Estensioni browser infette da malware, a rischio la sicurezza di milioni di utenti

Il team di ricercatori del *Threat Intelligence* di **Avast** ha identificato di recente, nascosto in almeno 28 estensioni realizzate da terze parti per i browser **Google Chrome e Microsoft Edge**, un malware con grande capacità di elusione in grado di reindirizzare il traffico di rete verso annunci o siti di phishing e rubare informazioni riservate alle ignare vittime.

Le estensioni e i plug-in dei browser

Per i browser di ultima generazione esiste la possibilità di aggiungere dei componenti che ne consentono la relativa personalizzazione. Si tratta di programmi integrativi che possono essere distinti in plug-in ed add-on. A differenza dei plug-in che sono componenti software che permettono di usufruire di contenuti speciali all'interno delle pagine web visualizzate come filmati, animazioni e presentazioni che il browser non è in grado di gestire, le estensioni sono componenti software che permettono di ampliare le funzionalità, aggiungendo o modificando le caratteristiche dei browser in uso. Si possono trovare estensioni per una miriade di scopi come, ad esempio, aumentare l'accessibilità del browser, gestire download o velocizzare la navigazione e tradurre pagine web.

Gli add-on incriminati

Sebbene sia i plug-in che gli add-on, spesso gratuiti e quasi sempre sviluppati da terze parti, possono essere potenzialmente alterati, senza un adeguato controllo e supervisione, per veicolare software malevolo o propinare servizi illeciti, sono gli add-on per i browser Chrome e Edge le estensioni contaminate oggetto di questa analisi.

Sulla base dei dati raccolti dagli analisti e del numero di download registrati sugli store di Microsoft e di Google Chrome WEB sarebbero circa tre milioni gli utenti nel mondo ad essere potenzialmente interessati al problema, considerando che queste estensioni malevole sarebbero, per lo più, servizi per note piattaforme social network:

Direct Message for Instagram™, DM for Instagram, Invisible mode for Instagram Direct Message, Downloader for Instagram, Instagram Download Video & Image, App Phone for Instagram, Stories for Instagram, Universal Video Downloader, Video Downloader for FaceBook™, Vimeo™ Video Downloader, Volume Controller, Zoomer for Instagram and FaceBook, VK UnBlock.Works fast, Odnoklassniki UnBlock. Works quickly, Upload photo to Instagram™, Spotify Music Downloader, Upload photo to Instagram™, Pretty Kitty. The Cat Pet, Video Downloader for YouTube, SoundCloud Music Downloader, The New York Times News, Instagram App with Direct Message DM.

Malware e browser: l’attività delle estensioni malevoli

I ricercatori che hanno iniziato a monitorare questa minaccia nel novembre 2020 ritengono che in realtà la campagna possa essere attiva già da diversi anni, grazie all’alta capacità di elusione posseduta dal malware. Dall’analisi dei campioni si è potuto infatti riscontrare che il malware ben nascosto nelle

estensioni, resta dormiente per qualche giorno dopo l'installazione e sarebbe anche in grado di rilevare comportamenti di personale esperto nelle attività dell'utente colpito, mantenendo in tal caso la propria inattività.

Il codice dannoso rilevato nelle estensioni basate su javascript consente anche di scaricare ulteriori malware, registrare ed inviare informazioni sui click eseguiti ad un server di comando remoto, effettuare reindirizzamenti URL, geolocalizzare e esfiltrare informazioni sui dispositivi, sistemi operativi e browser usati, consentendo agli attori della minaccia di capitalizzare ogni attività illecita eseguita.

Come difendersi dai malware

Gli analisti circa l'origine di queste estensioni hanno avanzato diverse ipotesi. Potrebbero essere state create con il malware integrato oppure potrebbero essere state infettate successivamente tramite un aggiornamento nocivo o una iniezione malevola da parte di terzi.

Avast, in ogni caso, ha contattato in modo responsabile i team degli store interessati segnalando l'elenco delle estensioni infette. Anche se Microsoft e Google dopo aver confermato il problema hanno prontamente provveduto a rimuovere gli add-on incriminati, nell'attesa che vengano eventualmente sostituiti resta comunque ancora valida la raccomandazione di disinstallare le estensioni in oggetto, se non ancora fatto, e eseguire quanto prima una bonifica antivirus.

https://www.key4biz.it/estensioni-browser-infette-da-malware-a-rischio-la-sicurezza-di-milioni-di-utenti/336400/