FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO

NETWORK AND INFORMATION SYSTEMS ENGINEERING
2023/2024

RANSOMWARE

CC4031 - NETWORK SECURITY

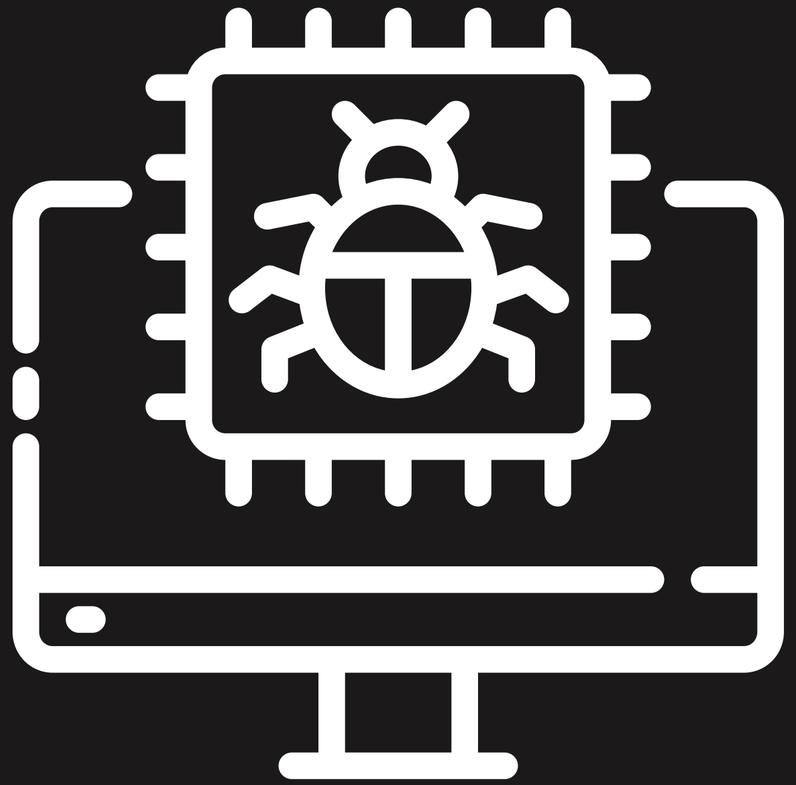
Patrícia Miranda up202007675
Raquel Carneiro up202005330
Tomás Carmo up202007590

OBJECTIVES

By the end of this presentation, you will be able to:

1. Define ransomware and identify common types used
2. Recognize the history timeline of ransomware and its evolution
3. Identify common vulnerabilities and ways to mitigate respective attacks
4. Reach to conclusions on the different topics discussed

WHAT IS RANSOMWARE?



Malware, short for malicious software, refers to a broad category of software designed to harm or exploit any programmable device, service, or network. Within existing malware, ransomware stands out as a **particularly subtle strain until it's shown to the user.** Ransomware sets itself apart from other types of malware by **actively extorting victims by data encryption or locking, then charging for the release of the data.**

TYPES OF RANSOMWARE?

CRYPTO RANSOMWARE

Encrypts a victim's files with sophisticated cryptography, demanding a ransom, typically in cryptocurrency, for the decryption key.

LOCKER RANSOMWARE

Hampers access to the entire system. The screen displays a ransom note prohibiting access to all system functions, rendering the computer inoperable until the ransom is paid

RANSOMWARE AS A SERVICE (RAAS)

Business model between ransomware operators and affiliates, where affiliates pay to launch ransomware attacks developed by the operators

MOBILE RANSOMWARE

Restricts access to the device or the data stored on it, typically by encrypting files or locking the screen with a ransom note

RANSOMWARE HISTORY

1989 — Present

EARLY STAGES

The AIDS Trojan is the first known instance of a ransomware attack.

RANSOMWARE HISTORY

1989 2006 Present

CRYPTOVIROLOGY

Ransomware embraced Cryptography.

RANSOMWARE HISTORY

1989 — 2013 — Present

POLICE TROJANS

Impersonation of police enforcement to scare victims.

CRYPTO-RANSOMWARE

Easy and untraceable method to extort victims.

RANSOMWARE HISTORY

1989 2015 Present

RANSOMWARE-AS-A-SERVICE

Ransomware developers write software, while partners launch attacks with it.

RANSOMWARE HISTORY

BIG GAME HUNTING

Target big organizations to obtain a bigger payout.

RANSOMWARE HISTORY

1989 2019 Present

DOUBLE AND TRIPLE EXTORTION

Leak sites and DDoS to pressure the victims to pay ransom.

RANSOMWARE HISTORY

1989 — Present

RANSOMWARE AS OF TODAY

Ransomware continues to grow in both its influence and destructive capacity.

PHISHING VULNERABILITIES

A very common attack and still very active to this day is the phishing attack. **It relies on deceiving the victim with a convincing email or pop-up impersonating a reputable business or alerting for a fake emergency**, for example.

Although it’s highly a human fault, phishing attacks, or at least the damage these cause, can be diminished.

Think of an email or message you received that asked for personal information. What made it suspicious?

COUNTERMEASURES

- **Blacklist and WhiteList**
- **Machine Learning Based**
- **Authentication Reinforcement**


1.
Attacker sends phishing mail to target
Hacker
Target
2.
Victim clicks on Phishing link and visits fake website
3.
Hacker collects important credentials
4.
Hacker uses victim's credentials to access private information
Original Website
Phishing Website

PHISHING ATTACKS EXAMPLES

WANNACRY, 2017

A famous attack that relied in phishing emails as its initial infection technique. It spread all across the globe, being **one of the most destructive ransomware attacks in history.**

Beyond healthcare, this ransomware manifested across many industries. **Major corporations such as Renault, Nissan, and FedEx's subsidiary TNT Express**, experienced substantial operational challenges.

