Dati rilevati dagli Enti certificatori o autocertificati
Tiratura: n.d.
Diffusione: n.d.
Lettori: n.d.
Quotidiano - Ed. nazionale

IL FOGLIO
inserto
Dir. Resp.: Claudio Cerasa

03-DIC-2021
da pag. 3 /
foglio 1 / 3
www.datastampa.it

THE DARK SHADOW

Tutto quello che sappiamo sul gruppo di hacker iraniani che è riuscito a infiltrare un uomo dentro la casa del ministro della Difesa israeliano. Operazioni aggressive commissionate dall'intelligence di Teheran

Capelli corti, magro, faccia smunta, Goren lavorava per Dark Shadow in casa di Benny Gantz

Spesso il movente finanziario e rastrellare dati vanno insieme. Ora sembra che si voglia fare solo del male

La società israeliana, nonostante l'alta tecnologia, non è protetta e sicura come sembra contro questi attacchi

Un esperto ci spiega come operano questi gruppi che riescono a trovare e pubblicare dati molto sensibili

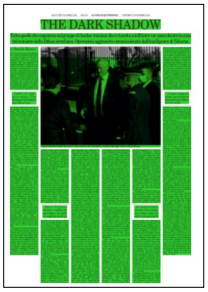
di Daniele Raineri

Ci sono due punti importanti da conoscere quando si parla dello scontro in corso tra gli hacker governativi dell'Iran e quelli di Israele. Il primo è che gli hacker iraniani sono più agguerriti di quanto pensiamo. L'Iran è una nazione in crisi dove la gente scende in piazza esasperata per i rincari del cibo e la mancanza di acqua e non può rivaleggiare dal punto di vista tecnologico con gli avversari. Eppure i servizi di sicurezza iraniani hanno creato gruppi Apt che colpiscono con successo i bersagli israeliani. Apt è una sigla usata nel settore per indicare le Advanced persistent threat, le minacce avanzate persistenti, quindi squadre di specialisti anonimi che da un luogo protetto dedicano tutto il loro tempo ad attaccare le reti internet degli altri. In questi anni abbiamo conosciuto i gruppi Apt russi, perché hanno rubato e pubblicato le mail del Partito democratico, e ci ricordiamo i gruppi Apt della Corea del nord che hanno rubato e pubblicato le mail della Sony. Ci sono anche i gruppi Apt iraniani. Non c'è contraddizione con la crisi economica in Iran, perché i gruppi Apt costano relativamente poco e fanno molto, sono un ottimo investimento per un governo che vuole infliggere danni seri agli avversari a prezzo contenuto. Il secondo punto da conoscere è che, come vedremo adesso, Israele è più vulnerabile di quanto pensiamo, a dispetto dell'immagine di nazione tech che ha a disposizione risorse e talenti senza pari in medio oriente. Questi assalti da parte dei gruppi Apt dell'Iran sono svelti e il velo di tecnologia e misure di sicurezza che avvolge la società israeliana offre soltanto un'illusione di sicurezza: è sottile, ha dei buchi e cede, come succede nel resto del mondo.

Partiamo da questo secondo punto, la debolezza di Israele. All'inizio di novembre compare di nuovo dopo una pausa di dieci mesi un gruppo Apt iraniano che si fa chiamare Dark Shadow e riversa su internet una mole enorme di dati di cittadini israeliani. Crea archivi online per contenere i dati, accessibili e scaricabili da chiunque, e poi pubblica i link su un canale Telegram aperto. Sono informazioni molto personali. Un archivio contiene tutta la memoria di Atraf, una app di incontri della comunità Lgbtq israeliana che permette di chattare in modalità privata con altri utenti e di scambiare foto e video. Atraf esiste fin dal 2002 – a quel tempo era un sito – e in pratica è l'anima di tutta la comunità Lgbtq in Israele. Un secondo archivio contiene i dati medici di circa trecentomila israeliani che sono passati per l'Istituto Mor, un ospedale, con informazioni e dettagli sulla loro salute. E' un'operazione simile a quella di Wikileaks, che riversò su internet i dispacci riservati del governo americano, ma in questo caso ci sono tutti i dati di Atraf e cartelle cliniche.

