METODOLOGIE PER LA TRASMISSIONE

- Non potendo contare sulla collaborazione volontaria degli utenti, i virus sono dotati di **metodologie di auto-caricamento** operanti all'insaputa dell'utente.
- I virus si classificano in 3 categorie in base al sistema di propagazione:
  - **Virus di boot**: agiscono sul settore di avvio del disco di sistema prendendone il controllo ogni qual volta si procede al suo avvio.
  - **Virus di file**: agiscono solo su file eseguibili provvedendo a trasmettersi ad ogni esecuzione del programma infetto.
  - **Macrovirus**: usano le Macro (linguaggi di programmazione per definire operazioni ricorrenti) di un'applicazione infetta per diffondersi ed agire.

TIPOLOGIE DI INFEZIONI

- **Infezioni diretta**: viene infettato uno o più file ad ogni esecuzione dell'applicazione infetta.
  - Se non si apre un documento infettato o non si carica un programma infettato il virus non può propagarsi.
- **Infezione rapida**: viene infettato qualsiasi file aperto da un programma infetto.
- **Infezione lenta**: il virus cerca di mascherare la sua presenza limitando l'infezione dei file a quelli appena creati o modificati dal programma.
- **Infezione regolare**: Il virus presenta un comportamento prudente come nel caso precedente ma limita ulteriormente la sua aggressività, procedendo pertanto all'infezione casuale e occasionale dei file.
- **Infezione residente in memoria**: il virus si auto-carica nella memoria **RAM** del computer e rimane nascosto in attesa di attivarsi.

IL VIRUS MELISSA

Melissa è un **macrovirus** creato dal programmatore statunitense David Smith. Diffuso il 26 marzo 1999, ha causato danni per circa 1,3 miliardi di euro ed è considerato il virus con la più alta diffusione di sempre.

Melissa è stato scritto ricorrendo al macrolinguaggio **Visual Basic for Applications** (**VBA**) integrato in **Microsoft Office**.
L'infezione ha colpito i sistemi operativi Microsoft Windows 95, Windows 98 e Windows NT con installata la suite Microsoft Office 97 oppure Microsoft Office 2000.

Il virus arrivava come allegato di un messaggio e-mail: l'allegato si chiamava "**LIST.DOC**" e conteneva un elenco di siti pornografici con le credenziali per l'accesso all'area a pagamento degli stessi. Se l'utente apriva l'allegato, il sistema eseguiva il codice del virus usando l'interprete VBA della suite Office.

Per prima cosa, il virus disattivava le protezioni per evitare l'esecuzione delle macro e poi modificava il file "*Normal.dot*" usato da Office come modello per tutti i documenti scritti con **Microsoft Word**, inserendovi il suo codice: da quel momento in poi tutti i file salvati con questo programma di videoscrittura risultavano infetti.
Il virus controllava poi se sul sistema era presente **Microsoft Outlook**: in caso affermativo, spediva una copia di se stesso ai primi 50 nominativi presenti nella rubrica dei contatti.

Il **payload** veniva rilasciato in corrispondenza di precisi istanti di tempo e consisteva nell'introduzione nel testo di una famosa frase tratta dal cartone animato I Simpson.

RIFERIMENTI

- https://www.c3t.it/projects/awareness/articoli&brochure/virus/

POR FESR 2014-2020 obiettivo Crescita e Occupazione (CreO)

I VIRUS

Scopri che cos'è un virus informatico e quali sono le caratteristiche che lo contraddistinguono dagli altri malware.

COS'È UN VIRUS INFORMATICO

Un **virus informatico** non è nient'altro che un semplice piccolo programma, un frammento di codice progettato e scritto per riprodursi e diffondersi da un sistema informatico ad un altro all'insaputa dell'utente, quindi senza la sua autorizzazione.

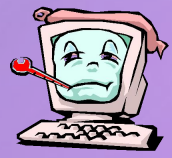
Proprio come un virus biologico (che sfrutta il sistema di riproduzione delle cellule del corpo umano per riprodursi) un virus informatico sfrutta le risorse di un computer.

