La silente guerra degli hacker italiani

C’è una guerra in atto all’interno del panorama internet italiano, una guerra silenziosa di cui i quotidiani praticamente non parlano ma molto importante perché corre sul filo della responsabilità del trattamento dei dati personali. Forse il termine “guerra” potrà sembrare eccessivo ad alcuni di voi, ma permettetemi di snocciolare qualche dato che, sinceramente, dovrebbe far riflettere: a giugno di questo anno sono stati attaccati il sito del Consiglio della Regione Toscana: http://www.consiglio.regione.toscana.it e il sito riguardante il potenziamento delle linee della TAV http://www.e78grossetosiena.it. A luglio sono stati attaccati il Ministero della Salute e il sito che collegava le attività dell’Expo di Milano alle attività commerciali in Basilicata (http://www.daexpoallabasilicata.it). Ad agosto, mentre molti di noi erano sotto l’ombrellone, è stato attaccato il sito della UILM (Unione Italiana Lavoratori Metalmeccanici). Per continuare:

- 12 agosto: data breach con esposizione pubblica di credenziali utenti appartenenti al MEF;
- 7 settembre: data breach con esposizione pubblica di oltre 37.500 account di utenti INAS;
- 11 settembre: data breach con esposizione pubblica di username e password appartenenti al Ministero dell’Ambiente e del Ministero del Tesoro;
- 16 settembre: data breach con esposizione pubblica di utenze appartenenti all’UNUCI (Unione Nazionale Ufficiali in Congedo d’Italia).

Ne sono previsti altri, entro il cinque novembre per l’esattezza, ma prima di proseguire credo sia giusto chiarire alcuni concetti chiave. Le azioni di cui parliamo si basano, grossomodo, su due tipologie di attacco: il *de facing* ossia la

modifica dell'aspetto grafico di un sito in modo che possa apparire come vuole l'hacker, e il *data-breach* che prevede l'entrata in possesso di database da cui estrarre i dati. La tipologia di attacco sembra dimostrare che gli hacker hanno una fitta rete di "aiutanti", pronti a garantire gli accessi ai dati o, quantomeno, in grado di semplificare le varie operazioni di sabotaggio. È un panorama preoccupante che lascia scoperti alcuni interrogativi ed il principale è *"come mai le protezioni non funzionano?*".

La protezione non è solo un fattore tecnico, è altresì garantita dalle componenti umane di professionalità, competenza ed etica; questi ultimi spesso dimenticati, sottovalutati o letteralmente ignorati. Dai vari tweet di gruppi hacker come Anonymous Italia o LulzSecITA si scoprono principalmente due aspetti: il primo riguarda le password in uso agli utenti, spesso non in linea con i comuni criteri di sicurezza. Il secondo riguarda le banche dati, popolate da tabelle in cui le credenziali sono "in chiaro", ossia in cui password dell'utente è leggibile a chiunque ne abbia accesso.

Esistono quindi due facce della stessa medaglia: da un lato c'è l'attaccante che viola la legge con un accesso abusivo al sistema informatico. Dall'altro c'è chi avrebbe dovuto gestire adeguatamente le informazioni e non lo ha fatto. A valle di un attacco c'è sempre un messaggio che lo reclama fornendo dati tecnici interessanti e ci si aspetterebbe provvedimenti legali in entrambe le direzioni, anche per chi non ha protetto adeguatamente tali informazioni. È il caso di Rogue0, l'hacker che ha ripetutamente penetrato la piattaforma utilizzata dal Movimento 5 Stelle e di proprietà della Casaleggio Associati. L'hacker ha garantito che può accedere alla piattaforma ripetutamente e senza troppi problemi e a poco sono valse le raccomandazioni del Garante sulla Privacy: già dopo il primo attacco la piattaforma era stata data per sicura e invece sappiamo come è finita: il 6 settembre su Twitter appaiono i numeri di cellulare di esponenti del Movimento 5 Stelle e dati

di tabelle provenienti dalla piattaforma. Come mai nessuno ha controllato che la falla fosse stata chiusa realmente e la piattaforma fosse davvero sicura e in grado di operare?

Diciamo la verità, in Italia abbiamo un brutto vizio: non controlla nessuno fino a quando non accade qualcosa di spiacevole e chi pensa che questi attacchi hacker abbiano finalità politica sbaglia anche se gli obiettivi sembrano suggerirlo. Questi gruppi hacker hanno lo scopo di detronizzare le istituzioni che vantano sicurezza e perfezione quando, in realtà, non sono in grado di fornirle. A valle dell'attacco all'INAS, il gruppo LulzSecITA ha scritto quanto segue: "**Ancora una volta, l'Istituzione Italiana si mostra incapace di #proteggere i #dati #sensibili dei propri cittadini, mettendo così in serio pericolo le loro vite, e se vogliamo parlare di numeri, sono ben 37.500**."

