



Malware e ransomware

I programmi dannosi, il ricatto dei file cifrati e la copia di sicurezza

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



Indice

Come usare questa dispensa 3

1. Che cos'è il malware 3

2. Virus, worm, trojan, spyware e keylogger 5

2.1 Il virus: ha bisogno che tu lo apra 5

2.2 Il worm: viaggia da solo 5

2.3 Il trojan: il regalo che nasconde il pericolo 5

2.4 Spyware e keylogger: chi ti guarda mentre lavori 6

2.5 Alcuni segnali che qualcosa non va 6

3. Il ransomware: il ricatto dei file cifrati 7

3.1 CryptoLocker, il nome che è rimasto 8

3.2 La doppia estorsione 8

4. Perché non si paga, e qual è la vera difesa 9

4.1 Perché non conviene pagare 9

4.2 La vera difesa: una copia che il ransomware non raggiunge 10

5. Come si prende un malware: i falsi file e i supporti sconosciuti 12

5.1 Allegati e link nelle mail 12

5.2 Il falso .pdf.exe 13

5.3 Chiavette e supporti sconosciuti 14

5.4 Programmi «gratuiti» e crack 15

5.5 Programmi non aggiornati 15

Esercitazione: sono visibili le estensioni? 17

Le domande che arrivano in aula 18

Glossario 19

Per approfondire 19

Come usare questa dispensa

Questa dispensa raccoglie, in forma scritta e ordinata, tutto quello che vediamo nella lezione. Non serve studiarla a memoria: serve a ritrovare le cose con calma, dopo, quando la lezione e' finita e resta una domanda in sospeso.

> **OBIETTIVO**
>
> Riconoscere le principali famiglie di malware, capire come funziona un ransomware e perché non conviene pagare il riscatto, e sapere come si prende un programma dannoso per evitare le trappole più comuni.

Che cosa saprai fare alla fine

- Spiegare che cos'è un malware e distinguere virus, worm, trojan, spyware e keylogger.
- Descrivere come agisce un ransomware e che cosa vede l'utente colpito.
- Motivare perché pagare il riscatto non è una soluzione.
- Riconoscere un falso file con doppia estensione e un supporto sconosciuto.
- Indicare il backup come difesa principale e collegarlo alla lezione dedicata.

