Tutti gli hacker di Kim

Pirati informatici rubano criptovalute e informazioni a grandi aziende e banche di Paesi «nemici» della Corea del Nord. Poi riciclano a vantaggio di Pyongyang. Da cui, si presume, sono guidati.

di Stefano Piazza e Luciano Tirinnanzi

«Hacker legati alla Corea del Nord sono responsabili di furti di criptovalute per un valore di quasi 1,7 miliardi di dollari, e questo riguarda soltanto lo scorso anno». A lanciare l'allarme è il gruppo di esperti sulle sanzioni del Consiglio di sicurezza delle Nazioni Unite, che monitora il rispetto delle regole da parte di Pyongyang. Il loro rapporto indica come il Nord, tramite queste valute digitali difficilmente tracciabili, abbia poi potuto comprare sottotraccia e importare prodotti petroliferi raffinati oltre il limite annuale consentito di 500 mila barili, così aggirando platealmente le sanzioni. Dal primo gennaio al primo maggio di quest'anno, infatti, ben 25 petroliere battenti bandiera nordcoreana, di cui nove già nel mirino del Consiglio di sicurezza, hanno potuto effettuare 46 consegne di prodotti petroliferi raffinati nei porti nordcoreani.

«Gli attori che lavorano per il Reconnaissance General Bureau (una delle molte articolazioni dei servizi di sicurezza nordcoreani, *ndr*), hanno continuato a utilizzare tecniche informatiche sempre più sofisticate per rubare fondi e informazioni» afferma il rapporto Onu. «La cifra di 1,7 miliardi di dollari rappresenta solo il 44 per cento dei 3,8 miliardi di dollari rubati nel 2022, l'anno d'oro per il furto di criptovalute» sottolinea in proposito Chainalysis, società di analisi su flussi informatici e blockchain.

Ma chi sono esattamente questi hacker? E quale il loro scopo? Si tratta principalmente del Lazarus Group, composto da informatici spregiudicati responsabili di azioni di «terrorismo informatico», come il furto di circa 100 milioni di dollari in criptovalute ai danni della società statunitense Harmony lo scorso giugno. «Uno dei colpi più grandi di quest'anno» afferma l'Fbi, dopo che già Lazarus aveva attaccato aziende informatiche internazionali, come Sony (81 milioni di dollari trafugati), Axie Infinity (625 milioni), Horizon Bridge (100), Alphapo (23), CoinsPaid e Atomic Wallet (100).

Secondo i federali Usa, il metodo di furto e riciclaggio del denaro è lo stesso usato già nel marzo di quest'anno, quando i cybercriminali nordcoreani hanno sottratto la cifra record di 625 milioni di dollari in asset crittografici dal popolare gioco Axie Infinity, utilizzando credenziali e password rubate in un precedente attacco. Poi hanno riconvertito parte del denaro digitale in altra valuta (da Ethereum a Bitcoin). «Il gruppo Lazarus opera conducendo molteplici operazioni nel corso dell'anno» spiega un funzionario di TrendMicro, azienda giapponese di cyber security. «La maggior parte comporta dissimulazioni, sabotaggi, furti finanziari e spionaggio. L'organizzazione dispone anche di gruppi "spin-off", che si concentrano su tipi specifici di attacchi e obiettivi. Come Bluenoroff, un sottogruppo focalizzato sull'aggressione alle istituzioni finanziarie straniere, compreso il grande attacco alla banca del Bangladesh del 2016, che ha fruttato loro 101 milioni di dollari, parte dei quali dirottati su conti bancari privati nelle Filippine e nello Sri

A Seoul, capitale della Corea del Sud, passanti guardano con preoccupazione un telegiornale che mostra Kim Jong-un, leader supremo della Corea del Nord, durante il test di un nuovo missile balistico.

GETTY IMAGES (2), REUTERS

Kim Jong-un e Vladimir Putin, presidente russo. Oggi tra i due leader c'è un accordo che include la cessione di armi nordcoreane alla Russia, in cambio (anche) del dislocamento di hacker nel mondo.

Lanka. Mentre Andariel è un sottogruppo focalizzato sul colpire le organizzazioni e le imprese sudcoreane, ossia i principali nemici del Nord».

La pericolosità di questi hacker è dovuta soprattutto «all'ampia varietà di strumenti a loro disposizione e delle diverse tattiche, a seconda dei bersagli e degli obiettivi, anche se il furto di informazioni resta uno degli obiettivi principali degli attacchi mirati». Lazarus lascia spesso tracce e indicazioni volutamente sbagliate, «anche emulando il modus operandi degli "hacktivisti", ossia degli hacker politicizzati, e inserisce false flag come depistaggio. Un esempio è la backdoor Klipod, che utilizza parole russe per i suoi comandi. Sebbene sia possibile che Lazarus abbia membri provenienti da Paesi diversi, le parole russe non sembrano essere scritte da un madrelingua e dunque è logico pensare che siano usate per depistare».

Sebbene gli obiettivi degli attacchi varino dal sabotaggio al guadagno finanziario, è chiaro a cosa servano questi soldi: aggirare le sanzioni internazionali e sviluppare parimenti il programma nazionale missilistico volto a ottenere l'arma nucleare.

Lazarus, infatti, non è in alcun modo un'organizzazione indipendente ma risponde direttamente a Kim Jong-un, il leader supremo che ha reso da tempo la Corea del Nord la più imponente potenza dell'hacking mondiale. Tutti i suoi hacker sono stati istruiti dal Reconnaissance General Bureau, l'agenzia di intelligence nazionale che opera all'estero, più o meno l'omologo della Cia americana.

«Quando sono pronti per l'impiego, vengono dislocati all'estero, nei Paesi con le migliori infrastrutture Internet dai quali possono sferrare attacchi di ogni sorta lasciando minime tracce per non essere accostati in modo certo a Pyongyang» spiega Patrick Winn, reporter della rete radiofonica Public Radio International di Minneapolis. «Nel 2014, quando la Sony Pictures si apprestava a rilasciare *The Interview*, un film commedia sull'assassinio di Kim Jong-un, gli hacker di Pyongyang hanno cancellato tutti i suoi dati sensibili e fatto circolare mail private finché il colosso giapponese non ha ceduto e ha cancellato la distribuzione del film. Un'azione dimostrativa a riprova della loro forza» riferisce Winn.

Lazarus in ogni caso è solo un appellativo di comodo. Per capire meglio come sia inquadrata appieno nell'amministrazione pubblica nordcoreana, basti il suo vero nome: Unità 121 che, insieme all'Unità 110 e all'Unità 180, è parte integrante del cyber-esercito di Kim. Come di recente ha confermato l'Australian Strategic Policy Institute, il regime impiega almeno 1.700 hacker per queste operazioni, a cui vanno aggiunte circa cinquemila persone di supporto. Inoltre, secondo fonti del National intelligence service (Nis), la principale agenzia di spionaggio della Corea del Sud, la Corea del Nord concerta con Mosca molte di queste azioni.

Di più, la Russia favorisce il dislocamento degli agenti-hacker di Pyongyang in giro per il mondo, in cambio di sostegno militare: solo da inizio di agosto, per fare un esempio, l'esercito russo ha ricevuto più di un milione di proiettili d'artiglieria, pari a circa due mesi di forniture per la guerra in Ucraina. In cambio, la Russia offre «tecnologia e supporto ai programmi militari della Corea del Nord», come ha denunciato il segretario di Stato degli Stati Uniti, Antony Blinken. ■