CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

Ransomware

Adding “*profit*” to your computer skills

Julio Cesar

What is ransomware?

Type of malware that encrypts files on a chosen target's computer or network and demands a ransom pay in exchange for the decryption key.

One name, many techniques

Encrypting, locker, scareware, doxware, RaaS, mobile, MBR, and so on.

It started long time ago

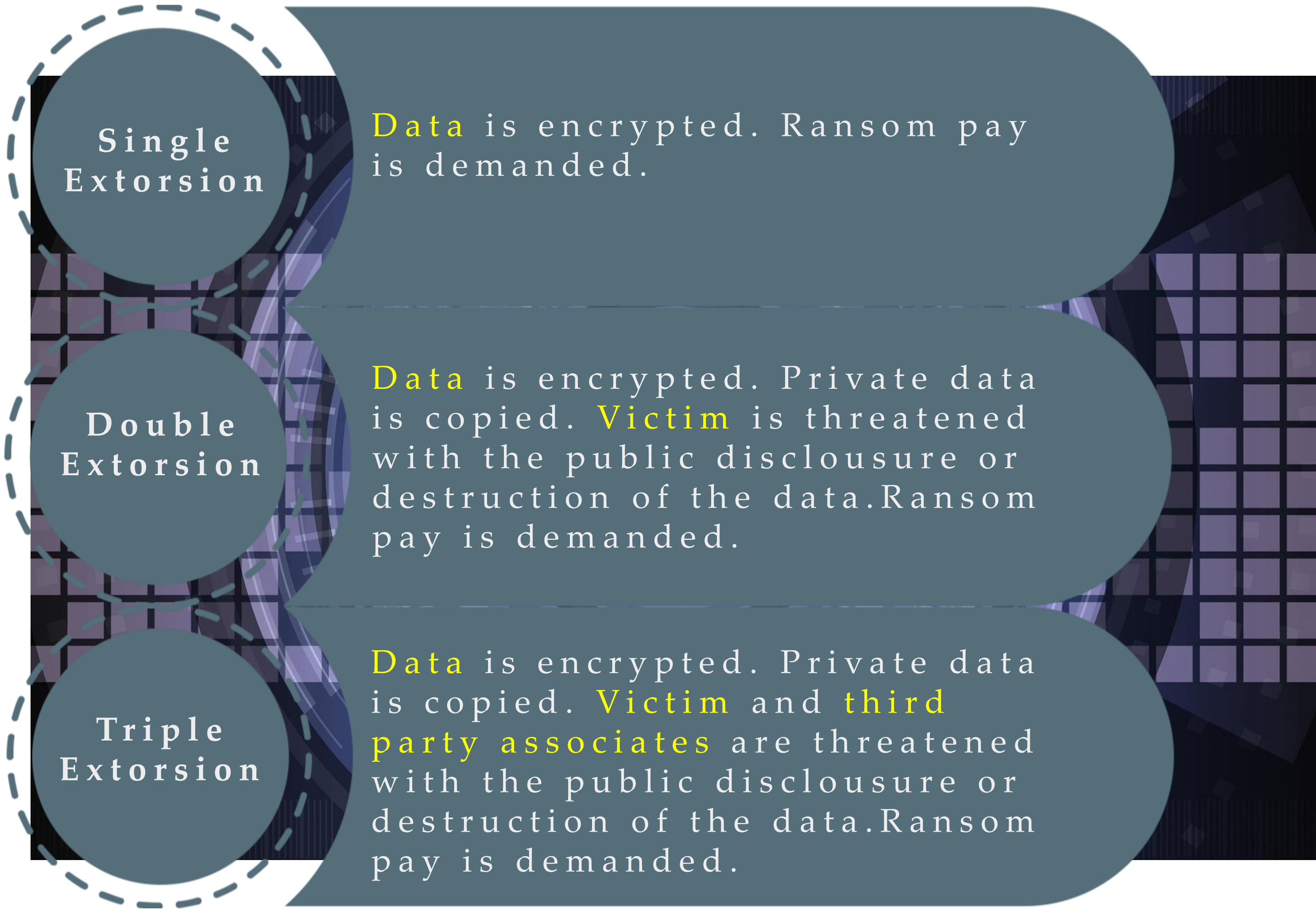
It's commonly accepted that the 1989 PC Cyborg Trojan (aka AIDS Trojan) was the first iteration of this long journey heading towards modern day ransomware code. It was phisically distributed via a 5,25" floppy disk to 20.000 AIDS Conference attendees. It demanded a payment of 189 USD. It was that long ago…