NOTPETYA, 2017

In contrast, the NotPetya attack, which followed shortly after in June 2017, was initially perceived as a ransomware outbreak but was later identified as a **more malicious state-sponsored act of cyber warfare,** primarily targeting Ukraine but quickly spreading globally.

NotPetya's design was much more destructive; it **aimed not just to ransom but to wipe data, leading to permanent loss of data and significant disruption of operations.**

WANNACRY, 2017

Massive ransomware cyber-attack hits nearly 100 countries around the world

More than 45,000 attacks recorded in countries including the UK, Russia, India and China may have originated with theft of 'cyber weapons' from the NSA

FedEx says cyber attack to hurt full-year results

By Reuters Staff

2 MIN READ

(Reuters) - Package delivery company FedEx Corp FDX.N said a disruption in services in its TNT Express unit following a cyber attack last month would hurt its full-year results.

NHS cyber-attack: GPs and hospitals hit by ransomware

13 May 2017

Throwback Attack: WannaCry ransomware takes Renault-Nissan plants offline

GARY COHEN APRIL 22, 2021

Security researchers with Kaspersky Lab have recorded more than 45,000 attacks in 99 countries, including the UK, Russia, Ukraine, India, China, Italy, and Egypt. In Spain, major companies including telecommunications firm Telefónica were infected.

NOTPETYA, 2017

CYBERCRIME

NotPetya Attack Costs Big Companies Millions

Some of the big companies hit by the NotPetya malware in late June have reported losing hundreds of millions of dollars due to the cyberattack.

By Eduard Kovacs
August 17, 2017

Some of the big companies hit by the NotPetya malware in late June have reported losing hundreds of millions of dollars due to the cyberattack.

With Ukraine as its primary target, NotPetya quickly spread to more than 60 countries, destroying the computer systems of thousands of multinationals.

The damage: One of these was the global transport and logistics giant Maersk, where NotPetya destroyed "all end-user devices, including 49,000 laptops and print capability", according to the company's head of technology Adam Banks.

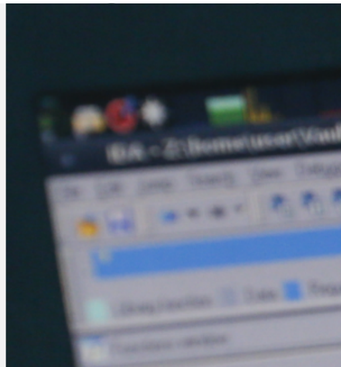
The damage caused by NotPetya has been pegged at more than $10 billion. Maersk alone lost $250 million and $300 million. Other companies affected included Mondelez, Merck, WPP,

Reckitt Benckiser, Saint-Gobain and TNT Express.

Danish shipping giant AP Moller-Maersk estimates that the attack has cost it $200-$300 million. The conglomerate believes the cyberattack will have a significant impact on its finances in the third quarter due to revenue lost in July.

American pharmaceutical giant Merck had still been working on restoring operations in late July. In its latest financial results announcement, the firm said the cyberattack had disrupted its worldwide operations, including manufacturing, research and sales, but did not specify the exact losses caused by the incident.

How the NotPetya attack is reshaping cyber insurance



RDP VULNERABILITIES

Remote Desktop Protocol (RDP) is a Microsoft network communication protocol that allows communication with a Windows Server. This remote access protocol has its security flaws that can prove to be very damaging to users and corporations involved.

Some of this include **weak authentication and default port exposure**. With these two combined, an attacker can scan IP's, intercept the default port if open, and deploy the desired ransomware.

COUNTERMEASURES

- **Strengthening Credentials**
- **Changing the Default Port**
- **Using virtual Private Network**

RDP ATTACKS EXAMPLES

MAZE, 2019

The Maze attack, used a new extortion method which leaked the victim's data if they refused to pay the ransom.

One of its main ways of propagation was through RDP brute force attacks, making victims of an IT services firm, the Hammersmith Medicine Research during the COVID-19 pandemic and many others.

NEMTY, 2019

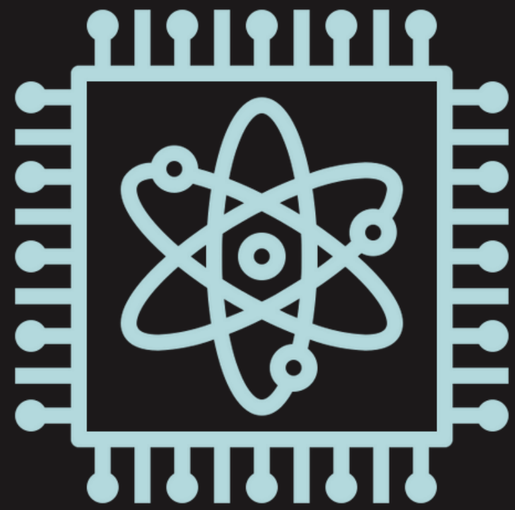
A notable ransomware attack that specifically targeted RDP servers was the Nemty attack, which, similar to Maze, threatened to leak the victim's important files, including their credentials.

This leak of RDP credentials would then feed other attacks, such as the Crysis ransomware attack that aimed at large organisations in New Zealand and Australia.

CONCLUSION

The cybersecurity community must remain **vigilant and innovative**, anticipating the next iteration of ransomware tactics and preparing for the inevitable convergence of cyber threats with emerging technologies such as **artificial intelligence and quantum computing**.

The battle against ransomware is not just about protecting data; it is about **safeguarding our societal, economic, and political pillars** against the insidious reach of cyber warfare.



ChatGPT