



Ransomware : Many victims, very few solutions

The rebirth of a lucrative attack technique


Attacks of this kind have long been common knowledge, and are widely used for their lucrative potential, as well as their ability to spread in a rapid and devastating way. We are currently seeing a rise in such threats. Figures from France's ANSSI cybersecurity agency show that **the number of attacks rose by 37% between 2020 and 2021**. Similarly, there has been a trend over time towards Ransomware as a Service (RaaS).




Ransomware is malware that takes your data hostage.



The first category: classic "Browlock" ransomware that **freezes your browser**, or completely paralyzes your computer.



The second: the most harmful crypto-ransomware ("Cryptoware") **encrypts the documents on your computer**, making them unreadable without the decryption key held by the hacker, who then demands a ransom in return for this key.



In the latter, more recent category, the malware **exfiltrates data and threatens to disclose it** to the owner, demanding a payment in bitcoin.

7,000 Euros

Average cost of a cyber attack

Source: Usine Digitale

The targeting of critical infrastructure for sabotage purposes remains a constant threat.

ACCORDING TO DATOST01 RANSOMWARE ATTACKS HAVE INCREASED BY 253%

WE ARE ALL AFFECTED

Individuals & Companies of all sectors and sizes

Phishing accounts for almost two thirds of ransomware victims (65%), far ahead of credential theft (39%), according to a Hiscox report.

AN ACTIVE AND VARIED FAMILY

- GPoode (AG, AK)
- LOCKBIT 2.0**
- TROJ.RANSOM.A
- Archivus
- Krotten
- RSA4096
- Cerber
- Cryzip
- MayArchive
- Petya**
- CryptoLocker
- TorrentLocker
- Cryptowall
- TeslaCrypt**
- Locky Ransomware**
- KeRanger**
- CTB-Locker
- WinLock
- Reveton
- WinWebsec

52% of victims are SMES

HACKER COMMUNITY

The various ransomware campaigns are now no longer carried out by a single group, but **by several groups of hackers.**

CRYPTOWARE

Ransomware is becoming increasingly difficult to decrypt, reducing the chances of being able to recover data without paying the ransom.

In a very short time, the size and strength of the keys have increased considerably.

OBSERVATION

This type of attack is constantly on the increase (new attacks or variants).

ALL OSs are affected

KERANGER
THE FIRST RANSOMWARE TO TARGET MAC OS X SYSTEMS (2016) (2016)

CTB-LOCKER (VARIANT)
TARGETS WEB SERVERS UNDER GNU/LINUX

CAMPAIGNS ARE TARGETED
A telling example: **Locky**

Locky targets businesses, and is spread via malicious email campaigns in French (fake invoice emails, free mobile, etc.). **Its effectiveness is increased through personalisation.**

MAKE YOUR OWN RANSOMWARE WITHOUT TECHNICAL KNOWLEDGE

RANSOMWARE-AS-A-SERVICE

It can now be used by anyone because

Malicious code generation is available for use

on the Dark Web.

HOW DOES IT WORK?

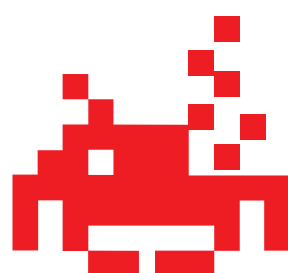
With very simple step-by-step tools, hackers can quickly build their own ransomware. They pay the provider of this service 25% of the transactions conducted under the campaign.

LOCKBIT 2.0

LockBit is a cybercriminal group operating under a ransomware-as-a-service (RaaS) model.

The LockBit 2.0 ransomware continues to adapt and evolve today, with targeted attacks in the US, Canada and Europe.

The most recent variants have adopted the "double extortion" model: first locate and exfiltrate the data, then encrypt systems.



FOR MORE INFORMATION



Find out how the LockBit attack threatens infrastructure with data exfiltration and encryption.

And Stormshield's response, with **the anti-ransomware protection component of its Endpoint Security Evolution solution.**

RANSOMWARE IS NO LONGER DISTRIBUTED JUST BY E-MAIL

- a compromised or malicious website,
- a USB stick,
- software/an application installed from an unreliable source,
- social networks (which facilitate social engineering), etc.



COMPUTER WORM



E-MAIL MALWARE



FILELESS ATTACK



HACKER



INFECTED DEVICES



SOFTWARE VULNERABILITIES



TROJAN

Step 1 Customization

1 The hacker chooses the attack method

- ☒ Blocking
- ☒ Encryption
- ☐ Countdown



2 then writes the message

Message

Your personal data is encrypted

You have just been locked out of your device. To get your data back, make a payment of €200 to this address:



3 then provides payment information

bitcoin



Step 2 Creation

4 The service prepares the malware according to the selected choices



5 The code is ready to use



Step 3 Distribution

IT'S SHOWTIME!

The ransomware will use multiple methods for propagation, such as using an "exploit kit" to exploit a vulnerability.



SOLUTIONS AGAINST RANSOMWARE EXIST



STORMSHIELD

Endpoint Security
Evolution

This proactive protection prevents malware from running on your computer and/or exploiting a vulnerability (via an exploit kit).

Stormshield Endpoint Security Evolution has proactive malware identification technology that can block ransomware before it is even identified by the cybersecurity community.

Your **company** is protected against ransomware

With Stormshield Endpoint Security Evolution



More information:

www.stormshield.com/products-services/products/endpoint-protection/

SOME ESSENTIAL ADVICE

To protect yourself from ransomware



Beware

of suspicious emails with attachments



Back up

regularly



Update

your applications, plugins and operating systems