Il malware arriva nelle librerie di sviluppo Ruby

Apr 21, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

L'attacco ha sfruttato i pacchetti di sviluppo del linguaggio di programmazione open source per diffondersi. Obiettivo: rubare Bitcoin.

Un complicato attacco **supply chain** che ha permesso di diffondere con straordinaria efficacia un malware che ha come obiettivo il furto di Bitcoin. È questa, in sintesi, l'operazione individuata da **ReversingLabs**, illustrata in un report pubblicato lo scorso 16 aprile.

A finire nel mirino dei pirati, spiega l'autore del rapporto **Tomislav Maljic**, è **Ruby**, un linguaggio di programmazione open source piuttosto popolare.

Nel dettaglio, i cyber-criminali hanno sfruttato come vettore di attacco **RubyGems**, un pacchetto software dedicato agli sviluppatori che usano Ruby e che mette a disposizione degli utenti un repository con le "gemme", cioè componenti software (sono circa 158.000) che possono essere utilizzati liberamente.

La tecnica utilizzata dai pirati è stata piuttosto banale: si sono affidati cioè alla tattica del **typo-squatting**, la pubblicazione di file con nomi simili a librerie molto popolari che, in questo modo, vengono scaricate dagli utenti.

L'operazione è stata porta avanti attraverso due account controllati dai pirati che hanno portato al download di migliaia di componenti infetti all'interno del repository.

L’attacco portato dai pirati, però, potrebbe non avere una grande efficacia. Lo schema di attacco, per funzionare, richiede infatti che quella specifica libreria infetta sia scaricata da uno sviluppatore che lavora in ambiente Windows.

Non solo: il codice malevolo inserito nelle librerie, che viene avviato attraverso una complessa catena di operazione che consentono di eseguire il malware senza alcuna interazione da parte dell’utente, prevede semplicemente **l’accesso ai dati contenuti nella clipboard** e la loro sostituzione con un indirizzo di un wallet Bitcoin controllato dai pirati.

In altre parole: il payload finale prevede, per essere efficace, che la vittima stia eseguendo una transazione in Bitcoin che può essere alterata dall’attacco. Quello che gli anglosassoni definirebbero un “long shot” e che, francamente, ha ben poche possibilità di andare a segno.

La vicenda, però, riaccende i riflettori sui rischi legati agli attacchi supply chain, soprattutto quando coinvolgono le filiere di sviluppo software. Per capirne la caratura, è sufficiente considerare che RubyGem, secondo quanto viene riportato sul sito, può vantare **49 miliardi di download**.

Insomma: il tema degli attacchi supply chain è più attuale che mai e rappresenta un fattore di rischio enorme a livello globale.

Condividi l’articolo

Nuova campagna di truffe per i buoni spesa gratuiti

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/04/21/il-malware-arriva-nelle-librerie-di-sviluppo-ruby/?utm_source=rss&utm_medium=rss&utm_campaign=il-malware-arriva-nelle-librerie-di-sviluppo-ruby