MODALITÀ DI ATTACCO

La prima cosa importante da capire è che un trojan è un programma eseguibile che per installarsi necessita dell'input da parte di un utente. Purtroppo ci sono molti modi in cui un programma può fingersi benevolo quindi l'unico modo per evitarlo è imparare a diffidare dei programmi dalla provenienza dubbia o sospetta e a non fidarsi ciecamente della presenza nel proprio sistema di un software antivirus, che può non essere "infallibile" nella rilevazione dei trojan.

EVITARE DI ESSERE INFETTATI

La regola principale per evitare di essere infettati è di essere sicuri della sorgente e del contenuto di ogni file che si scarica. Attenzione però che alcuni trojan possono essere inviati come allegati di posta elettronica da computer di conoscenti che sono stati infettati da un malware. In questo caso si dovrebbe dubitare della ricezione di file non richiesti da persone conosciute.

È quindi consigliato seguire queste semplici regole per evitare di essere infettati quando si vuole scaricare un file da internet:

- Conoscere la sorgente da dove si scarica il file e controllare se sia affidabile.
- Controllare se il file che si vuole scaricare corrisponda effettivamente a quello che si sta scaricando.
- Controllare che non vengano scaricati altri file insieme al file che si vuole effettivamente scaricare.
- Controllare che il file scaricato abbia senso sia come formato che come nome, ad esempio se volevo scaricare un'immagine controllare che non sia un file excel o eseguibile.
- In ogni caso una volta scaricato il file controllare l'eventuale presenza di virus o trojan tramite un antivirus.

CRONOLOGIA

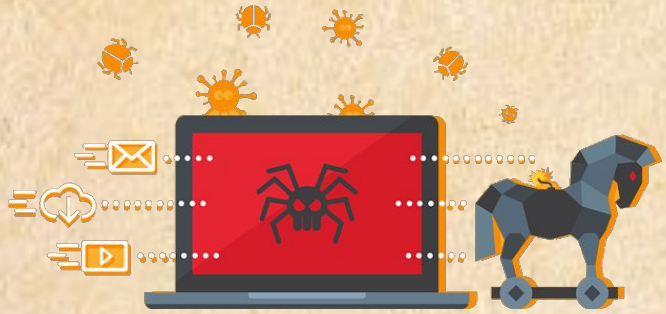
Ecco una lista dei più dannosi trojan horse sferrati nel corso degli anni e che sono stati scoperti dai ricercatori nel campo della sicurezza informatica.

NOME	ANNO	SISTEMA BERSAGLIATO
Clickbot.A	2006	Windows
Zeus	2007	Windows
Koobface	2008	multipiattaforma
Vundo	2009	Windows
Meredrop	2010	Windows
Coreflood	2010	multipiattaforma
Flashback trojan	2011	Mac OS X
ZeroAccess	2011	Windows
Tinba	2012	multipiattaforma
Shedun	2015	Android

RIFERIMENTI

➢ https://www.c3t.it/projects/awareness/articoli&brochure/trojan/

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



I TROJAN

Scopri cosa sono i trojan, come si diffondono e come puoi prevenire un'infezione da questi moderni malware.

COS'È UN TROJAN

Un trojan o **trojan horse** (in italiano "cavallo di Troia") è un tipo di malware che **nasconde il suo funzionamento all'interno di un altro programma apparentemente utile e innocuo**: l'utente, eseguendo o installando quest'ultimo programma, in effetti attiva anche il codice del trojan nascosto.

L'attribuzione del termine "cavallo di Troia" ad un programma (o file eseguibile) è dovuta al fatto che esso nasconde il suo vero fine. Proprio come i Troiani fecero entrare in città gli Achei celati nel mitico cavallo di legno progettato da Ulisse, allo stesso modo la vittima è indotta a far entrare il programma nel computer.

