Definizione di malware

News

Inviato da : Gennaro Piccolo
Pubblicato il : 5/5/2024 8:30:00

Si parla spesso di malware, cerchiamo di capire cosa sono e come vengono definiti. Malware: Si definisce malware un qualsiasi software creato con il solo scopo di causare danni piÃ¹ o meno gravi al computer su cui viene eseguito. Il termine deriva dalla contrazione delle parole inglesi malicious esoftware e ha dunque il significato letterale di "programma malvagio"; in italiano Ã¨ detto anche codice maligno. La diffusione di tali software risulta in continuo aumento. Si calcola che nel solo anno 2008 su Internet siano girati circa 15 milioni di malware, di cui quelli circolati tra i mesi di gennaio e agosto sono pari alla somma dei 17 anni precedenti, e tali numeri sono destinati verosimilmente ad aumentare.

Si distinguono molte categorie di malware, ecco le piÃ¹ conosciute e le piÃ¹ diffuse.

Virus:

Un virus Ã¨ un software che Ã¨ in grado, una volta eseguito, di infettare dei file in modo da riprodursi facendo copie di sÃ© stesso, generalmente senza farsi rilevare dall'utente. I virus possono essere o non essere direttamente dannosi per il sistema operativo che li ospita, ma anche nel caso migliore comportano un certo spreco di risorse in termini di RAM, CPU e spazio sul disco fisso. Come regola generale si assume che un virus possa danneggiare direttamente solo il software della macchina che lo ospita, anche se esso puÃ² indirettamente provocare danni anche all'hardware, ad esempio causando il surriscaldamento della CPU mediante overclocking, oppure fermando la ventola di raffreddamento.

Worm:

Un worm (letteralmente "verme") Ã¨ una particolare categoria di malware in grado di autoreplicarsi. Ã¨ simile ad un virus, ma a differenza di questo non necessita di legarsi ad altri eseguibili per diffondersi. Il termine deriva da un romanzo di fantascienza degli anni 1970 di John Brunner: i ricercatori che stavano scrivendo uno dei primi studi sul calcolo distribuito notarono le somiglianze tra il proprio programma e quello descritto nel libro e ne adottarono il nome. Uno dei primi worm diffusi sulla rete fu Internet Worm, creato da Robert Morris, figlio di un alto dirigente della NSA il 2 novembre 1988, quando internet era ancora agli albori. Tale virus riuscÃ~ a colpire tra le 4000 e le 6000 macchine, si stima il 4-6% dei computer collegati a quel tempo in rete.

Trojan horse:

Un trojan o trojan horse (dall'inglese per Cavallo di Troia), Ã¨ un tipo di malware. Deve il suo nome al fatto che le sue funzionalitÃ sono nascoste all'interno di un programma apparentemente utile; Ã¨ dunque l'utente stesso che installando ed eseguendo un certo programma, inconsapevolmente, installa ed esegue anche il codiceÃ trojannascosto.

In genere col termine Trojan ci si riferisce ai trojan ad accesso remoto (detti anche RAT dall'ingleseÃ Remote Administration Tool), composti generalmente da 2 file: il file server, che viene installato nella macchina vittima, ed un file client, usato dall'attaccante per inviare istruzioni che il server esegue.

Backdoor:

Le backdoor in informatica sono paragonabili aÅ porte di servizioÃ (cioÃ¨ le porte del retro) che consentono di superare in parte o in tutto le procedure di sicurezza attivate in un sistema informatico.

Possono anche essere installate autonomamente da alcuni malware (come virus, worm o trojan), in modo da consentire ad un utente esterno di prendere il controllo remoto della macchina senza l'autorizzazione del proprietario.

Keylogger:

Un keylogger Ã¨, nel campo dell'informatica, uno strumento in grado di intercettare tutto ciÃ² che un utente digita sulla tastiera del proprio computer.

I keylogger software sono semplici programmi che rimangono in esecuzione captando ogni tasto che viene digitato e poi, in alcuni casi, trasmettono tali informazioni ad un computer remoto.

