COME PREVENIRE UN'INFEZIONE

- Tenere aggiornati i sistemi operativi e software, così da arginare eventuali falle.
- Utilizzare software antivirus che abbiamo un database aggiornato delle definizioni.
- Utilizzare un firewall.
- Prestare massima attenzioni a file e allegati e-mail.
- Crittografare i dati sensibili presenti all'interno delle macchine.
- Effettuare periodicamente copie di sicurezza dei file utili.

SINTOMI DI UN'INFEZIONE

Come per l'influenza umana, per riconoscere lo worm è necessario conoscerne i sintomi, in quanto difficilmente viene rilevato.

I sintomi includono:

- prestazioni carenti del computer;
- blocco o arresto del sistema operativo in modo anomalo/imprevisto;
- blocco o arresto delle applicazioni in modo anomalo/imprevisto;
- scomparsa di icone e/o file;
- improvvisa comparsa di icone e/o file;
- strani messaggi di posta inviati dal tuo account.

COME RIMUOVERE UNO WORM

La rimozione di uno worm può essere difficile e comunque può avvenire solo mediante l'utilizzo di un valido antivirus. In casi estremi, potrebbe essere necessario formattare il sistema e reinstallare sistema operativo e software.

Prima di rimuovere lo worm, è necessario che la macchina sia disconnessa da Internet, dalla rete e da eventuali dispositivi di archiviazione esterna, che andranno anch'essi verificati alla ricerca di infezioni.

UN PÒ DI STORIA

Il primo worm, rilasciato nel 1988 e che ha avuto un'ampia propagazione grazie al primo utilizzo di Internet, è stato **Morris**.
Il codice malevolo era opera di Robert Tappan Morris Jr., uno studente laureato alla Cornell University che, secondo quanto riferito, stava tentando di elencare tutti i sistemi collegati al precursore della rete Internet, ARPANET. Mirato alle vulnerabilità in diversi programmi Unix, Morris era in grado di infettare un sistema più di una volta, rendendo difficile la completa rimozione.

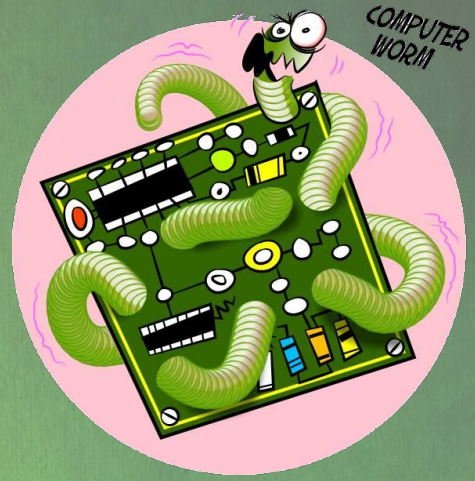
Uno degli worm più dannosi di sempre è stato **ILOVEYOU** che si è propagato attraverso diversi vettori, inclusi allegati di posta elettronica che sembravano essere file di testo, script eseguiti in sessioni di chat di messaggistica istantanea e copie del virus in file eseguibili rinominati con i nomi di file di sistema comuni e che si diffondeva senza la consapevolezza iniziale delle vittime.

Nel 2003 fu la volta di **Blaster** (anche conosciuto come **MSBlast** o **Lovesan**), un malware destinato principalmente alle piattaforme Microsoft. Blaster ha attaccato i computer sfruttando un difetto di sicurezza con il processo RPC (*Remote Procedure Call*) di Microsoft utilizzando il numero di porta TCP (*Transmission Control Protocol*) 135. Il malware causava il riavvio del sistema ogni 60 secondi e, in alcuni computer, una schermata di benvenuto vuota. Microsoft rilasciò uno strumento di rilevamento e rimozione di Blaster per sistemi operativi Windows XP e Windows 2000.

RIFERIMENTI

➢ https://www.c3t.it/projects/awareness/articoli&brochure/worm/

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



GLI WORM

Scopri cos'è un computer worm, come si diffonde e come puoi riconoscere un'infezione .

