Intrusioni anche nei sistemi della Dia “Ma i dati acquisiti erano pubblici”

Raid informatico alla Direzione investigativa antimafia, verifiche per capire quanto pervasivo Inchieste a Roma e Milano. L’opposizione attacca il governo: taglia i fondi alla cybersicurezza

di **ALESSANDRA ZINITI**
ROMA

Abbiamo *firewall* di alto livello, fino ad ora non sono stati rilevati assalti hacker ai nostri dati sensibili. Non siamo preoccupati e, tuttavia, per averne assoluta certezza, stiamo facendo tutte le verifiche del caso».

La Direzione investigativa antimafia ridimensiona l’ultimo allarme hacker scattato ieri mattina dopo la pubblicazione, sul dark web, di un annuncio di vendita di 302 file che sarebbero stati sottratti alla banca dati: dossier su 25 gruppi criminali, notizie di intelligence di interesse di Europol, registri di indagine e del personale, documenti finanziari, fotografie inedite e comunicati stampa sotto embargo. Pagamento richiesto agli interessati da “Weykofa” (questo il nickname del venditore) in Bitcoin e Moreno,le criptovalute usate dagli hacker. Ma, dopo verifiche approfondite, l’ipotesi più accreditata è che i file in vendita contengano solo dati pubblici e già presenti sul web, acquisiti dal sito della Dia.

La preoccupazione, però, resta alta. Perché il numero degli attacchi all’attenzione delle Procure italiane, a cominciare da quella di Roma, è assai più alto di quello che si sa e perché l’escalation di questi ultimi giorni è ritenuta dagli esperti una vera e propria strategia della tensione capace di creare panico, interrompere servizi di prima necessità, destabilizzare. Procurato allarme e pubblica intimidazione i reati ipotizzati dalla Procura di Milano che indaga sui quattro allarmi-bomba che la scorsa settimana hanno interessato la Lombardia.

I PRECEDENTI

1 I sistemi di refrigerazione
Lunedì scorso i banchi frigo di diversi supermercati in Italia e all’estero sono andati in tilt, la temperatura modificata dagli hacker



2 Gli allarmi-bomba
Trentacinque i voli per i quali è stato dichiarato il rischio di un ordigno a bordo,alcuni scortati a terra dai jet

3 La lista nera dei Noname
Pubblicati sul dark web i dati sensibili di 18 persone, “nemici della Russia,” tra cui il ministro degli Esteri Tajani

Da qui l’urgenza di una puntuale analisi e valutazione del rischio che il ministro dell’Interno Piantedosi ha chiesto agli specialisti dell’Intelligence e della Polizia postale. «Ho convocato il Comitato nazionale per l’ordine e la sicurezza pubblica non perché vi sia un’emergenza in atto tale da destare preoccupazione, ma perché faremo una valutazione delle eventuali ricadute sulla sicurezza pubblica degli episodi di attacchi hacker – spiega Piantedosi – Ci sono state alcune presenze sul dark web di richieste di dati riguardanti personalità importanti come il ministro degli Esteri, il procuratore di Roma e il capo del servizio di polizia postale. È giusto cercare di capire cosa c’è dietro e, soprattutto, quali ricadute possano esserci sulla sicurezza per mettere in campo i rimedi che devono essere approntati.



Pubblica amministrazione, sanità, tecnologico e manifatturiero. Password deboli, accessi da remoto impropriamente configurati, credenziali di posta elettronica. Eccole le fragilità che il sistema Italia offre ai gruppi di hacker. Il monitoraggio delle vulnerabilità partirà dall’ultimo report del *Computer security incident response team* dell’agenzia per la cybersicurezza nazionale che rileva mensilmente minacce e incidenti sulla rete. Correre ai ripari, chiudere le falle nei sistemi informatici della pubblica amministrazione, obbligare a protocolli più stringenti aziende e società che gestiscono ospedali e infrastrutture le priorità. Per le quali,però, servono risorse.

Quindici milioni l’anno in meno al Fondo di Strategia nazionale, accusano le opposizioni. «Il governo ha definanziato la cybersicurezza e butta 14 miliardi di euro in armi e difesa», accusa il presidente M5s Giuseppe Conte. E Angelo Bonelli di Avs invita il governo a «concentrarsi sulla difesa dell’Italia dagli hacker e venire a spiegare al Parlamento quale sia la sua strategia». La maggioranza taglia corto: «L’aumento dei fondi per la Difesa serve anche a contrastare la minaccia ibrida».

