Hacker nordcoreani all'attacco del ministero degli Esteri russo. Mosca intanto sgomina con gli Usa il gruppo REvil

Un gruppo di hacker nordcoreano soprannominato APT37 ha attaccato lo scorso ottobre il ministero degli Esteri russo e i suoi dipendenti e successivamente ha compromesso l'account di un dipendente del governo. A riportare la notizia il North Korea Times in base a fonti statunitensi.

Secondo i ricercatori delle società di sicurezza informatica statunitensi Cluster25 e Black Lotus Labs, ad ottobre è stata messa in atto una campagna di phishing (una truffa effettuata su Internet attraverso la quale un malintenzionato dei sistemi informatici cerca di ingannare la vittima convincendola a fornire informazioni personali, dati finanziari o codici di accesso) contro il ministero. "I ricercatori affermano che ad alcuni dipendenti sono stati inviati archivi di documenti e gli è stato chiesto di fornire dettagli sulla vaccinazione, mentre altri sono stati dirottati su collegamenti a malware mascherati da software". L'operazione è riuscita visto che da uno degli indirizzi compromessi, il 20 dicembre gli hacker sono riusciti a inviare un'e-mail di phishing al viceministro russo Sergey Ryabkov e hanno preso di mira anche l'ambasciata russa in Indonesia.

APT37 – riporta in NKT è noto per l'utilizzo di un software chiamato Konni, uno strumento di amministrazione remota. Secondo quanto riferito, è stato utilizzato per prendere di mira la Corea del Sud, così come organizzazioni politiche in Giappone, India e Cina, tra gli altri paesi. Secondo il quotidiano moscovita Kommersant, il gruppo esiste almeno dal 2017. Anche a novembre la Corea del Nord con il. gruppo hacker Kimsuky aveva inviato e-mail di phishing scritte per conto di noti esperti russi, scienziati e ONG a esperti in Corea del Sud per carpirne le credenziali.

La scorsa settimana, attraverso la collaborazione con gli Stati Uniti la polizia russa sarebbe riuscita a sgominare un gruppo di hacker. Il Servizio di sicurezza federale (FSB) ha infatti arrestato persone a Mosca, San Pietroburgo e nella regione di Lipetsk che sarebbero stati membri di REvil, un noto gruppo di ransomware

noto per aver ricevuto milioni di pagamenti di riscatto ed essere dietro al 42% di questo tipo di. cyber attacchi.

Read More