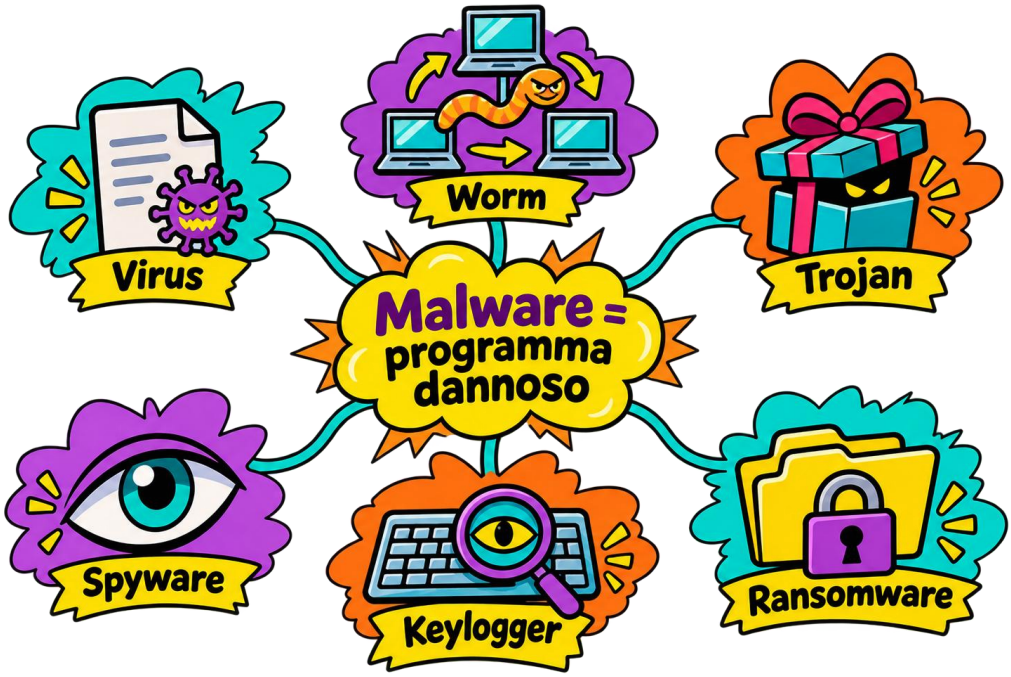
1. Che cos'è il malware

Il computer è lento, compaiono finestre mai viste, e un programma che non hai installato parte da solo.

Quando succede, molti pensano che «il computer sia vecchio». A volte è vero. Altre volte sul computer c'è un **malware**.

Malware viene dall'inglese *malicious software*, cioè programma dannoso. È il nome generico di tutti i programmi creati per danneggiare un computer, rubare dati, spiare chi lo usa o prenderne il controllo. Non è un difetto del computer: è un programma, scritto apposta, che qualcuno ha fatto arrivare sul tuo dispositivo.

Il malware non ha un solo volto. Si divide in famiglie, che si distinguono per come si diffondono e per ciò che fanno una volta dentro. Conoscere le famiglie serve a capire quali segnali cercare e quali abitudini correggere.



Malware è il nome generale dei programmi dannosi

Tipo	Che cosa fa
Virus	Si attacca a un programma o a un file e si diffonde quando lo si apre.
Worm	Si copia da solo attraverso la rete, senza bisogno che qualcuno apra qualcosa.
Trojan (cavallo di Troia)	Si finge un programma utile (un «crack», un convertitore gratuito) ma apre la porta a un malintenzionato.
Spyware e **keylogger**	Spiano ciò che si fa e registrano i tasti premuti per rubare password e numeri di carta.
Ransomware (cryptolocker)	Cifra i file e chiede un riscatto per restituirli.

Le famiglie principali di malware.

L'IDEA IN UNA RIGA

Malware è il nome del contenitore. Virus, trojan e ransomware sono i contenuti: cambiano il metodo e lo scopo, non il problema.

2. Virus, worm, trojan, spyware e keylogger

Vediamo le famiglie una per una, con un caso di tutti i giorni. I nomi sono un po' curiosi, ma ognuno racconta bene che cosa fa il programma.

2.1 Il virus: ha bisogno che tu lo apra

Come un virus biologico, quello informatico ha bisogno di un ospite. Si nasconde dentro un programma o un documento e si attiva quando lo apri. Se poi giri quel file a un collega, il virus viaggia con lui.

2.2 Il worm: viaggia da solo

Worm vuol dire verme. Si copia da un computer all'altro attraverso la rete, senza che nessuno clicchi. In un ufficio con i computer collegati fra loro, uno solo non protetto può contagiare gli altri. Per questo è così importante aggiornare i programmi, tema della lezione sui dispositivi.

2.3 Il trojan: il regalo che nasconde il pericolo

Il nome viene dal cavallo di Troia. Il programma si presenta come qualcosa di utile e gratuito: un convertitore da un formato all'altro, un programma a pagamento «sbloccato» (il cosiddetto *crack*), un finto aggiornamento. Lo installi tu, volontariamente, e intanto apri la porta a chi lo ha creato.



