NAZIONE - Carlino - GIORNO

11-GEN-2017
pagina 2
foglio 1

INTERVISTA PARLA IL DIRIGENTE DELLA POSTALE.
«I DANNI? LI SAPREMO DOPO AVER VISTO I SERVER SEQUESTRATI DALL'FBI»

L'investigatore che li ha scovati: «Decisiva una mail sospetta»

Super software

Occhionero aveva sistemi di alert che lo avvisavano quando tra i pc circolava un nome di interesse

Mega rete

I computer infettati non erano solo saccheggiati, ma venivano usati per compromettere altri pc

«GIULIO Occhionero aveva sistemi automatizzati raffinatissimi per la gestione della gran mole d'informazioni, tra questi software che, attraverso la ricerca di parole chiave, gli mandavano in tempo reale degli alert se tra le migliaia di computer sotto controllo circolava un nome o una parola di interesse. Un'arma potentissima». Ivano Gabrielli **(nella foto)**, vicequestore del Cnaipc, è uno degli investigatori della polizia postale che ha scoperto la mega rete segreta.

Come è nata l'indagine?

«Da una mail. Ci siamo attivati perchè il responsabile della sicurezza di una delle infrastrutture critiche che monitoriamo, Enav, si è insospettito per un messaggio di posta elettronica inviato da uno studio legale con il quale loro non collaboravano. L'intuizione era giusta. La mail è stata sviscerata, si è scoperto che in allegato aveva un malware ed era transitata da un nodo Tor che rende anonima la fonte. Sospetto. I nostri tecnici hanno allora studiato il malware e decrittato il percorso che avrebbero dovuto fare le informazioni carpite fino ad arrivare al centro di comando e controllo, che era negli Stati Uniti. Una serie di indagini attorno a quello ci ha permesso di capire l'infrastruttura e di ricondurla a chi l'aveva originata, che si celava dietro nomi di fantasia e scatole cinesi, ma non abbastanza per non essere raggiunto da noi».

Come?

«Studiando un account del dominio *hotspenta*, al quale venivano mandati i dati, abbiamo visto che era legato ad altri riconducibili a Giulio Occhionero e alla sorella. Inoltre, ulteriori accertamenti effettuati dall'Fbi hanno permesso di appurare che la licenza relativa al componente utilizzato dal malware dal 2010 al dicembre 2015 risultava acquista da Giulio Occhionero. E a quel punto abbiamo disposto una serie di accertamenti tecnici e siamo passati alle intercettazioni telematiche e telefoniche. E li abbiamo fatti arrestare. Da notare che durante l'arresto hanno cercato di distruggere i dati contenuti nei loro computer».

Quanto grande era la rete?

«La rete si è accresciuta ed evoluta negli anni, ed era in continua evoluzione. Per adesso parliamo di oltre 18mila computer infettati, solo una parte dei quali era sotto pieno controllo. I computer infetti non erano solo saccheggiati di ogni tipo di dati, ma venivano anche utilizzati per far partire mail con le quali infettare altri computer attraverso allegati contenenti il noto malware».

Avete la certezza che gli Occhionero siano davvero riusciti a rubare informazioni ai vertici politici ed economici?

«Abbiamo la certezza del tentativo di infezione si 18mila macchine, avremo la certezza dell'avvenuta infezione solo quando avremo in mano i server che abbiamo sequestrato con l'Fbi. Dall'analisi dei files scaricati da quando era sotto intercettazione abbiamo già un primissimo elenco di 100 computer certamente compromessi. Ma è solo la punta dell'iceberg. Andavano arrestati ora per evitare che fuggissero e inquinassero le prove, ma il lavoro continua».

Alessandro Farruggia


TRAPPOLA WEB
Smantellata centrale di cyber spioni «Dossier su Renzi, Draghi, Monti»
Massoneria e business
L'investigatore che li ha scovati: «Decisiva una mail sospetta»