Vittima del ransomware Muhstik reagisce hackerando i pirati

Ott 08, 2019 Marco Schiaffino Attacchi, Hacking, In evidenza, Malware, News, RSS 0

Il "White Hat" era stato colpito dal malware, ma ha violato il server usato dai criminali e rilasciato poi le chiavi di decrittazione che ha trovato in memoria.

L'ansia di colpire il maggior numero di bersagli possibili, qualche volta, può riservare ai pirati informatici anche una brutta sorpresa.

È successo alla banda di cyber-criminali che ha iniziato lo scorso settembre a diffondere il ransomware **Muhstik** prendendo di mira in particolari i NAS di **QNAP**, sfruttando tecniche di brute forcing per violare una password debole in **phpMyAdmin** e installare il loro malware.

Nel corso della loro attività, però, sono incappati nella "vittima" sbagliata. Tra i tanti proprietari di NAS QNAP colpiti dai pirati, infatti, c'era anche **Tobias Frömel**, un programmatore tedesco che ha reagito a modo suo all'attacco.

Quando si è ritrovato i file criptati accompagnati da un messaggio che chiedeva 700 dollari di riscatto in Bitcoin per avere la chiave di decrittazione, Frömel ha deciso di pagare ma ha anche cominciato ad analizzare il malware che lo aveva colpito.

Nel giro di poco tempo è riuscito a individuare il server utilizzato dai pirati informatici per controllare Muhstik e ha sottratto l'intero database con le chiavi usate per crittografare i file sui NAS compromessi, pubblicandole su una pagina di Pastebin.

Non solo: il programmatore ha anche realizzato un software per decodificare i file crittografati dal ransomware, che si può scaricare da MEGA. Qualsiasi vittima di Muhstik, quindi, può adesso riavere indietro tutti i suoi dati senza dover sborsare un euro.

Nel file di testo su Pastebin, Frömel spiega di essere consapevole di aver compiuto un'azione illegale violando il server dei criminali. Dubitiamo, in ogni caso, che qualcuno abbia intenzione di denunciarlo.

Condividi l'articolo

La sicurezza (al 100%) non esiste

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/10/08/vittima-del-ransomware-muhstik-reagisce-hackerando-i-pirati/