

IceRat: il trojan “virtuale” che sfugge agli antivirus

Dic 01, 2020 Marco Schiaffino In evidenza, Malware, News, RSS 0

Il malware utilizza una macchina virtuale JavaScript per avviare un PHP che ne esegue il codice. Solo 2 motori antivirus su 3 lo riconoscono.

Le tecniche di evasione che consentono ai malware di aggirare i controlli degli antivirus sono in costante evoluzione e sfruttano spesso tecniche innovative per eludere le analisi dei programmi di protezione. Il caso di **IceRat**, però, è davvero particolare.

Come spiegano i ricercatori di **G Data** in un report pubblicato sul blog ufficiale della società di sicurezza, il trojan utilizza uno stratagemma che gli consente di sfuggire a un discreto numero di motori antivirus utilizzando **JPHP**.

SI tratta di una implementazione che consente di **eseguire PHP su una macchina virtuale Java** attraverso file in formato **.PHB**, che buona parte degli antivirus non supportano.

Oltre a utilizzare questo stratagemma per aggirare i controlli antivirus, IceRat sfrutta una struttura modulare estremamente complessa, in cui ogni componente esegue operazioni apparentemente innocue, che assumono una funzione dannosa solo se viste nel contesto complessivo.

La procedura d'installazione di IceRat, inoltre, adotta un **trucchetto** che sembra essere pensato per “distrarre” la vittima dal vero obiettivo del malware.

L'installer principale (Browes.EXE) avvia infatti due installazioni. Una di queste è **CryptoTab**, l'altra è **cheats.EXE**. Il secondo eseguibile è quello che ha come obiettivo il download e l'esecuzione del componente principale del trojan, chiamato klient.EXE.

CryptoTab, invece, è **un browser con funzionalità dedicate al mining di criptovalute** e la sua procedura d'installazione non è occultata in alcun modo. Secondo l'autore del report, la sua installazione sarebbe un semplice diversivo per nascondere la reale attività del trojan.

Il modulo principale del malware è composto da numerosi eseguibili che hanno scopi diversi: il primo è in grado di sottrarre informazioni da numerosi browser. L'elenco completo comprende i più diffusi come **Chrome** e **Firefox**, ma anche software meno noti come **Amigo**, **kometa** e **Orbitum**.

Un altro eseguibile ha invece funzioni di miner (separate da quelle di CryptoTab) che consentono all'autore del trojan di sfruttare la potenza di calcolo del PC infetto per generare criptovaluta a insaputa della vittima.

Condividi l'articolo

Quando l'Intelligenza Artificiale diventa una minaccia

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/12/01/icerat-il-trojan-virtuale-che-sfugge-agli-antivirus/?utm_source=rss&utm_medium=rss&utm_campaign=icerat-il-trojan-virtuale-che-sfugge-agli-antivirus