



Malware and ransomware

Harmful programs, the blackmail of encrypted files, and why the real defence is a safety copy

Gianluca Bonomo · www.gianlu.it · info@gianlu.it



Contents

How to use this handout 3

1. What malware is 3

2. Viruses, worms, trojans, spyware and keyloggers 5

2.1 The virus: it needs you to open it 5

2.2 The worm: it travels alone 5

2.3 The trojan: the gift that hides the danger 5

2.4 Spyware and keyloggers: someone watching you work 6

2.5 A few signs that something is wrong 6

3. Ransomware: the blackmail of encrypted files 7

3.1 CryptoLocker, the name that stuck 8

3.2 Double extortion 8

4. Why you do not pay, and what the real defence is 9

4.1 Why paying is not worth it 9

4.2 The real defence: a copy the ransomware cannot reach 10

5. How malware gets in: fake files and unknown devices 12

5.1 Attachments and links in emails 12

5.2 The fake .pdf.exe 13

5.3 USB sticks and unknown devices 14

5.4 «Free» programs and cracks 15

5.5 Programs that are not updated 15

Exercise: can you see the extensions? 17

Questions that come up in class 18

Glossary 18

Further reading 19

How to use this handout

This handout gathers, in written and ordered form, everything covered in the lesson. You do not need to memorise it: it is there so you can find things again calmly, later, when the lesson is over and a question is left hanging.

> **GOAL**
>
> Recognise the main families of malware, understand how ransomware works and why paying the ransom is not worth it, and know how a harmful program gets in so you can avoid the most common traps.

What you will be able to do

- Explain what malware is and tell apart viruses, worms, trojans, spyware and keyloggers.
- Describe how ransomware acts and what the affected user sees.
- Explain why paying the ransom is not a solution.
- Recognise a fake file with a double extension and an unknown storage device.
- Name backup as the main defence and link it to the dedicated lesson.

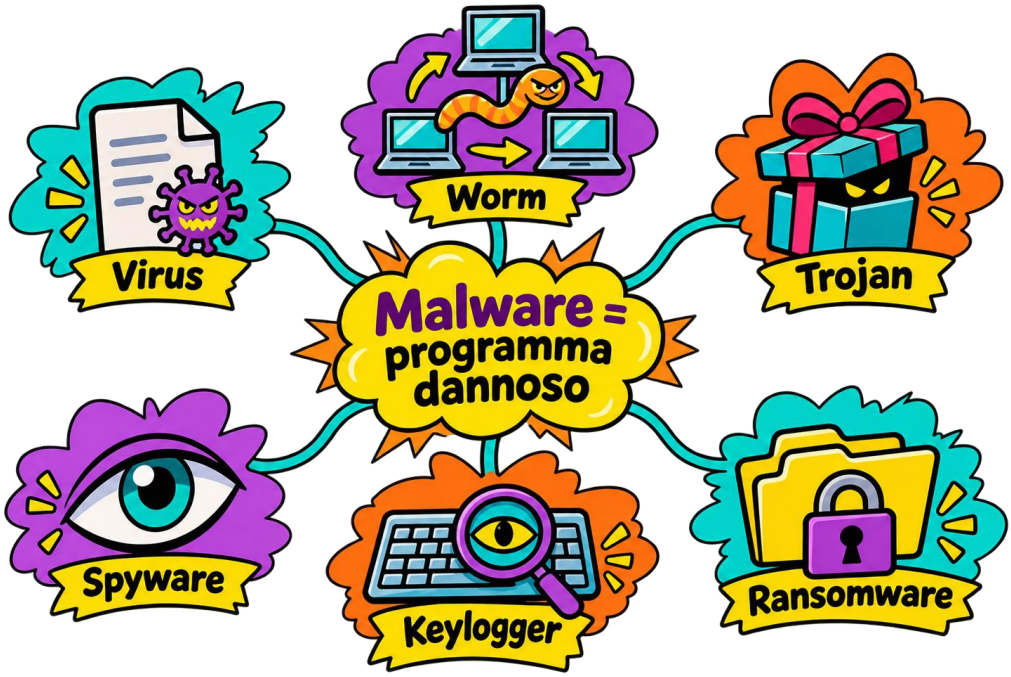
1. What malware is

The computer is slow, windows you have never seen pop up, and a program you did not install starts by itself.

