di **STEFANO PIAZZA**

Da un report segreto spunta la pista iraniana

In un documento rivelato da Sky i piani dell'intelligence di Teheran per attentati online all'Occidente

■ Una ridda di ipotesi avvolge l'attacco ancora in corso al Centro elaborazione dati della Regione Lazio che ha spento il portale Salute e quello della rete vaccinale. L'attacco sarebbe partito dall'estero. Ma chi è stato? I soliti hacker russi, forse i cinesi o nordcoreani? Chi è stato a inviare un ransomware, un virus che blocca i sistemi informatici criptandoli e che chiede quasi sempre un riscatto in bitcoin? E se l'attacco fosse stato sferrato dall'Unità cibernetica del corpo delle Guardie rivoluzionarie islamiche iraniane, meglio conosciuta come Unità 13 o Intelligence team 13, sottogruppo dell'Unità Irgc Shahid Kaveh?

Scorrendo un segretissimo report di 57 pagine che è stato pubblicato da *Sky News* lunedì scorso, emergono allarmanti notizie sulle attività degli hacker della Repubblica islamica. Nelle cinque cartelle troviamo sulla parte superiore di quasi tutti file una citazione di **Alì Khamenei**, leader supremo dell'Iran: «La Repubblica islamica dell'Iran deve diventare tra le più potenti al mondo nell'area della cyber»; ci sono i piani iraniani per hackerare le infrastrutture sensibili nei Paesi occidentali, comprese l'Europa e l'Italia.

Tra le strutture da violare ci sono banche dati di infrastrutture governative, sistemi idrici di zavorra delle navi da carico, serbatoi di carburante delle stazioni di servizio che potrebbero esplodere e sistemi satellitari utilizzati dall'industria navale globale. Grande attenzione degli hacker iraniani è rivolta ad alcuni software conosciuti come Building management system (Bms) che gestiscono luci, riscaldamento e ventilazione, ascensori, controllo accessi e sistemi di sicurezza negli edifici intelligenti in tutto il mondo compresi aeroporti, metropolitane, porti e stazioni ferroviarie. In particolare, i sistemi che gli iraniani vogliono e possono violare dopo attenti studi son quelli Honeywell, Schneider electric, Siemens e i sistemi della Kmc controls. Ma l'attacco alla Regione Lazio potrebbe essere opera di hacker iraniani?

Secondo **Pierluigi Paganini**, esperto di cybersecurity e intelligence: «L'Unità 13 ha le capacità tecniche per condurre un attacco come quello con il quale ci stiamo confrontando in queste ore, tuttavia le relative tecniche, tattiche e procedure (Ttps) sono dissimili da quelle che stiamo osservando per l'attacco alla Regione Lazio, che parrebbe avere una matrice criminale e non di *nation State*». Sulle modalità con le quali la Regione Lazio è stata messa in ginocchio **Paganini** non ha dubbi: «L'accesso è avvenuto attraverso credenziali Vpn (rete virtuale privata) di un dipendente. Le Vpn sono strumenti che consentono a un dipendente di connettersi in remoto, in sicurezza, alla rete della propria azienda. Gli attaccanti sono riusciti a ottenere le credenziali di accesso Vpn di un dipendente e quindi ad avere accesso alla rete della Regione. È come aver ottenuto le chiavi della porta di accesso alla struttura. Una volta entrati nella rete, gli attaccanti hanno utilizzato malware e tool per fare intelligence sulla struttura compromessa, rubare ulteriori credenziali per accedere a sistemi ospitati su essi e successivamente distribuire il ransomware che ne cifra le informazioni».

Gruppi come l'Unità 13 rappresentano una seria minaccia anche per le aziende di tutto il mondo proprio per gli interessi e le capacità rivelate dal report. Pensiamo alle società che operano nel settore energetico, in passato oggetto di importanti attacchi da parte di unità governative iraniane. Quanto accaduto dal gigante petrolifero Saudi Aramco anni addietro potrebbe accadere nuovamente: in quell'occasione, gruppi riconducibili al governo iraniano impiegarono un wiper, ovvero un malware che infettò e distrusse letteralmente oltre 30.000 sistemi della compagnia.

Oltre a sapere chi è stato a muovere l'attacco alla Regione Lazio, andranno chiarite le responsabilità di chi avrebbe dovuto vigilare e quindi impedire l'attacco cyber. Secondo una fonte della *Verità*, che opera a livello istituzionale in ambito Nato, lo scenario è ancora più allarmante: «Sono molte le cose che non hanno funzionato in questa vicenda e andranno chiarite al più presto perché nel mirino ci sono altre infrastrutture sensibili e quello che si sta vivendo in queste ore non è nulla in confronto alle potenzialità di questi gruppi criminali».