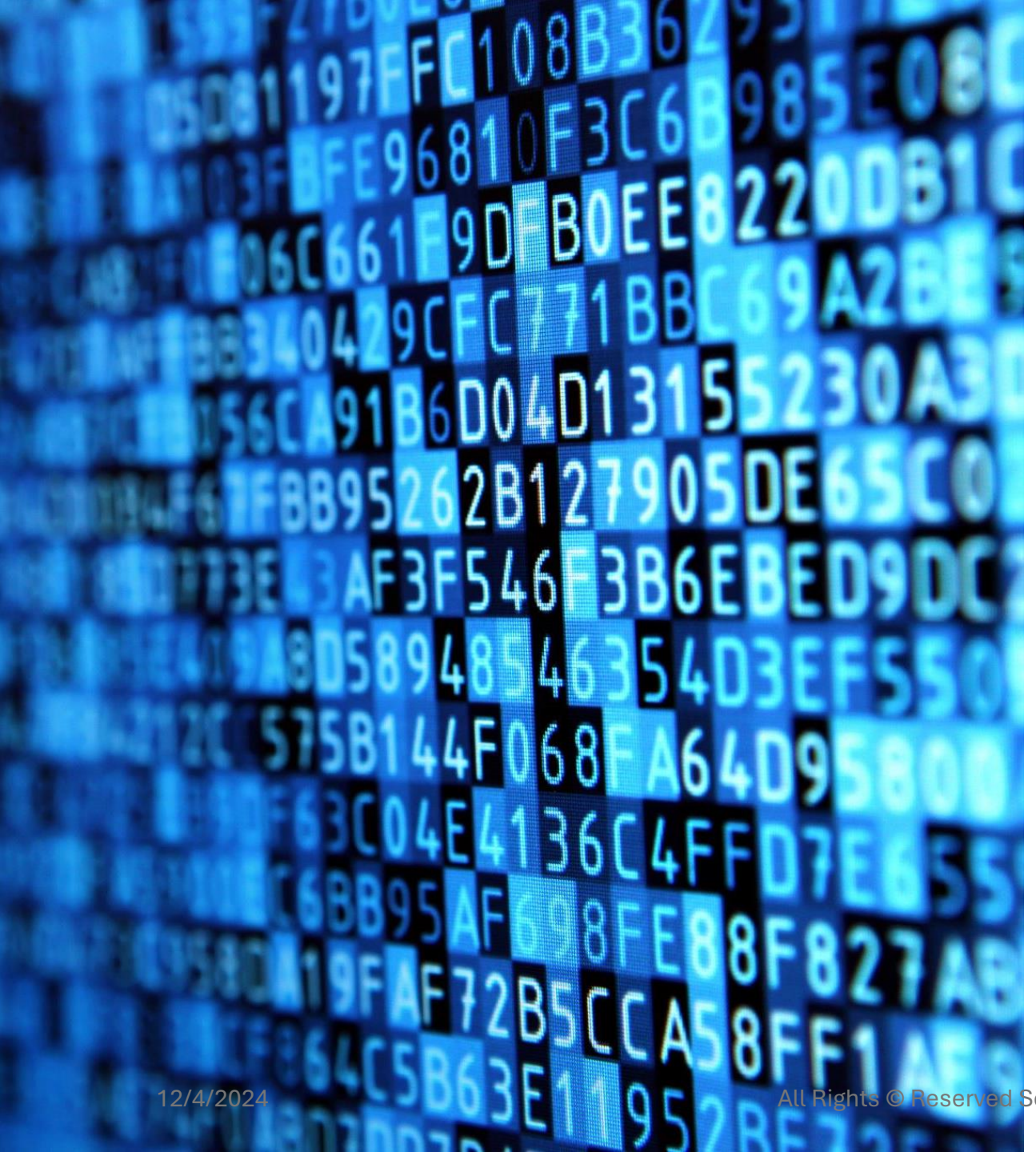
Enable Firewalls: Protection from unauthorized access.

Software Updates: Patching systems and applications.

User Education: Phishing recognition and safe browsing habits.

Regular Backups: Protection from data loss, especially against ransomware.

Access Controls: Multi-factor authentication and least privilege.



Case Study: WannaCry Ransomware Attack (2017)

- **Background**: Exploited EternalBlue vulnerability in Microsoft Windows.
- **Impact**: Affected over 200,000 systems in 150+ countries.
- **Lesson Learned**: Importance of timely patching and backups.

Case Study: Target Data Breach (2013)

- **Background**: Malware used to steal credit card info from point-of-sale systems.
- **Impact**: Compromised data of over 40 million customers.
- **Lesson Learned**: Importance of security monitoring and vendor assessment.

