Malware

Questo articolo vi guida nel mondo dei programmi dannosi. Imparerete qual è il funzionamento di base del malware e scoprirete i modi più comuni con cui esso si diffonde e arreca danno. Vedrete allora come le nostre «5 operazioni per la vostra sicurezza digitale» possono rappresentare una protezione efficace.

Punti principali:

- I malware sono programmi informatici con funzioni indesiderate e spesso dannose.
- Il malware si presenta in tantissime forme diverse che richiedono misure preventive ad hoc.
- Negli ultimi anni, i rischi posti dal malware non hanno mai smesso di aumentare.
- I rischi del malware si possono ridurre efficacemente con le nostre «5 operazioni per la vostra sicurezza digitale (https://www.ebas.ch/it/5-operazioni-per-la-vostra-sicurezza-digitale/) ».

Malware – un programma per computer indesiderato

La parola «malware» è un termine generico con cui si indicano i programmi informatici che nascono per lo più con il preciso intento di danneggiare gli utenti.

Come si è visto con il software tradizionale, anche la creazione e la distribuzione del malware si è evoluta negli anni. Lo sviluppo di questo genere di programmi si fa sempre più professionale, il che contribuisce a una loro maggiore volatilità. Oltre a questo, la diffusione è sempre più mirata. I privati e le PMI sono presi di mira sistematicamente.

Infezione

Come tutti i programmi informatici, anche il malware non è altro che un insieme di istruzioni eseguite dal computer.

Per produrre il suo effetto dannoso, il malware deve quindi essere eseguito dal sistema – su istruzione dell'utente o di un altro programma già in esecuzione.

La prima forma di esecuzione si ottiene, come è noto, inducendo gli utenti a credere che possano ottenere un beneficio o prevenire un danno. Il malware eseguito in questo modo viene denominato in generale «cavallo di Troia» o, usando il termine inglese, «trojan». Si maschera da programma utile e in generale viene avviato dalla vittima stessa. Una volta eseguito, sprigiona il suo potere dannoso.

Non si tratta necessariamente di classici file di programma eseguibili: anche i documenti Office e i file PDF possono contenere le cosiddette macro, le quali vengono eseguite dai rispettivi programmi.

Simili tentativi di inganno si possono spesso riconoscere ed evitare seguendo i consigli della nostra «fase 5 – fare attenzione ed essere vigili (https://www.ebas.ch/it/5-fare-attenzione-ed-essere-vigili/) ».

Il malware può anche essere avviato da un programma in esecuzione senza l'intervento di una persona, sfruttando una cosiddetta vulnerabilità. Si tratta in questo caso di errori nella logica del programma che possono avere un impatto sulla sicurezza.

Le falle di sicurezza dei browser (https://www.ebas.ch/it/browser/) , p. es., aprono le porte ai cosiddetti download drive-by (https://www.ebas.ch/it/download-drive-by/) . Anche le vulnerabilità del sistema operativo sono sfruttate con grande frequenza, p. es. per introdurre software dannoso tramite supporti di dati esterni come le chiavette USB o la rete. Il malware che si diffonde in autonomia sfruttando questo genere di errori è denominato «worm».

I produttori di software risolvono regolarmente le falle di sicurezza pubblicando opportuni aggiornamenti. Per questo motivo, la misura più importante per prevenire le infezioni da malware è la «fase 3 – prevenire con aggiornamenti software (https://www.ebas.ch/it/3-prevenire-con-aggiornamenti-software/) ».

Una volta eseguito, nella maggior parte dei casi il malware deve assicurarsi, per mezzo di diversi metodi, che il proprio codice dannoso venga avviato ripetutamente. A tale scopo, un «virus» inserisce il proprio codice dannoso all'interno di altri programmi. I cosiddetti «rootkit» giungono a questo risultato annidandosi direttamente nel codice del sistema operativo.

Effetto nocivo

È impossibile evitare del tutto il rischio di infezione da malware. Ecco perché è opportuno prevedere anche come reagire in caso di infezione.

Qui di seguito vengono presentati alcuni scenari comuni, con la spiegazione di come ridurre i danni con le nostre 5 operazioni per la vostra sicurezza digitale (https://www.ebas.ch/it/5-operazioni-per-la-vostra-sicurezza-digitale/) .

