Introduzione

A fine gennaio del 2014, un amministratore di sistema di Anthem, all'epoca uno dei maggiori fornitori di assicurazioni sanitarie al mondo, fece una scoperta preoccupante. La notte precedente, qualcuno aveva utilizzato il suo account per eseguire diverse query volte a raccogliere dai server di Anthem dati sensibili sui suoi clienti [1]. Gli hacker avevano sottratto informazioni di identificazione personale relative a quasi ottanta milioni di pazienti.

Nel 2015, i fornitori di sistemi di cybersicurezza Trend Micro e *Symantec* hanno identificato gli hacker: un gruppo soprannominato *Black Vine*, si ritiene originario di un paese nel Sudest asiatico [2]. Inoltre, la ricerca ha scoperto che l'operazione non puntava a un mero guadagno economico, come molti avevano ipotizzato, ma era piuttosto un passo di un'operazione di spionaggio su larga scala. Ho condotto personalmente alcune di queste ricerche iniziali; ulteriori informazioni si sono rese disponibili quattro anni dopo, quando un mandato d'arresto federale degli Stati Uniti ha accusato diversi hacker cinesi di aver partecipato all'operazione contro Anthem. Secondo l'accusa, gli hacker avevano preso di mira un programma responsabile della conduzione di indagini preliminari su alcuni cittadini statunitensi che avevano richiesto un nulla osta sulla sicurezza. Anthem forniva servizi sanitari ai dipendenti del Governo federale degli Stati Uniti; quindi, incrociando i dati sanitari sottratti con le informazioni sugli spostamenti divulgate nelle indagini sulle autorizzazioni, gli hacker sono stati in grado di individuare un elenco di persone ritenute agenti della CIA (*Central Intelligence Agency*) operanti segretamente in Africa ed Europa [3].

Tutto questo potrebbe sembrare la trama di un buon romanzo di spionaggio. Ma il problema è che questi eventi hanno effettivamente avuto luogo. All'epoca, pochi sospettavano che un attacco concepito per sottrarre dati sanitari potesse portare all'esposizione delle reti di spionaggio statunitensi. Sfortunatamente, come Anthem e molte altre organizzazioni colpite hanno imparato a proprie spese, le forze armate e i governi non sono più gli unici target degli hacker di livello governativo, i quali possono prendere di mira le aziende del settore privato perché queste o non pensano di poter essere attaccate da un governo straniero o semplicemente non sanno difendersi da attacchi così sofisticati. Questi hacker vengono spesso erroneamente considerati minacce minori, vengono mal gestiti o non vengono rilevati affatto. E le difese informatiche automatizzate, sebbene siano in grado di identificare e proteggere i sistemi dalla maggior parte delle minacce odierne, sono generalmente impotenti di fronte agli hacker di livello governativo.

Questo tipo di attacchi può avere un impatto devastante sulle aziende private. Come nell'attacco ad Anthem, le attività di spionaggio dei governi spesso finisce per esporre dati sensibili sui clienti, con gravi sottrazioni della proprietà intellettuale. Quando un malintenzionato sottrae la proprietà intellettuale di un'azienda o di un'organizzazione il danno può ammontare a milioni o addirittura a miliardi di dollari. Nel caso di Anthem, il costo totale della violazione non è noto; tuttavia, nel 2018 un tribunale degli Stati Uniti ha sanzionato Anthem per 115 milioni di dollari [4]. L'azienda ha anche subìto una massiccia tempesta di pubblicità negativa e ha dovuto informare i propri clienti dell'esposizione dei loro dati. Inoltre, la ricerca e lo sviluppo necessari per creare nuove tecnologie mediche o prodotti farmaceutici richiedono grandi quantità di tempo e di denaro. Se un governo sottrae tali proprietà intellettuali, diventa in grado di creare quello stesso prodotto risparmiando tale somma e anche tale tempo. Ciò non solo determina un indebito vantaggio sui mercati esteri, beneficiando del furto, ma, in alcuni casi, mette fuori gioco l'organizzazione o azienda originariamente proprietaria dei marchi e del prodotto. I governi spesso prendono di mira aziende che operano nel campo della finanza, delle tecnologie, della sanità, delle comunicazioni e di molti altri settori. Ma, per diversi motivi, questi attacchi sono difficili da prevedere, e la realtà è che chiunque può diventare un target. Per esempio, è probabile che abbiate sentito parlare dell'attacco contro Sony del 2014 [5]. Essendo una delle principali società al mondo nel campo dell'intrattenimento multimediale, Sony non sembrerebbe avere un profilo attraente per un governo straniero. Tuttavia, la Corea del Nord ha messo in ginocchio l'azienda utilizzando tattiche di guerra informatica in risposta alla produzione di *The Interview*, un film che ipotizza l'assassinio del leader della Corea del Nord, Kim Jong Un [6]. La Corea del Nord non voleva che il film uscisse, e ha affermato che avrebbe reso pubblici tutti i dati sottratti, a meno che Sony non avesse accettato di annullare l'uscita del film. Dopo aver sottratto i dati e le informazioni private di Sony, gli hacker hanno lanciato la seconda fase dell'attacco: il sabotaggio. Hanno utilizzato un malware "wiper" personalizzato, noto come *Backdoor. Destover* per eliminare i dati di computer e server, distruggendo l'infrastruttura interna di Sony. L'attacco ha lasciato a Sony ben poche scelte, se non quella di cedere.