Assignments

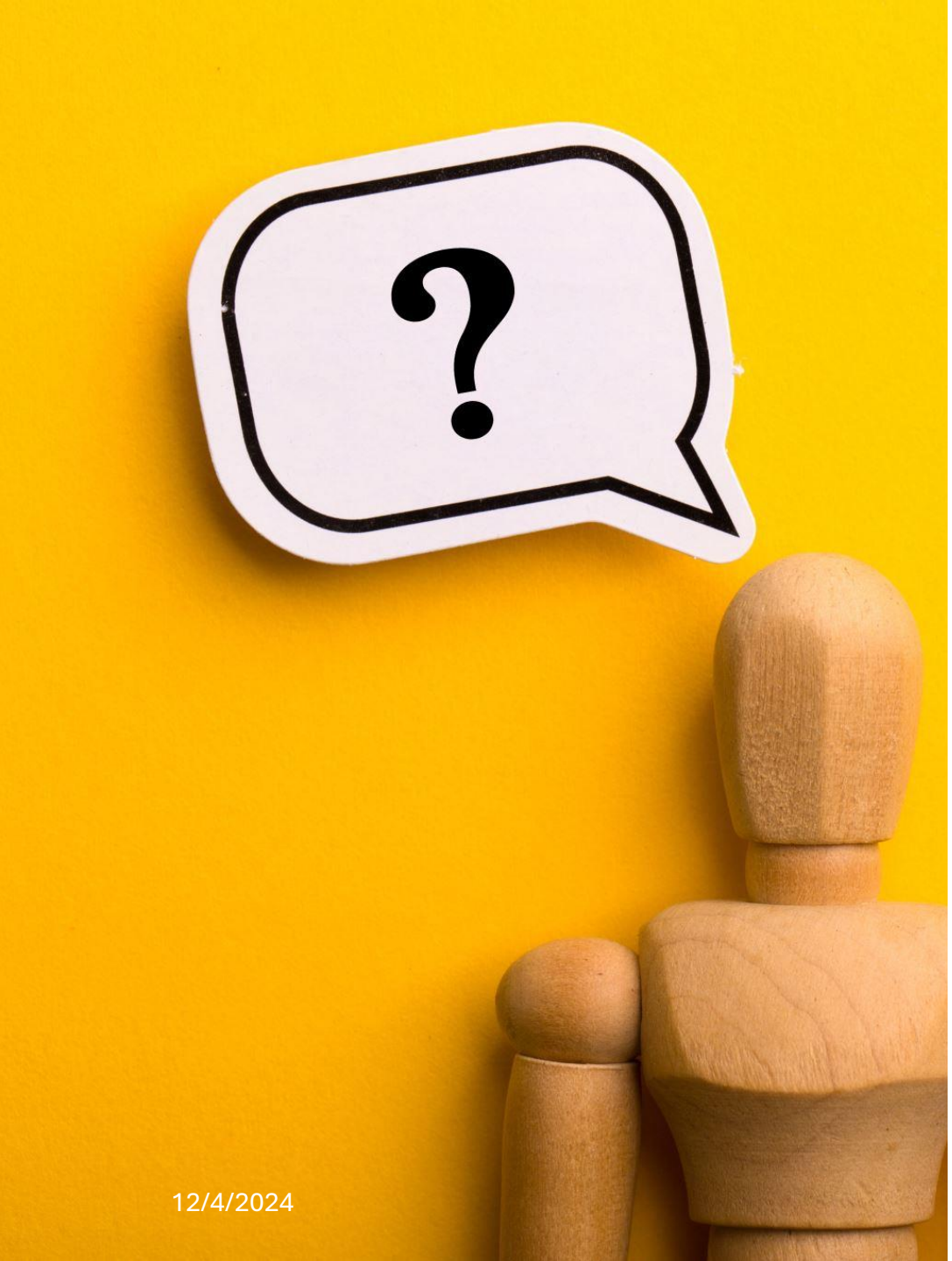
Research Assignment: Report on a recent malware attack, covering type, distribution, and impact.

Practical Assignment: Analyze a malware sample using VirusTotal or Cuckoo Sandbox.

Group Assignment: Presentation on ransomware evolution and defense measures.

Tools for Malware Analysis

- **Wireshark**: Analyzes network protocols to identify suspicious traffic.
- **Malwarebytes**: Anti-malware software for detecting infections.
- **Kali Linux**: Platform for penetration testing and malware analysis.
- **VirusTotal:** Anti-malware analysis tool



Thank You!

Questions?