

Hackerano siti di news per colpire decine di aziende

Lug 06, 2020 Marco Schiaffino Attacchi, In evidenza, Malware, News, RSS 0

Il gruppo Evil Corp ha usato una strategia in due fasi per introdursi nelle reti aziendali e installare il ransomware WastedLocker.

In un primo momento era sembrato un “normale” attacco di massa nei confronti di decine di imprese statunitensi. In seguito, però, i ricercatori di **Symantec** hanno scoperto che i tentativi di violazione subiti dalle aziende seguivano una strategia decisamente elaborata.

Come si legge nel report pubblicato dalla società di sicurezza, infatti, **gli autori degli attacchi hanno usato come “trampolino di lancio” una dozzina di siti di news che avevano compromesso in precedenza.**

Protagonista di questa vicenda è il gruppo **Evil Corp**, conosciuto per aver diffuso in passato il malware **Dridex**. Stando alla ricostruzione di Symantec, la gang di cyber criminali avrebbe preso di mira un gruppo editoriale statunitense, ottenendo l’accesso ai server che ospitano 12 siti di news.

I pirati hanno sfruttato questa opportunità iniettando sulle pagine dei siti il codice di **SocGholish**, un malware basato su piattaforma JavaScript che ha permesso loro di colpire i dipendenti delle aziende che visitavano le pagine infette.

I bersagli, tutti con sede negli USA, operano in settori molto diversificati e la loro scelta appare essere dettata più che

altro dalla possibilità di massimizzare il profitto derivante dagli attacchi.

La tecnica utilizzata è stata quella di visualizzare delle false richieste di aggiornamento software, che avviavano il download e l'installazione di **Cobalt Strike**, uno strumento di hacking che consente di eseguire comandi sul computer compromesso, avviare ulteriori processi e caricare e scaricare file.

Da qui, i pirati di Evil Corp hanno cercato di avviare una serie di attività nella logica del "movimento laterale", con l'obiettivo di individuare le infrastrutture critiche delle aziende e installare il ransomware **WastedLocker**.

L'attacco, come spiegano gli autori del report, è stato sventato. La vicenda, però, rappresenta l'ennesima dimostrazione del fatto che i gruppi di cyber criminali utilizzano strategie sempre più complesse, senza farsi scrupoli degli "effetti collaterali" legati ai loro attacchi.

Condividi l'articolo

La polizia hackera Encrochat per incastrare i criminali

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/07/06/evil-corp-hackerano-siti-di-news-per-colpire-decine-di-aziende/?utm_source=rss&utm_medium=rss&utm_campaign=evil-corp-hackerano-siti-di-news-per-colpire-decine-di-aziende