Quando gli iraniani di Dark Shadow pubblicano sul loro canale telegram anche i link che portano ad archivi con materiale della compagnia di bus Dan, della Radio israeliana 103 e della compagnia di assicurazioni Trip Guaranty Travel, si capisce che sono riusciti a violare i sistemi della Cyberserve, un server che ha tutte queste aziende fra i suoi clienti. A quel punto i controspecialisti israeliani chiedono a Telegram di chiudere il canale (ora non c'è più) e cancellano gli archivi accessibili online ma ormai il danno è fatto, non c'è dubbio che qualcuno è riuscito a scaricarli e userà quel materiale per fini suoi. Zohar Pinhasi, capo dell'azienda di sicurezza informatica israeliana Monstercloud, dice al Jerusalem Post che "attacchi come questi avvengono ogni giorno, ma spesso non sono pubblicizzati perché le aziende non vogliono ammettere di essersi fatte fregare".

Questa volta il ritorno di Dark Shadow finisce sui media. E fa scattare un interruttore nella testa di un addetto alle pulizie israeliano, Omri Goren, di 37 anni, che pensa di contattare il gruppo iraniano per un piano di ricatto che probabilmente coltivava da anni. Capelli corti, magro, faccia smunta, Goren lavora a casa di Benny Gantz, ex capo di stato maggiore, ministro della Difesa di Israele a partire dal 2016 e infine leader politico. L'uomo delle pulizie scrive a Dark Shadow sul canale Telegram – quando ancora c'era – con un falso nome e si offre di lavorare per loro. Per convincere gli interlocutori del fatto che ha davvero accesso alla casa di Gantz spedisce una serie di foto: la scrivania, il computer, il telefono, il tablet, la cassaforte, una macchina trita documenti, alcune fotografie incorniciate di Gantz e della sua famiglia e il bollettino di una tassa pagata. Poi chiede settemila dollari – che è una cifra molto bassa per uno che può entrare indisturbato nella casa del ministro della Difesa di Israele, ma è probabile che per istinto comprenda che l'improvviso arrivo di denaro nella sua vita fa-



Dati rilevati dagli Enti certificatori o autocertificati
Tiratura: n.d.
Diffusione: n.d.
Lettori: n.d.
Quotidiano - Ed. nazionale

IL FOGLIO
inserto
Dir. Resp.: Claudio Cerasa

03-DIC-2021
da pag. 3 /
foglio 2 / 3
www.datastampa.it

rebbe da segnale d'allarme. Parla con Dark Shadow della possibilità di piazzare sul computer di Gantz un malware.

Il piano di Goren e Dark Shadow è un rovesciamento delle parti rispetto alla celebre operazione dell'intelligence israeliana nel 2010 per infettare i computer del programma nucleare iraniano con il virus Stuxnet. Quel virus faceva funzionare male le centrifughe che arricchiscono l'uranio, le faceva andare fuori giri come se avessero avuto un difetto di fabbrica – gli iraniani impiegarono un po' di tempo a capire che erano stati sabotati – e causava la loro autodistruzione. Il malware Stuxnet era stato disegnato per rallentare la corsa verso la Bomba atomica. I computer da colpire erano separati dalla rete normale e per questo motivo un agente degli israeliani aveva dovuto inserire fisicamente una chiavetta Usb in uno di essi, dentro a uno dei centri di ricerca atomica. Da lì Stuxnet aveva infettato tutto il sistema – e poi era tracimato nel mondo esterno e aveva invaso senza conseguenze (perché era un programma specifico per le centrifughe che arricchiscono l'uranio) altre decine di migliaia di computer in tutti i continenti. Anche l'addetto alle pulizie Goren dovrebbe inserire una chiavetta nel computer del ministro della Difesa israeliano approfittando di una sua assenza. L'intelligence interna, lo Shin Bet, lo arresta prima. Salta fuori che lui era già finito in prigione cinque volte fra il 2002 e il 2013, aveva fatto due rapine in banca e l'ultima volta aveva passato in cella quattro anni e quindi in teoria non avrebbe dovuto avere accesso a quel lavoro. Il processo di vetting, quindi la scrematura di chi ha incarichi attorno a Gantz e potrebbe spiarlo da vicino per conto di qualche intelligence straniera per un movente così semplice come il denaro, ha fallito. Viene in mente che tre anni fa gli hacker iraniani erano riusciti a entrare nel telefono di Gantz, appena dopo il suo ingresso in politica. A febbraio 2019 lo Shin Bet aveva avvisato l'ex capo di stato maggiore che doveva considerare come un fatto compiuto che tutto il contenuto del suo telefono fosse stato rubato e fosse finito in mani altrui e quindi regolarsi di conseguenza. A questo punto comincia a vedersi un significato più generale della storia: se persino gli israeliani, che sono i più bravi in questo genere di operazioni, non riescono a evitare le incursioni iraniane in questo scontro quotidiano, vuol dire che tutti i sistemi di sicurezza hanno delle falle e ci sono troppi fattori e troppe ramificazioni da tenere d'occhio.