When this happens, many people think the computer is just old. Sometimes it is. Other times there is **malware** on it.

Malware comes from *malicious software*. It is the generic name for all programs created to damage a computer, steal data, spy on its user or take control of it. It is not a fault of the computer: it is a program, written on purpose, that someone has got onto your device.

Malware does not have a single face. It splits into families, which differ in how they spread and in what they do once inside. Knowing the families helps you understand which signs to look for and which habits to fix.



Malware is the general name for harmful programs

Type	What it does
Virus	Attaches itself to a program or file and spreads when that file is opened.
Worm	Copies itself across the network, with no need for anyone to open anything.
Trojan (Trojan horse)	Pretends to be a useful program (a «crack», a free converter) but opens the door to an intruder.
Spyware and **keylogger**	Spy on what you do and record the keys you press to steal passwords and card numbers.
Ransomware (cryptolocker)	Encrypts your files and demands a ransom to give them back.

The main families of malware.

> **THE IDEA IN ONE LINE**
>
> Malware is the name of the container. Viruses, trojans and ransomware are the contents: the method and the goal change, the problem does not.

2. Viruses, worms, trojans, spyware and keyloggers

Let us look at the families one by one, with an everyday case. The names are a little odd, but each one tells you well what the program does.

2.1 The virus: it needs you to open it

Like a biological virus, a computer virus needs a host. It hides inside a program or document and activates when you open it. If you then forward that file to a colleague, the virus travels with it.

2.2 The worm: it travels alone

A worm copies itself from one computer to another across the network, without anyone clicking. In an office where computers are connected, one unprotected machine can infect the others. That is why updating programs is so important, a topic of the lesson on devices.

2.3 The trojan: the gift that hides the danger

The name comes from the Trojan horse. The program presents itself as something useful and free: a converter from one format to another, a paid program «unlocked» (a so-called *crack*), a fake update. You install it yourself, willingly, and meanwhile you open the door to whoever made it.



A program can work and still hide an unwanted way in

THE FREE CONVERTER

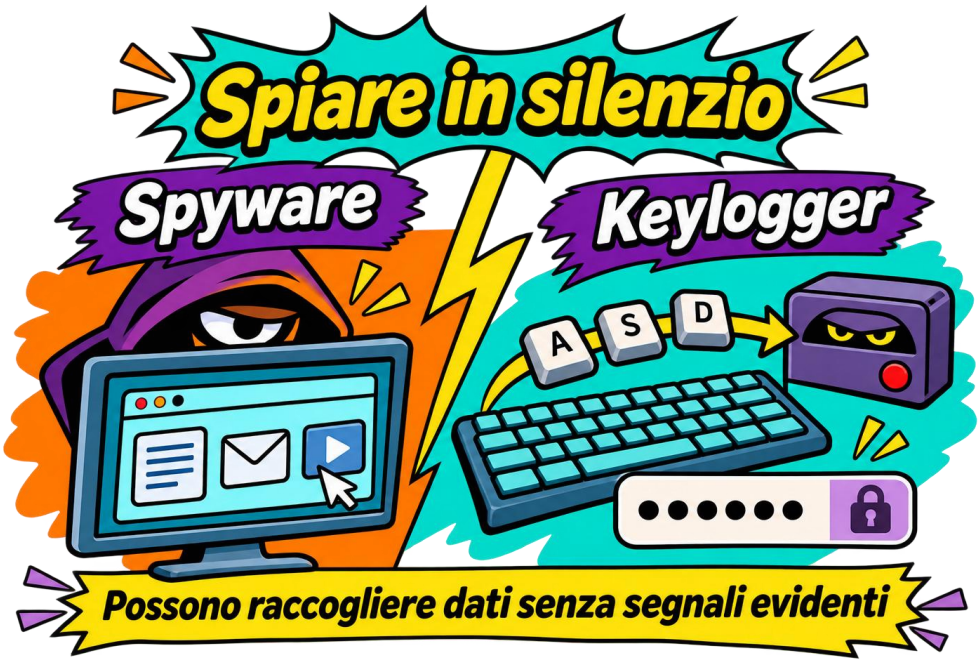
Anna (a made-up name), who works in the office of a dance school, needs to turn a form into another format. She searches for «free converter» and downloads the first program she finds on an unknown site.