Spyware:

Uno spyware Ã¨ un tipo di software che raccoglie informazioni riguardanti l'attivitÃ online di un utente (siti visitati, acquisti eseguiti in rete etc) senza il suo consenso, trasmettendole tramite internet ad un'organizzazione che le utilizzerÃ per trarne profitto, solitamente attraverso l'invio di pubblicitÃ mirata. I programmi per la raccolta di dati che vengono installati con il consenso dell'utente (anche se spesso negando il consenso non viene installato il programma) non sono propriamente spyware, sempre che sia ben chiaro all'utente quali dati siano oggetto della raccolta ed a quali condizioni questa avvenga (purtroppo ciÃ² avviene molto raramente).

In un senso piÃ¹ ampio, il termine spyware Ã¨ spesso usato per definire un'ampia gamma di malware (software maligni) dalle funzioni piÃ¹ diverse, quali l'invio di pubblicitÃ non richiesta (spam), la modifica della pagina iniziale o della lista dei Preferiti del browser, oppure attivitÃ illegali quali la redirezione su falsi siti di e-commerce (phishing) o l'installazione di dialer truffaldini per numeri a tariffazione speciale.

Rootkit:

Un rootkit Ã¨ un programma software creato per avere il controllo completo sul sistema senza bisogno di autorizzazione da parte di utente o amministratore. Recentemente alcuni virus informatici si sono avvantaggiati della possibilitÃ di agire come rootkit (processo, file, chiave di registro, porta di rete) all'interno del sistema operativo.

Se Ã¨ vero che questa tecnologia Ã¨ fondamentale per il buon funzionamento del sistema operativo, negli anni sono stati creati trojan e altri programmi maligni in grado di ottenere il controllo di un computer da locale o da remoto in maniera nascosta, ossia non rilevabile dai piÃ¹ comuni strumenti di amministrazione e controllo. I rootkit vengono tipicamente usati per nascondere delle backdoor. Negli ultimi anni, tuttavia, s'Ã¨ molto diffusa la pratica, tra i creatori di malware, di utilizzare rootkit per rendere piÃ¹ difficile la rilevazione di particolari trojan e spyware, indipendentemente dalla presenza in essi di funzioni di backdoor, proprio grazie alla possibilitÃ di occultarne i processi principali. Grazie all'alto livello di prioritÃ con la quale sono in esecuzione, i rootkit sono molto difficili da rilevare e da rimuovere con i normali software Antivirus.

Questi sono i malware piÃ¹ conosciuti e diffusi.

Ã Ã Ã NellaÃ sicurezza informaticaÃ il termineÃ malwareÃ indica genericamente un qualsiasiÃ softwareÃ creato con il solo scopo di causare danni piÃ¹ o meno gravi ad unÃ computer, ai dati degli utenti del computer, o a unÃ sistema informaticoÃ su cui viene eseguito. Il termine deriva dalla contrazione delle parole inglesiÃ maliciousÃ eÃ softwareÃ e ha dunque il significato letterale di "programma malvagio"; in italiano Ã¨ detto ancheÃ codice maligno.

La diffusione di tali software risulta in continuo aumento: si calcola che nel solo annoÃ 2008Ã suÃ InternetÃ siano girati circa 15 milioni di malware, di cui quelli circolati tra i mesi di gennaio e agosto sono pari alla somma dei 17 anni precedenti, e tali numeri sono destinati verosimilmente ad aumentare con l'espansione dellaÃ ReteÃ e il progressivo diffondersi della culturaÃ informatica.Ã

Si distinguono molte categorie di malware, anche se spesso questi programmi sono composti di piÃ¹ parti interdipendenti e rientrano pertanto in piÃ¹ di una classe. Vista inoltre la rapida evoluzione in questo campo, la classificazione presentata di seguito non Ã¨ da ritenersi esaustiva.

- Virus: sono parti di codice che si diffondono copiandosi all'interno di altriÃ programmi, o in una particolare sezione delÃ disco fisso, in modo da essere eseguiti ogni volta che iÃ fileÃ infetto viene aperto. Si trasmettono da unÃ computerÃ a un altro tramite lo spostamento di file infetti ad opera degli utenti.

