Ransomware, Don't be the next victim!

How it all began

Ransomware technology was first developed by a Harvard-trained evolutionary biologist by the name of Joseph L. Popp. While at the international AIDS conference held by the World Health Organization in Stockholm, Sweden, He launched the AIDS Trojan by giving diskettes infected with ransomware to attendees. The code hid file directories on their computers and demanded $189 be sent to Panama for their data to be recovered. [1]

[1]https://www.fortinet.com/tw/resources/cyberglossary/ransomware

A deeper dive into ransomware

Ransomware is a type of malicious software that threatens a victim by destroying or blocking access to critical data, networks or systems until a ransom is paid.

Recent ransomware attacks

Nvidia: The world's largest semiconductor chip company was compromised by a ransomware attack in February, 2022. The company confirmed that the threat actor had started leaking employee credentials and proprietary information online.

The ransomware group, Lapsus$, took responsibility for the attack and claimed that they had access to 1TB in exfiltrated company data that they would leak online. It also demanded $1 million.

Costa Rica Government: This has probably been the most spoken-of attack in 2022 as it's the first time a country declared a national emergency in response to a cyber-attack. The first ransomware attack on the nation began in early April and brought the ministry of finance to its knees, impacting not just government services but also the private sector engaged in import/export.

On May 31, another attack plunged the country's healthcare system into disarray. This attack, linked to HIVE, affected the Costa Rican social security fund. This attack directly affected the common Costa Rican person as it took the country's healthcare systems offline.

Bernalillo County, New Mexico: This was one of the first big attacks in 2022. On January 5, the largest county in New Mexico discovered that it had become the victim of a paralysing ransomware attack, taking several county departments and government offices offline.[2]

In May, 2022, **The Bank of Zambia** refused to pay ransom to a group known as Hive that was behind a cybersecurity breach that caused minimal damage to its systems.
"All of our core systems are still up and running," Greg Nsofu, information and communications technology director at the Bank of Zambia, told Journalists in Lusaka.(Lusakatimes)

Contacts:

cell : +260777680138

mail: frontdesk@zcsi-foundation.org

Common Types of Ransomware

Crypto ransomware or **encryptors** are one of the most well-known and damaging variants. This type encrypts the files and data within a system, making the content inaccessible without a decryption key.

Lockers completely lock you out of your system, so your files and applications are inaccessible. A lock screen displays the ransom demand, possibly with a countdown clock to increase urgency and drive victims to act.

Scareware is fake software that claims to have detected a virus or other issue on your computer and directs you to pay to resolve the problem. Some types of scareware lock the computer, while others simply flood the screen with pop-up alerts without actually damaging files.

Doxware or **leakware** threatens to distribute sensitive personal or company information online, and many people panic and pay the ransom to prevent private data from falling into the wrong hands or entering the public domain.

RaaS (Ransomware as a Service) refers to malware hosted anonymously by a "professional" hacker that handles all aspects of the attack, from distributing ransomware to collecting payments and restoring access, in return for a cut of the loot.

How to spot a ransomware attack

The **first** sign of a ransomware attack is when your device starts slowing down without any apparent reason. When ransomware finds its way into your device's system, it basically starts scanning it in the backdrop for hijacking files. This scanning process slows down the device's speed.

The **second** sign of a ransomware attack includes automatic alterations in your files. These alterations may include file name changes or file type changes.

Thirdly, if you notice an automatic encryption of files such as documents and images which you did not encrypt yourself and their number keeps multiplying, there is a high chance that you are under a ransomware attack.[3]

Best practices against ransomware

- Avoid clicking on links from unknown or untrusted sources.
- Utilize strong firewall and antivirus defences on your network.
- Keep backup hardware on hand in case the main hardware is damaged during a cyber assault so systems can be rebuilt.
- Update your network using the most recent software fixes.
- Consider network segmentation on a physical or logical level.
- Think about encrypting data to make it more difficult to access, copy, or transfer.
- Utilize an "allow list" for applications only to allow certain programs to run on your network.
- Create a business recovery plan that will enable you to continue operating even if some systems are unavailable.
- Employee training on internet safety practices.

[2] https://www.cm-alliance.com/cybersecurity-blog/5-major-ransomware-attacks-of-2022

[3] https://jt.org/how-to-spot-a-ransomware-attack/