

## **Capitolo 1: Definizione e fondamenti dell'hacking**

L'hacking informatico rappresenta, nella sua definizione più pura e tecnica, l'insieme delle procedure volte a comprendere, manipolare o superare le limitazioni operative di un sistema di elaborazione dati o di una rete di telecomunicazioni.

Sebbene la cultura di massa e i media generalisti associno spesso il termine a condotte esclusivamente criminali, l'origine del fenomeno affonda le sue radici nella curiosità intellettuale e nella ricerca delle vulnerabilità logiche dell'infrastruttura tecnologica. Un hacker è essenzialmente uno specialista capace di esaminare il codice sorgente, l'architettura hardware o le configurazioni di rete per individuare falle di sicurezza che gli sviluppatori originali non avevano previsto.

Dal punto di vista operativo, la disciplina si suddivide in differenti metodologie di approccio. L'hacking etico, condotto da professionisti noti nel settore come white hat, viene autorizzato dai proprietari dei sistemi con l'obiettivo preventivo di testare le difese ed eliminare i punti deboli prima che possano essere sfruttati. Al contrario, l'hacking malevolo, praticato dai cosiddetti black hat o cracker, persegue scopi di lucro, spionaggio, sabotaggio o distruzione dei dati. Esiste inoltre una zona grigia, popolata dai gray hat, i quali violano le difese senza formale autorizzazione ma senza fini apertamente distruttivi, spesso per dimostrare le proprie capacità o per segnalare pubblicamente la falla.

I meccanismi di aggressione informatica non si limitano all'analisi del codice software. Un elemento fondamentale dell'hacking riguarda la componente umana, nota come ingegneria sociale. Attraverso tecniche di manipolazione psicologica, come il phishing o il pretexting, l'aggressore convince gli utenti legittimi a cedere credenziali riservate o ad accedere a collegamenti compromessi. Parallelamente, gli attacchi puramente tecnici spaziano dall'iniezione di codice maligno nei database all'esecuzione di malware di vario tipo (come trojan, worm o ransomware), fino all'intercettazione dei flussi di comunicazione privi di cifratura adeguata.

Comprendere l'hacking significa quindi superare la semplificazione cinematografica per analizzare un confronto costante tra ingegneria della difesa e creatività dell'attacco.

## **Capitolo 2: Kevin Mitnick e la grande caccia degli anni Novanta**

Gli anni Novanta hanno visto la consacrazione mediatica di Kevin Mitnick, noto negli ambienti telematici con lo pseudonimo di Condor, una delle figure più emblematiche e controverse della storia dell'informatica. La traiettoria di Mitnick si è distinta non tanto per la scrittura di codice particolarmente sofisticato, quanto per una padronanza straordinaria delle tecniche di ingegneria sociale e del phreaking, la manipolazione delle reti telefoniche analogiche e digitali. Sfruttando la persuasione telefonica e la capacità di impersonare tecnici del settore, Mitnick è riuscito a penetrare nei sistemi riservati di colossi della tecnologia come Motorola, Fujitsu, Nokia, Sun Microsystems e Digital Equipment Corporation, sottraendo codice sorgente riservato e software aziendali di enorme valore.

La sua attività, trasformata in una vera e propria sfida alle autorità federali statunitensi, ha portato all'emissione di molteplici mandati di cattura e a una prolungata latitanza iniziata nel 1992. Durante la fuga, Mitnick ha continuato a violare reti informatiche utilizzando identità contraffatte e cellulari modificati per evitare la localizzazione geografica. Il punto di svolta della sua vicenda è avvenuto durante il periodo natalizio del 1994, quando ha deciso di violare il computer personale di Tsutomu Shimomura, uno dei massimi esperti mondiali di sicurezza informatica dell'epoca.

Shimomura, profondamente irritato dall'intrusione e dal furto di strumenti di analisi di sua proprietà, ha deciso di collaborare direttamente con l'FBI e con i tecnici della compagnia telefonica AT&T per rintracciare l'incursore. Attraverso l'uso di apparati di misurazione dei segnali radio e l'analisi dei log di connessione, la squadra di ricerca è riuscita a triangolare la posizione di Mitnick in un complesso residenziale a Raleigh, in Carolina del Nord. Il 15 febbraio 1995 le forze dell'ordine hanno fatto irruzione nel suo appartamento, ponendo fine a una caccia durata oltre due anni. Arrestato e condannato a cinque anni di reclusione, Mitnick ha successivamente convertito le sue competenze fondando una nota società di consulenza per la sicurezza aziendale.

### **Capitolo 3: David L. Smith e l'epidemia del worm Melissa**

Nel marzo del 1999 la diffusione capillare della posta elettronica aziendale e domestica è stata teatro di una delle prime vere epidemie informatiche su scala globale. L'autore dell'attacco, il programmatore americano David L. Smith, ha creato e distribuito un codice malevolo denominato Melissa, chiamato così in omaggio a una ballerina incontrata durante un viaggio in Florida. Questo attacco ha dimostrato per la prima volta la pericolosità dell'automazione dei processi informatici unita alla fiducia implicita riposta dagli utenti nelle comunicazioni digitali provenienti da contatti conosciuti.

