con la collaborazione di

Google™

SICURAMENTE ONLINE

DIFENDITI DAI **MALWARE**

PENSI CHE IL **PHISHING**

SIA SOLO UN TIPO DI PESCA?

PENSI CHE I **COOKIE**

SIANO SOLO BISCOTTI?

PENSI CHE UN **VIRUS**

SIA SOLO UN RAFFREDDORE?

DIFENDITI DAI **MALWARE**

Per malware si intende un programma software progettato per danneggiare intenzionalmente un computer o dispositivo mobile. I malware comportano un duplice rischio: il danneggiamento del dispositivo e dei dati in esso contenuti e la possibilità che qualcuno possa venire a conoscenza di informazioni riservate e addirittura utilizzarle fingendo di essere te (furto di identità online).

1 Quali sono i sintomi di un dispositivo infetto

I malware tendono ad essere molto poco evidenti viste le funzioni che svolgono. I sintomi che devono farci temere la presenza di un virus sono:
- rallentamento della navigazione;
- impossibilità di collegarsi ai siti degli antivirus;
- anomalie di funzionamento (programmi che non si avviano o che non si aprono automaticamente, comparsa di strani messaggi di errore, ecc.).
- riduzione immotivata dello spazio disponibile in memoria (che viene progressivamente saturato dal diffondersi dell'infezione);
- spegnimenti immotivati del dispositivo;
- impossibilità ad eseguire operazioni prima consentite.

2 Come difendersi dai malware

Per difenderti dai malware è utile adottare alcuni accorgimenti:
- aggiornamenti costanti dei sistemi operativi, antivirus, applicazioni e servizi che utilizzi
- attenzione ai contenuti che scarichi

Aggiornamenti costanti

Aggiorna il sistema operativo e i programmi software installati sul dispositivo. La maggior parte dei programmi software e dei sistemi operativi avvisa l'utente quando è disponibile un nuovo aggiornamento; è bene eseguire sempre l'aggiornamento appena possibile, poiché a volte le versioni meno recenti del software hanno problemi di sicurezza su cui fanno leva i criminali informatici per avere facile accesso ai tuoi dati.

Aggiorna costantemente il browser utilizzato per la navigazione. Alcuni browser effettuano gli aggiornamenti automaticamente.

Mantieni aggiornati tutti i plug-in. Tutti i browser moderni consentono l'utilizzo dei plug-in, componenti aggiuntivi che forniscono ulteriori funzionalità al software di base. Purtroppo, però, sempre più di frequente questi software veicolano contenuti nocivi capaci di sfruttare le vulnerabilità presenti nelle versioni più vecchie dei plug-in. Se si visita una pagina web malevola tramite un browser che utilizza una versione "datata" di un certo plug-in, è possibile che sul proprio sistema venga eseguito un codice nocivo che può causare danni al dispositivo. Prima di installare un plug-in richiesto da una pagina web è importante assicurarsi che sia davvero necessario e che il sito che si utilizza per scaricarlo sia affidabile.
È consigliabile controllare spesso la lista dei plug-in installati e caricati per ciascun browser web installato sul proprio sistema, verificando se sono tutti necessari, utili e provenienti da fonti riconosciute. Per tutti i principali browser la procedura da seguire

è identica, tranne per Internet Explorer.
In Internet Explorer è possibile accedere alla lista dei plug-in cliccando sull'icona dell'ingranaggio che compare nella barra degli strumenti dell'applicazione, e cliccando poi su *Gestione componenti aggiuntivi*. Seleziona poi dal menù a tendina *Mostra*, la voce T*utti i componenti aggiuntivi*. Cliccando con il tasto destro del mouse sul nome di un qualunque plug-in (detto anche add-on), si potrà richiederne la disattivazione cliccando su *Disabilita*.
Nel caso di Firefox, Chrome ed Opera, bisogna digitare nella barra degli indirizzi: "about:plugins:", tale digitazione farà comparire la lista completa dei plug-in abilitati e disabilitati.

