Data breach, il progetto americano ‘Sea Dragon’ hackerato dalla Cina

Secondo una notizia apparsa sul **Washington Post** i computers appartenenti ad una società appaltatrice della **US Navy** sarebbero stati hackerati. Le informazioni sottratte riguarderebbero alcuni progetti secretati relativi allo sviluppo di un missile supersonico anti-nave da equipaggiare sui sottomarini americani entro il 2020.

Il data breach sarebbe avvenuto fra gennaio e febbraio 2018. Gli hackers avrebbero preso di mira un contractor che lavora al progetto per conto del **Naval Undersea Warfare Center**, organizzazione militare con sede a **New Port** (Rhode Island), impegnata nella ricerca e sviluppo di sottomarini e dei relativi armamenti.

Il bottino degli hackers ammonterebbe a circa 614 gigabytes di materiale e consterebbe di telemetria, informazioni su un sistema crittografico installato sulle comunicazioni radio, informazioni sullo sviluppo di alcune unità di sottomarini, nonché informazioni relative ad un progetto noto come “Sea Dragon”.

Nonostante i dati rubati siano di evidente sensibilità per la sicurezza nazionale, essi si trovavano su una rete non classificata. Si tratta di reti che vengono utilizzate dal Dipartimento della Difesa (DOD) per lo scambio di informazioni non soggette a classifiche di segretezza. Tuttavia, secondo

quanto dichiarato da alcuni ufficiali della marina al Washington Post, se le informazioni rubate dovessero essere riunite il quadro risultante potrebbe essere identificato come classificato. Ciò solleva preoccupazioni in merito alla capacità del Dipartimento della Difesa americano nel mantenere elevati standard di segretezza anche quando le informazioni classificate vengono gestite e utilizzate dai contractor nella realizzazione degli appalti (si veda il caso del contractor Snowden).

La notizia del data breach è stata valutata dai giornalisti del Post all'interno della lunga corsa da parte americana nella ricerca della supremazia tecnologica militare e nel consolidamento militare nell'est asiatico. Inoltre, l'hackeraggio avviane nel momento in cui l'amministrazione Trump cerca il supporto della Cina nella contesa nucleare della penisola koreana.

Il progetto Sea Dragon

Il progetto Sea Dragon è un'iniziativa – valuta dall'ufficio affari speciali del Pentagono – originata nel 2012, con lo scopo di adattare le esistenti tecnologie militari dell'esercito amaricano in virtù delle moderne tecnologie e verificando nuove possibili applicazioni. Il Dipartimento della Difesa, sulla base delle classifiche di segretezza, non ha rilasciato al Post informazioni dettagliate, tuttavia ha ribadito che il progetto si prefigge di introdurre una capacità offensiva tale da rappresentare l'integrazione fra alcune tecnologie esistenti che riguardano i sistemi di armamento e una piattaforma navale. Il costo del progetto – terminato alla fine del 2015 – è di oltre i 300 milioni di dollari con l'inizio dei test previsto per settembre 2018.

La United States Navy è da sempre sinonimo di dominio militare sui mari. Ma la Cina, oltre ad aver creato una delle più grandi flotte mercantili – se non la più grande – al mondo, nel corso degli ultimi anni ha investito energie e denaro anche per ampliare le piattaforme e sottomarini militari. Proprio in virtù di questo impegno cinese, gli Stati Uniti hanno ritenuto necessario sviluppare progetti di ricerca di nuove armi o sistemi che potessero contrastare le "scoperte" della controparte cinese.

Secondo l'analista navale Bryan Clark, le forze della marina militare USA potrebbero avere difficoltà ad operare in alcune aree dell'Asia, ad eccezione dei sottomarini. Questo perché i cinesi non dispongono di un'adeguata capacità di risposta e adeguati armamenti che contrastino molteplici incursioni contemporanee di sottomarini. Questa constatazione ha fatto si che la marina militare americana identificasse nello sviluppo di una flotta di sottomarini l' elemento chiave di svolta per la supremazia nei mari asiatici.

Una lunga scia di hacking

Per anni la Cina è riuscita a raccogliere informazioni dall'esercito americano attraverso una serie di cyber operazioni. Alcuni esempi riguardano la raccolta di informazioni sul design degli F-35 Joint Strike Fighter, informazioni sul sistema missilistico Patriot Pac-3 e quelle relative al sistema di armamento Termal High Altitude Area Defense, nonché varie informazioni sulle navi da combattimento di nuova generazione. Alcune prove relative a tali hackeraggi riguardano ad esempio i droni utilizzati dall'esercito cinese che appaiono come vere e proprie imitazioni della controparte americana.

Dopo l’avvenuta pubblicazione di tale notizia da parte del Washington Post, **Jim Mattis**, Segretario della Difesa Americana, ha richiesto un’investigazione sull’accaduto da parte del Pentagono.

Da parte della Marina invece, oltre alla conferma del supporto da parte dell’FBI, il portavoce Bill Speaks afferma che la marina sta ponendo in essere una serie di misure che richiedono alla società appaltatrice di inviare un’immediata segnalazione quando si verificano cyber incidenti, che hanno un attuale o potenziale effetto avverso sulla propria rete in cui vengono custodite le informazioni.

Viste i recenti cambiamenti in ottica cyber sicurezza all’interno dell’amministrazione Trump, la domanda da porsi è in che modo verrà efficacemente affrontata tale situazione anche a fronte dell’avvenuta eliminazione della figura di Cyber Coordinator?

Ciò che è necessario considerare è che già a partire dal febbraio scorso, nella pubblicazione “Worldwide Threat Assessment of the US Intelligene Community”, Daniel Coats – Director of National Intelligence – aveva indicato come l’intelligence americana deteneva prove concordanti su una cyber operation cinese ai danni di alcune società appaltatrici e security firms che collaborano col Governo americano.

Quale sarà la prospettiva futura?

Nel settembre 2015 l’allora presidente americano Barak Obama e

il presidente cinese Xi Jinping raggiunsero un accordo per la limitazione del cyber spionaggio fra i due Paesi.

A marzo 2018 l'amministrazione Trump si è espressa affermando – con particolare chiarezza – che il governo cinese ha "rotto" quell'accordo, riprendendo intensamente una campagna per rubare informazioni alle business companies americane. Nello specifico, il Dipartimento del Tesoro ha pubblicato una dettagliata investigazione di 215 pagine in cui si evidenziano molteplici casi di cyber spionaggio ai danni della proprietà intellettuale. Va tuttavia sottolineato che il rapporto non fornisce dettagli specifici sugli incidenti e sulle loro modalità di engagement.

Questo quadro mostra come le autorità americane abbiano specificatamente monitorato tali operazioni cibernetiche avendo, a tal proposito, le necessarie prove per porre in essere una difesa cibernetica nazionale efficace. Come precedentemente ricordato, già nel febbraio 2018 l'intelligence Usa ha preventivamente identificato una possibile superficie d'attacco nelle reti delle società sotto contratto col Governo americano.

Tuttavia, sembra che, nonostante il quantitativo di prove raccolte, l'amministrazione Trump non sia ancora in grado di stabilire una politica efficace che prevenga le cyber intrusioni. Fattore particolarmente allarmante se si considera la mancanza di un responsabile al vertice della cyber sicurezza americana.

Questo articolo è apparso originariamente su *Cybersecitalia.it*

The post Data breach, il progetto americano ‘Sea Dragon’ hackerato dalla Cina appeared first on Key4biz.

https://www.key4biz.it/data-breach-il-progetto-americano-sea-dragon-hackerato-dalla-cina/224555/