Il funzionamento del malware Melissa si basava su una struttura apparentemente semplice ma devastante dal punto di vista diffusivo. Il programma si presentava sotto forma di un file di documento per Microsoft Word allegato a un messaggio di posta elettronica. Il messaggio prometteva un elenco di password d'accesso a siti web riservati. Quando la vittima aprendo il documento eseguiva la macro nascosta al suo interno, il malware prendeva il controllo dell'applicazione di posta Microsoft Outlook. Sfruttando la rubrica del computer infetto, il worm inviava automaticamente una copia di se stesso ai primi cinquanta contatti presenti nell'elenco.

La progressione geometrica dei messaggi generati ha saturato i server di posta elettronica di migliaia di aziende, istituzioni finanziarie e agenzie governative in tutto il mondo, costringendo società come Microsoft, Intel e Lucent Technologies a disattivare temporaneamente le proprie infrastrutture di comunicazione per arginare l'infezione. I danni complessivi stimati hanno superato gli ottanta milioni di dollari. L'identificazione del responsabile è avvenuta in tempi relativamente brevi grazie alla collaborazione tra la polizia dello Stato del New Jersey e l'FBI. Gli investigatori sono riusciti a tracciare il codice sorgente originale analizzando i metadati del documento Word, i quali contenevano l'indirizzo di identificazione dell'hardware utilizzato per la creazione del file. David L. Smith è stato arrestato il primo aprile 1999 e condannato a venti mesi di prigione federale oltre al pagamento di una pesante sanzione pecuniaria.

## **Capitolo 4: Michael Calce e l'attacco MafiaBoy che oscurò la rete**

Nel febbraio del 2000 l'architettura di internet ha subito una dimostrazione di vulnerabilità senza precedenti, capace di paralizzare i principali portali del commercio elettronico e dell'informazione mondiale. Il responsabile di questa operazione, nota con il nome in codice Rivolta, non era un gruppo strutturato o un servizio di intelligence statale, bensì un adolescente canadese di soli quindici anni di nome Michael Calce, conosciuto nella comunità clandestina con lo pseudonimo di MafiaBoy. L'evento ha evidenziato in modo drammatico l'impatto dei primi attacchi di tipo Denial of Service distribuito, comunemente indicati con l'acronimo DDoS. L'operazione ideata da Calce si è articolata attraverso la compromissione preliminare di centinaia di reti informatiche universitarie, le cui apparecchiature disponevano di connessioni ad alta velocità rare per l'epoca. Inserendo un software di controllo remoto all'interno dei server vulnerabili delle università, Calce ha creato una rete di macchine asservite, ponendo le basi per la generazione di flussi imponenti di traffico artificiale. A partire dal 7 febbraio 2000, l'adolescente ha sferrato un attacco coordinato contro Yahoo, all'epoca il motore di ricerca e portale web più visitato del pianeta, facendolo crollare per diverse ore. Nei giorni successivi l'offensiva si è estesa ad altri giganti dell'economia digitale, inclusi Amazon, eBay, CNN, Dell e E Trade. La saturazione delle linee di comunicazione rendeva impossibile agli utenti legittimi accedere ai servizi, provocando perdite economiche stimate in oltre 1,2 miliardi di dollari e una profonda crisi di fiducia dei mercati finanziari nei confronti dell'infrastruttura di internet. L'FBI e le autorità canadesi hanno avviato una caccia all'uomo culminata con l'arresto di Calce nel mese di aprile del 2000. L'identificazione del giovane non è avvenuta attraverso tracciamenti complessi della rete, ma a causa delle sue estese vanterie nelle chat IRC frequentate da altri hacker. Trattato come un minore dalle leggi canadesi, Calce è stato condannato a otto mesi di detenzione in una struttura giovanile.

## **Capitolo 5: Gary McKinnon e le intrusioni nei server militari americani**

Tra il febbraio del 2001 e il marzo del 2002 i sistemi informatici della difesa e dell'esplorazione spaziale degli Stati Uniti sono stati oggetto di una prolungata serie di intrusioni silenziose condotte da una sola persona. L'autore di queste azioni era Gary McKinnon, un amministratore di sistemi britannico che operava dalla sua abitazione a Londra utilizzando l'identità virtuale di Solo. La peculiarità del caso McKinnon risiede sia nella portata eccezionale della penetrazione, definita dalle autorità americane come il più grande attacco informatico militare di tutti i tempi, sia nelle motivazioni dichiarate dall'hacker, lontano dalle classiche logiche del profitto finanziario.

McKinnon era ossessionato dalla convinzione che le istituzioni governative statunitensi nascondessero tecnologie avanzate legate all'energia libera e all'esistenza di velivoli extraterrestri. Per verificare la sua ipotesi, l'amministratore britannico ha esaminato cinquantatré reti informatiche appartenenti alla Marina, all'Esercito, all'Aeronautica, al Ministero della Difesa degli Stati Uniti e alla NASA. La metodologia impiegata per superare le barriere d'accesso non richiedeva malware sofisticati: McKinnon utilizzava script scritti in linguaggio Perl per individuare macchine Windows prive di password di amministrazione o protette da credenziali predefinite mai modificate dal personale della difesa.

Una volta ottenuto il controllo degli apparati, McKinnon cercava file riservati, cancellava log di sistema e in alcuni casi lasciava messaggi polemici sui desktop delle autorità militari. L'intrusione ha causato l'inoperatività della rete informatica del distretto militare di Washington per tre giorni e l'interruzione dei sistemi di controllo delle munizioni della Marina in un momento critico dopo gli eventi dell'11 settembre 2001. Tracciato tramite l'analisi dei suoi indirizzi IP di connessione, McKinnon è stato arrestato dalla polizia britannica nel 2002. L'estradizione negli Stati Uniti, dove rischiava una pena fino a settanta anni di carcere, è stata al centro di una dura battaglia legale conclusasi solo nel 2012, quando il governo britannico ne ha bloccato il trasferimento per ragioni umanitarie e sanitarie.