Attenzione ai contenuti che scarichiamo

Poni attenzione ai popup. A volte i malware possono "nascondersi" dietro i **popup**: finestre che compaiono automaticamente durante la navigazione e che, a volte, inducono a installare software dannosi con l'inganno. Spesso infatti in queste finestre compaiono degli avvisi che affermano che il computer è stato infettato e che il loro download potrebbe eliminare il problema. In questi casi è consigliabile chiudere la finestra popup senza cliccare al suo interno.
Poni attenzione agli Script ActiveX e Applet Java. Gli Script ActiveX e Applet Java sono delle estensioni, dette anche "componenti aggiuntive", che forniscono funzionalità accessorie durante la navigazione (ad es. animazione ed interattività all'interno di un sito web). Le proposte di installazione di queste estensioni devono essere ben valutate dall'utente, poiché possono essere fonti di rischio, in quanto sono spesso usati per effettuare degli attacchi. Quindi, prima di mandarli in esecuzione, accertati di essere su un sito conosciuto, che faccia riferimento ad un marchio importante. Non sono rare le pagine web in cui sono presenti degli script che promettono utilità e vantaggi all'utente e che, invece, si rivelano dannosi per il computer, celando virus, malware e altro.Talvolta tali script possono attivarsi anche involontariamente, quindi è utile prestare attenzione

alla loro eventuale presenza, in modo tale da disattivarli.

Poni attenzione all'installazione dei plug-in. Può capitare che, all'apertura di una pagina web, venga richiesta l'installazione di un plug-in che il dispositivo ancora non possiede. Prima di installarlo, assicurati che sia effettivamente necessario e che il sito che stai usando per scaricarlo sia conosciuto, poiché anche questi software possono essere usati per attività malevole.

Poni attenzione ai programmi che scarichi. Prima di scaricare un programma puoi verificarne la reputazione tramite lo store, è possibile consultare l'appstore integrato nel telefono o nel browser o il sito web dello sviluppatore. Puoi così verificare anche la reputazione dello sviluppatore leggendo le opinioni di altri utenti. È utile cercare anche nella rete recensioni o commenti relativi al programma in questione. Se le informazioni raccolte sono negative sarebbe opportuno evitare il download.

In generale, è consigliabile non aprire file di tipo sconosciuto (inclusi gli allegati a e-mail di persone che non si conoscono o che sembrano strane!) e non seguire messaggi di avviso o di errore (i cosiddetti "prompt") che chiedono di aprire un file. Nel caso in cui un malware impedisca di uscire da una pagina, ad esempio aprendo più volte un messaggio di richiesta di download, può essere d'aiuto l'utilizzo dell'applicazione Task Manager o Monitoraggio Attività del computer per chiudere il browser.

3 Strumenti per proteggersi dai malware

Per difenderti dai malware, oltre agli accorgimenti descritti precedentemente, è necessario installare sul pc:
- un programma antivirus;
- un programma antispyware;
- un firewall personale sempre attivo.

Detti programmi di protezione vengono caricati in memoria all'av-

vio del sistema operativo (Windows, Chrome OS, Mac OS, Linux ecc.) e monitorano costantemente lo stato della protezione del computer. Inoltre, l'antivirus esercita un controllo costante anche sul programma di posta elettronica, ispezionando in tempo reale tutte le e-mail ricevute e spedite. È comunque opportuno controllare spesso il computer con l'antivirus, effettuando scansioni periodiche.
Anche in questo caso è fondamentale che sia l'antivirus che l'antispyware siano costantemente aggiornati. Non possiamo garantire l'efficacia di questi programmi, ma spesso l'utilizzo delle versioni più recenti fa la differenza. È possibile, inoltre, visitare il sito av-comparatives.org per trovare i vari programmi software antivirus ed esaminare i risultati dei test.

Tieni al sicuro i dati importanti che non vuoi perdere. È fondamentale impostare adeguatamente le opzioni di salvataggio e backup delle informazioni sulle unità di archiviazione interne ed esterne.

E' importante tenere i dati separati dal sistema operativo e dai programmi, poiché, se in seguito ad un grave crash causato da un malware dovesse essere necessario formattare il disco e reinstallare il sistema operativo, si può effettuare l'operazione senza il pericolo di perdere i dati, poiché questi ultimi si trovano su un altro disco fisso.
Non è necessario avere materialmente due hard disk all'interno del pc: è sufficiente partizionare (suddividere) l'unico disco presente.
Controlla se sul tuo dispositivo ci sono già due dischi fissi (molti sistemi vengono venduti con il disco fisso già suddiviso in due partizioni).
Un'altra soluzione, altrettanto (se non più) sicura, è di salvare i dati e documenti importanti all'interno di un sistema di cloud sicuro, al quale puoi accedere solamente attraverso una username e password sicura.

