“Explosion pagers”. Il Washington Post rivela: il piano di Israele ideato prima del 7 ottobre

lantidiplomatico.it/dettnews-explosion_pagers_il_washington_post_rivela_il_piano_di_israele_ideato_prima_del_7_ottobre/45289_57043

Clara Statello - 07 Ottobre 2024 17:00

Emirates ha vietato walkie-talkie e cercapersone a bordo dei propri aerei, in conseguenza ai due attacchi tecnologici condotti da Israele, in varie località del
Libano, il 17 e 18 settembre. L’avviso è apparso nei giorni scorsi, sul sito ufficiale della compagnia. Il divieto riguarda sia il bagaglio a mano che quello inviato in stiva. Saranno sottoposti a confisca della polizia i dispositivi rinvenuti durante i controlli pre-imbarco, in violazione delle nuove restrizioni.

Come avevamo sottolineato in una precedente analisi, l’operazione denominata “explosion pagers” condotta dal’'intelligence israeliani contro Hezbollah, ha segnato uno spartiacque nella guerra elettronica e allertato molti Paesi per la sua potenziale minaccia alla sicurezza (e dunque alla libertà) dei propri cittadini.

La reazione dei servizi russi

I dispositivi elettronici da portare addosso, come quelli utilizzati da Israele per far esplodere i cercapersone dei membri di Hezbollah in Libano e Siria, rappresentano una **minaccia diretta** per la sicurezza della Russia e di altri ex stati sovietici. Lo ha dichiarato il capo dei servizi di sicurezza russi (FSB), Alexander Bortnikov, intervenendo a un incontro dei capi dei servizi speciali della Comunità degli Stati Indipendenti (CSI):

"Come dimostrato dalle recenti azioni con l'esplosione di cercapersone e walkie-talkie in Libano e Siria – ha affermato - i risultati del lavoro dei servizi segreti nemici per raccogliere informazioni sulla vulnerabilità delle risorse informative e l'introduzione segreta di "bookmakers" non possono essere utilizzati solo per distruggere le infrastrutture informative critiche, ma anche per organizzare gli omicidi dei funzionari governativi al momento giusto con l'aiuto dell'elettronica indossabile".

Inoltre, secondo quanto riportato Reuters, per ragioni di sicurezza l'Iran avrebbe iniziato ad importare dispositivi di comunicazione da Cina e Russia, anche se il portavoce del Cremlino, Dmitry Peskov, non ha confermato tali indiscrezioni.

Timore anche per l'India

L'India affronta un'importante minaccia, dal momento in cui la maggior parte della sua componentistica per i dispositivi di comunicazione è importata dall'estero. L'allarme arriva da Pradip R. Sagar, un analista strategico della testata India Today.

La capacità di colpire attraverso dispositivi manomessi è un'azione piuttosto "normale" per le agenzie di sicurezza. Ad esempio l'SBU ha più volte compiuto esecuzioni extragiudiziali contro individui considerati ostili, come Daria Dugina o Vladlen Tatarsky, utilizzando ordigni esplosivi nascosti in auto o oggetti personali.

L'attacco tecnologico contro il Libano segna una svolta nelle operazioni di sabotaggio, per l'intervento a livello di supply chain, che ha consentito di intercettare un ampio stock di dispositivi e manometterli contemporaneamente. Ciò apre un nuovo capitolo nella guerra informatica per la potenzialità di colpire in maniera diffusa, su larga scala, obiettivi connessi a Internet, ad esempio sistemi di comunicazione civili e militari o reti elettriche, per paralizzare un Paese in guerra. La guerra informatica si evolve e viene inaugurata l'era della **guerra informatica cinetica**.

"Mentre gli attacchi informatici comportano un tentativo di danneggiare i computer o le reti informatiche di un'altra nazione tramite virus o attacchi denial-of-service, gli attacchi informatici cinetici utilizzano attacchi informatici per infliggere danni cinetici (o fisici) alle infrastrutture o causare lesioni o morte alle persone. La crescita dei sistemi informatici fisici

in ogni bene, dalle automobili, agli aerei, ai gadget personali e agli elettrodomestici, alle grandi risorse nazionali/militari, apre **spaventose possibilità di atti di sabotaggio** con elementi sia fisici che informatici", scrive Sagar.