Abbiamo chiesto a Emiel Haeghebaert, analista di Mandiant, una compagnia internazionale specializzata in sicurezza informatica, come giudica Black Shadow a partire dai soli dati che abbiamo, quindi dalle operazioni. Haeghebaert quando ci parla di questi gruppi li definisce "Iran-nexus clusters", per rendere l'idea di soggetti plurimi che orbitano attorno all'Iran: sono cluster, grappoli, della rete iraniana. "Questi cluster conducono operazioni 'hack-and-leak' contro molte organizzazioni nel settore privato e quello pubblico di Israele e di solito queste azioni sono formate da due elementi: il primo è la violazione della vittima e il secondo è la pubblicazione online dei dati rubati. Nel caso di Black Shadow abbiamo osservato un gruppo che storicamente si occupava di spionaggio informatico e che in seguito si è messo a pubblicare i dati di cui era entrato in possesso. Quindi pensiamo che ci siano due operatori separati che si occupano dei due tronconi di queste operazioni e collaborano in modo stretto, oppure che il mandato del gruppo che per tradizione era il cyber spionaggio sia stato allargato. Black Shadow ha lo scopo di mettere in imbarazzo le organizzazioni israeliane e di distruggere le interazioni sociali, e quindi alla fine di infliggere un colpo psicologico. Le rivendicazioni di Black Shadow menzionano spesso un movente finanziario, ma non siamo riusciti a trovare prove reali che il gruppo abbia monetizzato con successo le sue campagne. Non sono riusciti a farsi dare denaro. Tuttavia, non escludo che riusciranno a farlo in futuro".

Stiamo parlando di roba terra terra oppure di operazioni sofisticate? "I gruppi dell'Iran-nexus che si dedicano all'hack and leak usano tattiche, tecniche e procedure di moderata difficoltà. Fanno molto affidamento sulle web-shells" (senza andare troppo sul tecnico: le web-shells sono strumenti del mestiere più accessibili di altri, permettono di sfruttare un sistema già compromesso ma non possono compromettere da sole un sistema, sono una forma derivativa di hacking minore. Spero che questa spiegazione regga agli occhi di uno specialista).

Avete un'idea sull'origine dei gruppi come Black Shadow? In questi anni abbiamo già osservato le relazioni strette tra alcuni gruppi Apt e i servizi di intelligence di paesi come la Corea del nord, la Cina e la Russia. Black Shadow lavora sotto la protezione dell'intelligence iraniana? "La nostra valutazione, praticamente certa, è che l'Iran sfrutti come una leva le sue capacità informatiche per fare spionaggio, per raccogliere informazioni e per operazioni distruttive e di disturbo come mezzo per indebolire gli avversari e raggiungere i suoi obiettivi di sicurezza nazionale. Il programma dell'Iran in questo campo include organizzazioni militari, civili, governative, commerciali e anche del mondo dell'istruzione che sviluppano strumenti, identificano possibili bersagli e fanno operazioni offensive per appoggiare la sicurezza nazionale e l'economia. I link tra gruppi che storicamente si occupano di spionaggio informatico come Black Shadow e queste campagne hack and leak suggeriscono che le operazioni sono come minimo autorizzate o tollerate dai servizi di sicurezza e dal governo dell'Iran".

Ci sono altri gruppi Apt iraniani altrettanto efficienti e pericolosi? "Abbiamo visto molte operazioni hack and leak e altre di disturbo partire dall'Iran in questi mesi e in questi anni. Inoltre ci sono gruppi iraniani dediti da molto allo spionaggio come APT34 e UNC788 che continuano a soddisfare quelli che noi crediamo siano i loro mandati operativi – nel senso che sanno fare bene quello che viene ordinato loro di fare".

I gruppi Apt iraniani hanno nomi come Dark Shadow, Moses Staff, SiameseKitten conosciuti anche come Lyceum/Hexane, Lebanese Cedar conosciuti anche come Volatile Cedar, FoxKitten, OilRig e altri ancora. E' possibile che siano le stesse persone che cambiano nome, si mischiano in gruppi diversi, abbandonano un progetto e ne cominciano un altro, sempre sotto copertura per non farsi identificare. Queste campagne a distanza di spionaggio e di sabotaggio sono anche una lotta di persone fisiche contro altre persone fisiche. Ad agosto ClearSky, un'azienda di sicurezza israeliana con una buona reputazione, ha pubblicato un rapporto per descrivere quello che aveva trovato dopo avere studiato un'ondata di attacchi di un gruppo Apt iraniano che si fa chiamare SiameseKitten. Gli iraniani hanno cercato di far cadere in trappola alcuni specialisti israeliani che lavorano nel settore sicurezza informatica. Hanno creato finti siti di aziende dello stesso settore, hanno creato finti profili di persone su LinkedIn con nomi veri, hanno creato finti file di documenti da scaricare e poi dopo aver predisposto il set per la scena hanno contattato i bersagli.

