9colonne
Agenzia Giornalistica
direttore Paolo Pagliaro

Un hacker svela i segreti delle truffe informatiche

di Giovanni Criscione

L'attacco informatico che dal 1° agosto tiene offline i siti della Regione Lazio è nato "dalla violazione dell'utenza di un dipendente in smartworking" e la vulnerabilità ha consentito agli attaccanti di "criptare anche il backup dei dati". L'assessore regionale alla Salute Alessio D'Amato, in un'intervista a Repubblica, ha dichiarato che l'attacco è partito "dalla violazione di un'utenza di un dipendente in smartworking", sottolineando che gli attaccanti "hanno colpito in un momento particolare, quando il livello di attenzione si abbassa", come avviene col lavoro da remoto. La violazione ha consentito agli hacker di arrivare ai livelli di backup dei dati, criptandoli. "Sono state cambiate le chiavi della porta che fa accedere al Ced, il sistema che gestisce la prenotazione dei vaccini, i dati sanitari, le pratiche edilizie e molti servizi al cittadino". Quello che l'assessore non dice è che si è trattato di un attacco sferrato con tecniche di Social Engineering.

Per capire meglio di cosa stiamo parlando, risulta illuminante la lettura del libro "Lord Kelly - il ladro di informazioni" (Booksprint edizioni) di Corrado Fabbri, pubblicato lo scorso giugno e che, con un tempismo perfetto per le cronache di questi giorni, arriva ora nelle librerie e nei bookshop online. Corrado Fabbri (Bologna, 1970), al suo esordio come scrittore, è considerato dalla stampa internazionale e dalle forze dell'ordine uno degli hacker e ingegneri sociali più temuti degli ultimi decenni. Ha accumulato una fortuna violando i sistemi informatici di banche, governi e industrie su commissione di servizi governativi e aziende rivali. Ha subito oltre 80 processi per 290 violazioni al codice penale per truffe telematiche e furti di dati, ottenendo condanne a 15 anni di carcere, poi ridotti a 10 tra indulti e sconti di pena. Nel mezzo, due fughe e una vita da brividi. Pur avendo pagato il suo debito con la giustizia, oggi l'autore vive all'estero sotto falso nome «perché non ti mollano più, ti marchiano a fuoco come una vacca e non ti lasciano vivere». Il libro è stato scritto durante la detenzione, tra il 2002 e il 2014, per poi essere affidato alle stampe di recente, dopo gli ultimi rimaneggiamenti.

In questo libro autobiografico racconta coraggiosamente la propria vita avventurosamente vissuta oltre i confini della legalità e rivela gli stratagemmi, i metodi, le tecniche utilizzate in prima persona per violare dietro lauto compenso i sistemi informatici più inaccessibili di governi, banche, aziende in tutto il mondo per conto di agenzie governative, istituti finanziari e aziende rivali. Il tema che l'autore affronta è di scottante attualità. Il 2020, infatti, è stato un anno da record per i crimini informatici. A livello globale gli attacchi informatici di pubblico dominio classificati come gravi sono cresciuti del 12% rispetto all'anno precedente, del 66% rispetto al 2017 (fonte: Rapporto Clusit 2021). Ed è solo la punta di un iceberg: un gran numero di aggressioni non diventa mai di dominio pubblico. Nessuno può dirsi al sicuro dai pirati informatici. Non a caso tra i settori più colpiti ci sono la pubblica amministrazione, le forze dell'ordine, le forze armate, l'intelligence e le istituzioni, le multinazionali operanti nel campo della sanità e della ricerca farmaceutica, le banche e il mondo dell'alta finanza, i produttori di tecnologie hardware e software. Cioè a dire proprio quei settori che si fondano sulla sicurezza dei dati. I cyber attacchi sfruttano diverse tecniche, note solo in parte.