COS'È UNO WORM

Uno worm è un tipo di programma malevolo la cui caratteristica è quello di **infiltrarsi in maniera latente sulle macchine per poi propagarsi**, infettando altri PC sfruttando le capacità di comunicazione della macchina stessa (rete, Internet, contatti e-mail).

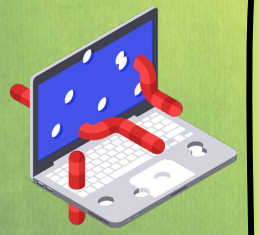
Si tratta a tutti gli effetti di un **malware con capacità autoreplicante** ed è comune che vengano notati solo quando la loro replica incontrollata impatta sulle risorse di sistema, rallentando o arrestando la macchina stessa.

COME SI DIFFONDONO

La caratteristica peculiare dello worm è di **diffondersi senza il bisogno dell'interazione dell'utente**, quindi dell'azione umana; gli basta diventare attivo una singola volta sul sistema infetto per avviarne il processo di clonazione e diffusione.

Prima dell'uso quotidiano e in larga scala di Internet e delle reti, gli worm venivano trasmessi esclusivamente mediante supporti di archiviazione esterna, come i floppy disk che, se montati su un sistema, infettavano altri dispositivi di archiviazione collegati al sistema "di partenza".

COME FUNZIONANO



I "vermi" informatici spesso si basano sulle azioni e sulle **vulnerabilità dei protocolli di rete** per propagarsi.

Una volta avuto accesso ad una macchina, il codice malevolo è in grado di continuare a propagarsi all'interno di un'organizzazione, ivi compresi i dispositivi di archiviazione esterna (HDD, USB, SSD) che, se connessi ad altre macchine facenti parte di altre reti, diventano facili veicoli verso altri computer.

Un'altra caratteristica degli worm è quella di avere la potenziale possibilità, per alcuni di essi, di **propagarsi via mail creando ed inviando automaticamente mail auto-infette** a tutta la lista contatti di un utente.

Mentre i virus sono programmi malevoli, con capacità autoreplicante, che infettano file e richiedono un'azione umana (esecuzione) per essere diffusi, gli worm, invece, **lavorano in modo latente sui dispositivi**, ed hanno l'obiettivo di rimanere nel sistema il più a lungo possibile per diffondersi con altre macchine.

L'obiettivo di questo tipo di malware è solitamente quello di **saturare computer e reti, impedendo che vengano utilizzati**.

TIPI DI WORM

1. **Worm su internet**

   Gli worm non colpiscono solo le reti informatiche, ma anche siti web popolari con misure di sicurezza insufficienti. Quando riescono a infettare il sito web, gli worm possono replicarsi su qualsiasi computer utilizzato per accedere al sito web in questione; da lì, si diffondono ad altri computer connessi attraverso le connessioni Internet e della rete locale.

2. **Worm nelle e-mail e nella messaggistica istantanea**

   Questi worm vengono generalmente diffusi tramite allegati compromessi. Di solito hanno doppie estensioni (ad esempio, .mp4.exe o .avi.exe) in modo che il destinatario possa pensare che siano semplici file multimediali e non programmi informatici dannosi.
   Un messaggio istantaneo (*WhatsApp*, *Telegram*, etc.) o di posta elettronica non deve per forza contenere un allegato scaricabile per poter diffondere uno worm; il corpo del messaggio potrebbe contenere un link abbreviato, in modo che il destinatario non possa sapere di cosa si tratta senza cliccare su di esso: quando clicca sul link, verrà indirizzato a un sito web infetto che inizierà automaticamente a scaricare software dannoso sul suo computer.

3. **Worm nella condivisione di file**

   Sebbene siano illegali, i trasferimenti di file eseguiti tramite condivisione di file sono ancora utilizzati da milioni di persone in tutto il mondo, che, così facendo, espongono inconsapevolmente i loro computer alla minaccia di worm.
   Anche questi worm sono camuffati da file multimediali con doppia estensione. Quando la vittima apre il file scaricato per vederlo o ascoltarlo, scaricherà lo worm sul proprio computer. Anche se gli utenti credono di aver scaricato un file multimediale riproducibile, un file dannoso eseguibile potrebbe essere nascosto nella cartella e potrebbe venire installato in maniera discreta quando viene aperto per la prima volta il file multimediale.