ELEARNINGNEWS ARTICLE

Year 9 - number 322 Wednesday 19 february 2025

Ransomware Attacks on the Rise: How to Protect Yourself from Cybercriminals?

The number of ransomware attacks is growing exponentially: discover the main techniques used by hackers and learn to defend against cyber risks.

In recent years, **cyber threats have increased exponentially**, affecting companies, public and private entities. Hackers use increasingly sophisticated techniques to infiltrate computer systems, steal sensitive data, and cause economic damage. Among the main dangers are malware, trojans, spyware, and especially ransomware. Criminal organizations operate globally, exploiting software vulnerabilities, human weaknesses, and advanced technologies to compromise entire systems.

The consequences of a cyber attack can be devastating: data theft, paralysis of business activities, reputational damage, and in the most serious cases, ransom demands for system restoration. Victims often find themselves having to choose between paying large sums of money or suffering the irreversible loss of their files. **Prevention and awareness of cyber dangers** are therefore fundamental to protect both the company and oneself.

Ransomware: What Is It?

Among all cyber threats, **ransomware** is one of the most insidious and harmful. This type of malware **blocks access to data on an infected system and demands payment to unlock it**.

Ransomware can target both large companies and small entrepreneurs and private users, and has seen a worrying evolution in recent years. Criminal organizations have specialized in creating increasingly sophisticated malware capable of evading antivirus software and spreading rapidly within corporate networks. Some attacks aim to encrypt files and prevent victims from accessing them, while others target the theft and dissemination of sensitive data, threatening to make them public if the ransom is not paid.

A disturbing aspect is that, even in case of payment, there is no guarantee that the data will be returned. Many companies have suffered attacks that irreparably compromised their digital archives, despite following the hackers' demands. For this reason, **prevention is the best strategy against ransomware**.

Below, we analyze the main ways ransomware is spread, illustrating concrete examples to understand the extent of the threat.

1. Phishing (Malicious Emails)

One of the most common techniques for spreading ransomware is **phishing**, or sending **fraudulent emails** containing harmful links or infected attachments. These seemingly come from trusted sources, such as banks, companies, or colleagues, and often include an urgent message to push the victim to immediately open the attachment.

- **Example:** an employee receives an email that appears to come from their company's human resources office, with an attached Excel file called "Salary Update 2024". The document requires enabling macros to view the data. As soon as the user activates the macros, ransomware installs and begins encrypting all company documents, blocking access to files and paralyzing work activity.

2. Software Vulnerability Exploitation

Hackers exploit **vulnerabilities in outdated software** to infiltrate devices and install ransomware. Operating systems, servers, and obsolete applications represent an ideal access point for criminals, who can inject malicious code without the user noticing.

- **Example: The WannaCry attack of 2017** hit thousands of companies worldwide by exploiting a Windows vulnerability that Microsoft had already fixed with an update. However, many companies hadn't installed the security patch in time and were infected, suffering multimillion-dollar damages and prolonged interruptions.

3. Drive-by Download

This technique involves automatic infection of the device when a user visits a **compromised site**. No clicking is necessary: just accessing the page downloads the ransomware.

- **Example:** an employee searches for free images online and accesses a wallpaper site that has been compromised by hackers. Without realizing it, their browser downloads and executes malware that encrypts company files.

4. Compromised Remote Access (RDP)

The use of **weak or stolen passwords** allows hackers to enter company systems through Remote Desktop Protocol (RDP) and manually install ransomware.

- **Example:** a company uses RDP to allow employees to work remotely. A criminal finds access credentials on a hacker forum and accesses the internal network, launching ransomware that blocks all servers.

Read also: **Cybersecurity: How to Set a Secure Password**

5. Malvertising (Malicious Advertising)

Hackers inject malicious code into **advertisements** on legitimate websites. When a user views or interacts with the advertisement, the ransomware is downloaded.

- **Example:** a user visits a well-known news site and sees an advertisement for a contest. By clicking on it, their browser is redirected to a malicious site that downloads ransomware in the background.

6. USB and Removable Devices

Criminals can also spread ransomware through **infected USB devices**, intentionally left in public places to induce victims to pick them up and connect them to their computers. Once connected, the malware installs automatically and compromises files.

- **Example:** an employee finds an abandoned USB drive in the company parking lot. They connect it to their PC out of curiosity, and the ransomware contained within activates, encrypting all company files and spreading to the internal network.

7. Supply Chain Attacks

Attackers compromise legitimate software or services, infecting end users through **tampered software updates** or breached cloud services.

- **Example: the attack on Kaseya's software** by the REvil cybercrime group in 2021 exploited a vulnerability to distribute ransomware to hundreds of companies through an infected software update.

8. Chain Infections (Worm-like Behavior)

Some ransomware is designed to **spread automatically between devices on a network** without requiring human intervention, exploiting system vulnerabilities or compromised credentials.

- **Example:** the **NotPetya** ransomware in 2017 infected entire companies by automatically propagating from one device to another, exploiting exploits not fixed promptly.

9. Fileless Attacks

These attacks use legitimate operating system tools, such as PowerShell or WMI, to execute ransomware directly in memory, **avoiding leaving obvious traces on the disk** and making detection more difficult.

- **Example:** a hacker exploits a vulnerability in PowerShell to launch ransomware without saving any files to disk, evading traditional antivirus systems.

10. Advanced Social Engineering

Cybercriminals use **social engineering** techniques to deceive victims, convincing them to download malicious files or provide access credentials.

- **Example:** an executive receives an email that appears to be from their IT administrator, asking them to download a security update. In reality, the file contains ransomware that blocks the entire company system.

11. Backup System Attacks

To prevent victims from restoring their data, attackers try to **delete or corrupt backups** before activating the ransomware.

- **Example:** hackers access company backup servers, delete recent saves, and then release the ransomware, leaving the company without possibility of recovery.

Ransomware represents a concrete and evolving threat. Protection means not only adopting advanced security solutions but also **training** to recognize the signs of a possible attack.

Online training to protect ourselves

Training is the first and most effective **defense tool against cyber threats**. For this reason, **Mega Italia Media** offers a series of **online courses** designed to improve employee awareness and skills in **information security**. Each course is structured to address the main risks related to cybersecurity in a clear and practical way, providing concrete solutions and preventive strategies.

Find out our online course and become an expert of data protection!

Cybersecurity ? Company information protection (40 minutes)

Online course about risks and responsibilities related to data and information treatment via IT devices. The lesson is intended for all workers who use IT devices (PC, laptops, tablets, smartphone, etc...) both in office and in smart working/remote working.