

I pirati di REvil cercano soci e mettono sul piatto 1 milione di dollari

Set 29, 2020 Marco Schiaffino Hacking, In evidenza, Malware, News, Scenario 0

Lo strano annuncio su un forum hacker, sul quale i cyber criminali hanno depositato 99 Bitcoin per dimostrare che si tratta di un ottimo affare.

Il marketing nel settore del cyber crimine non va tanto per il sottile e a dimostrarlo, in questi giorni, sono i pirati informatici del gruppo **REvil**, tra i più attivi negli ultimi mesi.

I cyber criminali di REvil si sono fatti un nome attraverso la formula del **malware as a service**, una strategia sempre più utilizzata nei bassifondi del Web e che prevede una sorta di “affiliazione” tra criminali per spartirsi i profitti dei loro attacchi.

I REvil, nel dettaglio, forniscono ai loro partner il malware **Sodinokibi** in uno schema piuttosto semplice: i “collaboratori” che riescono a colpire un bersaglio incassano il 70-80% del riscatto eventualmente versato dalla vittima, mentre agli sviluppatori rimane in tasca il 20-30%.

L’ultima trovata per promuovere la loro attività, segnalata dai ricercatori di **Sophos** nel blog ufficiale della società di sicurezza è un annuncio su un forum hacker in cui il gruppo spiega di essere alla ricerca di “esperti in penetration testing”.

Quali siano le loro intenzioni è evidente, soprattutto quando parlano di avere intenzione di “espandere la composizione dei team dedicati alla pubblicizzazione con risorse di talento” per “aumentare i profitti”.

Dopo aver specificato che i “candidati” saranno sottoposti a una selezione, i pirati calano l’asso sul tavolo: **un deposito di 99 Bitcoin (circa un milione di dollari) sullo stesso forum per dimostrare quale sia la loro disponibilità economica.**

La logica è chiara: dal momento che chiunque può verificare il saldo dei conti in Bitcoin, il deposito rappresenta la migliore assicurazione che l’attività che propongono è decisamente lucrosa.

D’altra parte, il gruppo REvil non è nuovo a trovate piuttosto “estrose”. In una campagna ransomware individuata dai ricercatori lo scorso dicembre, cercavano di convincere le loro vittime a pagare il riscatto sventolando lo spauracchio delle sanzioni legate al GDPR in caso di mancato pagamento.

Al di là delle note di colore, la vicenda conferma ancora una volta in quale direzione si stia muovendo il mondo della pirateria informatica, sempre più orientato a schemi “commerciali” ispirati alla collaborazione e affiliazione.

Condividi l’articolo

Dispositivi FortiGate VPN esposti ad attacchi Man in the Middle

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/09/29/i-pirati-di-revil-cercano-collaboratori-e-mettono-sul-piatto-1-milione-di-dollari/?utm_source=rss&utm_medium=rss&utm_campaign=i-pirati-di-revil-cercano-collaboratori-e-mettono-sul-piatto-1-milione-di-dollari