Sony ha assunto *Mandiant*, una società indipendente specializzata in risposte agli incidenti, per ripulire e contrastare la minaccia. Sfortunatamente, quando *Mandiant* iniziò a tentare di risolvere la situazione, gli hacker avevano già causato troppi danni. Le azioni di Sony subirono un duro colpo, così come la sua reputazione. E comunque l'attacco non si è fermato. La Corea del Nord ha rilasciato ulteriori raccolte di e-mail aziendali sensibili, riguardanti stipendi e trattative finanziarie relative ai film Sony. Ha sottratto film che avrebbero fruttato alla società milioni di dollari e li ha rilasciati pubblicamente affinché chiunque potesse scaricarli gratuitamente. Nel frattempo, i milioni di dollari spesi per produrre quei film dovevano comunque essere pagati. Alla fine, Sony ha ceduto agli hacker e ha deciso di non rilasciare *The Interview* nelle sale, come richiesto dalla Corea del Nord. In sostanza, gli antagonisti avevano vinto, mettendo a tacere Sony. Alla fine, Sony ha potuto realizzare solo un lancio cinematografico molto limitato, che ha reso molto meno di quanto inizialmente previsto. Questo è uno degli esempi più noti e pubblicizzati che dimostrano come gli hacker che lavorano per conto di un governo ostile possano prendere di mira anche le società private.

Un altro esempio risale al maggio del 2021, quando *DarkSide*, una gang di criminali russa, ha violato la Colonial Pipeline e vi ha introdotto un ransomware, provocando il blocco del più grande oleodotto della costa orientale degli Stati Uniti. Tuttavia, la gang ha presto fatto marcia indietro, sostenendo che il suo attacco non era intenzionale: si trattava di un'infezione accidentale causata da un loro partner, e ha accettato di contribuire alla risoluzione degli attacchi in cambio di una quota del riscatto. Ciononostante, l'impatto ha provocato carenze di carburante in tutta la costa orientale per quasi una settimana. Serpeggiò il panico, quando i consumatori trovarono i cartelli "Fuori servizio" nelle stazioni di servizio. La gang *DarkSide* responsabile dell'attacco si sciolse e infine entrò in clandestinità. Tuttavia, le perdite per l'attacco a carico di Colonial Pipeline ammontano a milioni di dollari. Il danno, poi, è andato ben al di là dell'oleodotto: l'attacco e i suoi effetti sugli Stati Uniti hanno provocato pubblico imbarazzo all'amministrazione Biden, per non essere riuscita a fermare gli hacker o a riattivare rapidamente l'erogazione dei carburanti.

Si può discutere sul fatto che Anthem, Sony o Colonial Pipeline avrebbero potuto gestire questi attacchi in modo differente, ma nessuna di queste aziende avrebbe potuto impedire del tutto gli attacchi di un governo straniero o di un hacker criminale sofisticato. Questo perché nessuna delle aziende ha compreso la forza del proprio avversario né poteva rispondere adeguatamente. Come scoprirete in questo libro, la più grande differenza tra un hacker tradizionale e un hacker sofisticato è quell'essere umano seduto davanti a quella tastiera. Una volta contrastate, la maggior parte delle minacce automatiche diviene obsoleta; gli attacchi mirati e guidati dall'uomo, al contrario, tornano sempre, scegliendo strade differenti. E a differenza di altre minacce, gli hacker di livello governativo operano sul lungo periodo. Sono pazienti, hanno precisi obiettivi e dispongono di risorse ingenti. Per questi motivi, spesso il contrasto è l'aspetto più frainteso e mal gestito della difesa dagli attacchi di livello governativo. Se iniziate a prepararvi per un attacco da parte di un governo ostile mentre tale attacco è già in corso, o anche quando vi rendete conto di poter essere un bersaglio, sarà comunque troppo tardi.