## **Capitolo 6: Albert Gonzalez e il furto di massa di carte di credito**

La seconda metà degli anni Duemila ha segnato la transizione dell'hacking da fenomeno prevalentemente dimostrativo o vandalico a vera e propria industria del crimine organizzato a scopo di lucro. Il simbolo di questo cambiamento è Albert Gonzalez, un giovane informatico di Miami noto con gli pseudonimi di SoupNazi e Segvec. Gonzalez è stato la mente strategica dietro le più ingenti sottrazioni di dati finanziari della storia, arrivando a compromettere oltre centosessanta milioni di numeri di carte di credito e di debito appartenenti a cittadini americani ed europei. La carriera di Gonzalez si è sviluppata su un doppio binario paradossale. Dopo essere stato arrestato nel 2003 per frodi informatiche, il giovane era diventato un informatore retribuito del Secret Service americano, aiutando le autorità a smantellare ShadowCrew, un portale clandestino dedicato al commercio di dati rubati. Tuttavia, mentre collaborava con gli investigatori federali percependo un lauto stipendio, Gonzalez gestiva in segreto una propria rete criminale internazionale composta da hacker russi ed europei. Il gruppo si era specializzato nelle intrusioni all'interno delle reti aziendali delle più importanti catene commerciali degli Stati Uniti, tra cui TJX Companies, OfficeMax e Barnes & Noble. Il metodo privilegiato dal gruppo per penetrare nelle infrastrutture aziendali consisteva nello sfruttamento delle vulnerabilità nei protocolli di cifratura dei sistemi radio WiFi dei punti vendita, il cosiddetto wardriving. Una volta collegatosi alle reti dei negozi, Gonzalez installava programmi capaci di intercettare in tempo reale i dati delle transazioni finanziarie mentre passavano dai registratori di cassa ai server centrali. L'operazione più clamorosa è stata condotta nel 2007 contro Heartland Payment Systems, una società di elaborazione dei pagamenti. Sfruttando un'iniezione di codice SQL sul sito dell'azienda, il gruppo ha installato un software spia nella rete interna, sottraendo centotrenta milioni di carte. Arrestato nel maggio del 2008 in un albergo di Miami dove custodiva un milione di dollari in contanti sotterrati nel giardino dei genitori, Gonzalez è stato condannato nel 2010 a venti anni di reclusione federale.

## **Capitolo 7: Stuxnet e la nascita del sabotaggio cybernetico statale**

Nel giugno del 2010 il mondo della sicurezza informatica è entrato in una nuova era con la scoperta di Stuxnet, il primo malware concepito esplicitamente come arma digitale per la distruzione fisica di infrastrutture industriali critiche. Sviluppato congiuntamente dalle intelligence di Stati Uniti e Israele nell'ambito di un'operazione coperta, Stuxnet aveva l'obiettivo di sabotare il programma nucleare iraniano senza scatenare un conflitto armato convenzionale. L'attacco è stato diretto in modo specifico contro la centrale di arricchimento dell'uranio di Natanz, in Iran. A differenza dei malware convenzionali orientati allo spionaggio o al furto di credenziali, Stuxnet mostrava una complessità ingegneristica mai vista in precedenza. Il codice sfruttava ben quattro vulnerabilità sconosciute, denominate in gergo zero day, oltre a certificati digitali autentici rubati a rinomate aziende taiwanesi per eludere i controlli dei sistemi operativi Windows. Per penetrare all'interno della rete di Natanz, totalmente isolata da internet per motivi di sicurezza, gli ideatori hanno impiegato dispositivi di memoria USB infetti introdotti inconsapevolmente da tecnici di ditte esterne.

Una volta diffuso nella rete target, Stuxnet cercava specifici controllori logici programmabili della marca Siemens, utilizzati per regolare la velocità di rotazione delle centrifughe a gas per l'arricchimento dell'uranio. Il malware alterava la frequenza dei motori delle centrifughe, facendole accelerare e decelerare a livelli distruttivi fino alla rottura meccanica del rotore. Contemporaneamente, il programma inviava ai sistemi di monitoraggio dei tecnici iraniani segnali falsi che mostravano un funzionamento del tutto regolare. L'operazione ha portato alla distruzione fisica di circa mille centrifughe iraniane, ritardando significativamente il programma nucleare di Teheran. La scoperta di Stuxnet, avvenuta a causa della diffusione involontaria di una variante del codice al di fuori dell'impianto, ha confermato che l'hacking si era ormai trasformato in una componente fondamentale della geopolitica militare.

## **Capitolo 8: Hector Monsegur e la meteora devastante di LulzSec**

Nel corso del 2011 una serie di attacchi informatici coordinati ha sconvolto grandi corporazioni, agenzie governative e organizzazioni di sicurezza in tutto il globo. La responsabilità di questa campagna di devastazione digitale fu rivendicata da LulzSec, un gruppo ristretto composto da sei individui scaturito dalla galassia di Anonymous. Il leader carismatico e portavoce del gruppo si faceva chiamare Sabu, identità dietro la quale si celava Hector Xavier Monsegur, un bravo programmatore disoccupato residente nei complessi di edilizia popolare di New York.

