TALENTO TECH

REGIÓN 3
CAUCA - NARIÑO
LESSON 2 -UNIT 2

TIC

Universidad Tecnológica de Pereira

faceIT

Lesson 2: Reading: What is malware?and types of malware What is malware?

Malware, a type of intrusivesoftware, is createdby cybercriminals (often called hackers)to steal data and damage computers, including viruses, worms, Trojan viruses, spyware, adware, and ransomware, which have been widely used in recent attacks.

What is the intent of malware?
Malware is harmfulsoftware that corruptscomputer networks, aiming to cause chaos, steal information, or steal resources for monetary gain or sabotage.

- Intelligence and intrusion techniques: involvethe extraction of sensitive data like passwords from sensitive sources like emails and plans.
- Disruption and extortion: Ransomware is a type of disruption and extortion that locks up networks and PCs, holding them hostage for financial gain.

- Steal computer resources: The act of stealing computer resources involves using your computing power to run botnets, cryptomining programs, or send spam emails.
- Monetary gain:Selling your organization's intellectual property on the dark web can lead to monetary gain.

How do I protect my network againstmalware?

In order to stop breaches, firms usually concentrate on preventative tactics. Businesses believe they are protected when the perimeter is secured. But soon, some sophisticated malware will infiltrate your network. Deploying technologies that continuously monitor and identify malwarethat has eluded perimeter defensesis therefore essential. High-level network visibility and intelligence, as well as several layers of defense, are necessary for effective sophisticated malware protection.

7 types of malware

- Virus: Viruses are malicious software that executes macros and spreads from host to host, disrupting a system's functionality and causing significant operational issues and data loss.
- Worms: Worms are malicious software that rapidlyreplicate and spreadto devices within a network, causing disruption and data loss, unlike viruses

- Trojan virus: Trojan viruses, disguised as helpful software, can access sensitive data, modify,block, or deleteit, causing severedevice performance issuesand not self-replicating.
- Spyware: Spyware is maliciousssoftware that secretlyruns on a computer, targeting sensitive information and allowing remote access to predators, often stealing financial or personal data, particularly through keyloggers.
- Adware: Adware is malicious software that collectscomputer usage data and offers ads, potentially causing system issues like redirection to unsafe sites, Trojan horses, and spyware. Intelligent scanning of adware is crucial for protection.
- Ransomware: Ransomware is malicious software that encrypts sensitive system data, demandsa financial payoutfor its release,often part of a phishingscam. The attacker uses a mathematical key to unlock the data.
- Fileless malware: a memory-resident type, operates from a victim's computer's memory, making detection harder than traditional malware. It disappears when the
- victim reboots, making forensics more challenging. Cisco Talos posted an example in 2017.

TIC

What are the benefitsof advanced malwareprotection?

Advanced malware protection software helps prevent, detect, and remove threats from computer systems by modifying common malware, testingfor sandbox conditions, and fooling security software into believing it's not malware.

TALENTO TECH

Universidad Tecnológica de Pereira

faceIT