Diversamente da quello che potrebbe pensare, le vulnerabilità o le falle che gli hacher sfruttano per insinuarsi nei server non sempre si trovano nei sistemi informatici. Molto spesso il tallone d'Achille di un'organizzazione sta proprio nella componente umana. Di questo si occupa la Social Engineering o Ingegneria sociale, settore di elezione di Corrado Fabbri. Con "Ingegneria sociale" si indicano le tecniche hacker atte a ingannare il personale di una società, di una banca o di un ente governativo, inducendolo a rivelare informazioni sensibili, grazie alle quali penetrare nei sistemi di sicurezza più inaccessibili. Le informazioni essenziali possono essere carpite in vari modi: persino nei cestini dell'immondizia possono trovarsi fogli appallottolati con promemoria di password, codici, numeri di telefono, dati sensibili, ecc. . Per aumentare la sicurezza, dunque, occorre rafforzare i sistemi informatici ma anche addestrare il personale a tenere comportamenti corretti e a saper riconoscere un attacco informatico. Sopratutto è il personale che opera ai livelli più bassi dell'organizzazione - stagisti, impiegati, segretarie, addetti alle pulizie, sorveglianti - ad essere più esposto e meno preparato ad attacchi con le tecniche della Social Engineering. Non a caso, l'autore racconta a mo' di esempio diversi attacchi messi a segno nei confronti di multinazionali, banche e industrie - camuffando i nomi dei malcapitati e delle aziende - e poi ne analizza la dinamica. Nel libro Fabbri racconta la passione per la tecnologia informatica, la laurea in Information Technology all'università di Miami in Florida, l'ascesa nel mondo degli hacker, dalle prime innocenti violazioni informatiche fino agli attacchi più articolati nel campo dello

Italiani nel

NOVE COLONNE ATG

- MADE IN ITALY: IL DE NEI MERCATI DEI SA (4)
- MADE IN ITALY: IL DE NEI MERCATI DEI SA (3)
- MADE IN ITALY: IL DE NEI MERCATI DEI SA (2)
- MADE IN ITALY: IL DE NEI MERCATI DEI SA (1)

NOVE COLONNE ATG /

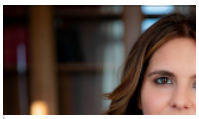
- Ultimo numero
- Archivio notiziario

I RITORNATI

Al via la serie 'I ri di emigrazione vi

spionaggio industriale, remunerati con cifre da capogiro. Le straordinarie competenze informatiche, l'attenta pianificazione alla ricerca dei punti deboli di un sistema e l'abilità psicologica nel manipolare gli altri, quasi elevate ad arte, unite a un'etica del crimine («Ho sempre e solo aggredito aziende o persone che potessero reggere il colpo. [...] Nessun stipendiato delle holding o delle grandi banche che ho ripulito, [...] ha mai dovuto rinunciare neppure a un solo pasto per causa mia»), hanno fatto di Corrado Fabbri una sorta di Arsenio Lupin delle truffe informatiche. L'autore, però, mette in guardia il lettore dal volerlo seguire sui sentieri dell'illegalità. Le sue azioni, infatti, gli sono costate un decennio di sofferenze e di tormenti dietro le sbarre, seguite da un difficile periodo di sfiducia e isolamento. Nel libro c'è anche una dura requisitoria contro il sistema carcerario italiano, ancora lontano dall'essere uno strumento di riabilitazione e reinserimento degli ex detenuti nella società. Solo dopo lungo tempo, l'autore ha ristabilito un corretto rapporto con la società e riscoperto il valore della libertà e l'importanza dell'amore e degli affetti, sole cose in grado di dare un senso alla nostra vita. La ritrovata serenità e la volontà di rimediare in qualche modo alla sofferenza causata con la sua passata attività spingono l'autore, che oggi fornisce consulenze sulla sicurezza informatica per società e aziende in tutto il mondo, a suggerire trucchi validi e buone pratiche per prevenire il rischio di attacchi informatici e furti di dati. Suggerimenti tanto più preziosi, questi, dal momento che sono il frutto dell'esperienza di uno degli hacker e ingegneri sociali più temuti nel mondo.

PROTAGONISTI



Green pass, Sirag
Governo faccia ch
Aire vaccinati all'

10/8/2021

STUDY IN ITALY

SPECIALI PER L'ESTER

DOCUMENTI

DONNE D'ITALIA

Gic
dei

Cat
XXI

La
Bat
la r