- Worm: questi malware non hanno bisogno di infettare altri file per diffondersi, perchÃ© modificano iÃ sistema operativoÃ della macchina ospite in modo da essere eseguiti automaticamente e tentare di replicarsi sfruttando per lo piÃ¹Ã Internet. Per indurre gli utenti ad eseguirli utilizzano tecniche diÃ ingegneria sociale, oppure sfruttano dei difetti (Bug) di alcuniÃ programmiÃ per diffondersi automaticamente. Il loro scopo Ã¨ rallentare il sistema con operazioni inutili o dannose.

- Trojan horse: software che oltre ad avere delle funzionalitÃ "lecite", utili per indurre l'utente ad utilizzarli, contengono istruzioni dannose che vengono eseguite all'insaputa dell'utilizzatore. Non possiedono funzioni di auto-replicazione, quindi per diffondersi devono essere consapevolmente inviati alla vittima. Il nome deriva dal famosoÃ cavallo di Troia.

- Backdoor: letteralmente "porta sul retro". Sono deiÃ programmiÃ che consentono un accesso non autorizzato al sistema su cui sono in esecuzione. Tipicamente si diffondono in abbinamento ad un trojan o ad un worm, oppure costituiscono una forma di accesso lecita di emergenza ad un sistema, inserita per permettere ad esempio il recupero di una password dimenticata.

- Spyware:Ã softwareÃ che vengono usati per raccogliere informazioni dal sistema su cui sono installati e per trasmetterle ad un destinatario interessato. Le informazioni carpite possono andare dalle abitudini di navigazione fino alle password e alleÃ chiavi crittograficheÃ di un utente.

- Dialer: questiÃ programmiÃ si occupano di gestire la connessione adÃ InternetÃ tramite la normale linea telefonica. Sono malware quando vengono utilizzati in modo illecito, modificando il numero telefonico chiamato dalla connessione predefinita con uno a tariffazione speciale, allo scopo di trarne illecito profitto all'insaputa dell'utente.

- Hijacker: questi programmi si appropriano di applicazioni di navigazione in rete (soprattuttoÃ browser) e causano l'apertura automatica diÃ pagine webÃ indesiderate.

- Rootkit: i rootkit solitamente sono composti da unÃ driverÃ e, a volte, da copie modificate di programmi normalmente presenti nel sistema. I rootkit non sono dannosi in sÃ©, ma hanno la funzione di nascondere, sia all'utente che a programmi tipo antivirus, la presenza di particolari file o impostazioni del sistema. Vengono quindi utilizzati per mascherareÃ spywareÃ eÃ trojan.

- Scareware: sono cosÃ¬ chiamati quei programmi che ingannano l'utente facendogli credere di avere il proprio PC infetto, allo scopo di fargli installare dei particolari malware, chiamati in gergorogue antivirus, caratterizzati dal fatto di spacciarsi per degli antivirus veri e propri, talvolta spacciati anche a pagamento.

- Rabbit: i rabbit sono programmi che esauriscono le risorse del computer creando copie di sÃ© stessi (inÃ memoriaÃ o suÃ disco) a grande velocitÃ .

- Adware: programmi software che presentano all'utente messaggi pubblicitari durante l'uso, a fronte di un prezzo ridotto o nullo. Possono causare danni quali rallentamenti del pc e rischi per laprivacyÃ in quanto comunicano le abitudini di navigazione ad unÃ serverÃ remoto.

- Batch: i Batch sono i cosiddetti "virus amatoriali". Non sono sempre dei file pericolosi in quanto esistono molti file batch tutt'altro che dannosi, il problema arriva quando un utente decide di crearne uno che esegua il comando di formattare il pc (o altre cose dannose) dell'utente a cui viene mandato il file. Non si apre automaticamente, deve essere l'utente ad aprirlo, perciÃ² dato che l'antivirus non rileva i file Batch come pericolosi Ã¨ sempre utile assicurarsi che la fonte che vi ha mandato il file sia attendibile oppure aprirlo con blocco note per verificare o meno la sua pericolositÃ . Bisogna perÃ² anche dire che esistono modi per camuffare i Batch e farli sembrare dei fileÃ exe, aumentandone anche il peso per sedare ogni sospetto. L'utilizzo di questo particolare "malware" Ã¨ spesso ricorrente nelÃ Cyberbullismo.