©RIPRODUZIONE RISERVATA

IL RITRATTO

I NoName italiani affiliati dai russi che puntano aerei, porti e banche

di **GIULIANO FOSCHINI**

Dalle carte dell’indagine nella Capitale emerge il profilo dei pirati. Non sono geni del web, a volte basta avere un computer

Sono ragazzi italiani. Alcuni giovanissimi, altri figli di immigrati, cresciuti nel nostro Paese. Hanno competenze informatiche discrete, ma non sono geni del computer. Si incontrano nelle chat Telegram filorusse, scaricano un programma, ricevono un obiettivo. E attaccano. A volte per convinzione politica, altre per il gusto di partecipare a qualcosa di più grande. Quasi sempre gratis. Perché per mandare temporaneamente in tilt il sito di un ministero, di una banca o di un aeroporto, e dunque creare disagi e paure, non servono necessariamente sofisticate conoscenze informatiche. Basta mettere il proprio computer a disposizione di una macchina molto più grande. Quella degli hacker di NoName057(16), il collettivo filorusso che da anni prende di mira l’Occidente.

A raccontare chi siano i suoi fiancheggiatori italiani è un’indagine della Procura di Roma e della Polizia postale, arrivata alla fase conclusiva. Un’inchiesta delicatissima, con il coordinamento della Procura antiterrorismo guidata da Giovanni Melillo, con il sostituto Eugenio Albamonte. La stessa attività investigativa che ha contribuito a far finire nel mirino della propaganda russa il procuratore capo di Roma, Franco Lo Voi, e il capo della Postale, Ivano Gabrielli. La prima sorpresa riguarda proprio il profilo degli indagati. Non militanti organizzati. Piuttosto ragazzi reclutati attraverso Telegram, in una galassia digitale nella quale propaganda politica, attivismo e piccoli attacchi informatici finiscono per confondersi. Il sistema si chiama DDosia. È una piattaforma che consente a NoName di moltiplicare la potenza degli attacchi utilizzando i computer dei volontari. Il meccanismo è relativamente semplice: vengono indicati gli obiettivi, gli utenti scaricano uno strumento automatizzato e i loro dispositivi cominciano a inviare contemporaneamente enormi quantità di richieste ai server prescelti. Sono gli attacchi DDoS: non rubano informazioni, ma quella mole di dati punta a rendere irraggiungibili i siti, anche per ore. E soprattutto permettono di rivendicare un colpo contro un’istituzione occidentale.





Alcune immagini postate sul web dagli hacker del collettivo Noname057(16)

C’è anche un sistema di ricompense. Piccole somme in criptovalute, talvolta poche decine di euro, trasferite attraverso servizi finanziari online. Ma gli investigatori non hanno individuato pagamenti di questo tipo per gli italiani coinvolti nell’inchiesta. Gli obiettivi, invece, erano tutt’altro che marginali. Nell’elenco ricostruito dagli investigatori compaiono gli aeroporti di Malpensa e Linate, il ministero degli Esteri, Intesa Sanpaolo, Monte dei Paschi, la Consob, i porti di Taranto e Trieste. E ancora Carabinieri, Marina, Aeronautica, trasporti pubblici: l’Atac di Roma, l’Amat di Palermo, l’Amt di Genova.

Per arrivare ai responsabili è servita un’operazione internazionale. Quindici Paesi, con il coordinamento di Eurojust e la collaborazione di Europol, Interpol e Fbi. Un passaggio decisivo è stato l’esame di un database della rete, localizzato in Russia e condiviso dagli investigatori svizzeri. Nell’agosto 2024, durante l’operazione Eastwood, la polizia spagnola è riuscita a collegare nove account Telegram ad altrettanti numeri telefonici italiani. Dalla Francia sono arrivate tracce relative ad altri nove account, dagli Stati Uniti elementi su ulteriori tre soggetti. Un lavoro di incrocio tra identità digitali, indirizzi Ip e utenze telefoniche che ha consentito di individuare i presunti partecipanti italiani.

Ad alcuni di loro sono stati già notificati gli avvisi di conclusione delle indagini: rischiano il processo. Altre posizioni sono state archiviate. I loro amici, intanto, hanno già rilanciato: stesso metodo, nuove campagne, diversi o biettivi.

©RIPRODUZIONE RISERVATA