The program really does convert the file. But in secret it also installs a second program that lets a stranger into the computer. Anna does not notice for weeks.

2.4 Spyware and keyloggers: someone watching you work

Spyware spies on what you do: the sites you visit, the documents you open. The **keylogger** (from *key* and *logger*, a recorder) is its more insidious cousin: it notes every key you press. If you type a password, it records it. If you type a card number, it records it.

What marks these two families is silence. They encrypt nothing, slow things down little, show no messages. Often you only notice when someone uses one of your accounts or charges a purchase you did not make.



Some malware collects information with no obvious signs

2.5 A few signs that something is wrong

- the computer has become very slow for no obvious reason;
- programs or browser toolbars appear that you do not remember installing;
- the browser home page changes by itself;

- your accounts show logins or operations you do not recognise;
- the antivirus has turned itself off and you cannot turn it back on.

> **WARNING**
>
> These signs are not proof: they can have other causes. If you notice more than one, do not try to fix it alone and tell your IT contact.

3. Ransomware: the blackmail of encrypted files

Ransomware does not steal your files: it locks them in a safe and asks you for money for the key.

The name combines *ransom* and *software*. Ransomware locks the computer or, more often, **encrypts** all your documents. To encrypt means to transform a file with a mathematical procedure so that it becomes unreadable without a key, a secret code.

When the encryption is done, a message appears. It says your files have been locked and demands a payment, usually in cryptocurrency (digital money that is hard to trace), in exchange for the key.



Ransomware encrypts files and demands a ransom

3.1 CryptoLocker, the name that stuck

CryptoLocker is one of the first widely spread ransomware programs, which appeared in 2013. It encrypted the documents of Windows computers and demanded a payment to unlock them. Its name became a synonym: today many people say «cryptolocker» to mean any ransomware.

Since then the phenomenon has grown and become organised. Today it hits hospitals, town councils, schools, professional firms and small businesses, because where there is important data there are people willing to pay.

3.2 Double extortion

Many criminal groups copy an organisation's data before encrypting it. Then they ask for two payments: one for the key and one for not publishing the data. Even with a good backup, you are left with the problem of what has ended up in the wrong hands.