Un programma può funzionare e nascondere un accesso indesiderato

IL CONVERTITORE GRATUITO

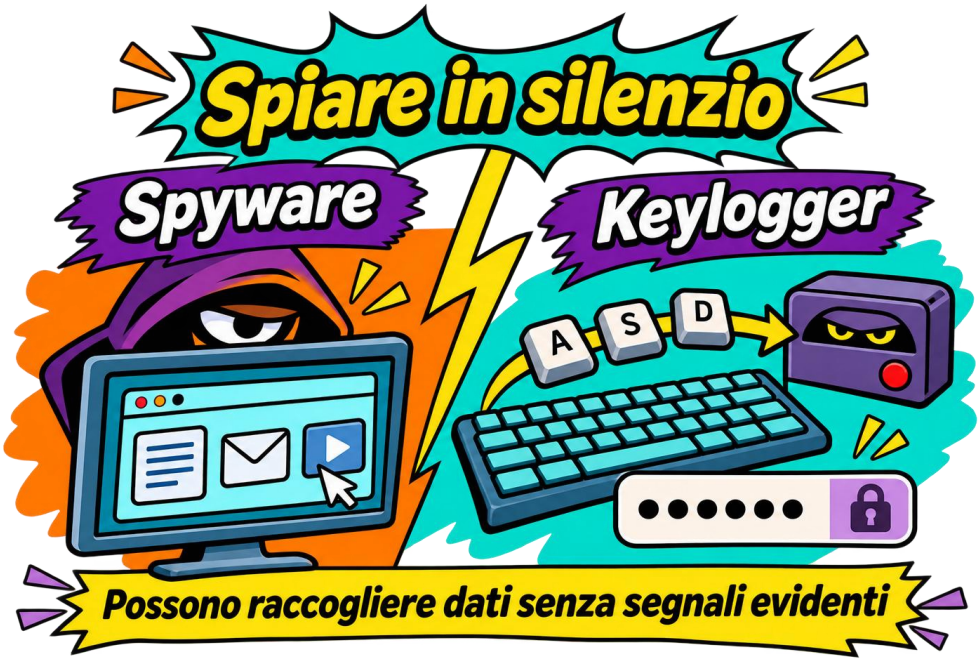
Anna (nome di fantasia), segretaria di una scuola di danza, deve trasformare un modulo in un altro formato. Cerca «convertitore gratuito» e scarica il primo programma che trova da un sito sconosciuto.

Il programma converte davvero il file. Ma in segreto installa anche un secondo programma che permette a un estraneo di entrare nel computer. Anna non se ne accorge per settimane.

2.4 Spyware e keylogger: chi ti guarda mentre lavori

Lo **spyware** spia ciò che fai: i siti visitati, i documenti aperti. Il **keylogger** (da *key*, tasto, e *logger*, registratore) è il suo cugino più insidioso: annota ogni tasto che premi. Se scrivi una password, la registra. Se digiti il numero di una carta, lo registra.

La caratteristica di queste due famiglie è il silenzio. Non cifrano nulla, non rallentano molto, non mostrano messaggi. Spesso te ne accorgi solo quando qualcuno usa un tuo account o addebita un acquisto che non hai fatto.



Alcuni malware raccolgono informazioni senza segnali evidenti

2.5 Alcuni segnali che qualcosa non va

- il computer è diventato molto lento senza una ragione evidente;
- compaiono programmi o barre del browser che non ricordi di aver installato;

- la pagina iniziale del browser cambia da sola;
- i tuoi account mostrano accessi o operazioni che non riconosci;
- l'antivirus si è spento e non riesci a riattivarlo.

> **ATTENZIONE**
>
> Questi segnali non sono una prova: possono avere altre cause. Se ne noti più di uno, non cercare di risolvere da solo e avvisa il referente informatico.

3. Il ransomware: il ricatto dei file cifrati

Il ransomware non ruba i tuoi file: te li chiude in cassaforte e ti chiede soldi per la chiave.

Il nome unisce *ransom* (riscatto) e *software*. Un ransomware blocca il computer o, più spesso, **cifra** tutti i documenti. Cifrare significa trasformare un file con un procedimento matematico, così che diventi illeggibile senza una chiave, cioè un codice segreto.

A cifratura finita compare un messaggio. Dice che i file sono stati bloccati e chiede un pagamento, di solito in criptovaluta (denaro digitale difficile da rintracciare), in cambio della chiave.