Guidati dal motto di agire per puro divertimento e per mettere in piazza l'incompetenza delle grandi aziende, i membri di LulzSec hanno intrapreso una campagna di attacchi durata esattamente cinquanta giorni. Nel loro percorso di incursioni hanno violato i server di Sony Pictures, sottraendo dati personali di oltre un milione di utenti, hanno reso inaccessibile il sito pubblico della CIA mediante attacchi di saturazione, hanno sottratto informazioni riservate dai database della rete televisiva Fox, della polizia federale americana e del Senato degli Stati Uniti. Le loro azioni erano accompagnate da un uso spregiudicato delle piattaforme social, dove pubblicavano i dati rubati sbeffeggiando apertamente le vittime.

Ciò che il gruppo non sapeva era che l'FBI era arrivata a identificare Sabu già nel giugno del 2011 a causa di una disattenzione nell'uso dei suoi indirizzi IP di connessione. Messo di fronte alla prospettiva di una condanna a decine di anni di prigione e alla perdita della custodia dei suoi familiari, Monsegur ha accettato di trasformarsi immediatamente in un informatore sotto copertura della polizia federale. Per mesi Sabu ha continuato a dirigere le operazioni di LulzSec e di altre formazioni correlate mentre ogni singola conversazione, strumento e bersaglio veniva registrato in tempo reale dagli agenti dell'FBI. La collaborazione di Monsegur ha consentito alle autorità americane ed europee di identificare e arrestare tutti i principali componenti del gruppo tra il 2012 e il 2013, svelando la totale infiltrazione statale all'interno del collettivo hacker più temuto del momento.

## **Capitolo 9: Edward Snowden e le rivelazioni sulla sorveglianza globale**

Nel giugno del 2013 la percezione globale della riservatezza e della sicurezza informatica è stata radicalmente trasformata dalla più grande fuga di notizie della storia dell'intelligence moderna. Il protagonista dell'operazione è stato Edward Snowden, uno specialista informatico ed ex analista della CIA che lavorava come consulente esterno per la National Security Agency statunitense presso il centro direzionale delle Hawaii. Sfruttando le sue credenziali di amministratore di sistema, Snowden ha eseguito un'infiltrazione interna mirata, prelevando centinaia di migliaia di documenti Top Secret dalle banche dati della sicurezza americana. L'azione di Snowden, che può essere classificata come un attacco dall'interno basato sul superamento dei privilegi d'accesso aziendali, non mirava al danneggiamento dei sistemi o al guadagno economico, ma alla divulgazione pubblica dell'esistenza di una rete di sorveglianza di massa globale. I documenti sottratti, successivamente consegnati a giornalisti di testate internazionali come The Guardian e The Washington Post, hanno rivelato programmi segreti come PRISM e XKeyscore. Questi sistemi permettevano alle agenzie d'intelligence anglosassoni di intercettare direttamente nei dorsali di fibra ottica e nei server delle maggiori compagnie tecnologiche (come Google, Microsoft, Apple e Yahoo) le comunicazioni private di centinaia di milioni di cittadini in tutto il pianeta.

Le rivelazioni di Snowden hanno dimostrato che l'hacking non era soltanto una pratica riservata ad attori clandestini o criminali, ma costitutiva dell'architettura operativa degli stessi Stati democratici. La fuga di informazioni ha costretto i colossi tecnologici ad adottare protocolli di cifratura end to end di default su larga scala per proteggere i propri clienti da intrusioni governative indiscrete. Snowden, fuggito inizialmente a Hong Kong e poi bloccato a Mosca a causa della revoca del suo passaporto americano, è stato incriminato negli Stati Uniti per spionaggio e furto di beni statali, trasformandosi in una figura spartiacque della cultura informatica globale.

## **Capitolo 10: The Impact Team e il ricatto digitale ad Ashley Madison**

Nel luglio del 2015 il mondo delle violazioni informatiche ha registrato un salto di qualità distruttivo con l'attacco mirato alla società Avid Life Media, proprietaria di Ashley Madison, una piattaforma online di incontri per persone coniugate. Un gruppo di hacker rimasto anonimo sotto la denominazione di The Impact Team è riuscito a penetrare completamente nelle reti interne dell'azienda, sottraendo l'intero database contenente le informazioni personali, gli archivi di pagamento e il codice sorgente del portale.

A differenza delle tradizionali violazioni indirizzate al furto di credenziali bancarie, The Impact Team ha utilizzato i dati personali sottratti come strumento di ricatto etico e reputazionale. Gli aggressori hanno intimato alla proprietà aziendale la chiusura immediata e definitiva del sito Ashley Madison e di un portale affiliato, denunciando le pratiche commerciali ingannevoli della società (tra cui la vendita di un servizio di cancellazione dei dati personali che in realtà manteneva i record nei server e l'uso intensivo di profili falsi generati da bot per attirare clienti maschili). Di fronte al rifiuto della società di cedere al ricatto, nel mese di agosto del 2015 The Impact Team ha pubblicato sul dark web oltre trenta gigabyte di dati riservati. La fuga di informazioni ha reso pubblici nomi, indirizzi di posta elettronica, preferenze personali, dettagli delle transazioni finanziarie e geolocalizzazioni di oltre trentasette milioni di iscritti. Le conseguenze del diffuso smascheramento sono state devastanti sia sul piano umano che aziendale: l'evento ha provocato licenziamenti, disgregazioni familiari, tentativi di estorsione secondaria contro le singole vittime e casi segnalati di suicidio. L'attacco ad Ashley Madison ha dimostrato che il valore strategico dei dati informatici risiede spesso nella loro capacità di distruggere la reputazione e la vita privata degli individui.

