COME PROTEGGERSI DAI MALWARE

Ecco alcune semplici norme (pratiche di buon senso) per rimanere in allerta e prevenire infezioni da malware:

1. Prestare particolare attenzione ai domini che finiscono con strane combinazioni di lettere, ossia in qualcosa di diverso da **com**, **org**, **edu** o **gov**, per dirne alcuni, poiché possono indicare la pericolosità di un sito web.
2. Non cliccare su **pop-up pubblicitari** mentre si naviga su internet. Non aprire **allegati e-mail** non richiesti o scaricare software da **siti web inaffidabili** o reti di trasferimento peer-to-peer.
3. Assicurarsi che il sistema operativo, i browser e i plugin utilizzati siano **sempre aggiornati**, poiché questo contribuisce a tenere a bada i criminali.

4. Per gli utenti di dispositivi mobili: scaricare soltanto app provenienti da **app-store ufficiali**.
5. Non cliccare su **link non verificati** nelle e-mail, SMS e messaggi whatsApp di **origine sconosciuta**. Evitare anche gli strani link provenienti da amici e contatti, a meno che tu non ne abbia verificato la veridicità.
6. Per mantenere al sicuro le aziende: adottare **rigide politiche di sicurezza** dei dispositivi mobili e implementare una soluzione per metterle in pratica. Questo è fondamentale nell'ambiente commerciale di oggi, con numerosi sistemi operativi che operano in varie sedi.
7. Ottenere un buon programma **anti-malware**: questo dovrebbe includere un sistema di protezione a più livelli con la capacità di eseguire scansioni e rilevare malware mantenendo una **difesa proattiva** in tempo reale che possa bloccare le minacce.

ANTI-MALWARE

Storicamente chiamati **antivirus**, gli **anti-malware** sono oggi dei veri e propri "programmi di sicurezza" che rappresentano la prima linea di difesa contro le minacce informatiche.

I primi antivirus eseguivano un controllo sostanzialmente "meccanico" basato sul controllo della **firma dei virus**.

La seconda generazione di antimalware si basa su un'**analisi euristica** che consente di effettuare una scansione di un file eseguibile per analizzarne la struttura, il comportamento e gli attributi. In quesro modo si supera il problema del possibile *malware polimorfico* (che cambia la sua firma ogni volta che agisce).

La nuova frontiera della sicurezza informatica è rappresentata dall'**intelligenza artificiale** che non si limita alla mera esecuzione di una serie limitata di controlli; al contrario, analizza determinati comportamenti e ne individua le anomalie.

Tra i programmi anti-malware più efficaci attualmente troviamo: **Avast Premium Security**, **AVG Internet Security**, **Avira Internet Security Suite** e **Kaspersky Internet Security**.

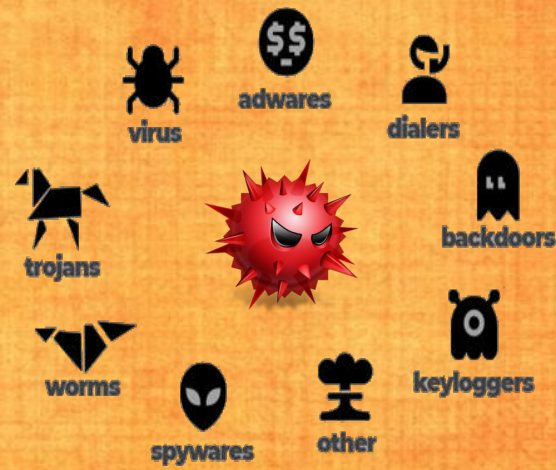
RIFERIMENTI

➢ http://www.c3t.it/projects/awareness/articoli&brochure/malware/

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

I MALWARE

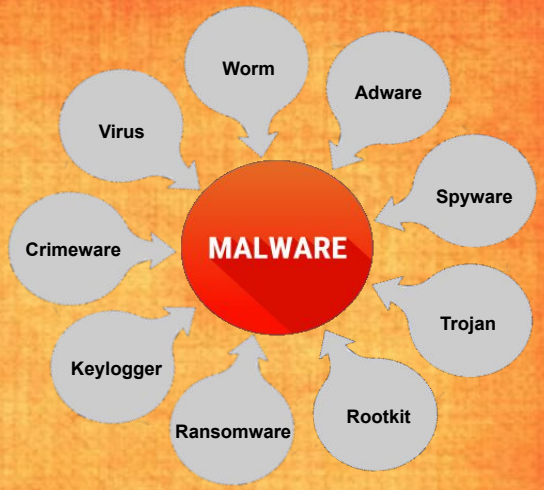
Scopri cosa è un malware, quali sono i tipi, le forme, le modalità in cui esso si può presentare e come puoi difenderti.



