MALWARE

Malware più diffusi

Fonti:

- *Wikipedia: Malware*
- *Fastweb Plus*
- *Agenzia per la Cybersicurezza Nazionale*
- *Wikipedia: Virus*
- *Politecnico di Torino: Anatomia del Malware*
- *Kaspersky: Tipi di Malware*

PREMESSA

ATTENZIONE

ATTENZIONE

Le seguenti slide contengono materiale potenzialmente pericoloso, fornito **esclusivamente a scopo didattico** per l'apprendimento delle tecniche di sicurezza informatica. Questi strumenti devono essere utilizzati **in modo etico e responsabile**, esclusivamente per scopi legittimi come il miglioramento della sicurezza e la protezione dei sistemi.

È vietato utilizzare queste informazioni per attività **malevoli o illegali**. Ogni uso improprio che violi le leggi o i principi etici è severamente sanzionato dalla legge.

MALWARE

MALWARE

DEFINIZIONE

Un **Malware** (abbreviazione dell'inglese malicious software, letteralmente "software malevolo"), indica un **qualsiasi programma informatico usato per disturbare le operazioni svolte da un utente di un computer**. Termine coniato nel 1990, precedentemente veniva chiamato virus per computer.

Il malware non necessariamente è creato per arrecare danni tangibili ad un computer o un sistema informatico, ma va inteso anche come un programma che può rubare di nascosto informazioni di vario tipo, da commerciali a private, in genere senza essere rilevato dall'utente anche per lunghi periodi di tempo.

Curiosità
Breve storia dei Malware

RABBIT

RABBIT

DEFINIZIONE

Tipo di malware che **attacca le risorse del sistema** duplicando in continuazione la propria immagine su disco, o attivando nuovi processi a partire dal proprio eseguibile, in modo da **consumare tutte le risorse disponibili** sul sistema in pochissimo tempo. Il nome si riferisce proprio alla prolificità di questo "infestante".

Esempio
Fork Bomb

RABBIT - ESEMPIO FORK BOMB

1. Creare un file di testo RABBIT.txt;
2. Inserire la Fork Bomb nel file digitando: **start cmd /k echo BOMB | %0**
3. Modificare l'estensione del file da .txt a .bat
4. Preparare un terminale con l'istruzione: **taskkill /F /IM cmd.exe** per stoppare il malware;
5. Eseguire il file RABBIT.bat e terminarlo con il comando preparato sul terminale.

RABBIT - ESEMPIO FORK BOMB

1. Creare un file di testo RABBIT.txt;
2. Inserire la Fork Bomb nel file digitando: **start cmd /k echo BOMB | %0**
3. Modificare l'estensione del file da .txt a .bat
4. Preparare un terminale con l'istruzione: **taskkill /F /IM cmd.exe** per stoppare il malware;
5. Eseguire il file RABBIT.bat e terminarlo con il comando preparato sul terminale.

RABBIT - ESEMPIO FORK BOMB

1. Creare un file di testo RABBIT.txt;
2. Inserire la Fork Bomb nel file digitando: **start cmd /k echo BOMB | %0**
3. Modificare l'estensione del file da .txt a .bat
4. Preparare un terminale con l'istruzione: **taskkill /F /IM cmd.exe** per stoppare il malware;
5. Eseguire il file RABBIT.bat e terminarlo con il comando preparato sul terminale.

RABBIT - ESEMPIO FORK BOMB

1. Creare un file di testo RABBIT.txt;
2. Inserire la Fork Bomb nel file digitando: **start cmd /k echo BOMB | %0**
3. Modificare l'estensione del file da .txt a .bat
4. Preparare un terminale con l'istruzione: **taskkill /F /IM cmd.exe** per stoppare il malware;
5. Eseguire il file RABBIT.bat e terminarlo con il comando preparato sul terminale.

RABBIT - ESEMPIO FORK BOMB

1. Creare un file di testo RABBIT.txt;
2. Inserire la Fork Bomb nel file digitando: **start cmd /k echo BOMB | %0**
3. Modificare l'estensione del file da .txt a .bat
4. Preparare un terminale con l'istruzione: **taskkill /F /IM cmd.exe** per stoppare il malware;
5. Eseguire il file RABBIT.bat e terminarlo con il comando preparato sul terminale.