A chi è rivolto questo libro

Questo libro punta a fornire una conoscenza approfondita del comportamento degli hacker ransomware governativi, criminali e specializzati. Pertanto, le informazioni presentate in questo libro saranno estremamente utili a tutti coloro che si occupano della sicurezza informatica nel settore privato, governativo o militare. Imparerete alcune abilità pratiche, per esempio come attribuire un attacco a un determinato hacker, incrociando le analogie tra gli attacchi, come analizzare le e-mail di phishing, come studiare i dati del fuso orario e altre prove e anche come monitorare ogni fase di una campagna mirata multifase. Il mio obiettivo più ambizioso è quello di offrire questo materiale a chi si occupa della sicurezza informatica per un'azienda, che ha sicuramente molte meno risorse per difendersi da attività di hacking avanzate come quelle condotte da hacker ransomware e di livello governativo. Discuteremo delle differenze fra gli hacker di livello governativo e le altre minacce, spiegheremo perché gli hacker ransomware possono essere devastanti, a causa dei loro obiettivi, e vi insegnerò a identificare, attribuire e contrastare i loro attacchi attraverso esempi concreti.

Come è organizzato questo libro

Questo libro è diviso in due parti. La prima tratta gli attacchi ransomware più elaborati e devastanti mai visti fino a oggi condotti da hacker di livello governativo, criminali e specializzati. Esamineremo le tattiche utilizzate per violare gli obiettivi e gli stratagemmi adottati dagli hacker. Inizierete anche a veder emergere dei modelli nel modo in cui vengono condotti questi attacchi. Questi modelli vi aiuteranno poi a riconoscere alcune tecniche comunemente impiegate per la difesa da nuovi attacchi.
La seconda parte del libro tratta i metodi e i modelli analitici che possono essere impiegati nelle indagini sugli attacchi più sofisticati. Imparerete alcuni potenti trucchi che potete utilizzare per rimanere anonimi mentre date la caccia agli hacker che vi stanno attaccando. Inoltre, esplorerete le tecniche di intelligence impiegabili per tracciare e identificare nuove infrastrutture e personaggi ostili, utilizzati per le cyberminacce più sofisticate.
Combinando le conoscenze sugli hacker di livello governativo presentate nella Parte I con i contenuti analitici esplorati nella Parte II, sarete in grado di difendere meglio la vostra azienda o organizzazione da questi attacchi mirati.

L'autore

Jon DiMaggio è Chief Security Strategist di Analyst1 e ha un'esperienza di oltre quindici anni nel campo della caccia, ricerca e realizzazione di cyberminacce avanzate. In qualità di specialista nella difesa da attacchi ransomware ad aziende e da intrusioni di livello governativo, tra cui quella del primo cartello di ransomware al mondo e del famigerato gruppo di cyberspionaggio *Black Vine*, ha smascherato le organizzazioni criminali responsabili dei principali attacchi ransomware, ha collaborato con le forze dell'ordine nelle accuse federali relative ad attacchi di livello governativo, e ha parlato del suo lavoro sul "New York Times" e su Bloomberg, Fox, CNN, Reuters e "Wired". Potete ascoltarlo parlare delle sue ricerche in conferenze come *RSA* e *Black Hat*.

Il revisore tecnico

Chris Sperry è un veterano della cybersicurezza, con oltre vent'anni di esperienza nel settore, quindici dei quali dedicati ad affinare la propria abilità nell'intelligence sulle cyberminacce. Ha collaborato con numerosi enti governativi e aziende *Fortune 500* per individuare, tracciare e contrastare gli attacchi provenienti da Stati e dai più sofisticati cybercriminali. La sua missione è quella di rendere Internet un luogo più sicuro, educando la prossima generazione di professionisti della cyberintelligence.