Il ransomware cifra i file e chiede un riscatto

3.1 CryptoLocker, il nome che è rimasto

CryptoLocker è uno dei primi ransomware largamente diffusi, apparso nel 2013. Cifrava i documenti dei computer Windows e chiedeva un pagamento per sbloccarli. Il suo nome è diventato un sinonimo: oggi molti dicono «cryptolocker» per indicare qualunque ransomware.

Da allora il fenomeno è cresciuto e si è organizzato. Oggi colpisce anche ospedali, comuni, scuole, studi professionali e piccole imprese, perché dove ci sono dati importanti c'è chi è disposto a pagare.

3.2 La doppia estorsione

Molti gruppi criminali, prima di cifrare, copiano i dati dell'organizzazione. Poi chiedono due pagamenti: uno per la chiave e uno per non pubblicare i dati. Anche se avessi un buon backup, resterebbe il problema di che cosa è finito in mani sbagliate.



I criminali possono minacciare sia il blocco dei file sia la pubblicazione dei dati

Per questo la sicurezza non si riduce al backup: serve anche impedire l'ingresso e, per i dati di persone, sapere che cosa fare in caso di violazione. Ne parleremo nelle lezioni su privacy e su che cosa fare se succede.

IL LUNEDÌ DELLO STUDIO ESEMPIO

Venerdì sera un collaboratore dello «Studio Esempio» (nome di fantasia) apre un allegato che sembra una fattura di un fornitore. Non succede niente di visibile.

Lunedì mattina tutte le cartelle condivise hanno file con un'estensione sconosciuta. Sul desktop c'è un file di testo con le istruzioni per il pagamento. Lo studio non ha un backup recente fuori dal computer.

4. Perché non si paga, e qual è la vera difesa

Davanti a un messaggio di riscatto, la tentazione è pagare per far finire tutto. Capisco bene la pressione, ma pagare è quasi sempre una cattiva idea.



Pagare il riscatto o ripristinare dal backup

4.1 Perché non conviene pagare

- **non c'è garanzia:** chi ricatta non è tenuto a mantenere la parola; a volte la chiave non arriva, a volte non funziona, a volte i file restano danneggiati;
- **finanzi chi attacca:** ogni pagamento rende il crimine più redditizio e incoraggia nuovi attacchi;
- **puoi essere ricolpito:** chi sa che hai pagato può considerarti un bersaglio facile;
- **i dati rubati restano rubati:** pagare non cancella la copia che gli aggressori hanno già fatto.

Per questo le autorità di polizia, in Italia come in Europa, sconsigliano il pagamento. Il progetto internazionale *No More Ransom* (nomoreransom.org), nato dalla collaborazione

tra forze di polizia e aziende di sicurezza, mette a disposizione gratuitamente strumenti per sbloccare alcuni tipi di ransomware. Non per tutti, ma vale sempre la pena controllare.



Pagare non garantisce il recupero e non cancella i rischi

4.2 La vera difesa: una copia che il ransomware non raggiunge

Se hai una copia recente dei tuoi dati, il ricatto perde forza: formatti il computer, rimetti i file dalla copia e riparti. Il danno è fastidioso, ma limitato.

Attenzione però: il ransomware cifra anche i dischi collegati al computer. Un backup lasciato sempre inserito, o su una cartella di rete raggiungibile, può essere cifrato insieme al resto. La copia deve stare **fuori dal computer**: un disco esterno scollegato dopo l'uso, oppure un servizio cloud (archivio online) che conserva le versioni precedenti dei file.



Anche un backup collegato può essere colpito

ATTENZIONE

Pagare il riscatto non garantisce di riavere i dati e finanzia chi attacca. La vera difesa è avere copie di sicurezza recenti, tenute fuori dal computer.



Una copia recente deve poter essere recuperata

Come si organizzano le copie, quante, dove e ogni quanto è l'argomento della lezione dedicata al backup e alla regola 3-2-1. Qui ti basta ricordare un principio: **senza una copia fuori dal computer, un ransomware può trasformarsi in una perdita definitiva**.

> **L'IDEA IN UNA RIGA**
>
> Il ricatto funziona solo se i tuoi dati esistono in un unico posto. Con una copia al sicuro, il ricattatore non ha più niente da vendere.

