Una proposta di lavoro via LinkedIn? No: è un malware

Feb 25, 2019 Marco Schiaffino Attacchi, In evidenza, Malware, Minacce, News, RSS, Trojan 0

La tecnica di attacco sfrutta messaggi privati sul social network e l'invio di documenti Word che contengono codice malevolo.

Una volta le minacce arrivavano quasi esclusivamente via email. Poi, coi social network, i vettori di attacco si sono moltiplicati e hanno acquisito maggiore efficacia. A fare la differenza, però, sono prima di tutto le tecniche di ingegneria sociale adottate dai cyber-criminali.

Nel caso di **LinkedIn**, i pirati informatici hanno fatto bingo. Nella loro ottica, infatti, il social network dedicato al business e alle offerte di lavoro rappresenta una sorta di parco dei divertimenti. **Quale iscritto a LinkedIn si mette a fare il sospettoso quando gli arriva un messaggio che propone un'occasione lavorativa?**

Come riporta **Proofpoint** in un report pubblicato qualche giorno fa, la tecnica di attacco messa a punto da un gruppo di cyber-criminali fa leva esattamente sull'effetto "ansiogeno" provocato dalla possibilità di accedere a un'offerta di lavoro.

Tutto comincia con un messaggio privato sul social network, che offre un'opportunità di lavoro. Per rendere più credibile il messaggio, i pirati che hanno architettato la campagna di distribuzione del malware hanno pensato bene di creare una pagina che sfrutta il nome e il logo di una società che si occupa realmente di reclutamento.

Al messaggio iniziale, fa seguito un’email che può contenere un allegato (un documento Word) o un collegamento Internet. **In questo secondo caso, la pagina collegata al messaggio è impostata per avviare in automatico il download del documento**. Anche se la procedura è sospetta, la potenziale vittima rischia di scambiare il tutto per una “normale” procedura per fornire al potenziale candidato le informazioni riguardanti la posizione cercata.

Un trucchetto abbastanza efficace. Di solito, infatti, le campagne per la distribuzione dei malware utilizzano l’invio massiccio di messaggi o email a numerosi contatti, senza preoccuparsi di “seguire” la potenziale vittima.

Insomma: l’idea è di suscitare nel destinatario l’idea che qualcuno stia davvero cercando di contattarlo utilizzando tutti i mezzi che ha a disposizione.

Il file in formato DOC, tanto per cambiare, richiede immediatamente l’attivazione delle funzioni Macro. Ancora una volta i pirati contano sul fatto che la vittima faccia una valutazione “costi benefici” terribilmente semplice: **accettare un l’attivazione di funzioni potenzialmente pericolose o**

rinunciare all’opportunità di un nuovo lavoro?

Manco a dirlo, in questo caso chi si prende il rischio di attivare le funzionalità Macro è destinato a pentirsene. Le istruzioni integrate nel documento, infatti, avviano il download e l’installazione di **More_eggs**, una backdoor che è in circolazione da quasi due anni.

Il malware, una volta installato sul computer, consente di controllare a distanza la macchina e di installare con estrema facilità ulteriore codice malevolo.

Please follow and like us:

Le estensioni di Google Chrome? Un incubo per la sicurezza

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/02/25/una-proposta-di-lavoro-via-linkedin-no-e-un-malware/