Attacco hacker a Twitter: individuati i responsabili

Ago 03, 2020 Marco Schiaffino Attacchi, Hacking, In evidenza, News, Phishing, RSS 0

La "mente" è un diciassettenne che avrebbe aggirato le protezini con una semplice telefonata. I truffatori traditi da una serie di errori incredibili.

Si è parlato della possibilità di un coinvolgimento di gruppi hacker collegati a governi stranieri e di professionisti del cyber crimine. Niente di tutto questo: dietro all'attacco che ha permesso di hackerare decine di profili **Twitter** di celebrità c'è la mano di un 17enne originario della Florida.

La ricostruzione della vicenda, resa possibile dai documenti giudiziari pubblicati dalla procura del distretto della California, rende l'idea di come una simile "impresa" non richieda grandi mezzi o conoscenze specifiche. Anzi: tutto sarebbe cominciato con una semplice telefonata che avrebbe permesso all'hacker di aggirare il sistema di autenticazione a doppio fattore usato per proteggere gli account degli amministratori Twitter.

Tutto comincia il 15 luglio, quando l'hacker diciassettenne originario di Tampa (Florida) ma residente in California, contatta telefonicamente alcuni operatori di Twitter utilizzando classiche tecniche di ingegneria sociale per farsi fornire le credenziali di accesso al backend del social network.

Il trucchetto funziona e l'autore dell'attacco ottiene, attraverso una serie di ulteriori attacchi portati tra le pieghe dei sistemi di Twitter, un accesso pressoché libero a

tutti gli account.

A questo punto, il pirata informatico si è preoccupato di procurarsi dei complici e lo ha fatto contattando alcuni utenti che frequentavano un canale dedicato all'hacking su **Discord**, offrendo loro anche delle dimostrazioni delle sue possibilità di accesso.

Nel dettaglio, **Kirk#5270** (il suo nickname su Discord) ha convinto uno dei suoi futuri complici (**Rolex#0373**, identificato con il 22enne **Nima Fazeli**) alterando il suo profilo Twitter.

2020-07-15 17:28:55.093000	Kirk#5270	I work for twitter
2020-07-15 17:29:02.307000	Kirk#5270	I can claim any @ for you.
2020-07-15 17:29:03.448000	Kirk#5270	Let me know.
2020-07-15 17:29:06.470000	Kirk#5270	Don't tell anyone.
2020-07-15 17:29:17.161000	Rolex#0373	Lol
2020-07-15 17:29:25.103000	Rolex#0373	Prove it
2020-07-15 17:29:25.604000	Kirk#5270	Give me your twitter @
2020-07-15 17:29:50.665000	Kirk#5270	I'll pull it up

2020-07-15 17:30:23.536000	Kirk#5270	Give me your twitter @
2020-07-15 17:30:27.461000	Rolex#0373	viennacat921
2020-07-15 17:30:31.573000	Kirk#5270	Yours?
2020-07-15 17:30:33.221000	Rolex#0373	Yes

Dopo aver reclutato un terzo membro della gang, il britannico **Mason Sheppard**, il gruppo sarebbe passato all'azione sfruttando l'accesso ai sistemi per violare circa 130 account Twitter, per 45 dei quali avrebbero avviato il reset della password.

Il loro obiettivo, come abbiamo spiegato in un articolo precedente, era quello di mettere in atto una classica truffa "give away", utilizzando gli account Twitter di celebrità per indurre le potenziali vittime a trasferire Bitcoin sui loro conti.

Lo stratagemma avrebbe permesso loro di raccogliere la bellezza di 117.000 dollari in poche ore. Il bottino, però,

avrebbe potuto essere più ricco. Secondo quanto dichiarato da **Coinbase**, una delle più celebri piattaforme per il commercio di criptovalute, nelle tasche dei truffatori avrebbero potuto finire altri **280.000 dollari**. A impedirlo, è stato il tempestivo blocco dei conti utilizzati per la truffa.

A tradire gli hacker sarebbe stato un uso troppo "disinvolto" dei social media e di alcuni forum, che ha permesso all'FBI di incrociare i dati e risalire all'identità dei truffatori. In particolare, Fazeli si è tradito utilizzando lo stesso nickname sia in Discord, sia sul forum di **OGUsers**.

Non solo, il truffatore avrebbe usato per i suoi conti su Coinbase gli stessi indirizzi email utilizzati per registrarsi sul forum e violare un account Twitter. **Nella registrazione a Coinbase avrebbe confermato la procedura caricando un'immagine della sua carta d'identità**.

E ancora: lo stesso Fazeli avrebbe usato la sua connessione domestica per connettersi sia a Discord, sia ai conti su Coinbase.

Errori simili sarebbero ascrivibili anche a Mason Sheppard, che avrebbe utilizzato un conto Coinbase connesso alla truffa per acquistare un videogioco. **Conto che aveva registrato, peraltro, utilizzando la sua vera patente come documento di riconoscimento**.

Insomma: da quanto emerge leggendo i documenti della Procura, gli hacker che hanno messo a segno il "colpo dell'anno" non sarebbero propriamente dei geni.

Condividi l'articolo

Da Windows a Linux: TrickBot si evolve

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/08/03/attacco-hacker-a-twitter-individuati-i-responsabili/?utm_source=rss&utm_medium=rss&utm_campaign=attacco-hacker-a-twitter-individuati-i-responsabili