Software Security

By Lassine Pierre Guindo

What is Software Security?

- Software security means protecting applications from threats and vulnerabilities.
- Ensures that software functions correctly, safely, and resists attacks.
- Protects company data, customer information, and financial assets.

Why Software Security is Important

- Prevents data breaches, financial losses, and reputational damage.
- Security failures can lead to:
  - Loss of customer trust
  - Legal penalties and fines
  - Expensive recovery efforts
  - Example: A small vulnerability in an application can let hackers steal customer data, leading to lawsuits and lost business.

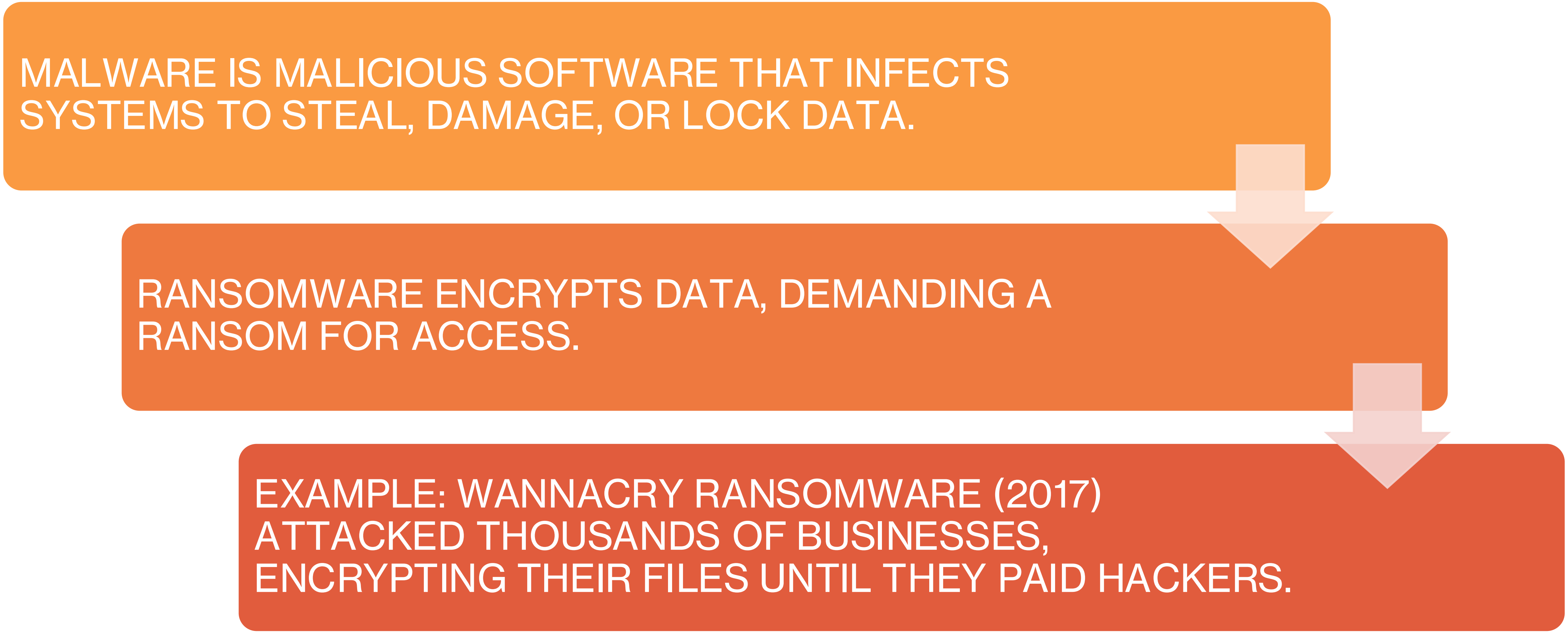
Phishing Attacks

Cybercriminals trick employees into revealing sensitive information through fake emails or messages.

Often leads to stolen credentials and malware infections.

Example: A hacker sends an email pretending to be from IT, asking an employee to reset their password on a fake website.