In April 2020 EDP Ragnar Locker ransom note demanded 10,9M

It started long time ago

It's commonly accepted that the 1989 PC Cyborg Trojan (aka AIDS Trojan) was the first iteration of this long journey heading towards modern day ransomware code. It was phisically distributed via a 5,25" floppy disk to 20.000 AIDS Conference attendees. It demanded a payment of 189 USD. It was that long ago…

In April 2020 EDP Ragnar Locker ransom note demanded 10,9M



Single Extorsion

Data is encrypted. Ransom pay is demanded.

Double Extorsion

Data is encrypted. Private data is copied. Victim is threatened with the public disclousure or destruction of the data.Ransom pay is demanded.

Triple Extorsion

Data is encrypted. Private data is copied. Victim and third party associates are threatened with the public disclousure or destruction of the data.Ransom pay is demanded.

It's all about money

Even when no ransom is paid:

20% of ransomware costs are attributed to reputation and brand damage.

In many cases, downtime costs and other indirect losses are hard to calculate.

In 2021, Brazilian food industry JBS paid $11 million in ransom after a ransomware attack by REvil, a russian collective.

Ransomware is bad

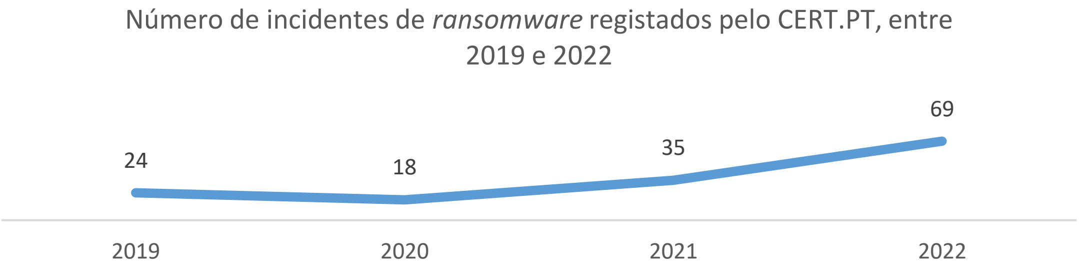
But it's worse in the telecom sector

- Downtime means losses in revenue, productivity and customer trust,
- Critical systems are really critical in telcos, recovery is usually slow,
- Reputation damage is even worse when customer data is compromised (30% of data violations reported to CNPD, R&C2023)
- **Customer data** is usually both sensitive and extensive,
- Impacts on the network impact the **productivity of customers**, companies and State,
- Telcos often invest in R&D, intelectual property might be compromised,
- Legal and Regulatory consequences, if non-compliances are found after.

Revil attacked Telecom Argentina in 2020, critical data was deleted. Nefilim exposed sensitive data after attacking Orange France.

Brace for impact

We are going slow, but wrongly


Número de incidentes de *ransomware* registados pelo CERT.PT, entre 2019 e 2022

- Preparation is key – redundant backup systems, network segmentation, draconian credential policy
- Prevention - Information, Education, Training
- Early Detection – Behaviour analisys. Signatures are not enough and perimeter is overrated
- Termination – Persistence is deadly. Sanitize your systems
- Recovery – Business continuity plan

In 2022 phishing was the original vehicle for 45% of all ransomware attacks.

Future Outlook

Cloudy days ahead

- Running to the cloud? So is ransomware.
- Ransomware compromised file sharing services
- RansomCloud attacks cloud-based email services, such as Office 365, using phishing.
- Compromising cloud vendors is a growing option
- 5G enabled smart cities and it's autonomous (unpatched) systems are likely targets
- Ransonware, war biased, can become destructionware.

Smarter gangs are targeting smaller companies – and even individuals – that hold valuable sensitive information with tailor-made, social engineered, phishing attacks leading to more profitable ramsoms.

Thank You

Julio Cesar

julio.cesar@cncs.gov.pt

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL