# REvil è tornato: il famigerato gruppo ransomware riprende le operazioni

https://www.hwupgrade.it/i/n/hacking_720.jpg,

Il ransomware che ha colpito bersagli di alto profilo sta tornando attivo dopo le operazioni di contrasto effettuate negli scorsi mesi. Alla base del ritorno, il deterioramento dei rapporti tra USA e Russia

di Andrea Bai pubblicata il **02 Maggio 2022**, alle **16:41** nel canale Sicurezza

Torna alla ribalta il famigerato ransomware **REvil**, le cui operazioni erano state chiuse lo scorso mese di ottobre a seguito di un intervento delle forze dell'ordine con il dirottamento dei server Tor e l'arresto, da parte delle forze dell'ordine russe, dei membri della banda che manovrava il ransomware.

Il conflitto russo-ucraino ha però cambiato le carte in tavola, con la Russia che ha dichiarato agli USA il ritiro dal processo di negoziazione per la banda REvil, sospendendo ogni comunicazione. E' bastato poco perché **la vecchia infrastruttura Tor di REvil tornasse a funzionare**, indirizzando però i visitatori non ai vecchi siti web ma a nuovi URL per operazioni ransomware senza nome.

> *A few hours ago, we blocked a #ransomware sample in-the-wild that looks like a new #Sodinokibi / #REvil variant. Timestamp 2022-04-27, new config, new mutex, campaign ID, etc. Funny thing… it does not encrypt files; only adds a random extension  42 BTC https://t.co/UL1ECGLpmg pic.twitter.com/A8p5SLjcZr*
>
> *— Jakub Kroustek (@JakubKroustek) April 29, 2022*

Per confermare che si trattasse del ritorno di REvil è stato necessario
riuscire ad individuare un campione del crittografo ransomware e
analizzarlo per determinare se derivasse dal codice sorgente originario.
Il ritrovamento e l'analisi sono stati effettuati ad opera del ricercatore
**Jakub Kroustek di AVAST**, che ha confermato i legami della nuova
campagna ransomware con REvil.

Il fatto che REvil abbia ripreso le operazioni dopo le conseguenze del
conflitto in Ucraina e il progressivo deteriorarsi delle relazioni tra
Russia e Stati Uniti non è una sorpresa. Ciò che invece è insolito è il
fatto che tutto stia avvenendo alla luce del sole, quando di norma questo
genere di operazioni avvengono a seguito di una sorta di "rebranding", per
poter eludere le forze dell'ordine o quelle sanzioni che impediscono il
pagamento dei riscatti.

REvil ha condotto in passato numerose campagne rivolte verso bersagli di
alto profilo come ad esempio nel 2019 l'attacco allo studio
legale di celebrità come Madonna, gli U2 e Lady Gaga, oppure le
infiltrazioni presso il produttore Quanta
Computer, o ancora il noto attacco all'impianto
statunitense di distribuzione carburanti Colonial
Pipeline, seguito settimane dopo da quello a JBS, azienda di

lavorazione carni.

Read More