## **Capitolo 11: WannaCry e la piaga globale dei ransomware**

Il maggio del 2017 ha segnato il punto di massimo impatto per la minaccia dei ransomware, codici malevoli progettati per cifrare i dati contenuti in un sistema e chiedere un riscatto in criptovalute per la chiave di sblocco. Il protagonista di questa crisi globale è stato il malware WannaCry, la cui velocità di infezione è stata resa possibile dall'integrazione di strumenti di spionaggio militare sottratti alle agenzie d'intelligence e successivamente resi pubblici dal gruppo clandestino The Shadow Brokers.

Il cuore tecnologico di WannaCry conteneva un exploit chiamato EternalBlue, sviluppato in origine dalla National Security Agency americana per penetrare nei sistemi Windows non aggiornati sfruttando una falla nel protocollo di condivisione file Server Message Block. Quando gli autori del ransomware (successivamente identificati dagli inquirenti internazionali nei servizi di spionaggio della Corea del Nord, noti come Lazarus Group) hanno accoppiato l'exploit EternalBlue a un meccanismo di auto propagazione autonoma tipico dei worm, l'infezione si è diffusa a macchia d'olio in poche ore.

Il 12 maggio 2017 WannaCry ha colpito oltre duecentomila computer situati in centocinquanta nazioni. Tra le vittime più illustri figurava il sistema sanitario nazionale britannico, dove l'inagibilità dei computer ha costretto al blocco delle ambulanze e all'annullamento di migliaia di interventi chirurgici d'urgenza. Grandi aziende multinazionali della logistica, delle telecomunicazioni e dell'energia hanno subito il blocco totale delle attività produttive. La diffusione contagiosa è stata arrestata quasi casualmente da Marcus Hutchins, un giovane ricercatore britannico di sicurezza noto online come MalwareTech, il quale analizzando il codice del malware ha individuato e attivato una funzione di interruzione di emergenza presente nel programma. WannaCry ha rivelato la drammatica fragilità delle infrastrutture civili di fronte alla proliferazione incontrollata di armi digitali.

## **Capitolo 12: L'attacco SolarWinds e la compromissione della supply chain**

Nel dicembre del 2020 la scoperta di una sofisticata campagna d'intrusione ha ridefinito il concetto di vulnerabilità nelle reti aziendali e statali avanzate. L'attacco, attribuito dagli apparati d'intelligence al gruppo di spionaggio russo noto come APT29 o Nobelium, non ha colpito direttamente i bersagli finali, ma ha compromesso la catena di distribuzione del software (la cosiddetta supply chain), dimostrando come sia possibile penetrare nei sistemi più protetti del pianeta attraverso la porta di servizio dei fornitori di fiducia.

Gli aggressori sono riusciti ad accedere non visti ai sistemi di sviluppo della società americana SolarWinds, produttrice di una piattaforma di monitoraggio delle reti chiamata Orion utilizzata da migliaia di organizzazioni globali. Tra il marzo e il giugno del 2020 gli hacker hanno inserito una porta sul retro completamente invisibile, denominata Sunburst, all'interno degli aggiornamenti software ufficiali distribuiti da SolarWinds. Quando i clienti hanno scaricato e installato i pacchetti di aggiornamento muniti di firma digitale autentica, hanno aperto inavvertitamente le proprie difese agli spioni.

Oltre diciotto mila organizzazioni pubbliche e private hanno ricevuto il codice infetto. Gli aggressori hanno poi selezionato con cura un numero ristretto di bersagli di alto valore geografico e strategico su cui condurre attività approfondite di estrazione dati. Tra i soggetti violati figuravano diversi dipartimenti del governo degli Stati Uniti, tra cui il Dipartimento del Tesoro, del Commercio, della Sicurezza Interna e la National Telecommunications and Information Administration, oltre a multinazionali della tecnologia come Microsoft e FireEye. La violazione è rimasta inosservata per oltre nove mesi, evidenziando che l'hacking contemporaneo ad alto livello ha abbandonato l'impatto e il clamore mediatico del passato per privilegiare la persistenza invisibile, il controllo silenzioso delle infrastrutture tecnologiche e il dominio strategico dell'informazione.

## **Capitolo 13: Il caso Hacking Team e il cacciatore Phineas Fisher**

Nel luglio del 2015 il settore della sorveglianza digitale italiana ha subito uno shock senza precedenti quando la società milanese Hacking Team è stata vittima di una devastante intrusione informatica. L'azienda guidata da David Vincenzetti era specializzata nella creazione e nella vendita di software spia avanzati alle forze dell'ordine e ai servizi segreti di tutto il mondo. Il loro prodotto di punta chiamato Remote Control System permetteva ai clienti governativi di intercettare comunicazioni, attivare microfoni e sottrarre file dai dispositivi bersaglio. L'attacco è stato condotto da un hacker solitario noto con lo pseudonimo di Phineas Fisher il quale ha agito per motivazioni prettamente politiche volendo esporre le pratiche commerciali dell'azienda.