VIRUS

VIRUS

DEFINIZIONE

Un **Virus** è un Malware che **infetta dei file in modo da creare copie di se stesso**, generalmente senza farsi rilevare dall'utente. Il termine viene usato per un programma che si integra in qualche codice eseguibile (incluso il sistema operativo) del sistema informatico vittima, in modo tale da **diffondersi su altro codice eseguibile** quando viene eseguito il codice che lo ospita, senza che l'utente ne sia a conoscenza.

Approfondimento
Geopop: Malware

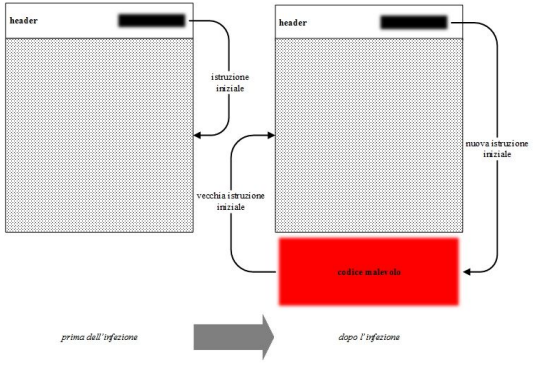

Figura 1: fonte Politecnico di Torino

ELENCO PRINCIPALI MALWARE

ELENCO PRINCIPALI MALWARE

PRINCIPALI MALWARE

Di seguito un elenco delle principali tipologie di Malware esistenti:

- **Adware**: Malware che mostra pubblicità indesiderata sul web o sul dispositivo;
- **Spyware**: Malware che raccoglie informazioni sull'utente senza il suo consenso;
- **Keylogger**: Spyware che registra le digitazioni da tastiera per rubare informazioni sensibili;
- **Trojan**: Malware che si maschera da software legittimo per ingannare l'utente e infettare il sistema;
- **Backdoor**: Trojan che crea un accesso nascosto al sistema per consentire l'accesso non autorizzato;
- **Worm**: Virus che si replica autonomamente diffondendosi attraverso la rete;

Curiosità
Microsoft: Nomenclatura Malware

ELENCO PRINCIPALI MALWARE

PRINCIPALI MALWARE

Di seguito un elenco delle principali tipologie di Malware esistenti:

- **Adware**: Malware che mostra pubblicità indesiderata sul web o sul dispositivo;
- **Spyware**: Malware che raccoglie informazioni sull'utente senza il suo consenso;
- **Keylogger**: Spyware che registra le digitazioni da tastiera per rubare informazioni sensibili;
- **Trojan**: Malware che si maschera da software legittimo per ingannare l'utente e infettare il sistema;
- **Backdoor**: Trojan che crea un accesso nascosto al sistema per consentire l'accesso non autorizzato;
- **Worm**: Virus che si replica autonomamente diffondendosi attraverso la rete;

Curiosità
Microsoft: Nomenclatura Malware

PRINCIPALI MALWARE

Di seguito un elenco delle principali tipologie di Malware esistenti:

- **Adware**: Malware che mostra pubblicità indesiderata sul web o sul dispositivo;
- **Spyware**: Malware che raccoglie informazioni sull'utente senza il suo consenso;
- **Keylogger**: Spyware che registra le digitazioni da tastiera per rubare informazioni sensibili;
- **Trojan**: Malware che si maschera da software legittimo per ingannare l'utente e infettare il sistema;
- **Backdoor**: Trojan che crea un accesso nascosto al sistema per consentire l'accesso non autorizzato;
- **Worm**: Virus che si replica autonomamente diffondendosi attraverso la rete;

Curiosità
Microsoft: Nomenclatura Malware

PRINCIPALI MALWARE

Di seguito un elenco delle principali tipologie di Malware esistenti:

- **Adware**: Malware che mostra pubblicità indesiderata sul web o sul dispositivo;
- **Spyware**: Malware che raccoglie informazioni sull'utente senza il suo consenso;
- **Keylogger**: Spyware che registra le digitazioni da tastiera per rubare informazioni sensibili;
- **Trojan**: Malware che si maschera da software legittimo per ingannare l'utente e infettare il sistema;
- **Backdoor**: Trojan che crea un accesso nascosto al sistema per consentire l'accesso non autorizzato;
- **Worm**: Virus che si replica autonomamente diffondendosi attraverso la rete;

Curiosità
Microsoft: Nomenclatura Malware

PRINCIPALI MALWARE

Di seguito un elenco delle principali tipologie di Malware esistenti:

