il Fatto Quotidiano

29-NOV-2016
pagina 16
foglio 1 / 2

KAPUSTKIY A soli 17 anni, scopre le falle nei siti istituzionali

Chi è l'hacker buono che aiuta i governi

■ "Dicono che in Italia sono bravi con la cyber security e volevo controllare", spiega l'attivista che ha "bucato" uno dei siti del ministero della Pubblica amministrazione. "Alla fine mi hanno anche ringraziato", spiega

DELLA SALA
A PAG. 16

L'ATTACCO Il 17enne ha copiato il database di una piattaforma della Pa

Kapustkiy, chi è l'hacker buono che ha bucato il sito del governo

Avevo sentito dire che in Italia sono esperti di cyber sicurezza: così ho voluto verificarlo di persona

» VIRGINIA DELLA SALA

"Guarda, lo hanno fixato": Kapustkiy è felice quando si accorge che il sito che ha hackerato è stato aggiustato. Mostra l'email che ha ricevuto dal direttore del servizio per lo sviluppo dell'innovazione del dipartimento italiano della funzione pubblica. "Caro amministratore - gli aveva scritto Kapuskiy - vedo che il sito *mobilita.gov* è tornato in funzione. Ne sono felice. Se doveste avere bisogno di altro aiuto, sono qui".

LA SETTIMANA scorsa questo hacker (che però non ama essere definito così) aveva bucato il sito della funzione pubblica dedicato alla mobilità del personale della Pa, *www.mobilita.gov.it*. Era riuscito a entrare nei database e ad appropriarsi dei dati di oltre 45 mila utenti registrati: account, password, informazioni sensibili. Per dimostrare l'impresa ne aveva pubblicata una parte su un *pastebin* (sorta di bacheca pubblica virtuale anonima) per poi rimuoverla dopo qualche ora. Da allora, la piattaforma era stata messa offline. "E dall'Italia nessuno mi ancora ringraziato" aveva spiegato dopo qualche giorno dal suo attacco. Poi, giovedì 24 novembre il sito è tornato online e Kapuskiy ha ricevuto la risposta del dirigente del governo: "Caro Kapustkiy, se abbiamo risolto il problema è soprattutto grazie al tuo intervento. Grazie mille".

Questo giovane hacker (dice di avere 17 anni) è uno dei buoni. Vuole aiutare. Il suo sogno è lavorare, un giorno, nel campo della cybersecurity dei governi. Ha iniziato a 13 anni bucando il sito della University of England. Si muove da solo, non ha una *community* online né gli interessa averla. Quello che fa, dal suo punto di vista, è come consegnare curriculum nella speranza che in futuro possa essere assoldato. "Non mi piace descrivermi come un hacker - racconta in una notte trascorsa online nei messaggi privati su Twitter - voglio solo che le mie violazioni siano conosciute perché così si inizierà a fare più attenzione alla sicurezza".

Con gli esperti informatici indiani (aveva bucato il sito dell'ambasciata) ha intrattenuto un altro tipo di corrispondenza: si sono confrontati, l'hacker ha fornito loro le sue spiegazioni e i suoi consigli. "Sono stati gentili e corretti. E hanno capito lo spirito con

cui lavoro".

Gli chiediamo perché ha colpito l'Italia: "Avevo sentito dire che in Italia sono esperti nel proteggere i propri siti web. Così ho cercato un sito importante sito legato al governo e ne ho segnalato la vulnerabiltà all'amministratore e al ministero degli Esteri. Poi ho fatto un *leak* di una piccola parte degli utenti come prova". Kapuskiy spiega che per bucare il sito è bastata una manovra elementare, alla portata di molti. E gli altri siti? "Non ho trovato altre vulnerabilità: il governo è ben protetto contro gli attacchi con metodi basilari". La tecnica che ha utilizzato è definita *SQL injection* ed è utilizzata per attaccare applicazioni di gestione dati. Si inseriscono stringhe di codice malevole per far eseguire comandi a favore di chi sta hackerando, ad esempio l'invio dei database. Assicura di aver cancellato i dati. Nessun interesse a venderli o a usarli per ricatti. "Studio It security a scuola - racconta - e vorrei lavorare nella cybersecurity".

DICE DI NON ESSERE un nerd dell'informatica né un pirata. "Sono stato ispirato dal gruppo di hacker che si chiama LulzSec (a cui in passato è stata attribuita la messa offline anche del sito della Cia, *ndr*): con loro ho capito che voglio hackerare, ma che non voglio seguire la strada Black hat". Cioè quella dei "cracker", hacker con intenti criminali. Kapustkiy si considera un *pen-tester*, esperto di *penetration test* nei sistemi informatici. Commenta anche la notizia delle denunce dei due italiani che avrebbero lanciato, tramite Anonymous, la campagna di attacchi #OPS_ItalyBeDemocratic contro alcuni siti istituzionali in periodo pre-referendario: "Dovrebbero aiutare il governo, non attaccarlo. Così si rischia solo di essere arrestati per qualcosa di stupido".

Ora, dopo aver penetrato - tra gli altri - i siti dell'ambasciata indiana, del consiglio regionale indiano, della funzione pubblica italiana, della fondazione per i diritti umani ungherese - dice che si fermerà per un po': "Credo che mi concentrerò sulla scuola almeno fino a Natale. E sullo sport". Ma dopo soli due giorni dall'impegno, segnala di aver bucato i siti delle ambasciate di Ghana e Finlandia (sempre in India). I *leak* dei dati acquisiti sono ancora online "Lo so - spiega Kapustkiy - avevo detto che mi sarei fermato. Ma li avevo avvisati delle vulnerabilità e non hanno fatto nulla. Non ho avuto altra scelta se non pubblicare. Così si decideranno a intervenire".

Precedenti

- **INDIA** Il 19 novembre, Kapustkiy sottrae 17mila credenziali da un sito del Consiglio Regionale indiano. Come prova, ne pubblica circa 2mila
- **UNGHERIA** Il 21 novembre, l'hacker attacca il sito della Hungarian Human Rights Foundation: anche in questo caso riesce a procurarsi centinaia di dati. In entrambe le occasioni ha poi rimosso le informazioni pubblicate come prova