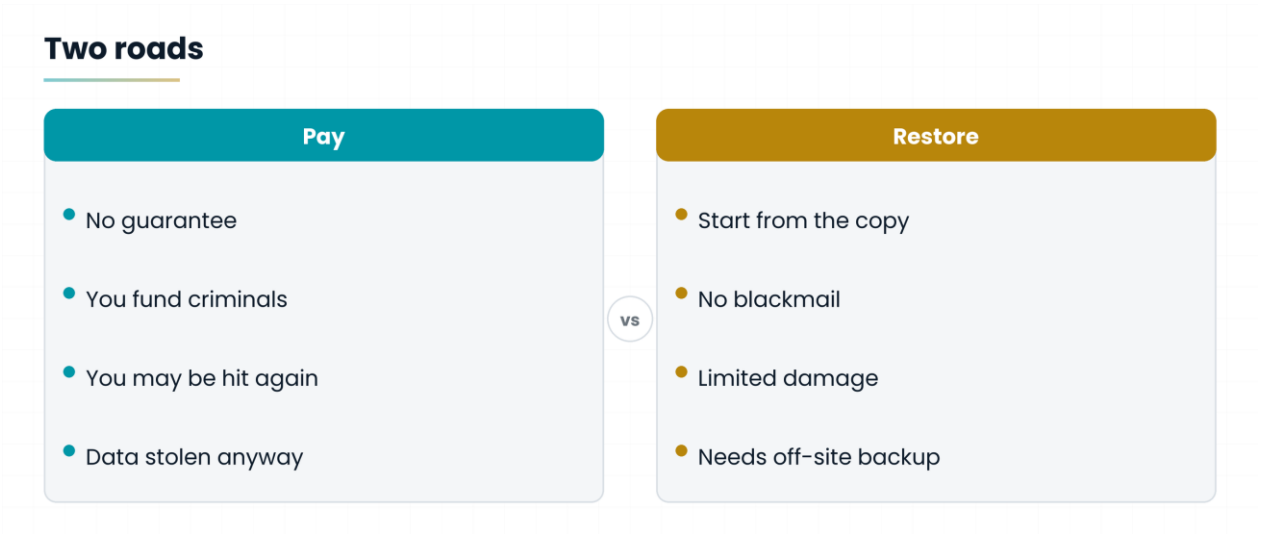
Criminals can threaten both to lock the files and to publish the data

That is why security is not just backup: you also need to keep intruders out and, for personal data, know what to do in case of a breach. We cover this in the lessons on privacy and on what to do when it happens.

> **STUDIO ESEMPIO'S MONDAY**
>
> On Friday evening a staff member at «Studio Esempio» (a made-up name) opens an attachment that looks like a supplier's invoice. Nothing visible happens.
>
> On Monday morning all the shared folders have files with an unknown extension. On the desktop there is a text file with payment instructions. The firm has no recent backup outside the computer.

4. Why you do not pay, and what the real defence is

Faced with a ransom message, the temptation is to pay and make it all stop. I understand the pressure, but paying is almost always a bad idea.



Paying the ransom or restoring from backup

4.1 Why paying is not worth it

- **there is no guarantee:** the blackmailer is not bound to keep their word; sometimes the key never arrives, sometimes it does not work, sometimes the files stay damaged;
- **you fund the attacker:** every payment makes crime more profitable and encourages new attacks;
- **you can be hit again:** whoever knows you paid may see you as an easy target;
- **stolen data stays stolen:** paying does not delete the copy the attackers have already made.

That is why police authorities, in Italy as in Europe, advise against paying. The international project *No More Ransom* (nomoreransom.org), born from cooperation

between police forces and security companies, offers free tools to unlock some types of ransomware. Not all of them, but it is always worth checking.



Paying does not guarantee recovery and does not remove the risks

4.2 The real defence: a copy the ransomware cannot reach

If you have a recent copy of your data, the blackmail loses its force: you wipe the computer, put the files back from the copy and start again. The damage is annoying, but limited.

Beware, though: ransomware also encrypts the disks connected to the computer. A backup that stays plugged in all the time, or sits in a network folder that can be reached, can be encrypted along with everything else. The copy must live **outside the computer**: an external disk unplugged after use, or a cloud service (online storage) that keeps previous versions of your files.



Even a connected backup can be hit

WARNING

Paying the ransom does not guarantee you will get your data back and it funds the attacker. The real defence is to have recent safety copies kept outside the computer.