- **Adware**: Malware che mostra pubblicità indesiderata sul web o sul dispositivo;
- **Spyware**: Malware che raccoglie informazioni sull'utente senza il suo consenso;
- **Keylogger**: Spyware che registra le digitazioni da tastiera per rubare informazioni sensibili;
- **Trojan**: Malware che si maschera da software legittimo per ingannare l'utente e infettare il sistema;
- **Backdoor**: Trojan che crea un accesso nascosto al sistema per consentire l'accesso non autorizzato;
- **Worm**: Virus che si replica autonomamente diffondendosi attraverso la rete;

Curiosità
Microsoft: Nomenclatura Malware

ELENCO PRINCIPALI MALWARE

PRINCIPALI MALWARE

Di seguito un elenco delle principali tipologie di Malware esistenti:

- **Adware**: Malware che mostra pubblicità indesiderata sul web o sul dispositivo;
- **Spyware**: Malware che raccoglie informazioni sull'utente senza il suo consenso;
- **Keylogger**: Spyware che registra le digitazioni da tastiera per rubare informazioni sensibili;
- **Trojan**: Malware che si maschera da software legittimo per ingannare l'utente e infettare il sistema;
- **Backdoor**: Trojan che crea un accesso nascosto al sistema per consentire l'accesso non autorizzato;
- **Worm**: Virus che si replica autonomamente diffondendosi attraverso la rete;

Curiosità
Microsoft: Nomenclatura Malware

ELENCO PRINCIPALI MALWARE

PRINCIPALI MALWARE

Di seguito un elenco delle principali tipologie di Malware esistenti:

- **Adware**: Malware che mostra pubblicità indesiderata sul web o sul dispositivo;
- **Spyware**: Malware che raccoglie informazioni sull'utente senza il suo consenso;
- **Keylogger**: Spyware che registra le digitazioni da tastiera per rubare informazioni sensibili;
- **Trojan**: Malware che si maschera da software legittimo per ingannare l'utente e infettare il sistema;
- **Backdoor**: Trojan che crea un accesso nascosto al sistema per consentire l'accesso non autorizzato;
- **Worm**: Virus che si replica autonomamente diffondendosi attraverso la rete;

Curiosità
Microsoft: Nomenclatura Malware

RANSOMWARE

RANSOMWARE

DEFINIZIONE

Il ransomware è una tipologia di minaccia che ha lo **scopo di cifrare i dati del bene informatico target in modo da comprometterne la disponibilità, integrità e riservatezza**. Inoltre, in questa tipologia di minaccia spesso l'attaccante crea dei file, detti ransom notes, tramite i quali viene richiesto alla vittima un riscatto in cambio dell'accesso ai propri dati. In alcuni casi i dati, prima di essere cifrati, vengono **esfiltrati** in modo da offrire all'attaccante uno strumento in più di ricatto nei confronti della vittima.

Curiosità
Monitoraggio gruppi Ransomware

ZERO CLICK

ZERO CLICK

DEFINIZIONE

Questo tipo di malware **non richiede che la vittima esegua azioni**, ma sfrutta le vulnerabilità dei software o la presenza di bug non ancora corretti per farsi strada nei dispositivi e infettarli. Questo significa che **la vittima non si rende conto dei malware** che operano sul proprio PC, smartphone o tablet e non ha modo di individuare la minaccia alla sua sicurezza online.

Curiosità
Graphite: Paragon Software Group

ELENCO MALWARE STORICI

ELENCO MALWARE STORICI

MALWARE STORICI

Di seguito un elenco di alcuni dei malware più famosi e pericolosi della storia dell'informatica ordinati per anno di comparsa:

- 1971 - **Creeper**: Primo Malware (Worm) della storia;
- 2000 - **Iloveyou**: Malware (Worm) che sfruttava tecniche di social engineering via email (Phishing);
- 2010 - **Stuxnet**: Malware (Virus) sviluppato per sabotare il programma nucleare iraniano;
- 2016 - **Pegasus**: Malware (Spyware) sviluppato dalla NSO Group per spiare dispositivi mobili;
- 2017 - **WannaCry**: Malware (Ransomware) che si è diffuso in tutto il mondo sfruttando l'exploit "EternalBlue";
- 2024 - **Graphite**: Malware (Spyware) sviluppato da Paragon Software Group per spiare dispositivi mobili.

"L'unico vero sistema sicuro è un sistema spento, chiuso in una gettata di cemento, sigillato in una stanza rivestita di piombo protetta da guardie armate. Ma anche in questo caso ho i miei dubbi."