Sfruttando vulnerabilità nei dispositivi di rete e una scarsa segmentazione dell'infrastruttura interna, Phineas Fisher è riuscito a ottenere le credenziali di amministrazione dei server principali di Hacking Team. Il risultato dell'incursione è stata la pubblicazione online di oltre quattrocento gigabyte di dati riservati. Questo archivio conteneva il codice sorgente dei software spia, l'elenco completo dei clienti internazionali e migliaia di comunicazioni di posta elettronica interne. I documenti hanno rivelato che l'azienda italiana forniva i propri strumenti anche a governi noti per le gravi violazioni dei diritti umani, innescando uno scandalo politico e diplomatico di vaste proporzioni.

Le rivelazioni hanno costretto le autorità italiane a revocare temporaneamente le licenze di esportazione globale della società, evidenziando le profonde ambiguità morali e legali del mercato dei software di spionaggio. La caduta di Hacking Team ha dimostrato come anche le aziende tecnologicamente più avanzate nella sicurezza offensiva possano soccombere di fronte a carenze basilari nella propria difesa perimetrale. Questo evento ha segnato un punto di svolta nel dibattito sulla regolamentazione delle armi cibernetiche in Europa, mostrando al pubblico i meccanismi di una guerra digitale silenziosa e costantemente attiva.

## **Capitolo 14: L'operazione EyePyramid e lo spionaggio politico italiano**

Nel gennaio del 2017 le autorità italiane hanno svelato una delle più estese operazioni di spionaggio politico e finanziario della storia repubblicana, culminata con l'arresto dell'ingegnere nucleare Giulio Occhionero e di sua sorella Francesca Maria. L'indagine, denominata EyePyramid dal nome del codice malevolo utilizzato per le intrusioni, ha portato alla luce una rete di sorveglianza illegale attiva da anni contro le massime cariche istituzionali del Paese. L'obiettivo degli aggressori era la raccolta sistematica di informazioni sensibili, dati finanziari e comunicazioni riservate appartenenti a politici, banchieri, prelati e dirigenti di logge massoniche. Il metodo di attacco si basava su campagne mirate di ingegneria sociale tramite posta elettronica. Le vittime ricevevano messaggi fraudolenti che apparivano provenire da studi legali o istituzioni pubbliche contenenti allegati infetti. Una volta aperto il documento, il malware EyePyramid si installava nel computer eludendo i sistemi antivirus commerciali, garantendo agli aggressori il controllo totale della macchina. I fratelli Occhionero sono riusciti a compromettere oltre mille e ottocento dispositivi, creando un gigantesco archivio segreto conservato in server situati negli Stati Uniti per tentare di ostacolare le indagini della polizia postale italiana.

Tra i bersagli del monitoraggio illegale figuravano figure di spicco come l'ex presidente del Consiglio Matteo Renzi e il banchiere Mario Draghi, oltre a numerosi parlamentari e funzionari ministeriali. La scoperta della rete di spionaggio è avvenuta quasi per caso, grazie a un'anomalia rilevata nei server di posta di un amministratore di rete che ha segnalato un traffico sospetto verso domini esteri. Questo caso di cronaca ha rivelato l'allarmante fragilità delle comunicazioni istituzionali italiane e la facilità con cui soggetti privati, dotati di competenze tecniche medio alte, possano infiltrarsi nei gangli vitali delle infrastrutture decisionali di una nazione per scopi di dossieraggio e ricatto.

## **Capitolo 15: Le vulnerabilità della piattaforma Rousseau e l'intrusione di Rogue0**

Nel corso del 2017 il panorama politico italiano, fortemente influenzato dalle nuove dinamiche della democrazia digitale, è stato scosso dalle ripetute violazioni della piattaforma Rousseau. Questo sistema informatico rappresentava il cuore operativo del Movimento Cinque Stelle, utilizzato dagli iscritti per votare le proposte di legge, selezionare i candidati e finanziare le attività del partito. Un hacker rimasto anonimo e operante sotto lo pseudonimo di Rogue0 ha dimostrato pubblicamente la drammatica inconsistenza delle misure di sicurezza adottate dai gestori della piattaforma, esponendo i dati personali di decine di migliaia di cittadini e parlamentari.

L'attacco non ha richiesto l'impiego di tecnologie particolarmente sofisticate. Sfruttando vulnerabilità basilari nel codice della piattaforma, come falle di tipo SQL injection che permettevano di interrogare e manipolare direttamente il database sottostante, Rogue0 è riuscito a ottenere i privilegi di amministratore. In una serie di azioni dimostrative documentate su piattaforme social e blog indipendenti, l'hacker ha pubblicato tabelle contenenti nomi, numeri di telefono, indirizzi e le donazioni finanziarie degli utenti registrati. Inoltre ha dimostrato di poter alterare a piacimento l'esito delle votazioni interne, minando alla base la credibilità del processo democratico virtuale proposto dal movimento politico.

L'intrusione ha scatenato aspre polemiche sulla sicurezza dei dati e ha portato all'intervento del Garante per la protezione dei dati personali, il quale ha inflitto pesanti sanzioni ai responsabili dell'infrastruttura informatica. Il caso di Rogue0 rappresenta un capitolo fondamentale nella storia dell'hacking italiano perché ha evidenziato il pericoloso divario tra le ambizioni politiche della democrazia elettronica e la reale capacità di proteggere le infrastrutture informatiche dalle manomissioni esterne. L'identità dell'hacker non è mai stata scoperta ufficialmente, trasformando la sua figura in un monito costante sui rischi della transizione digitale non supportata da adeguate competenze ingegneristiche.

