Download drive-by

Basta aprire una pagina infetta per trasmettere l'infezione sul proprio dispositivo. Molte volte le pagine Internet infette contengono offerte serie e sono state manomesse per diffondere il malware. Ma ci si può proteggere.

Proteggetevi dai download drive-by così:

- Utilizzate sempre le versioni aggiornate del browser e dei rispettivi plug-in (Adobe Flash Player, Java ecc.).
- Mantenete aggiornati il sistema operativo e tutti i programmi installati (Office, Adobe Acrobat Reader ecc.).
- Aggiornate sempre l'antivirus ed effettuate regolarmente un controllo del disco rigido.

I rischi dei download drive-by

Alcuni siti Internet vengono manipolati in modo mirato dagli hacker per sfruttarne i punti deboli. Solitamente, i gestori del sito Internet non si accorgono di nulla per parecchio tempo.

I punti riportati di seguito mostrano che cosa rende tanto pericoloso e imprevedibile un download drive-by:

1. In un dispositivo si introduce del codice nocivo semplicemente visitando un sito Internet infetto, quindi non c'è bisogno che l'utente avvii alcun download né installi esplicitamente qualcosa.
2. Il download del malware si avvia automaticamente in background con la normale apertura del sito Internet. In questo modo vengono bypassati i firewall, che non offrono più nessuna protezione.
3. Anche siti Internet seri, noti e molto frequentati potrebbero essere infetti.

Contromisure

Per proteggervi dovreste utilizzare sempre la versione più recente del browser e di tutti i suoi plug-in (programmi di supporto che ampliano le funzionalità del browser).

Un'ulteriore e importante misura di protezione consiste nell'avere sempre un antivirus aggiornato. Poiché molti virus vengono scaricati in formato compresso e si decomprimono solo sul dispositivo dell'utente, non sempre gli antivirus sono in grado di riconoscerli. Per questo motivo è essenziale eseguire periodicamente (p. es. ogni settimana) una scansione completa del disco rigido per verificare che non ci siano virus.

Verifica dei siti Internet

Norton (Symantec) offre sul suo sito Internet un servizio che permette di conoscere le condizioni di sicurezza (e le eventuali minacce) di alcuni siti noti.

Aprite il sito Internet Norton Safe Web (https://safeweb.norton.com/?ulang=deu) e digitate l'indirizzo del sito da verificare nell'apposito riquadro. Potrete vedere come Norton valuta il sito Internet.

Con il termine «download drive-by» (o «infezione drive-by») si intende l'infezione di un dispositivo per mezzo di mal-

ware (p. es. virus, cavalli di Troia) per il tramite di una normale visita a un sito Internet. Solitamente vengono sfruttati i punti deboli del browser o dei plug-in installati.

Maggiori informazioni

Aspetti tecnologici

Non di rado i siti Internet contengono funzioni dinamiche che vengono eseguite per mezzo di tecnologie come JavaScript, Java, Adobe Flash ecc. Queste tecniche consentono di instaurare una comunicazione continua tra browser e server Web nel corso di una sessione (il tempo trascorso dal visitatore sul sito Internet), senza che l'utente debba eseguire alcuna azione specifica. In questo modo, p. es., è possibile cambiare a rotazione i banner pubblicitari, caricare elenchi o trasmettere dati al server Web.

Solitamente queste azioni vengono eseguite all'interno di una cosiddetta «sandbox» del browser. In genere una sandbox è un elemento integrante del browser o di un plug-in volto a ridurre il potenziale dannoso del contenuto presente in Internet. Agli script di origine ignota viene permesso di agire all'interno di un'area limitata che ne rende più sicura l'esecuzione (in altre parole, viene dato loro un accesso limitato al disco rigido locale, per esempio).

Tuttavia, se il browser o uno dei plug-in presenta una falla di sicurezza in questo componente, gli script possono accedere direttamente al dispositivo dell'utente. Di conseguenza, senza che venga eseguita una particolare azione il malware è in grado di passare dal server Web al browser raggiungendo così il dispositivo dell'utente attraverso la falla di sicurezza.

Proteggersi disattivando gli script?

Per il momento non esistono misure di protezione davvero efficaci contro i download drive-by. Un livello di sicurezza maggiore si può avere disattivando gli script. Questa, però, rappresenta una soluzione non proprio pratica, dato che circa il 95 per cento dei siti Internet si basa sulle tecnologie citate e quindi moltissimi siti non sarebbero più visualizzati correttamente.