Rallentamento del sistema

L'uso improprio delle risorse di sistema e di rete può rallentare notevolmente – se non addirittura rendere impossibile – il lavoro su un dispositivo infetto. Un impatto notevole sulle prestazioni di un sistema è quello prodotto dal malware creato, p. es., per coniare criptovalute (crypto miners), decifrare password o sferrare attacchi ad altri sistemi (p. es. Distributed Denial-of-Service).

Questo tipo di malware consegue il proprio obiettivo infettando il maggior numero possibile di sistemi che vanno a formare una cosiddetta «botnet».

Questo malware è progettato per imperversare in un sistema a lungo termine, e presto o tardi dovrebbe essere rilevato da un programma antivirus. Tuttavia, per funzionare correttamente, l'antivirus va aggiornato a intervalli regolari, ripetendo la scansione dell'intero sistema. Maggiori informazioni nella «fase 2 – monitorare con antivirus e firewall (https://www.ebas.ch/it/2-monitorare-con-antivirus-e-firewall/) ».

Visualizzazione di pubblicità

I programmi noti con il termine «adware» sono poco apprezzati dalle loro vittime perché visualizzano annunci pubblicitari.

La comparsa di una quantità insolita di pubblicità nel sistema è spesso sintomo di infezioni da malware e dovrebbe spronare a eseguire una pulizia del sistema (https://www.ebas.ch/it/reinstallazione-di-windows-10/) .

Se la pubblicità è limitata alle pagine Internet e viene visualizzata solo all'interno del browser, potrebbe essere utile seguire i nostri suggerimenti per una maggiore privacy e protezione dei dati (https://www.ebas.ch/it/privacy-e-protezione-dei-dati-in-internet/) su Internet o l'uso di ad blocker (https://www.ebas.ch/it/ad-blocker-e-strumenti-anti-tracking/) .

Raccolta di informazioni

Il malware con caratteristiche da spyware si contraddistingue per il fatto che raccoglie e inoltra informazioni mirate

sulle sue vittime. Tra i dati carpiti vi possono essere, p. es., l'analisi del comportamento di navigazione, la registrazione di sequenze di tasti (keylogger) o il furto di dati sensibili.

Per contenere i rischi dello spyware si consiglia di segmentare le proprie attività digitali e di mostrare una condotta di navigazione a basso consumo di dati. Seguendo i consigli della «fase 4 – proteggere gli accessi online (https://www.ebas.ch/it/4-proteggere-gli-accessi-online/) » si riduce efficacemente l'entità dei danni qualora un attacco di spionaggio di questo tipo abbia successo. Per esempio, se si utilizza l'autenticazione a due fattori, il furto di una password non compromette immediatamente il vostro account di e-banking.

Cifratura o distruzione di dati
La cifratura dei dati viene utilizzata principalmente come forma di coercizione nei tentativi di ricatto sferrati con il cosiddetto «ransomware».

In questo caso, solitamente dopo aver ripulito il sistema l'unico rimedio utile è ripristinare i dati da un backup creato in precedenza. La «fase 1: salvare i dati (https://www.ebas.ch/it/1-salvare-i-dati/) » è quindi il pilastro portante del corretto ripristino dei dati.

Attacchi combinati
Il malware può manifestarsi secondo modalità che vanno anche oltre gli scenari descritti. Spesso, infatti, molti dei comportamenti presentati si combinano tra loro, oppure vengono sviluppate procedure nuove e diverse.

Nel primo caso vengono impiegati cosiddetti «downloader» che scaricano – automaticamente o a comando – ulteriore malware sul sistema preso di mira.

Un esempio lampante di attacchi combinati è quello dell'estorsione, con il quale il contenuto del sistema bersaglio viene dapprima spiato e copiato e poi crittografato. Ciò permette ai ricattatori di esercitare maggiore pressione sulle loro vittime, p. es. minacciando di pubblicare i dati sottratti o di renderli noti alla concorrenza.

Identificazione e pulizia

Applicando le nostre «5 operazioni per la vostra sicurezza digitale (https://www.ebas.ch/it/5-operazioni-per-la-vostra-sicurezza-digitale/) » riducete efficacemente la probabilità di subire un'infezione da malware e i danni conseguenti.

Tuttavia, il rischio non può essere escluso del tutto. Leggete il nostro articolo «Infezione da malware (https://www.ebas.ch/it/infezione-da-malware/) » per imparare a riconoscere e correggere un'infezione.

Il termine «malware» è un composto delle parole inglesi «malicious» (maligno) e «software». Si tratta di un termine generico per indicare qualsiasi genere di software che esegue funzioni dannose su un dispositivo (come virus, worm, cavalli di Troia e ransomware).