Il gruppo Lazarus mette nel mirino i ricercatori di cyber security

Feb 05, 2021 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS, Vulnerabilità 0

I pirati legati al governo della Corea del Nord stanno attaccando gli esperti di sicurezza utilizzando exploit zero-day di Chrome e Internet Explorer.

Sembra essere la nuova tendenza tra i pirati informatici: prendere di mira gli esperti di sicurezza per rubare strumenti di hacking e informazioni riservate che gli consentano di affinare o ampliare le loro tecniche di attacco.

A darsi un gran da fare in questo senso sembra essere il gruppo **Lazarus**. I pirati del gruppo APT, considerato molto "vicino" al governo della Corea del Nord, avrebbero portato una serie di attacchi indirizzati a ricercatori che operano nella cyber security sfruttando una serie di exploit Zero-day.

Il primo, individuato da **Microsoft** che lo ha descritto in un report pubblicato su Internet, fa leva su una vulnerabilità (CVE-2021-21148) nelle versioni di Chrome per **Windows**, **Linux** e **macOS**. SI tratta di un bug nel **motore V8 JavaScript** del browser di **Google**.

I pirati lo sfrutterebbero attraverso complesse tecniche di social engineering, che prevedono l'instaurazione di un "rapporto di fiducia" con le potenziali vittime attraverso contatti sui social network, per poi inviare link malevoli che permettono di portare l'attacco. **Google ha corretto il bug con l'aggiornamento alla versione 88.0.4324.150 del browser, già**

disponibile.

L’exploit basato su Internet Explorer è invece stato segnalato da **ENKI**. La società di sicurezza sud-coreana ha descritto le caratteristiche dello zero-day in un report (a meno che non conosciate il coreano serve Google Translator per leggerlo) in cui i ricercatori spiegano che l’attacco sfrutta come vettore un file in formato **MIME HTML**.

La sua apertura, in Windows, avvia automaticamente **Internet Explorer** (sì, c’è ancora) nel quale è presente un bug zero-day che consente l’esecuzione di codice in remoto.

Anche in questo caso, stando a quanto si legge, la tecnica è sfruttata dal gruppo Lazarus per colpire ricercatori di

sicurezza e compromettere i loro dispositivi.

Dalle parti di Microsoft sembra stiano ancora lavorando all’aggiornamento che consentirà di correggere la vulnerabilità.

Condividi l’articolo

La botnet Matryosh sfrutta i dispositivi Android per portare attacchi DDoS

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2021/02/05/il-gruppo-lazarus-mette-nel-mirino-i-ricercatori-di-cyber-security/?utm_source=rss&utm_medium=rss&utm_campaign=il-gruppo-lazarus-mette-nel-mirino-i-ricercatori-di-cyber-security