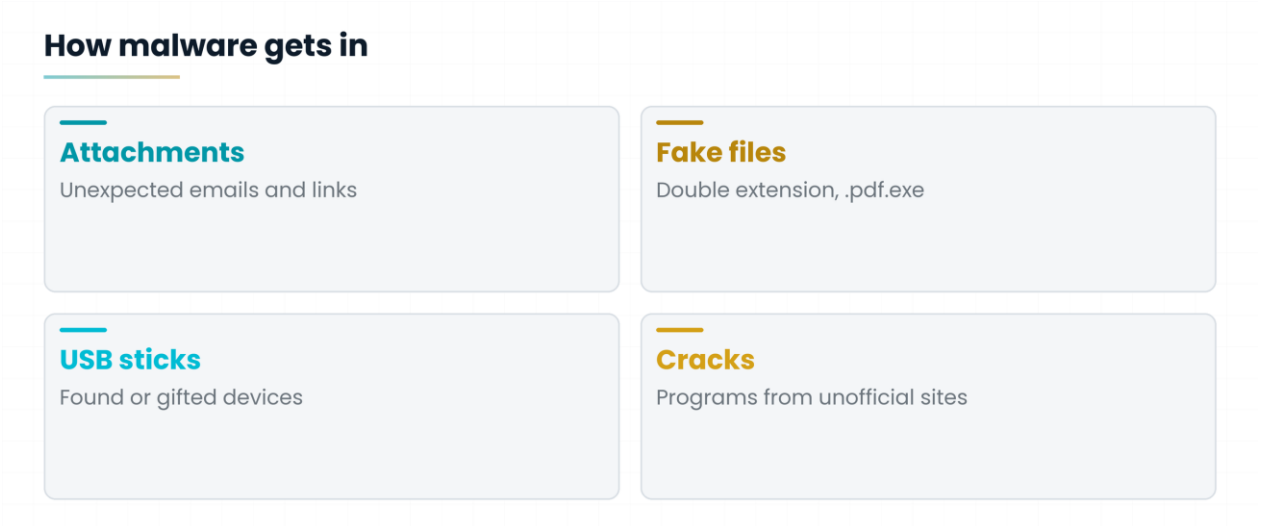
A recent copy must be recoverable

How to organise the copies, how many, where and how often is the subject of the lesson on backup and the 3-2-1 rule. Here it is enough to remember one principle: **without a copy outside the computer, ransomware can turn into a permanent loss**.

> **THE IDEA IN ONE LINE**
>
> Blackmail only works if your data exists in one place. With a copy safely stored, the blackmailer has nothing left to sell.

5. How malware gets in: fake files and unknown devices

Malware does not come in by magic. Almost always someone lets it in, without knowing. The most frequent routes are few, and they are the same ones you will meet again in the next lessons.



The most common routes for malware

5.1 Attachments and links in emails

This is the most widespread method. Ransomware is usually caught by opening an infected attachment or clicking a link in an email. The message looks like an invoice, an order, a courier notice. How to recognise them is the topic of the lesson on phishing.



An unexpected email calls for care before you open attachments or links

5.2 The fake .pdf.exe

A classic trap is the file with a **double extension**. The extension is the final part of the name, after the dot, which tells the computer what kind of file it is. A file called *invoice-october.pdf.exe* looks like a PDF, but it really ends in *.exe*: it is an executable program, and if you open it, it runs.



fattura.pdf.exe ends in .exe: it is a program, not a PDF

The problem is that Windows, by default, may hide the extensions of known file types. Then you see only *invoice-october.pdf* and you do not know there is more behind it. To see them all, open File Explorer, go to the **View** menu, choose **Show** and tick **File name extensions**.



Windows 11: View, Show, File name extensions

File name	What it really is
invoice-october.pdf	A PDF document, if the extension really is .pdf.
invoice-october.pdf.exe	A program dressed up as a PDF.
new-pricelist.xlsx.js	A script dressed up as a spreadsheet.
event-photo.jpg.scr	A program dressed up as a photo.

What counts is the last extension, the one furthest to the right.

5.3 USB sticks and unknown devices

A USB stick (the small memory you plug into a computer) that you found, were given or borrowed can contain malware that starts as soon as you insert it. The same goes for external disks and memory cards of unknown origin.

The rule is simple: **do not plug devices you do not know into a work computer**. If you really must open the contents, ask your IT contact: they have tools to check it safely.



On your work computer, avoid media from unknown sources

5.4 «Free» programs and cracks

The paid program given away on an unknown site, the free converter, the «special» document viewer. If it does not come from an official source, the price you pay may be yourself. Download only from the maker's site or from the system's official software stores.