Tipologie di malware

Esistono diverse tipologie di malware. Vediamo insieme le più comuni:

• **keylogger:** sono programmi che, una volta installati sul dispositivo, registrano tutto ciò che viene digitato sulla tastiera. Possono eseguire anche istantanee dello schermo, ottenendo così informazioni riguardo l'uso di Internet e le password utilizzate dall'utente per accedere ai vari account personali (casella di posta, banca, ecc). Non è necessario che il malintenzionato che vuole rubare i dati acceda fisicamente al computer, poiché molti keylogger odierni inviano i loro rapporti per posta. Un Keylogger può insinuarsi nel sistema mediante file scaricati e/o ricevuti tramite chat/e-mail;
• **hijacker**: questi programmi sono utilizzati per causare l'apertura automatica di pagine Web indesiderate. Lo scopo di tale dirottamento è quello di incrementare in modo artificioso il numero di accessi e di click diretti al sito indesiderato per incrementare i guadagni dovuti alle inserzioni pubblicitarie presenti in esso;
• **rabbit**: sono programmi che esauriscono la memoria del computer replicandosi di continuo (in memoria o su disco) a grande velocità;
• **spyware**: è un software che raccoglie piccoli frammenti di informazioni riguardanti l'attività online di un utente a sua insaputa. Di solito viene scaricato senza che l'utente ne sia consapevole, ad esempio, può essere nascosto in alcuni programmi shareware;
• **adware**: è una variante dello spyware, che visualizza, riproduce o scarica automaticamente pubblicità sul dispositivo. Si differenzia dagli altri spyware poiché la sua attività consiste nella sola visualizzazione di banner pubblicitari, su cui riceve informazioni da internet. È quindi meno dannoso degli altri spyware, i quali possono, invece, spiare i dati personali dell'utente;
• **virus**: è il tipo più comune di malware, si tratta di un programma nocivo che ha come scopo quello di infettare il computer e i file memorizzati. Il virus si attiva solo quando il programma o il file viene aperto o eseguito, in caso contrario il virus non viene attivato e non intacca il sistema;

• **worm**: è un programma software dannoso che, una volta attivato, si diffonde automaticamente su altri computer, senza bisogno che un utente invii un file o un' e-mail infetta. In alcuni casi può autoeseguirsi, ma, più spesso, ha bisogno di essere attivato dall'utente per iniziare il ciclo di infezione;
• **trojanhorse**: come si può intuire dal nome, il trojanhorse basa tutta la sua potenza sull'inganno. Esso appare infatti inizialmente come un'applicazione utile e desiderabile, in modo tale da invogliare l'utente ad eseguirla. Una volta installata, invece, questo software compie una serie di operazioni dannose sul sistema, che vanno dal rubare informazioni al danneggiare il computer o il dispositivo mobile. Si differenzia dai virus e worm perché non si diffonde da solo ma, nella maggior parte dei casi, viene installato inconsapevolmente dall'utente, il quale, spesso, lo scarica insieme al programma di cui necessita;
• **backdoor**: le backdoor o porte di servizio, sono dei virus informatici che permettono di entrare nel sistema aggirando parzialmente o totalmente le misure di sicurezza attivate. Tali porte possono essere create per scopi positivi e utili, come quelle utilizzate per l'amministrazione o la manutenzione di una rete, oppure, nel caso in cui si tratti di malware, vengono create dagli hacker con scopi fraudolenti. Le backdoor possono essere anche di tipo autoinstallante;
• **rootkit**: è un programma software prodotto per entrare nel sistema eludendo i controlli di sicurezza. La sua funzione è quella di nascondere, sia all'utente che a software di sicurezza, la presenza di particolari file o impostazioni del sistema. Viene quindi utilizzato per mascherare diversi tipi di malware, come backdoor, spyware e trojan, permettendo ai malintenzionati di avere il controllo sul sistema senza che la loro attività sia segnalata e bloccata.