COS'È UN MALWARE

Malware o **"software malevolo"** è un termine generico che descrive un programma/codice dannoso che mette a rischio un sistema. I malware possono rubare, criptare o eliminare i dati, alterare o compromettere le funzioni fondamentali di un computer e spiare le attività degli utenti senza che questi se ne accorgano o forniscano alcuna autorizzazione.
Tra gli indizi più comuni che segnalano la **presenza di un malware** nel sistema si ha:

1. Riduzione della velocità del sistema operativo, sia nella navigazione su internet che nel semplice utilizzo delle applicazioni.
2. Un'ondata di irritanti annunci pubblicitari, che non dovrebbe comparire, riempie lo schermo.
3. L'utilizzo delle risorse di sistema è insolitamente elevato e la ventola del computer inizia a girare all'impazzata.
4. Toolbar, estensioni o plugin compaiono inaspettatamente nel browser.



COME SI INFILTRANO I MALWARE

- ❏ Navigando in siti web oggetto di **hacking**.
- ❏ Scaricando applicazioni apparentemente legittime tramite **siti web non ufficiali**.
- ❏ **"Click-shaming"** : quando si aprono allegati e-mail sconosciuti o si installa qualcosa che proviene da una fonte inaffidabile.
- ❏ **"Social engineering"** : tecnica utilizzata dagli aggressori per indurre le vittime a violare il protocollo di sicurezza o a fornire informazioni private (ad esempio tramite e-mail di **phishing**). Si basano sulla manipolazione psicologica, come sedurre le vittime giocando alla loro avidità, vanità o alla loro volontà di aiutare qualcuno.
- ❏ **"Drive-by download"** : si riferisce al download involontario di uno o più file dannosi sul sistema dell'utente senza il suo consenso o la sua conoscenza.
- ❏ Dispositivi **USB infetti**: metodo molto efficace in ambienti aziendali e produttivi.
- ❏ Intrusioni dirette nelle reti locali attraverso falle nella sicurezza del perimetro virtuale.
- ❏ Vulnerabilità del sistema operativo o delle applicazioni installate sui dispositivi delle vittime.

TIPI DI MALWARE PIÙ DIFFUSI

- ➔ **Adware**: software indesiderati che visualizzano messaggi pubblicitari sullo schermo, spesso all'interno delle finestre del browser.
- ➔ **Spyware**: particolare tipologia di malware progettata per spiare le attività dell'utente sul computer, senza autorizzazione, per poi comunicarle ai *criminal hacker* che hanno sviluppato il codice malevolo.
- ➔ **Virus**: si tratta di un codice malevolo che, così come avviene in natura, si "attacca" ad altri programmi infettandoli. Quando l'utente lo esegue, di solito inavvertitamente, il virus si riproduce modificando altri programmi e file e infettandoli con il proprio codice.
- ➔ **Worm**: malware che sfrutta le falle si sistema per diffondersi sugli altri computer di una rete e li danneggia, di solito, mediante la distruzione di file e cartelle di sistema.
- ➔ **Trojan**: i "cavalli di Troia" sono tra i malware più pericolosi in circolazione. Di solito si presentano sotto forma di qualcosa di utile, ad esempio come tool per lo sblocco delle versioni a pagamento di noti software commerciali.
- ➔ **Ransomware**: sono malware che impediscono alla vittima di accedere al proprio dispositivo e criptano i suoi file, obbligandola a pagare un riscatto per riottenerli.
- ➔ **Rootkit**: consentono ai *criminal hacker* di ottenere i privilegi da amministratore sul sistema infetto. Generalmente, sono progettati per rimanere nascosti agli occhi dell'utente, degli altri software e del sistema operativo stesso.
- ➔ **Keylogger**: semplici codici malevoli capaci di registrare tutto ciò che la vittima digita sulla tastiera, inviando poi le informazioni raccolte agli hacker che, in questo modo, riescono a rubare informazioni sensibili.
- ➔ **Crimeware**: categoria di programmi malware appositamente progettati per condurre in maniera automatica azioni cybercriminali legate alla sfera finanziaria.