**Department of Systemics**

**School of Computer Science**

University of Petroleum and Energy Studies

cid:image003.png@01D81F60.F8BDA810

**IT APPLICATION SECURITY  
Assignment**

Submitted by

**Akshat Negi**

**R2142220414**

**Batch - 2**

B.Tech Computer Science and Engineering(CSF)

Submitted to

**Dr. Gopal Rawat**

Assistant Professor (SS)

SOCS, UPES

**Report On Malware**

**Introducing Malware:**

Malware, which is a software i.e., any program or file that is intentionally harmful to a computer, network, or server. The various types of malware include computer viruses, worms, Trojan horses, ransomware, and spyware. These malicious programs steal, encrypt, and delete sensitive data; alter or hijack core computing functions; and monitor end users' computer activity.

**Malware Origins:**

The term malware was firstly used by computer scientist and security researcher Yisrael Radai back in 1990. However, malware existed much before that. One of the earliest known examples of malware was the Creeper virus in 1971, an experiment by BBN Technologies engineer Robert Thomas. Creeper targeted mainframes on ARPANET and displayed a teletype message that said, "I'm the creeper: Catch me if you can." Later on, computer scientist Ray Tomlinson enhanced Creeper, giving it the ability to self-replicate and creating the initial computer worm.

**Evolution of Malware:**

As technology progressed, malware instances began to appear on Apple and IBM PCs in the 1980s, gaining popularity with the advent of the World Wide Web and commercial internet in the 1990s. Since then, malware attacks and defensive measures to combat them have only become more intricate.

**Types of malwares:**

* A virus is the most common type of malware that can execute itself and spread by infecting other programs or files.
* A worm can self-replicate without a host program and typically spreads without any interaction from the malware authors.
* A Trojan horse is designed to appear as a legitimate software program to gain access to a system. Once activated following installation, Trojans can execute their malicious functions.
* Spyware collects information and data on the device and user, as well as observes the user's activity without their knowledge.
* Ransomware infects a user's system and encrypts its data. Cybercriminals then demand a ransom payment from the victim in exchange for decrypting the system's data.
* A rootkit obtains administrator-level access to the victim's system. Once installed, the program gives threat actors root or privileged access to the system.
* A backdoor virus or remote access Trojan (RAT) secretly creates a backdoor into an infected computer system that enables threat actors to remotely access it without alerting the user or the system's security programs.
* Adware tracks a user's browser and download history with the intent to display pop-up or banner advertisements that lure the user into making a purchase. For example, an advertiser might use cookies to track the webpages a user visits to better target advertising.
* Keyloggers, also called system monitors, track nearly everything a user does on their computer. This includes emails, opened webpages, programs and keystrokes.

**Malware Functions:**

Malware is crafted to infect networks and devices, aiming to harm those entities and their users in various ways. The effects of malware, depending on its type and objective, can range from relatively mild to catastrophic. Regardless, all forms of malware are designed to exploit devices for the benefit of hackers who deploy them.

**Malware Detection:**

Users might notice malware through abnormal activity like sudden loss of disk space, sluggish speeds, frequent crashes, or increased unwanted internet activity. Antivirus and antimalware tools can be installed to identify and erase malware. Windows Defender, for instance, is one such tool offered by Microsoft, guarding against spyware, adware, and viruses. It provides scanning options of different intensities.

**Removing Malware:**

Numerous security products are available to detect, prevent, and eliminate malware from infected systems. Malwarebytes, a popular antimalware tool, scans and removes malware from various platforms. It can quarantine and delete malicious software upon detection.

**Preventing Malware:**

Users can take several steps to prevent malware infections, such as installing antimalware software and avoiding suspicious email attachments. Updating security software regularly is crucial to safeguard against evolving hacker tactics. Neglecting updates can expose users to preventable exploits.

**Impact of Malware**

* **Financial Impact:**
* Data breaches and ransom demands leading to monetary losses.
* Business disruption and downtime costs.
* Data recovery and remediation expenses.
* Reputational damage.
* **Operational Impact:**
* Loss of data availability, integrity, and confidentiality (CIA triad).
* System crashes, slowdowns, and instability.
* Productivity losses due to user downtime and remediation efforts.
* **Personal Impact:**
* Identity theft and fraud.
* Privacy violations and exposure of sensitive information.
* Emotional distress and loss of trust.

**Attack Patterns**

* **Common Attack Vectors:**
* Phishing emails and malicious attachments.
* Drive-by downloads from compromised websites.
* Exploiting software vulnerabilities (zero-day, unpatched).
* Social engineering tactics (tricking users into installing malware).
* Malicious mobile apps and infected media.
* Supply chain attacks targeting software dependencies.
* **Attack Stages:**

1. Initial Infection: Gaining access to the system.
2. Persistence: Establishing foothold and avoiding detection.
3. Lateral Movement: Spreading within the network.
4. Payload Delivery: Executing the intended malicious actions.

**Specific Example Attack Patterns:**

* Ransomware: Encrypting data and demanding payment for decryption.
* Spyware: Stealing sensitive information like passwords and financial data.
* Botnets: Controlling compromised devices for distributed tasks like spam or attacks.
* Cryptojacking: Using victims' devices for cryptocurrency mining

**Recently Found Malware**

**Xamalicious:** Android Backdoor Malware on the Google Play Store

*Xamalicious* is a newly discovered Android backdoor malware that infected an estimated 338,300 devices through malicious apps on the Google Play Store.

*Xamalicious* is a backdoor malware that grants unauthorized remote access to infected Android devices. Attackers can exploit this access to steal sensitive data, install additional malware, or disrupt device functionality.

**Type of Malware:**

*Backdoor:* *Xamalicious* functions as a backdoor, creating a hidden channel for attackers to establish remote control over compromised devices.

**Impact:**

Data Theft: Xamalicious can steal various sensitive information, including login credentials, financial details, and contact information.

Malware Installation: Attackers can leverage the backdoor to install additional malware, further compromising the device and expanding the attack scope.

Disrupted Functionality: Malicious actors can manipulate the infected device, potentially leading to data loss, performance issues, or even complete device control.

**Technical Details:**

Distribution: Xamalicious was found embedded within seemingly legitimate applications on the Google Play Store, primarily targeting functionalities like photo editing, language learning, and utilities.

Functionality: Upon installation

Establishes a persistent connection with a remote server controlled by attackers.

Grants remote access capabilities, allowing attackers to execute commands, steal data, and manipulate the device.

Avoids detection by employing obfuscation techniques and hiding malicious activities within legitimate app functionalities.

**Countermeasures:**

Download apps only from trusted sources: Primarily rely on the official Google Play Store and exercise caution with third-party app stores or websites.

Scrutinize app permissions: Be wary of apps requesting excessive permissions unrelated to their advertised functionality.

Maintain updated security software: Install a reputable mobile security solution and keep it updated with the latest malware definitions.

Stay vigilant: Avoid downloading unknown apps or clicking suspicious links, and exercise caution with unsolicited attachments or messages.

**Recommendations:**

Users who suspect Xamalicious infection should immediately uninstall any recently downloaded suspicious applications.

Security researchers and app store providers should continue collaborating to identify and remove malicious apps from circulation.

Users are encouraged to stay informed about emerging cybersecurity threats and adopt safe mobile practices to protect their devices and data.