Alla base vi è la voglia di sbugiardare la sicurezza che molti soggetti istituzionali sembrano palesare e le tecniche adottate per riuscire in questo obiettivo, sono quelle che fanno più male perché mettono a nudo l'incapacità tecnica di difendersi oltre che la scarsa professionalità nella gestione dei dati. In un'intervista al sito Motherboard.it si leggono due risposte molto interessanti dell'hacker Rogue0:

Domanda di Motherboard.it: Hai anche accesso in scrittura al database?

Risposta dell'hacker: L'accesso è sempre lo stesso quindi sì, in uno dei tweet ho scritto nome e tipo di user e i suoi privilegi, quindi è una cosa pubblica

Domanda di Motherboard.it: Cosa pensi dell'idea della

democrazia diretta e del voto elettronico? La tua è anche una battaglia di principi o solo legata al comportamento del partito M5S?

Risposta dell'hacker: Ancora queste domande. 🙂 Questo non è un hack politico, a me del comportamento del partito non frega niente. Se vuoi è una battaglia di principi informatici. Se ti riferisci ai numeri dei ministri è solo perché fanno rumore, a scapito di Davide [Casaleggio, ndr]. Povero Davide. lol

Si evince la totale e reiterata incapacità a proteggere la piattaforma su cui sono ospitati i dati degli utenti. A valle del data breach condotto dal gruppo LulzSecITA su INAS, in molti hanno contestato che alcuni dati erano stati ottenuti utilizzando SQL Map, un penetration test tool parecchio conosciuto da chi si occupa di cyber security. Parliamo di uno strumento che è stato immesso sulla rete nel 2006 e la cui ultima edizione (la 1.1) risale a gennaio 2017. SQL Map è noto per la sua semplicità di utilizzo e altro non fa che lanciare una raffica diversificata di attacchi contro una banca dati per saggiarne la resistenza; per questo motivo, ad esempio, viene utilizzato per testare la qualità e la sicurezza di un sito web. Usare SQL Map per un attacco dovrebbe essere inutile, perché reso inefficace tramite il corretto sviluppo del codice sorgente. Portare e concludere con successo un attacco con tale strumentazione rivela la completa inadeguatezza tecnologica dell'attaccato e la totale superficialità con cui viene fatta la manutenzione del codice sorgente e dei database. Torniamo al concetto dei controlli: chi scrive ha profondo rispetto e stima per il Garante ma si rende anche conto che probabilmente la struttura di quest'ultimo è pesantemente sotto-organico rispetto a ciò che servirebbe per fronteggiare eventi di questo tipo. Il ruolo del Garante rischia di essere relegato a quello di semplice ammonitore quando invece la completezza delle sue funzioni

sono fondamentali per una gestione corretta delle informazioni.

Il cinque novembre si avvicina: il gruppo hacker LulzSecITA ha già lasciato intendere che ci sarà un altro nuovo e pesante attacco, magari anche con la collaborazione di Anonymous. I due gruppi hanno collaborato spesso insieme e lo hanno fatto dando vita ad AntiSec, un nome che racchiude un concetto fin troppo chiaro (Anti Security). È ragionevole pensare che LulzSecITA sia già in possesso delle informazioni e le stia elaborando per presentarle in maniera massiccia in quella data. Il tweet che hanno pubblicato è abbastanza eloquente e cita un passaggio di "La tempesta" (Shakespeare-Angeli) /Atto primo/Scena seconda. Inoltre, come è stato fatto notare più volte su internet (l'ultima dalla Dott.ssa Claudia Cofini), il 5 novembre è una data rilevante:

"Il 5 novembre rimanda anche alle congiure delle polveri di cui uno dei protagonisti è Guy Fawkes, da cui prende ispirazione la maschera di Anonymous e il film V for Vendetta"

Questa guerra, perché di questo si tratta, è nel pieno svolgimento ed obiettivamente trova fondamento sulla superficialità tecnica e professionale di chi dovrebbe tutelare i dati dei cittadini; citando Sun Tzu: "il generale esperto attacca la strategia del meno esperto. Questa è la prima cosa da fare." La speranza è che il vento cambi e che vi sia maggiore senso di responsabilità nel trattare queste informazioni, tenendo sempre a mente che il valore di un'azienda è data dalle informazioni in suo possesso e speriamo che il vento cambi in fretta.

Riferimenti utili

Intervista dell'hacker R0gue0 al sito Motherboard.it: https://motherboard.vice.com/it/article/3ke8qj/rousseau-hack-r

ogue0-intervista-movimento-5-stelle

A cura di: **Edoardo Limone**

L’articolo La silente guerra degli hacker italiani proviene da ICT Security Magazine.

https://www.ictsecuritymagazine.com/articoli/la-silente-guerra-degli-hacker-italiani/