## **Capitolo 16: Aaron Swartz e la battaglia per la liberazione della conoscenza**

La storia dell'hacking annovera episodi in cui le competenze tecniche vengono impiegate non per profitto o distruzione, ma per promuovere cause ideali di interesse collettivo. La vicenda del programmatore e attivista americano Aaron Swartz incarna perfettamente l'etica originaria dell'hacking volta alla condivisione libera della conoscenza. Swartz era un prodigio dell'informatica che aveva contribuito in giovanissima età alla creazione del formato RSS e allo sviluppo della piattaforma Reddit. La sua profonda convinzione morale si fondava sull'idea che il sapere accademico e la ricerca scientifica, spesso finanziati con fondi pubblici, dovessero essere accessibili a tutta l'umanità senza restrizioni o barriere a pagamento.

Tra la fine del 2010 e l'inizio del 2011, Swartz ha deciso di agire direttamente contro il sistema di editoria accademica. Collegando un computer portatile alla rete informatica del Massachusetts Institute of Technology, ha scritto uno script automatizzato per scaricare sistematicamente quasi cinque milioni di articoli scientifici e saggi storici dal database chiuso di JSTOR. Il suo obiettivo non era arricchirsi, bensì liberare quegli scritti per renderli disponibili gratuitamente su internet a chiunque non potesse permettersi i costosi abbonamenti universitari. L'operazione tecnica era relativamente semplice, ma la mole di traffico generata ha attirato l'attenzione degli amministratori di rete.

Identificato e arrestato dalle autorità federali statunitensi, Swartz è stato accusato di frode informatica e furto di dati, rischiando fino a trentacinque anni di carcere e multe milionarie. Il procuratore ha adottato una linea dura e inflessibile, equiparando l'azione ideologica di Swartz al peggior dei crimini telematici al fine di creare un precedente deterrente. Sottoposto a una pressione psicologica ed economica insostenibile, Aaron Swartz si è tolto la vita nel gennaio del 2013 all'età di soli ventisei anni. La sua morte ha scatenato un'ondata di indignazione globale e ha accelerato in modo decisivo il movimento per l'accesso aperto alla letteratura scientifica, consolidando la sua figura come martire della libertà d'informazione digitale.

## **Capitolo 17: La botnet Mirai e la fragilità intrinseca della domotica**

L'espansione pervasiva della tecnologia ha portato alla proliferazione di dispositivi domestici connessi a internet, fenomeno noto come domotica o Internet delle Cose. Questa evoluzione ha introdotto nuove vulnerabilità strutturali, drammaticamente evidenziate nell'autunno del 2016 dalla comparsa della botnet Mirai. Creato da un giovane studente universitario identificato in seguito con lo pseudonimo di Anna Senpai, questo codice malevolo non colpiva computer tradizionali o server aziendali, ma prendeva di mira telecamere di sicurezza, registratori digitali, termostati intelligenti e router domestici.

La meccanica di diffusione di Mirai sfruttava una negligenza imperdonabile dei produttori hardware e degli utenti. Il malware esplorava costantemente la rete globale alla ricerca di dispositivi intelligenti che avessero le porte di comunicazione aperte e utilizzassero ancora le credenziali di accesso predefinite di fabbrica (come la combinazione utente admin e password admin). Quando Mirai individuava un dispositivo vulnerabile, vi si installava in modo silente, arruolandolo in un esercito di macchine infette chiamato botnet. Il proprietario della telecamera o del termostato non notava alcun malfunzionamento, poiché il dispositivo continuava a operare normalmente, celando al suo interno il comando ostile.

Nell'ottobre del 2016 gli operatori della botnet hanno attivato la loro rete composta da centinaia di migliaia di dispositivi domestici infetti per sferrare un massiccio attacco di negazione del servizio contro i server di Dyn, una società americana fondamentale per l'instradamento del traffico web mondiale. Il bombardamento simultaneo di dati ha paralizzato l'infrastruttura, rendendo irraggiungibili piattaforme primarie come Twitter, Netflix, Spotify e GitHub in gran parte del Nord America e dell'Europa. Il caso Mirai ha dimostrato in modo inequivocabile che i dispositivi di domotica, spesso privi di aggiornamenti di sicurezza e progettati con criteri di risparmio economico, costituiscono un potenziale arsenale diffuso nelle case dei cittadini, sfruttabile per abbattere le strutture portanti dell'intera rete globale.

## **Capitolo 18: Il software Pegasus e la sorveglianza mobile invisibile**

L'onnipresenza degli smartphone nella vita quotidiana li ha resi il bersaglio finale e più prezioso per lo spionaggio governativo e industriale. La percezione di sicurezza legata a questi dispositivi è stata definitivamente infranta dalle rivelazioni sul software Pegasus, sviluppato dall'azienda israeliana NSO Group. Questo strumento rappresenta l'apice tecnologico dell'hacking mobile, progettato per compromettere dispositivi iOS e Android senza richiedere alcuna interazione o errore da parte della vittima. Questo approccio invisibile e silenzioso è tecnicamente definito come attacco zero click.

Dal punto di vista teorico, la violazione di uno smartphone moderno richiede il superamento di architetture difensive a scompartimenti stagni (note come sandbox) che isolano le singole applicazioni dal nucleo del sistema operativo. Nel caso di Pegasus, gli aggressori sfruttano vulnerabilità sconosciute ai produttori, dette zero day, presenti in applicazioni di uso comune come WhatsApp o iMessage. Inviando un pacchetto di dati malformato tramite una semplice chiamata o un messaggio invisibile, il codice malevolo sfrutta una falla nella decodifica delle immagini o dell'audio per eseguire istruzioni nella memoria del telefono. Una volta superata la prima barriera, il software concatena una serie di exploit per ottenere i permessi di amministrazione suprema del dispositivo.

