Tecnologia - *Cybersecurity advisory internazionale sulle atttività del Gru russo, Claroty: "Una delle prime campagne davvero strutturate"*

Roma - 29 mag 2025 (Prima Notizia 24) **Pubblicato dalla Nsa in collaborazione con partner europei, il report segnala una campagna di cyber-spionaggio contro enti logistici e tecnologici, con obiettivi colpiti anche in Italia.**

Il 21 maggio, la National Security Agency (NSA), in collaborazione con numerose agenzie statunitensi e internazionali, ha pubblicato un nuovo avviso congiunto di sicurezza informatica (Cybersecurity Advisory - CSA) dal titolo “Russian GRU Targeting Western Logistics Entities and Technology”. L’iniziativa mira a sensibilizzare governi e aziende su una sofisticata campagna di cyber-spionaggio sponsorizzata dal governo russo e condotta dalla Unità 26165 del GRU (Russian General Staff Main Intelligence Directorate), nota anche come APT28 o Fancy Bear. Secondo il CSA, l’operazione – attiva almeno dal febbraio 2022 – prende di mira organizzazioni governative e aziende attive nei settori della logistica, dei trasporti e della tecnologia, in particolare quelle coinvolte nel supporto all’Ucraina. Gli attacchi sfruttano vulnerabilità in dispositivi IoT, come telecamere di sorveglianza connesse a Internet, dislocate anche nei Paesi confinanti con l’Ucraina. Tra i Paesi colpiti figura anche l’Italia, dove sono stati identificati obiettivi strategici nel settore pubblico e privato, tra cui nodi logistici, hub di trasporto e fornitori di servizi IT. Il CSA fornisce una serie di raccomandazioni operative per le organizzazioni potenzialmente a rischio, tra cui il potenziamento delle attività di monitoraggio, l’adozione di pratiche di threat hunting e l’attenta analisi degli indicatori di compromissione (IOC) e delle metodologie operative associate a questa minaccia. “Pur non facendo ricorso a tecniche particolarmente sofisticate, questa rappresenta una delle prime campagne davvero strutturate che ho avuto modo di osservare, in cui attacchi informatici coordinati e pianificati vengono utilizzati contro sistemi IT e sistemi cyber-fisici per ottenere una comprensione dettagliata dei sistemi d’arma e di altri supporti forniti all’Ucraina. Il GRU non è interessato solo al tipo di supporto che le nazioni stanno fornendo all’Ucraina, ma ha effettuato un targeting dettagliato lungo tutta la catena di approvvigionamento per comprendere quali attrezzature stanno circolando, quando e come, che sia per via aerea, navale o ferroviaria. Un livello di precisione che può alimentare tanto le operazioni d’intelligence quanto eventuali attacchi cinetici mirati alle infrastrutture critiche. Il fatto che ci siano oltre 10.000 telecamere IoT compromesse, l’83% delle quali in Ucraina, mostra fino a che punto siano disposti a spingersi per ottenere conferme spaziali e analisi di ciò che accade nel mondo fisico. Sebbene a questo stadio l’operazione sembri oggi focalizzata principalmente sull’attività di spionaggio per ottenere informazioni, non è difficile immaginare una sua evoluzione verso interruzioni operative nelle catene logistiche e nei sistemi di trasporto, con potenziali ripercussioni a livello globale. La pubblicazione dell’avviso,

che coincide con un momento di discussione su possibili scenari di pace, invita alla riflessione. Ciò che emerge con chiarezza, però, è che questa campagna è in corso almeno dal febbraio 2022 e testimonia come i conflitti moderni si estendano anche al dominio digitale, coinvolgendo reti, sensori e sistemi di sorveglianza. Le organizzazioni nei settori della logistica, dei trasporti e della tecnologia devono trattare questa minaccia con la massima serietà, seguendo le raccomandazioni del CSA per prevenire attacchi informatici e cinetici. Siamo abituati a pensare alla cybersicurezza come qualcosa che riguarda solo i sistemi IT. Ma questo avviso dimostra chiaramente come la Russia stia sfruttando in modo sistematico le vulnerabilità degli asset IoT – come i sistemi di videosorveglianza – per mappare il mondo reale in tempo reale, a supporto dei propri sforzi bellici", ha commentato Grant Geyer, Chief Strategy Officer di Claroty.

(Prima Notizia 24) Giovedì 29 Maggio 2025