- Keylogger: I Keylogger sono dei programmi in grado di registrare tutto ciÃ² che un utente digita su una tastiera o che copia e incolla rendendo cosÃ¬ possibile il furto di password o di dati che potrebbero interessare qualcun altro. La differenza con gliÃ AdwareÃ sta nel fatto che il computer non si accorge della presenza del keylogger e il programma non causa rallentamento del pc, passando cosÃ¬ totalmente inosservato. Generalmente i keylogger vengono installati sul computer daiÃ trojanÃ o daiÃ worm, in altri casi invece il keylogger viene installato sul computer da un'altra persona che puÃ² accedere al pc o attraverso l'accesso remotoÃ (che permette a una persona di controllare un altro pc dal suo stesso pc attraverso un programma) oppure in prima persona, rubando cosÃ¬ dati e password dell'utente.

- Rogue antispyware: malware che si finge un programma per la sicurezza del PC, spingendo gli utenti ad acquistare una licenza del programma.

- Bomba logica: Ã¨ un tipo di malware che "esplode" ovvero fa sentire i suoi effetti maligni al verificarsi di determinate condizioni o stati del PC fissati dal cracker stesso.

Nell'uso comune il termineÃ virusÃ viene utilizzato come sinonimo di malware e l'equivoco viene alimentato dal fatto che gliÃ antivirusÃ permettono di rilevare e rimuovere anche altre categorie di software maligno oltre ai virus propriamente detti.

Si noti che un malware Ã¨ caratterizzato dall'intento doloso del suo creatore, dunque non rientrano nella definizione data iÃ programmiÃ contenentiÃ bug, che costituiscono la normalitÃ anche quando si sia osservata la massima diligenza nello sviluppo di unÃ software.

Grayware

GraywareÃ Ã¨ la definizione generica che si riferisce alleÃ applicazioniÃ che presentano un comportamento molesto, indesiderabile o nascosto.

Le applicazioni grayware non rientrano in nessuna delle categorie delle principali minacce (virusÃ oÃ cavalli di Troia) poichÃ© sono soggette alla funzionalitÃ del sistema e costituiscono oggetto di dibattito tra gli utenti. Alcuni elementi nella categoria del grayware sono stati collegati ad attivitÃ dannose, mentre altri vengono utilizzati per fornire agli utenti informazioni mirate relative ad annunci sui prodotti. Per le aziende che si occupano di informazioni sensibili, le funzionalitÃ di raccolta dati di qualsiasi tipo di applicazione dovrebbero suscitare preoccupazione.

AttivitÃ criminose legate ai malware

La legislazione relativa ai malware Ã¨ estremamente variabile a seconda delle nazioni ed Ã¨ in continua evoluzione. In generale se iÃ virus, iÃ wormÃ e iÃ trojanÃ sono illegali in quasi ogni parte del mondo non si puÃ² dire lo stesso per le altre categorie. IÃ dialerÃ in particolare sono di per sÃ© legali, tanto che ogni sistema operativo moderno ne contiene almeno uno. L'ambiguitÃ Ã¨ peggiorata dal fatto che molti software si situano sul limite che separa un vero e proprio malware da un programma forse fastidioso ma non dannoso.

Attualmente i malware (in particolareÃ trojan,Ã wormÃ spywareÃ e malware) vengono utilizzati per inviare grandi quantitÃ di file non richiesti dall'utente; quest'ultimi vengono solitamente venduti aglispammer. Esiste un vero e proprio mercato nero legato ai malware: oltre alla compravendita di dati personali, Ã¨ possibile acquistareÃ l'utilizzoÃ di computer infetti, cioÃ¨ la possibilitÃ di impiegare, per i propri fini e a insaputa dei legittimi proprietari, una certa quantitÃ (nell'ordine delle migliaia) di computer controllati da remoto tramite unaÃ backdoor.

Ã