Ci sono prove di un attacco degli hacker russi di APT28 anche in Italia

Lo sostiene una ricerca presentata dallo Z-lab di Cybersec: "Il bersaglio potrebbe essere la Marina italiana". La società di cybersecurity italiana ha incrociato i dati con analisti di una piattaforma aperta: si tratta del medesimo malware del gruppo legato al GRU, un software maligno che ha agito anche nell'hackeraggio delle mail democratiche nelle presidenziali Usa

Alla long story dell'interferenza della Russia nei processi elettorali occidentali, si potrebbe aggiungere un altro tassello. Questa volta la vittima sarebbe l'Italia. Ricercatori di un'azienda di cybersecurity italiana (CSE Cybersec) hanno scoperto che sulle reti italiane è circolato un malware in tutto simile a quello usato dai russi

di Apt28 (aka Fancy Bear, o Pawn Storm), un gruppo paramilitare di hacker ritenuti collegati al GRU, il servizio segreto militare russo. Apt28 è stato a lungo ritenuto l'autore di tante operazioni molto importanti di hacking, tra le quali spicca l'hackeraggkio della primavera del 2016 ai danni delle mail del Comitato nazionale dei democratici, nella corsa verso le elezioni presidenziali americane – prima che il nuovo indictment del Procuratore speciale Robert Mueller accusasse direttamente dodici ufficiali del GRU di aver eseguito, gestito e diretto l'operazione.

L'operazione di spionaggio – che i ricercatori chiamano "Operation Roman Holiday" – dura da alcune settimane, e non è certo chi sia la vittima dell'hackeraggio, ma potrebbe trattarsi della Marina italiana. Lo spiega Pierluigi Paganini, capo tecnologo di CSE Cybsec, che tra l'altro è direttore del Master in cybersecurity alla ormai famosa Link Campus University, intervistato da Agi: «Se adottiamo le logiche degli attaccanti parrebbe un riferimento alla Marina militare italiana e ci invita a verificare l'ipotesi che quel codice malevolo sia stato sviluppato come parte di una serie di attacchi mirati contro la Marina o altre entità ad essa associate, come i suoi fornitori».

Scoperta la "backdoor", la porta posteriore nelle reti, una serie di esempi del malware sono stati inviati da Cybersec a una piattaforma di cybersecurity aperta, Virus Total, attraverso un analista conosciuto online con il nome @drunkbinary. E da questo incrocio di verifiche è risultato confermato, spiegano i ricercatori, che esiste un pezzo di malware (il software maligno che di solito si impianta in un computer nemico, inducendolo a cliccare un link malevolo inviato alla vittima) in tutto analogo a quelli usati dagli hacker di Apt28.

Le somiglianze sono, dal punto d vista dell'evidenza informatica, molto rilevanti: il linguaggio in cui è scritto il codice del malware è uguale a quello di un malware usato dai russi (linguaggio Daphni). I luoghi remoti di command and control verso i quali vengono indirizzati i dati; anche alcune

«librerie dinamiche" che il malware spinge surrettiziamente i computer attaccati a caricare. Non sarebbe il primo attacco russo contro l'infrastruttura italiana: di almeno un'altra circostanza è stato scritto già un anno e mezzo fa dal Guardian, che citò fonti governative, mai smentito da nessuno.
«Non possiamo escludere – sostiene Cybersec – che Apt abbia sviluppato la backdoor per colpire specifiche organizzazioni, tra le quali la Marina militare italiana, o qualche altro subcontractor. Nelle nostre analisi non siamo riusciti a collegare il file malevolo dll ai sample di X-agent trovati, ma crediamo che entrambi siano parte di un attacco ben coordinato e chirurgico di Apt28». Varrà la pena notare che anche nel nuovo indictment di Mueller si racconta delle modalità X-agent con cui ha agito – in questo caso direttamente il GRU -contro le mail dell'ufficio di Hillary Clinton.
La ricerca, pubblica, è stata messa a disposizione sul sito dello Z-Lab di Cybersec. La piattaforma online che l'ha incrociata – VirusTotal – mette a disposizioni alcuni samples riscontrati. Cresce, negli ambienti degli analisti e degli osservatori internazionali, la preoccupazione che il caso Usa non sia affatto isolato. E inquietudini geopolitiche si sommano a quelle forensi: specialmente nel momento in cui il presidente americano Donald Trump, a Helsinki, ha detto di credere a Vladimir Putin, che nega che la Russia abbia hackerato le elezioni Usa, anziché a tutta la comunità dell'intelligence americana, che sostiene il contrario; e nel momento in cui il ministro dell'Interno italiano Matteo Salvini, incontrando a Mosca prima esponenti del Consiglio per la sicurezza nazionale russo, poi il ministro dell'interno russo, ha spiegato che l'Italia coopererà proprio con la Russia «nella cybersecurity e contro gli attacchi informatici», arrivando a scambiarsi – ha scritto Salvini – anche «banche dati» con Mosca.