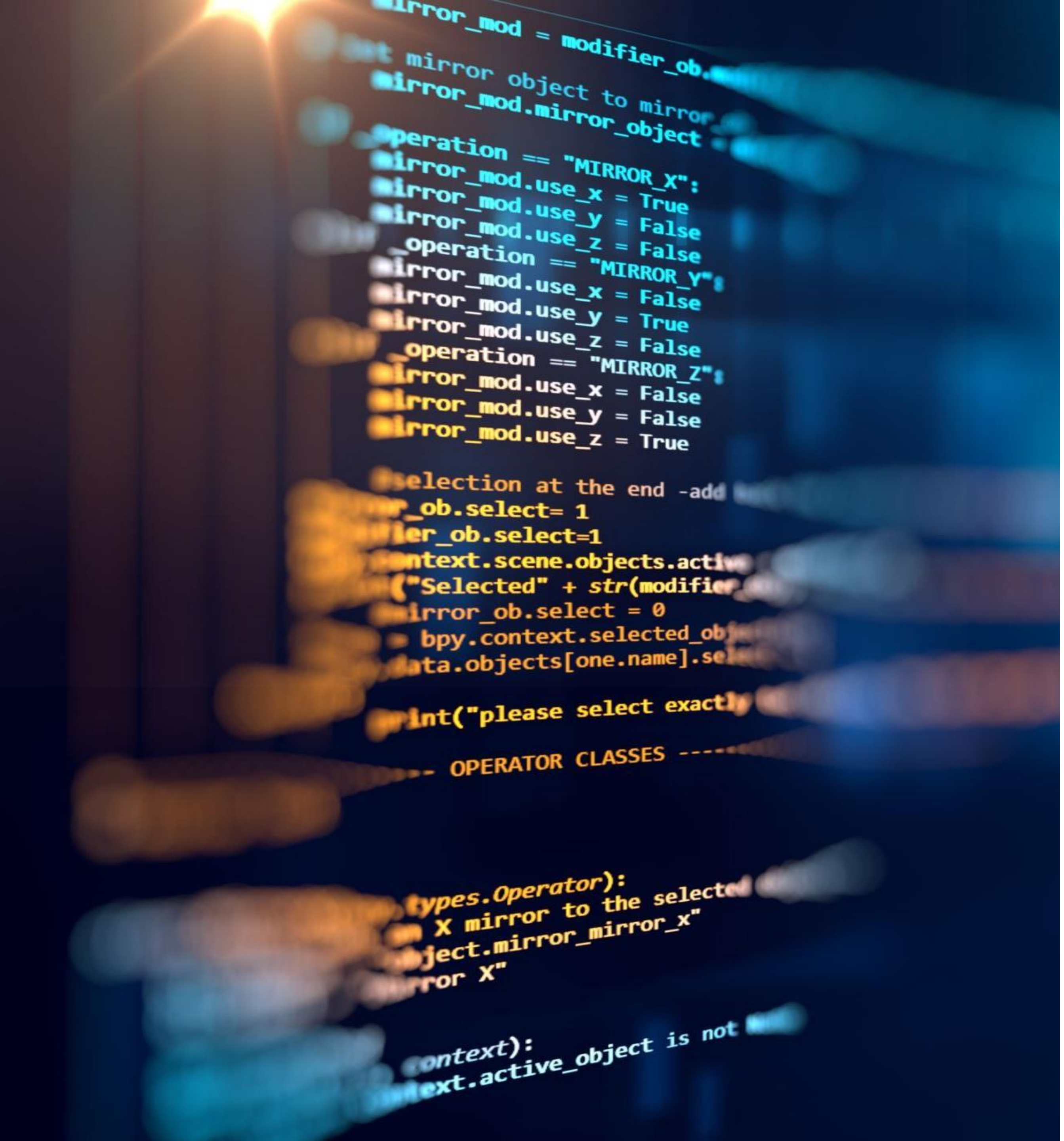
Malware (Viruses, Ransomware)



MALWARE IS MALICIOUS SOFTWARE THAT INFECTS SYSTEMS TO STEAL, DAMAGE, OR LOCK DATA.

RANSOMWARE ENCRYPTS DATA, DEMANDING A RANSOM FOR ACCESS.

EXAMPLE: WANNACRY RANSOMWARE (2017) ATTACKED THOUSANDS OF BUSINESSES, ENCRYPTING THEIR FILES UNTIL THEY PAID HACKERS.



SQL Injection (SQLi)

- Attackers inject malicious code into a website’s database query.
- Can steal, delete, or modify company data.
- Example: The 2011 Sony PlayStation Network breach exposed 77 million user accounts due to an SQL injection flaw.

Cross-Site Scripting (XSS)

Attackers insert malicious scripts into websites to steal user data or hijack accounts.

Happens when websites fail to properly validate user input.

Example: An attacker inserts a fake login form on a company's website to steal customer passwords.

Weak Passwords

Simple or reused passwords make hacking easy.

Most common passwords: *123456, password, qwerty*.

Solution: Use strong, unique passwords and enable multi-factor authentication (MFA).

Example: In 2012, LinkedIn suffered a data breach because many users had weak passwords.

Why Security Matters to the Company

A security breach can result in:

Financial loss – fines, lawsuits, and recovery costs.

Reputational damage – customers lose trust.

Operational disruptions – systems go offline, affecting business operations.

Example: In 2017, Equifax lost $700 million after a breach exposed 147 million customer records.

Best Practices for Non-Technical Staff

Strong Passwords & Multi-Factor Authentication (MFA)

- Use long, unique passwords (at least 12 characters).
- MFA adds an extra layer of security by requiring a second verification step

Recognizing Phishing Emails & Suspicious Links

- Be cautious of unexpected emails asking for login details.
- Hover over links before clicking – look for misspelled URLs.
- Never open attachments from unknown senders.
- Example: A phishing email may claim to be from your bank but contains a fake login page.

Reporting Security Threats Immediately

Report suspicious emails, slow computers, or unexpected pop-ups.

The faster IT knows about an issue, the less damage it can cause.

Best Practices for Technical Teams

Secure Coding Practices

Input validation: Ensure all user inputs are properly filtered.

Sanitization: Remove harmful code before processing user input.

Proper error handling: Prevent errors from revealing system details to attackers.

Regular Vulnerability Assessments & Updates

- Run penetration tests to find weak spots before hackers do.
- Keep software, libraries, and frameworks updated to patch security holes.
- Remove outdated software that could be exploited.

Encryption & Data Protection

- Encrypt sensitive data to protect it from unauthorized access.
- Ensure secure communication (HTTPS, TLS) for online transactions.
- Store passwords securely using strong hashing algorithms.
- Example: Without encryption, a stolen database could expose all customer information.

Conclusion

- Software security is essential for protecting company data and customer trust.
- Common threats include phishing, malware, SQL injection, and weak passwords.
- Both non-technical and technical staff play a role in keeping systems secure.

Reference

- OWASP Foundation. (2023). *Top 10 Web Application Security Risks.*
- Schneier, B. (1996). *Applied Cryptography: Protocols, Algorithms, and Source Code in C.* Wiley.
- Equifax Data Breach Report (2018). *U.S. Government Accountability Office (GAO).*