5.5 Programs that are not updated

Some malware, like worms, gets in by exploiting known flaws in programs. Makers close them with updates: if you postpone them for months, you leave open a door everyone knows about.

> **A RULE TO REMEMBER**
>
> If you were not expecting it, do not open it. If you installed it from an unofficial source, do not trust it. If it comes from a device you do not know, do not plug it in.



If something looks odd, stop and ask your IT contact

Exercise: can you see the extensions?

A short exercise to do on your Windows 11 computer, with any folder of documents.

1. Open File Explorer and go to a folder that contains a few documents.
2. Look at the names: do you see the final part after the dot, such as .pdf or .docx? If not, open the View menu, choose Show and turn on File name extensions.
3. On a sheet of paper write three file names and next to each one what kind of file it really is according to its extension.
4. Imagine you receive an email with an attachment called «quote.pdf.exe». Write in one line what it is and what you would do.
5. Check whether there is a recent copy of your important documents outside the computer itself (external disk or cloud). Write down where it is, or note that it is missing.

CHECK YOUR RESULT

Can you see the full extension of your files?

Can you say why «quote.pdf.exe» is not a PDF?

Have you located your safety copy, or realised you need to create one?

Questions that come up in class

How do I know if my computer is infected?

You do not always know. Some malware, like spyware and keyloggers, is silent. The typical signs are unusual slowness, programs you never installed, changed settings, an antivirus that is off. If in doubt, tell your IT contact and run a full scan with Windows Security.

Are Macs and phones immune to malware?

No. Attackers target Windows most because it is so widespread, but malware exists for Mac, Android and, less often, iPhone. Careful habits apply to every device.

If I pay the ransom, will I get my files back?

There is no guarantee. Sometimes the key does not arrive, sometimes it does not work, sometimes the criminals ask again. Payment also funds new attacks. Authorities advise against paying.

Is antivirus enough to stop ransomware?

It helps a lot, but it is not guaranteed: criminals keep changing their programs. That is why you need several barriers together: attention to messages, updates and, above all, a backup outside the computer.

My backup is on a disk that is always plugged in: is that fine?

It is better than nothing, but not enough. Ransomware also encrypts connected disks. Keep a copy you unplug after use, or a cloud service that keeps previous versions of your files.

I opened a strange attachment and nothing happened. Am I safe?

Not necessarily. Some malware works silently for days before acting. Tell your IT contact right away: better a needless check than damage discovered too late.

Glossary

Term	What it means
Backup	A safety copy of data, kept outside the computer, so it can be restored.
Encryption	A procedure that makes a file unreadable without the right key.
Extension	The final part of a file name, after the dot, which shows the file type (for example .pdf).

Term	What it means
Keylogger	A program that records the keys pressed to steal passwords and card numbers.
Malware	From «malicious software»: a program created to damage a computer, steal data or take control of it.
Ransomware	Malware that encrypts files and demands a ransom to give them back. Also called cryptolocker.
Spyware	Malware that spies on what the user does.
Trojan	Malware that pretends to be a useful program to get itself installed.
Virus	Malware that attaches itself to a program or file and spreads when it is opened.
Worm	Malware that copies itself across the network, with no need for anyone to open anything.

Further reading

No More Ransom - international project of police forces and security companies, nomoreransom.org

Agenzia per la cybersicurezza nazionale (ACN) and CSIRT Italia, Italy's national cybersecurity agency and incident response team - guides and alerts on ransomware, acn.gov.it

Polizia Postale e delle Comunicazioni, Italy's online-crime police unit (in the US, the FBI's IC3) - guidance and reporting, commissariatodips.it

Microsoft documentation on Windows Security - for the features of the antivirus included in Windows 11

> **WATCH OUT**
>
> Information up to date as of October 2026. CryptoLocker is cited as one of the first widely spread ransomware programs (2013). Names of people, firms and domains in the examples are made up. Windows menu names may vary slightly with updates: if you cannot find an item, look for the function described. Italian bodies are explained in brackets for readers outside Italy.