I virus sono un caso specifico di **malware** che evidenziano comportamenti caratteristici e differenti da altri tipi di malware.

TIPOLOGIE

Esistono due macro tipologie di virus:

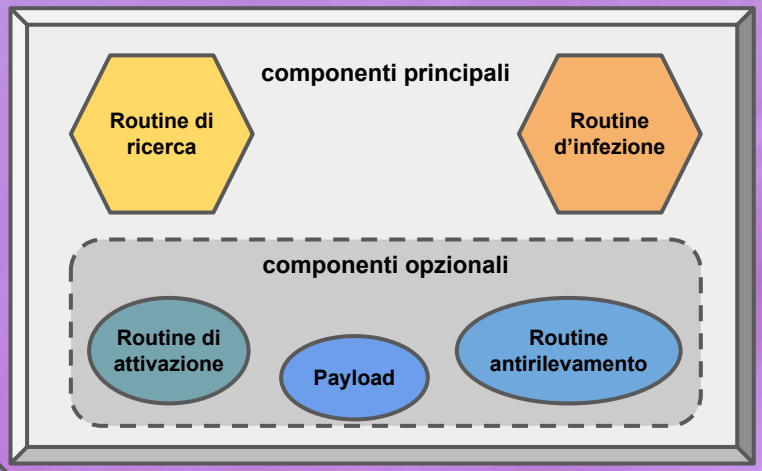
- quelli cosiddetti **ITW** (**In the Wild**), ovvero in libera circolazione nella rete telematica mondiale (*Internet*);
- quelli da laboratorio (**zoo virus**), che esistono esclusivamente all'interno di laboratori di ricerca in reti isolate e sorvegliate.



COMPONENTI

Generalmente i virus sono costituiti da 2 componenti principali e 3 componenti opzionali.

- **Routine di ricerca** (*principale*).
- **Routine d'infezione** (*principale*).
- **Routine di attivazione** (*opzionale*).
- **Payload** (*opzionale*).
- **Routine antirilevamento** (*opzionale*).



LA ROUTINE DI RICERCA

Si occupa della lettura dei dischi rigidi di memorizzazione alla ricerca di un determinato obbiettivo.

- Es. : i file creati con un certo applicativo (*Word*, *Excel*, etc.).
- Es. : il **boot sector** (settore di avvio) dello stesso disco rigido utilizzato per l'avvio del sistema.

A questa routine è inoltre affidata l'identificazione dei file precedentemente infettati, al fine di prevenire una contaminazione recidiva dello stesso target da parte del virus.

LA ROUTINE D'INFEZIONE

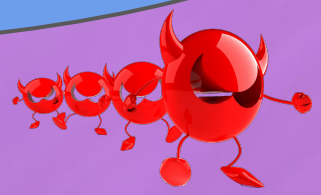
- Entra in azione al termine della routine di ricerca.
- Ha l'obbiettivo di iniziare il processo d'infezione del target precedentemente identificato.
- La discrezione di tale processo è vitale per la diffusione del virus stesso.
- La sopravvivenza del virus è strettamente legata alla sua capacità di saper rimanere occultato il più a lungo possibile.

IL PAYLOAD

- Viene attivato dalla routine di attivazione e consiste nelle tipiche azioni eseguite dal virus:
  - cancellazione di file;
  - formattazione di hard disk;
  - disattivazione di tasti sulla tastiera;
  - visualizzazione di messaggi a video;
  - altro.

LA ROUTINE DI ATTIVAZIONE

- Ha il compito di indicare al virus il momento più idoneo al lancio dell'attacco.
- Eventi di attivazione tipici possono essere costituiti da date o accadimenti significativi.
  - Es. : il livello di occupazione di un hard disk.



LA ROUTINE ANTIRILEVAMENTO

- Ha il compito di impedire o rendere più difficoltosa la rilevazione del virus.
- Il suo funzionamento può essere:
  - molto semplice (es. modifica di data, ora e dimensione del file infetto);
  - estremamente complesso.
- Le routine antirilevamento più sofisticate si caricano nella **RAM** del computer e tentano di ingannare i software antivirus che si occupano dell'esame del disco.