La guerra arriva nelle nostre case, nelle nostre borse, nelle nostre tasche.

Nuovi dettagli dell'attacco tecnologico rivelati dal Washington Post

Il piano per colpire Hezbollah con pager trasformati in ordigni esplosivi azionabili da remoto, è stato concepito prima dell'attacco del 7 ottobre in Israele, nella sede centrale del Mossad a Tel Aviv. L'intelligence israeliana si è avvalsa di un gruppo di agenti e complici inconsapevoli in tutto il mondo. Lo si apprende da un dettagliato report pubblicato sabato 5 ottobre dal Washington post. Alcune parti del piano sono state sviluppate anni prima. Il Mossad ha iniziato ad inserire in Libano gli walkie talkie con trappole esplosive nel 2015. Contenevano batterie sovradimensionate, un esplosivo nascosto e un sistema di trasmissione che dava a Israele accesso completo alle comunicazioni di Hezbollah. "Per nove anni, gli israeliani si sono accontentati di origliare Hezbollah, riservandosi l'opzione di trasformare i walkie-talkie in bombe in una crisi futura", scrive il WP, citando funzionari sotto anonimato. L'occasione è arrivata quando Hezbollah si è mostrata interessata ai cercapersone Apollo, un modello "leggermente ingombrante ma robusto, costruito per sopravvivere alle condizioni del campo di battaglia". La batteria sovradimensionata, infatti, poteva funzionare per mesi senza essere ricaricata. Inoltre la casa produttrice (taiwanese) non era riconducibile a Israele. Quello che Hezbollah non poteva sapere era che la produzione dei lotti ordinati fosse stata esternalizzata ed i dispositivi assemblati in Israele sotto la supervisione del Mossad, tramite un intermediario.

I cercapersone "ciascuno del peso di meno di tre once, includevano una caratteristica unica: un pacco batteria che nascondeva una piccola quantità di un potente esplosivo, secondo i funzionari a conoscenza della trama", viene riferito.

Anche se il dispositivo fosse stato smontato, l'esplosivo era stato nascosto con tanta cura da non poter essere rilevato neanche ai raggi X. Invisibile a qualsiasi controllo. Ed è esattamente questo che desta la preoccupazione delle agenzie di sicurezza di tutto il mondo.

Invisibile era anche l'accesso remoto del Mossad ai dispositivi. Ad innescare contemporaneamente l'esplosione di migliaia di dispositivi era un segnale elettronico dal servizio di intelligence. Per garantire il massimo danno, l'esplosione era innescata da una speciale procedura in due fasi richiesta per visualizzare messaggi sicuri che erano stati crittografati. Al destinatario veniva chiesto di premere contemporaneamente due pulsanti per leggere poter leggere un messaggio crittografato, in modo da ferire o amputare entrambe le mani e renderlo incapace di combattere.

Le conseguenze sulla sicurezza globale

Hezbollah aveva iniziato ad utilizzare tecnologia “legacy” per ragioni di sicurezza, in quanto i vertici del gruppo ritenevano tali sistemi irrintracciabili e non hackerabili dai servizi israeliani. Ciò non ha impedito all’intelligence israeliana di sfruttare le vulnerabilità di questi dispositivi, causando un'interruzione diffusa dei sistemi di comunicazione delle milizie sciite e creando caos nei protocolli di risposta alle emergenze. L’attacco con i cercapersona ha anche dimostrato come persino tecnologie apparentemente innocue possano essere trasformate in moderne armi della guerra informatica.

Sono notevoli le conseguenze sulla dimensione psicologica: la popolazione è scioccata, impaurita e vive in un diffuso senso di insicurezza dall’attacco informatico-cinetico.

Le ripercussioni principali, però, riguardano la sicurezza informatica. Secondo il sito specializzato Techdotreviews l’attacco informatico-cinetico mette in luce non solo le vulnerabilità di sistemi considerati sicuri in quanto obsoleti, ma dei servizi critici in generale. Il rischio di una loro compromissione rappresenta una sfida non solo per la sicurezza nazionale ma anche pubblica.

Di conseguenza la minaccia di un attacco tecnologico, simile a quello lanciato da Israele, non riguarda soltanto gli attori della regione, ma tutto il mondo. La nuova guerra informatica non conosce confini.