# Gli errori commessi dagli hacker di Twitter

Sono stati arrestati in tempi record gli hacker responsabili del grave incidente informatico che ha coinvolto **Twitter** lo scorso 15 luglio.

Per le autorità statunitensi **Graham Ivan Clark**, 17enne appena diplomato proveniente dalla Florida; **Mason John Sheppard**, 19enne del Regno Unito, e **Nima Fazeli**, 22enne di Orlando (Florida), sono i criminal hacker del maxi attacco che giorni fa hanno violato gli account degli uomini più ricchi del mondo: **Bill Gates, Jeff Bezos, Elon Musk, Warren Buffett, Michael Bloomberg.** Questi account, ciascuno con milioni di follower, sono stati compromessi per promuovere una truffa basata su **Bitcoin**.

Secondo alcuni documenti relativi all'indagine in corso e diffusi venerdì, la figura centrale dell'attacco sarebbe una persona che usava il nome Kirk, e che potrebbe essere proprio Clark. Clark è stato arrestato a Tampa (Florida), ed è accusato di oltre 30 reati tra cui frode e attacco informatico.

## Gli errori dei criminal hacker

L'hack di Twitter, stando alle ricostruzioni e alla veloce cattura dei responsabili, è stato non organizzato e gestito particolarmente bene, da hacker non particolarmente esperti.

Secondo il New York Times, alcuni di loro avrebbero finito per depositare parte dei bitcoin rubati sui loro account personali di alcuni exchange crypto, in particolare **Coinbase**, e questi

avrebbero prontamente segnalato alle autorità il deposito sospetto, compresa l'identità dei proprietari dell'account. Tra l'altro proprio Coinbase ha rivelato qualche giorno fa di essersi già adoperata durante l'attacco per impedire ai propri utenti di versare bitcoin all'indirizzo utilizzato dai truffatori.

In modo particolare è stato facile tracciarli grazie ad appositi software di analisi della blockchain pubblica di **Bitcoin**, che le autorità americane hanno utilizzato.

# Twitter: 'hackerati gli smartphone dei dipendenti tramite phishing'

Twitter, tramite un comunicato ufficiale, ha spiegato che i pirati informatici hanno contattato un "numero ristretto" di dipendenti attraverso tecniche di phishing, riuscendo così ad avere accesso ad alcuni strumenti interni che poi hanno permesso agli hacker di violare il sistema di controllo degli account.

La tecnica di ingegneria sociale ha avuto successo perché i dipendenti lavorano in smart working (a causa della pandemia COVID-19), per cui non hanno potuto verificare l'identità dei (falsi) colleghi con le procedure di sicurezza presenti in ufficio.

"*Questo attacco si è basato sul tentativo massiccio di ingannare alcuni dipendenti e sfruttare le vulnerabilità umane per ottenere l'accesso al nostro sistema interno*", ha dichiarato Twitter, sottolineando come quanto è avvenuto sia "*un monito*" per ogni dipendente a mantenere le misure di protezione e sicurezza.

https://www.key4biz.it/gli-errori-commessi-dagli-hacker-di-twitter/317283/