METODO DI DIFFUSIONE

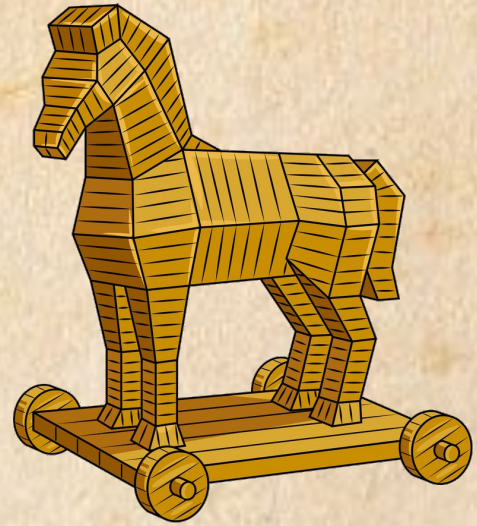
A differenza di altri malware (come worm e virus), i trojan **non hanno diffusione autonoma**, ma devono essere scaricati dall'utente che ha un ruolo attivo nella propagazione del programma malevolo.

Si presentano come dei file eseguibili, anche se spesso **mascherano la loro origine** con dei trucchetti. Come quello di rinominare il file contenente il trojan con diverse estensioni, per esempio "*Documento.txt.exe*". In questo modo, l'allegato non è visibile come ".exe" perché l'attaccante sfrutta il fatto che i sistemi operativi firmati da Windows non mostrano di default tutte le estensioni.

TIPI DI TROJAN PIÙ COMUNI

I trojan vengono classificati in base al tipo di azioni che riescono a svolgere sul computer:

- **Trojan banker**: progettati per rubare i dati degli account sui sistemi di banking online.
- **Trojan DDoS**: Questi programmi sferrano attacchi DoS (Denial of Service) contro un indirizzo Web ben preciso (vedi brochure 'Gli attacchi denial of service').
- **Trojan downloader**: può scaricare e installare nuove versioni di programmi nocivi sul computer, compreso trojan e adware.
- **Trojan dropper**: utilizzato dagli hacker per installare altri trojan e/o altri malware, oppure per impedire il rilevamento dei programmi nocivi.



- **Trojan FakeAV**: simulano l'attività del software antivirus. Progettati per estorcere denaro agli utenti, in cambio del rilevamento e dell'eliminazione delle minacce, anche se le minacce che notificano in realtà non esistono.
- **Trojan IM**: rubano le credenziali di accesso e le password dei programmi di messaggistica immediata, come ICQ, MSN Messenger, AOL Instant Messenger, Yahoo Pager, Skype e molti altri.
- **Trojan spy**: possono spiare tutto ciò che l'utente sta ricercando, ad esempio tenendo traccia dei dati immessi con la tastiera, catturando schermate del monitor o procurandosi un elenco delle applicazioni in esecuzione.

COSA FANNO I TROJAN

Grazie alla loro versatilità e alla **capacità di passare inosservati**, la popolarità dei trojan è esplosa, rendendoli la forma di malware preferita da molti criminali online.

Le azioni comunemente svolte dai trojan sono:

Creare backdoor: solitamente i trojan apportano modifiche al sistema di sicurezza, in modo da consentire l'ingresso ad altro malware o persino a un hacker. In genere è il primo passo per la creazione di una botnet, una rete controllata da criminali e composta da dispositivi infettati da malware specializzato.

Spiare: alcuni trojan sono sostanzialmente una forma di spyware, poiché sono progettati per restare in attesa fino a quando l'utente non accede ai propri account online o immette dati e numeri delle carte di credito. Da quel momento iniziano a inviare password e altri dati al loro "padrone".

Trasformare il computer in uno zombi: a volte un hacker non è interessato ai dati e alle informazioni dell'utente, ma vuole solo utilizzarne il computer come strumento al proprio servizio all'interno di una rete di cui ha il controllo (botnet).

Inviare costosi messaggi SMS: anche gli smartphone vengono presi di mira dai trojan e un modo comune di fare soldi per i criminali informatici è indurre il telefono del malcapitato a inviare costosi SMS a numeri a pagamento.

COME SI PRESENTA UN TROJAN

Il punto è proprio questo, i trojan possono avere l'aspetto di qualsiasi cosa: il videogioco che hai scaricato da uno strano sito Web, il file MP3 "gratuito" del tuo gruppo preferito, persino un messaggio pubblicitario che cerca di convincerti a installare qualche software nel computer.
È importante prestare attenzione ai siti Web non sicuri ed essere sempre prudenti quando si esegue un download.