# CYBERSECURITY

# RANSOMW ARE

Antonio Gonzalez Cuellar Taboada
Jorge Rosco Martin

# TABLE OF CONTENTS

# WHAT IS RANSOMWARE ?

Ransom malware, or ransomware, is a type of malware that prevents or limits users from accessing to their system or personal files employing encryption.

Then, a ransom is demanded to provide access. Usually, once the computer is infected, the virus spreads through the network, encrypting other systems such as databases, servers or other devices.

# HOW DOES RANSOMWARE WORK ?

## 1st SYSTEM INFECTION

The system is infected using different techniques such as phishing spam, malicious advertisement, social engineering or others

## 2nd NETWORK PROPAGATION

Malware attempts to spread across all network systems, exploiting vulnerabilities or getting administrator permissions

## 3rd SYSTEM ENCRYPTION

Ransomware searches and encrypts valuable files using asymmetric encryption: public-private keys

## 4th RANSOM DEMAND

The user is required to pay a fee to decrypt the files. If the user refuses, the files are lost forever or, if there are sensitive files, they are published

# COMPANIES AFFECTED







# WannaCry

Infected a total of more than $200{,}000$ computers on $150$ countries worldwide.

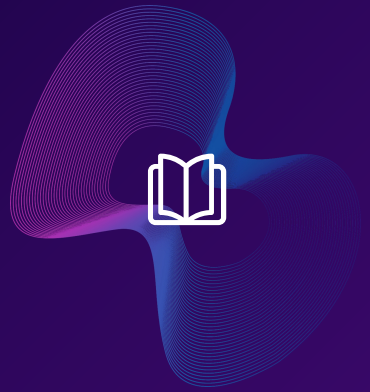
Its operation was based on Eternal Blue, an exploit allegedly developed by the NSA and used to propagate on local networks and remote hosts.

# Ryuk

Used by two or more criminal groups, probably Russian, targeting government organizations rather than individuals

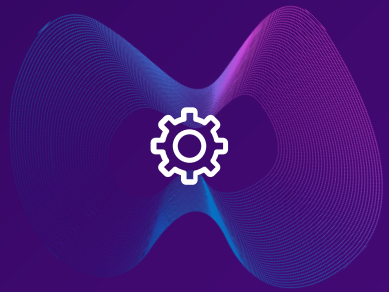
In many cases, days or weeks may pass between device infection and the time of mass encryption, as criminals penetrate deeper into the network to inflict maximum damage. It also disables the "system restore" function preventing possible file recovery.

# CONCLUSIONS



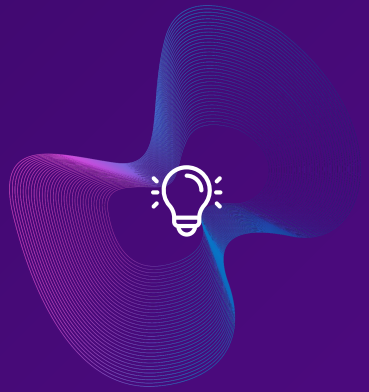
## DEFINITION

Malware that limits users from accessing to their system or personal files employing encryption



## MECHANISM

Infection, Encryption, Propagation and Ransom demand



## USAGES

Employed by cybercriminals to get the victim to pay for the restoration of their systems or personal data