5. Come si prende un malware: i falsi file e i supporti sconosciuti

I malware non entrano per magia. Quasi sempre qualcuno li fa entrare, senza saperlo. Le strade più frequenti sono poche, e sono le stesse che ritroverai nelle prossime lezioni.



Le strade più comuni da cui entra un malware

5.1 Allegati e link nelle mail

È il metodo più diffuso. Un ransomware si prende di solito aprendo un allegato infetto o cliccando un link in una mail. Il messaggio sembra una fattura, un ordine, una notifica di un corriere. Come riconoscerli è il tema della lezione sul phishing.



Una mail inattesa richiede attenzione prima di aprire allegati o link

5.2 Il falso .pdf.exe

Una trappola classica è il file con **doppia estensione**. L'estensione è la parte finale del nome, dopo il punto, che dice al computer di che tipo di file si tratta. Un file chiamato *fattura-ottobre.pdf.exe* sembra un PDF, ma in realtà finisce con *.exe*: è un programma eseguibile, e se lo apri, parte.



fattura.pdf.exe termina in .exe: è un programma, non un PDF

Il problema è che Windows, di base, può nascondere le estensioni dei file conosciuti. Allora vedi soltanto *fattura-ottobre.pdf*, e non sai che dietro c'è altro. Per vederle tutte, apri Esplora file, vai nel menu **Visualizza**, scegli **Mostra** e spunta **Estensioni nomi file**.



Windows 11: Visualizza, Mostra, Estensioni nomi file

Nome del file	Che cosa è davvero
fattura-ottobre.pdf	Un documento PDF, se l'estensione è davvero .pdf.
fattura-ottobre.pdf.exe	Un programma travestito da PDF.
listino-nuovo.xlsx.js	Uno script travestito da foglio di calcolo.
foto-evento.jpg.scr	Un programma travestito da foto.

Quello che conta è l'ultima estensione, quella più a destra.

5.3 Chiavette e supporti sconosciuti

Una chiavetta USB (la piccola memoria che si infila nel computer) trovata, regalata o prestata può contenere un malware che parte appena la inserisci. Vale per le chiavette, ma anche per dischi esterni e schede di memoria di origine ignota.

La regola è semplice: **non inserire nel computer di lavoro supporti che non conosci**. Se devi proprio aprire il contenuto, chiedi al referente informatico: ha strumenti per controllarlo in sicurezza.



Nel computer di lavoro evita supporti di provenienza sconosciuta

5.4 Programmi «gratuiti» e crack

Il programma a pagamento regalato su un sito sconosciuto, il convertitore gratuito, il lettore di documenti «speciale». Se non arriva da un sito ufficiale, il prezzo che paghi potresti essere tu. Scarica solo dal sito del produttore o dagli archivi di programmi ufficiali del sistema.

5.5 Programmi non aggiornati

Alcuni malware, come i worm, entrano sfruttando falle già note nei programmi. I produttori le chiudono con gli aggiornamenti: se li rimandi per mesi, lasci aperta una porta che tutti conoscono.

> **UNA REGOLA DA RICORDARE**
>
> Se non te lo aspettavi, non lo aprire. Se lo hai installato da una fonte non ufficiale, non fidarti. Se arriva da un supporto che non conosci, non lo inserire.



Se qualcosa ti sembra strano, fermati e chiedi al referente informatico

Esercitazione: sono visibili le estensioni?

Una breve esercitazione da fare sul tuo computer Windows 11, con una cartella di documenti qualsiasi.

1. Apri Esplora file e vai in una cartella che contiene alcuni documenti.
2. Guarda i nomi: vedi la parte finale con il punto, come .pdf o .docx? Se non la vedi, apri il menu Visualizza, scegli Mostra e attiva Estensioni nomi file.
3. Scrivi su un foglio tre nomi di file e, accanto a ciascuno, di che tipo è davvero secondo l'estensione.
4. Immagina che ti arrivi una mail con un allegato chiamato «preventivo.pdf.exe». Scrivi in una riga che cosa è e che cosa faresti.
5. Controlla se sul tuo computer c'è una copia recente dei documenti importanti fuori dal computer stesso (disco esterno o cloud). Scrivi dove si trova, oppure annota che manca.

