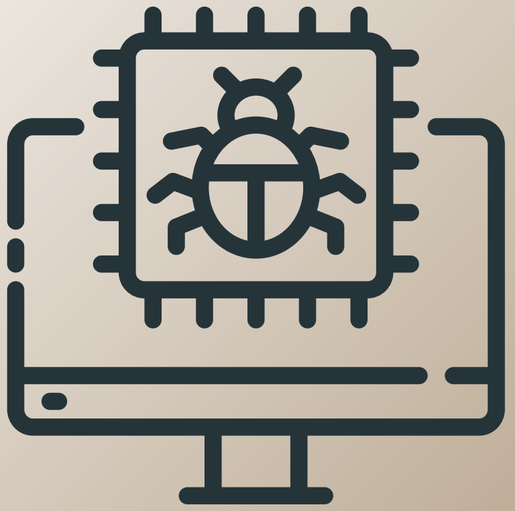
enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY



Cybersecurity
Ransomware

CONFIDENT PROJECT - JESSE TORNI

WHAT IS RANSOMWARE?

- "Ransomware is a type of attack where threat actors take control of a target's assets and demand a ransom in exchange for the return of the asset's availability and confidentiality."
- Every ransoware has three key elements: **assets, actions** and **blackmail**
- The concept of ransomware has changed through-out the years
- Ransonwares can **lock, encrypt, delete** and **steal**

Table 1: Capabilities of current ransomware in terms of actions they perform and assets they target

	Actions			
Assets	Lock	Encrypt	Delete	Steal
Files	✗	✓	✓	✓
Memory	✗	✓	✓	✓
Folders	✗	✓	✓	✓
Database Content	✗	✓	✓	✓
MFT	✓	✓	✓	✗
MBR	✓	✓	✓	✗
Cloud	✗	✓	✓	✓
CMS	✗	✓	✓	✗
Screen	✓	✓	✓	✗

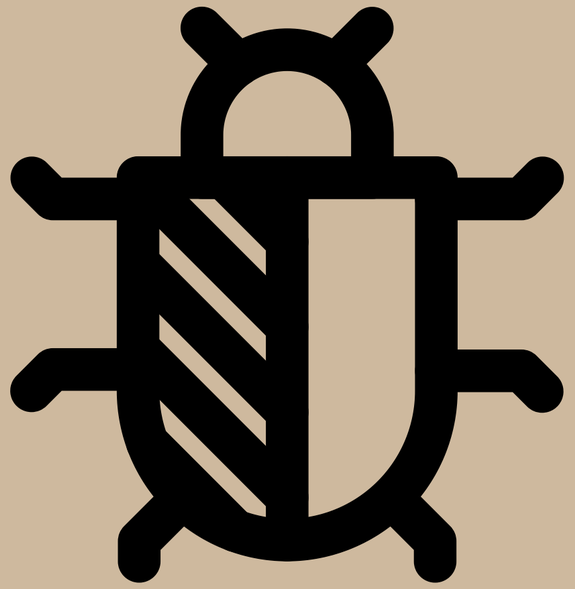
WHAT IT TARGETS?

- Small businesses are a popular targets of attack for ransomware, because they have typically less cyber security walls
- Ransomware is one of the most common cyber threat and 623 million incidents were recorded of ransomware in 2021 (upguard, 2022)
- Targets sensitive informations
- Multiple types of assets are targeted by ransomware (Table 2)

Table 2: Commonly observed assets in Ransomware incidents

ASSETS TARGETED BY RANSOMWARE	
FILES	We refer to files used by the user, traditionally searched by ransomware using file extensions due to their potential value. These can also be system files that contain configurations. Files also include network files as remotely mounted in the local computer.
FOLDERS	We refer to user and system folders that attackers may be interested in due to the files they may contain.
MEMORY	Some ransomware actually uses memory mapped I/O to encrypt cached documents in memory and force applications to save the encrypted file back to disk
DATABASE CONTENT	We refer to the content of databases, including rows and tables, and not particularly to the files where the dataset is stored. Some databases have the whole content in one file. Some databases have some of their rows and tables encrypted, but not all. And some databases are in-memory databases without any files.
SCREEN	We refer to the screen of the graphical user interface of an operating system. Ransomware is known for creating a special screen where users can interact with and disabling any other screen of the operating system.
MASTER FILE TABLE (MFT)	The MFT is a special file stored in the hard drive that contains an index of all files and folders in the volume.
MASTER BOOT RECORD (MBR)	The MBR is a special partition in a hard disk used in the booting process of the operating system. This partition can be locked by ransomware that modifies it.
CLOUD	Cloud assets fall into a very broad category, but these assets are purposely searched and attacked. It refers to third-party cloud providers (no private cloud) that are used as part of the operation of the target.
CONTENT MANAGEMENT SYSTEM (CMS).	CMS refers both to the web server running the web page and to the files of the web service. The files can be the configuration, data and code. This asset was especially distinguished due to a large number of attacks on web services.

How to stay safe from ransomware?



Contact national cybersecurity authorities

They will quide on how to handle and deal with ransomware

Do not negotiate

Ransom payments increase the growth of ransomware and does not solve the problem

Take quick actions on locking down access to backups

This should be until after infection is removed

Hide information

Cut the infected system from other systems to prevent it from spreading

Visit The No More Ransom Project

This Europol intiative can decrypt multiple variants of malwares

Sources:

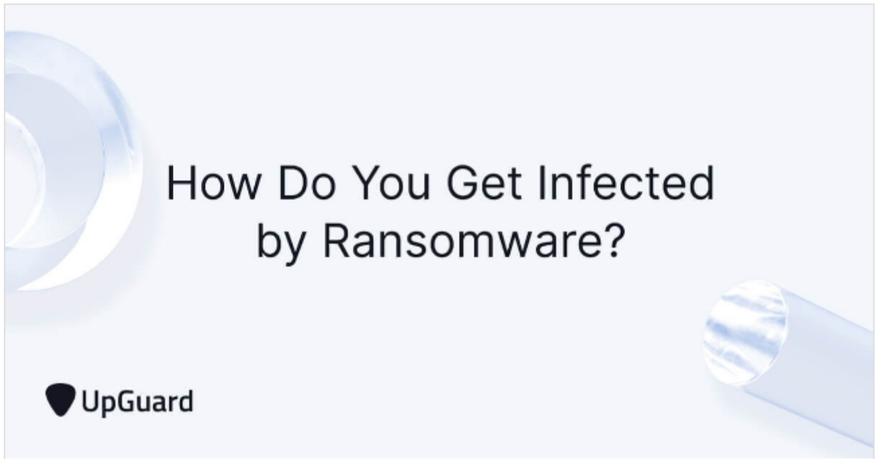
ENISA Threat Landscape for Ransomware Attacks

This report aims to bring new insights into the reality of ransomware incidents through mapping and studying...

ENISA

The U.S. is the top target of ransomware attacks, report says

The majority of ransomware attacks worldwide targeted industries that play a "critical role" in domestic and international supply chains, according to new research.



How Do You Get Infected by Ransomware?

Learn how you can get infected by ransomware and how to prevent it.

upguard.com