

DeathStalker: mercenari al servizio del miglior offerente

Ago 25, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, Scenario 0

Il gruppo di pirati informatici agisce al soldo di governi e sarebbe attivo dal 2012. La scoperta è dei ricercatori Kaspersky che ne descrivono le tecniche di attacco.

Talmente bravi da riuscire a viaggiare sotto i radar degli esperti di sicurezza per almeno 2 anni, il gruppo **DeathStalker** rappresenta quella nuova generazione di “hacker di stato” che si sta affacciando alle cronache: freelance estremamente preparati che non sono inquadrati in organizzazioni statali ma agiscono dietro un compenso in denaro.

Come spiegano in un dettagliatissimo report i ricercatori di **Kaspersky**, i cyber-spioni sembrano essere interessati in primo luogo al settore dello spionaggio industriale e finanziario, agendo come mercenari per conto del miglior offerente.

La loro attività, sottolineano gli autori dello studio, è emersa solo quando i sistemi della società antivirus hanno rilevato per la prima volta **Powersing**, un impianto basato su Power Shell che i pirati informatici usano per portare i loro attacchi.

Il malware, estremamente complesso, utilizza come vettore di attacco email di spear phishing cui sono allegati degli archivi contenenti un file LNK malevolo che punta a **cmd.exe**.

La catena di processi che porta all'installazione di Powersing prevede diverse fasi, che sfruttano tecniche di crittografia per offuscare l'attività. Il risultato finale è l'installazione di **un trojan che consente di prendere il completo controllo della macchina infetta.**

Nella loro analisi, gli esperti di Kaspersky hanno individuato delle analogie tra Powersing e **Janicab**, un malware comparso per la prima volta nel 2012.

Oltre alle similitudini a livello tecnico, le due campagne di attacchi informatici hanno in comune altri elementi, come il profilo delle vittime (aziende private attive nel settore finanziario o industriale) e gli stratagemmi adottati per evitare le macchine virtuali utilizzate nelle sandbox dai software di sicurezza.

IL quadro che emerge dallo studio, in ogni caso, è quello di un gruppo con notevoli capacità tecniche, che non raggiungono però il livello di pericolosità dei veri e propri gruppi **APT** (Advanced Persistent Threat) che agiscono normalmente in sinergia con servizi segreti e organizzazioni governative.

Condividi l'articolo

Nuovo attacco contro Firefox sfrutta il “puntatore truffaldino”

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/08/25/deathstalker-mercenari-al-servizio-del-miglior-offerente/?utm_source=rss&utm_medium=rss&utm_campaign=deathstalker-mercenari-al-servizio-del-miglior-offerente