NAWA Media

Types of Malware

Section: 3.1

Threats of Journalists: Malware

Journalists are becoming increasingly dependent on devices, such as laptop and mobile phones for accessing information, posting content and contacting individuals and groups.

This makes a journalist's device one of the most valuable tools in their arsenal, also making them the most vulnerable.

Journalists, particularly those on the go, use their devices on different networks, sometimes even on public WiFi, and are in touch with several contacts.

Our devices often contain sensitive and private information about stories, the people we work with and ourselves.

Thus it is of the utmost importance that we keep these devices safe and secure from harmful elements such as viruses and malware.

What is Malware?

Malware can be injected into your devices to do harmful activities like deleting a file, making a log of your keystroke, changing system settings, silently spying on your online surfing or even accessing your webcam without you knowing.

Malware can be categorized based on the intention of what the hacker wants to achieve.

It can prevent your network from functioning correctly and also take down the whole system so that limited capacity is left for real work to be performed.

Types of Malwares

Malware is a catchall term for different types of malicious programs which include:

- **Adware:** Short for advertising-supported software, adware subjects those infected to unwanted and automatically-generated advertising. Adware is often downloaded unknowingly by users as it is bundled together with unauthorised, 'free' versions of software.
- **Spyware:** As the name suggests, spyware is a software used to monitor the activities of the targeted user. Commonly used tactics include monitoring keystrokes, collecting saved data, financial data, passwords, pages you visit and activity on your device.
- **Ransomware:** Ransomware is a type of malware that holds the data and systems of users captive or for ransom. The hackers often ask for a sum of money to be paid before the data or system is released by the attacker.
- **Rootkits:** A rootkit is a type of malware that allows an unauthorized user to remote access to a device or security programs. The malware can exist secretly on a system and be used to control, access and modify programs and files on a device.
- **Trojan horses:** As the name suggests, a Trojan horse, or "Trojan", malware disguises itself as a normal, harmless file or program. Once installed, trojans give the attacker remote access to the computer system to monitor, steal files or cause damage to existing files.

Types of Malwares

- **Worms:** These are standalone malwares that spread from one computer to another and cause harm to systems they enter through a variety of different ways; i.e. slowing down systems, consuming bandwidth or containing “payloads” that damage host computers by stealing or deleting data. Worms are among the most common types of malware.
- **Viruses:** A computer virus is a type of malware that spreads from file to file. The virus works by embedding itself into a file or program and will be activated once the embedded code is executed.

NAWA Media

In the **next** section we will explore the ways in which Malware can Infect your device/network

BCMCR | Birmingham Centre for Media and Cultural Research

BIRMINGHAM CITY University

MEEDAN

Check

Sida