L'installazione completata trasforma lo smartphone in uno strumento di sorveglianza totale. L'attaccante acquisisce la capacità di estrarre messaggi cifrati prima della loro crittografia, attivare microfoni e fotocamere all'insaputa dell'utente, tracciare la posizione geografica in tempo reale e accedere a ogni singolo file archiviato. L'impiego di Pegasus, ufficialmente venduto solo a governi per la lotta al terrorismo, è stato documentato in numerosi casi di spionaggio contro giornalisti investigativi, dissidenti politici e capi di Stato in tutto il mondo. Questa vicenda ha svelato la natura asimmetrica dell'hacking contemporaneo, dove le vulnerabilità dei dispositivi mobili sono considerate veri e propri segreti militari venduti sul mercato internazionale a prezzi esorbitanti.

## **Capitolo 19: Il collasso di EncroChat e l'infiltrazione governativa**

L'hacking dei dispositivi mobili non si limita allo sfruttamento di vulnerabilità nei telefoni di uso comune, ma abbraccia anche la compromissione delle reti di comunicazione cifrata progettate su misura per eludere le intercettazioni. Un caso paradigmatico di questa metodologia è rappresentato dalla distruzione di EncroChat, un'azienda che forniva smartphone modificati e un'infrastruttura di messaggistica impenetrabile, adottata in modo massiccio dalle reti della criminalità organizzata europea. Nel 2020 le forze di polizia di Francia e Paesi Bassi, supportate dall'Europol, hanno condotto un'operazione tecnica di infiltrazione senza precedenti, capovolgendo il paradigma della sicurezza difensiva.

Il funzionamento teorico di dispositivi come quelli forniti da EncroChat si basa sulla rimozione fisica di componenti tracciabili (come il ricevitore GPS o la fotocamera) e sull'installazione di sistemi operativi modificati che instradano ogni comunicazione attraverso server crittografati situati all'estero. Poiché decifrare matematicamente le singole comunicazioni in transito risultava impossibile, le autorità investigative hanno scelto di colpire l'infrastruttura centrale. Le forze dell'ordine sono riuscite a individuare e penetrare i server principali dell'azienda situati in Francia, inserendo un codice malevolo direttamente negli aggiornamenti di sistema che venivano inviati periodicamente ai telefoni dei clienti.

Questo approccio, noto come attacco alla catena di fornitura, ha permesso agli investigatori di bypassare l'intera architettura crittografica. Il malware di Stato installato sui dispositivi estraeva il testo in chiaro dei messaggi direttamente dallo schermo, le password e le note salvate, trasmettendo silenziosamente tutto il materiale ai server della polizia prima che venisse applicata la cifratura.

L'operazione ha permesso di intercettare oltre cento milioni di messaggi in tempo reale per mesi, portando all'arresto di migliaia di criminali, al sequestro di tonnellate di stupefacenti e a centinaia di perquisizioni in tutta Europa, dimostrando che nessuna architettura hardware risulta invulnerabile quando l'infrastruttura di distribuzione centrale viene compromessa.

## **Capitolo 20: L'anatomia teorica di un attacco e le difese strutturali**

Comprendere le dinamiche di un'intrusione informatica richiede l'abbandono delle semplificazioni per abbracciare un modello teorico rigoroso, noto in ambito militare e aziendale come Cyber Kill Chain. Questo framework analitico descrive le fasi sequenziali che compongono un attacco avanzato, permettendo ai difensori di predisporre contromisure adeguate per interrompere la catena ostile. L'operazione non inizia mai con la stesura impulsiva di codice, ma con una fase di ricognizione minuziosa (spesso definita OSINT), durante la quale vengono raccolte informazioni pubbliche sull'architettura di rete del bersaglio, sulle abitudini dei dipendenti e sulle tecnologie impiegate, al fine di mappare la superficie esposta.

Nella teoria della sicurezza, l'anonimato e l'offuscamento del traffico rappresentano concetti centrali. Gli analisti studiano come le connessioni vengano fatte rimbalzare attraverso reti crittografate o server proxy compromessi per impedire l'identificazione della sorgente originale. L'arsenale teorico analizzato dai difensori comprende sistemi operativi dedicati alla sicurezza (che integrano strumenti di analisi del traffico e verifica delle vulnerabilità) e piattaforme di test di penetrazione. Successivamente alla ricognizione, la metodologia prevede la creazione di un vettore di attacco (un file infetto o un link malevolo) e la sua consegna al bersaglio tramite ingegneria sociale o lo sfruttamento di servizi esposti. La difesa proattiva si concentra sulla comprensione delle fasi successive: l'esecuzione del codice, l'installazione di un canale di comunicazione persistente (il cosiddetto Command and Control) e l'esfiltrazione dei dati. Per contrastare queste minacce, l'ingegneria dei sistemi moderni adotta il principio del privilegio minimo, la segmentazione rigorosa delle reti, l'autenticazione a più fattori e l'impiego di intelligenze artificiali per l'analisi comportamentale del traffico dati. Lo studio delle procedure di intrusione non mira alla formazione offensiva, ma costituisce il pilastro fondamentale della scienza della difesa cibernetica, essenziale per proteggere le infrastrutture critiche in un panorama tecnologico sempre più ostile.