Il piano funzionava così: gli iraniani fingevano di essere aziende occidentali desiderose di assumere gli specialisti israeliani, si dicevano interessati a parlare con loro e riuscivano a reggere la finzione grazie ai siti e ai profili preparati in precedenza. Nel settore della si-

Dati rilevati dagli Enti certificatori o autocertificati
Tiratura: n.d.
Diffusione: n.d.
Lettori: n.d.
Quotidiano - Ed. nazionale

IL FOGLIO
inserto

Dir. Resp.: Claudio Cerasa

03-DIC-2021
da pag. 3 /
foglio 3 / 3
www.datastampa.it

curezza informatica cambiare lavoro con una certa frequenza e ricevere proposte da altri paesi è normale, non si trattava di un'attività sospetta. Ma i file che contenevano i dettagli dell'offerta di lavoro nascondevano un malware che si sarebbe installato nei computer degli specialisti. Da lì, una volta ottenuto l'accesso invisibile ai computer degli specialisti di sicurezza informatica, gli iraniani intendevano passare ai computer dei loro clienti. In questo modo avrebbero trasformato gli specialisti in inconsapevoli cavalli di Troia. SiameseKitten ha attaccato a due riprese, prima a maggio e poi a luglio. Mercoledì 17 novembre l'agenzia Fars, legata ai Guardiani della rivoluzione dell'Iran, ha pubblicato il nome, l'indirizzo e le foto di casa di un esperto che lavora a ClearSky, l'azienda che ha pubblicato il rapporto su questo e su altri attacchi. E' uno scontro fra persone fisiche, come si diceva, prende di mira persone fisiche e questa è stata una piccola vendetta.

Come dice Haeghebaert, ci sono diversi elementi che fanno pensare all'Iran. In teoria gli specialisti che giocano in attacco possono nascondere l'origine delle aggressioni, in pratica ci sono modalità di esecuzione che sono come una firma agli occhi di chi le studia. E a volte ci sono errori di esecuzione che lasciano tracce in giro. Inoltre nella primavera del 2019 c'è stato un terremoto nel mondo dei gruppi Apt iraniani: per settimane qualcuno si è messo a pubblicare su internet e in chiaro informazioni riservate che li riguardavano, incluse le identità di alcuni hacker. Una fuga di notizie che ha fatto da contrappasso per gli iraniani: erano loro che facevano queste cose e di colpo sono diventati vittime dello stesso trattamento. Quelle informazioni hanno permesso di ricostruire come funzionano le campagne iraniane.

Poco più di un anno fa, nel settembre 2020, un gruppo Apt che si fa chiamare Muddy Water (ma si fa chiamare anche TEMP.Zagros, Static Kitten e Seedworm: è esasperante ma funziona così) dette il via alla cosiddetta "Operazione Sabbie mobili", che era una ennesima sequenza di attacchi contro aziende israeliane. Muddy Water era già stato identificato come un gruppo a contratto che lavora per le Guardie della rivoluzione iraniane.

E poi c'è la questione ricorrente dello scopo finale degli attacchi. Nella maggior parte dei casi le incursioni dei gruppi Apt iraniani contro bersagli israeliani hanno una doppia finalità. Gli hacker danneggiano un'azienda, ne paralizzano il lavoro, rubano una quantità immensa di dati e ottengono anche il pagamento di un riscatto per sbloccare i computer infettati – e a volte non ci riescono, come nel caso di Black Shadow. E' una versione moderna della guerra da corsa, quando le nazioni europee autorizzavano i corsari ad attaccare le navi commerciali avversarie e a tenersi, in cambio, il bottino. Ma un'analisi pubblicata a metà novembre che riguarda un gruppo costola di Black Shadow che si fa chiamare Moses Staff nota che gli attacchi di questo gruppo sono soltanto distruttivi. Non c'è più il movente economico, si tira soltanto a fare più male possibile. E' un indizio che gli specialisti dietro alla sigla sono remunerati in un altro modo e che possono permettersi di dedicarsi alle devastazioni senza preoccuparsi di un ritorno in denaro. Come se fossero un settore fra tanti della guerra in corso tra Israele e l'Iran.

Il ministro della Difesa israeliano, Benny Gantz, a inizio novembre è stato il bersaglio di un tentativo di spionaggio sventato all'ultimo (LaPresse)