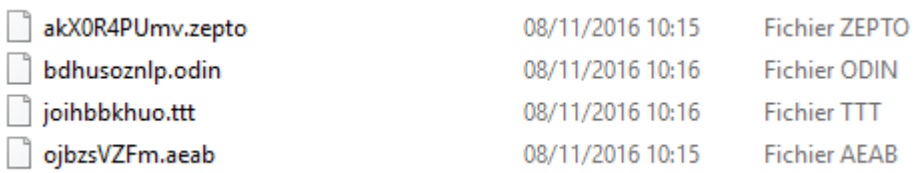
Ransomware and crypto-ransomware

Guilhem VERGON - 2024-04-04 - Issues and solutions

Ransomware and crypto-ransomware

You just opened an email with with malevolent attached file, or you downloaded malware from the internet, and all of your files have their name changed, just like in this picture :



When you try to open these files, you get a content which is not yours.

Your data has been ciphered and most of the time you can see a .txt file, mostly called Readme.txt, where you are asked to pay for getting your data back with a cipher key.
→ *You've been hacked with a ransomware.*

What is a ransomware?

Ransomwares are malevolent softwares that cipher your data to make them unusables, or they can also **block your computer and ask you to pay a ransom to**

get your data back.

Ransomware

On distingue:

- **cipher ransomwares :** cipher your data to make it unusable without the cipher key.
- **lockers :** they totally block your computer.

Most of ransomwares use a cipher algorythm that is very hard to override. You will need a key to uncipher your data and get it back.
It is strongly unadvised to pay the ransom, as you have no guarantee to get your data back afeter payment.

More over, by paying you will supply development of this type of threats.

They've been estimated to 24 million dollars in 2015.

How does it happen ?

Most of time, infection spreads itself by opening attached file from an email. Ransomware actions are totally invisible for most of users.
When ransomware shows itself it has already finished encrypting your data, and it is already too late to save it.
Therefore, it can spend several days between infection and symptoms like the creation of a Readme.txt file right on your desktop.

Types of files that can contain ransomware :

- executables (.exe ou .scr)
- archives with extensions like .zip or .rar
- Office files with vulnerable macros (.doc, .doxw, xls, xlsx, ppt, pptx,...)
- shortcuts

If you do not have a backup of your data, it is more than likely unrecoverable.
On the opposite, if you synced data with NetExplorer, you will be able to get it back !

How to :

Here is what you have to do to get your data back when ransomware has infected your computer :

1 - Check for latest inserts of files from **event logs** and spot **malevolent extensions** (listed above).
2 - Do a search with **malevolent extensions on your platform and delete all results**.
3 - Restore **from your platform trash** all elements that have been moved due to ciphering.

4 - On restored folders, set access rights again, directly from platform.
5 - On **infected computer**, **do a search** on your disks with malevolent extensions and **delete every result**.
6 - Launch an **antivirus** scan on computer to ensure it is not infected anymore.

Data stocke on NetExplorer platform are recoverable directly from user trashes.
On the opposite, on your computer, data that has not been backup on platforme are unlikely to be recovered after encryption.

If you wish, we can offer an **all-in-one solution of cleaning.** All you have to do is call the Sales Department at **+33 5 61 61 20 10**.

A few recommendations

- **Keep an up-to-date antivirus on your computer**.
- **Install updates of your operating system.**
- **Be cautious when opening files from mailbox** and open them **only if you know the sender.**
- Do not open links in emails, especially when you don't trust sender.
- **Prefer a secure cloud hosting like NetExplorer** instead of keeping everything locally.

Careful : Even from MacOs, you can be infected by ransomwares, same for Linux systems.

Filter malevolent extensions

Our tools filter malevolent extensions to avoid contaminate your synchronized dataon NetExplorer.

Here is the list of filtered extensions :

Extensions considérées comme dangereuses			
1999	_crypt	0x0	aaa
abc	aeab	bleep	ccc
crinf	crjoker	crypt	crypto
CTB2	CTBL	ecc	ekybtc
@inbox_com	EnCiPhErEd	encrypted	encryptedRSA
exx	ezz	good	HA3
LeChiffre	locked	locky	LOL!
magic	micro	odin	OMG!
pzdc	R16M01D05	r5a	RDM
ROGER	RRK	SUPERCRYPT	XTBL
toxcrypt	ttt	vault	vvv
XRNT	xxx	zzz	zepto

If you try to add a file with one of these extensions, it will not be uploaded, no matter the tool you are using. (NetSync, platform,...).

Your account will deactivate itself if you try to add one of these files.

On the other hand, virus can impact your synchronized data if extension is not known yet. Every week, new ransomwares are created and it is hard to know all of them.

We try to keep up to date but there is always a possibility that an extension is not filtered.

In that case, encrypted files will appear in COMPANY SPACE and your files will be in the trash of infected user. You will then be able to get them back by restoring them from the trash.

Known ransomwares

It is hard to establish a list of ransomwares, as new ones appear avery day.
However, these are the most famous in France : *Locky, Petya, CryptXXX, TeslaCrypt, Cerber, CTB Locker,*...