CONTROLLA IL RISULTATO

Riesci a vedere l'estensione completa dei file?

Sai dire perché «preventivo.pdf.exe» non è un PDF?

Hai individuato dove si trova la tua copia di sicurezza, o hai capito che devi crearla?

Le domande che arrivano in aula

Come faccio a sapere se il mio computer è infetto?

Non sempre si capisce. Alcuni malware, come spyware e keylogger, sono silenziosi. I segnali tipici sono lentezza insolita, programmi mai installati, impostazioni cambiate, antivirus spento. Nel dubbio, avvisa il referente informatico e fai una scansione completa con Sicurezza di Windows.

Un Mac o un telefono sono immuni dai malware?

No. Chi attacca prende di mira soprattutto Windows perché è molto diffuso, ma esistono malware per Mac, Android e, in modo meno frequente, per iPhone. Le abitudini prudenti valgono per tutti i dispositivi.

Se pago il riscatto, riavrò i miei file?

Non c'è alcuna garanzia. A volte la chiave non arriva, a volte non funziona, a volte i criminali chiedono di nuovo. Inoltre il pagamento finanzia nuovi attacchi. Le autorità sconsigliano di pagare.

L'antivirus basta a fermare un ransomware?

Aiuta molto, ma non è garantito: i criminali modificano continuamente i loro programmi. Per questo servono più barriere insieme: attenzione ai messaggi, aggiornamenti e, soprattutto, un backup fuori dal computer.

Il mio backup è su un disco sempre collegato: va bene?

È meglio di niente, ma non basta. Un ransomware cifra anche i dischi collegati. Tieni una copia che scolleghi dopo l'uso oppure un servizio cloud che conserva le versioni precedenti dei file.

Ho aperto un allegato strano e non è successo niente. Sono salvo?

Non necessariamente. Alcuni malware lavorano in silenzio per giorni prima di agire. Avvisa subito il referente informatico: meglio un controllo inutile che un danno scoperto in ritardo.

Glossario

Termine	Che cosa significa
Backup	Copia di sicurezza dei dati, conservata fuori dal computer, per poterli ripristinare.
Cifratura	Procedimento che rende un file illeggibile senza la chiave giusta.
Estensione	La parte finale del nome di un file, dopo il punto, che indica il tipo di file (per esempio .pdf).
Keylogger	Programma che registra i tasti premuti per rubare password e numeri di carta.
Malware	Dall'inglese «malicious software»: programma creato per danneggiare un computer, rubare dati o prenderne il controllo.
Ransomware	Malware che cifra i file e chiede un riscatto per restituirli. Detto anche cryptolocker.
Spyware	Malware che spia ciò che fa l'utente.
Trojan	Malware che si finge un programma utile per farsi installare.
Virus	Malware che si attacca a un programma o a un file e si diffonde quando viene aperto.
Worm	Malware che si copia da solo attraverso la rete, senza che nessuno apra nulla.

Per approfondire

No More Ransom - progetto internazionale di polizia e aziende di sicurezza, nomoreransom.org

Agenzia per la cybersicurezza nazionale (ACN) e CSIRT Italia - guide e avvisi sul ransomware, acn.gov.it

Polizia Postale e delle Comunicazioni - indicazioni e segnalazioni, commissariatodips.it

Documentazione di Microsoft su Sicurezza di Windows - per le funzioni dell'antivirus incluso in Windows 11

ATTENZIONE

Informazioni aggiornate a ottobre 2026. CryptoLocker è citato come uno dei primi ransomware diffusi (2013). Nomi di persone, studi e domini degli esempi sono di fantasia. I nomi dei menu di Windows possono variare leggermente con gli aggiornamenti: se non trovi una voce, cerca la funzione descritta.