Corriere del Mezzogiorno - Campania - Domenica 6 Dicembre 2020

Cyberwar a Pomigliano, spiati i Pc della Leonardoe rubati centomila file

Arrestati un ex collaboratore e un dipendente del team security

L'azienda: «Ma i dati top secret sono conservati in server protetti»

napoli Il computer che gira troppo lentamente, come mai aveva fatto fino a poco prima. E la stessa cosa accade ad un certo numero di altri Pc. Se fossimo nel tinello di casa penseremmo ad una macchina ormai alquanto vecchiotta. Ma non siamo nel tinello di casa. Siamo negli uffici della Leonardo di Pomigliano (ex Alenia) ed un pc che non va — così come molti altri — accende un allarme. Siamo nel 2017; ma è soltanto ieri che si è stabilito che Pomigliano potrebbe essere diventata una delle importanti tessere della silenziosa cyberwar che mira a trafugare progetti industriali, specifiche militari, big data classificati. L'obiettivo? Venderli ad un qualche Paese straniero o a una qualche fazione terroristica. Uno scenario inquietante.

Era il 2017, dunque. I tecnici del Cyber emergency response team di Leonardo (organismo deputato alla gestione degli attacchi informatici subiti dall'azienda) hanno un grattacapo: avevano notato un traffico di rete anomalo in uscita da alcune postazioni di lavoro dello stabilimento, generato da un software artefatto denominato "cftmon.exe", sconosciuto ai sistemi antivirus aziendali. Ma quello che ancora non sapevano è che tra loro ci sarebbe stata una talpa, addirittura il loro responsabile: Antonio Rossi. Il cerchio delle indagini si è chiuso ieri, portate avanti dal gruppo di lavoro sul cybercrime della Procura di Napoli (pm Claudio Onorati e Maria Sofia Cozza, procuratore aggiunto Vincenzo Piscitelli) e culminate nell'esecuzione di due ordinanza di custodia cautelare: una a carico proprio di Rossi, attualmente nella pianta organica di Leonardo, accusato di depistaggio e finito ai domiciliari; l'altra nei confronti di Arturo D'Elia — la vera cyber-spia attorno alla quale ruota tutta l'inchiesta — già ex collaboratore di Leonardo negli anni scorsi (e che gli inquirenti affermano essere stato troppo tardivamente allontanato), accusato di «accesso abusivo a sistema informatico, intercettazione illecita di comunicazioni telematiche e trattamento illecito di dati personali» e che il gip ha messo dietro le sbarre.

Per dirne una: D'Elia era riuscito addirittura a mettere a segno con successo un attacco informatico a una base Nato americana, operante sul territorio italiano. Un'azione per la quale andava così fiero tanto da annotarla sul suo curriculum, senza però specificare che proprio per quel crimine informatico era stato condannato.

Era il 2017, dunque. Il traffico anomalo risultava diretto verso una pagina web denominata www.fujinama.altervista.org , di cui è stato richiesto e disposto e ieri eseguito il sequestro preventivo. Secondo la prima denuncia di Leonardo, l'anomalia informatica sarebbe stata circoscritta ad un numero ristretto di postazioni e connotata da un'esfiltrazione di dati ritenuta non significativa. Le successive indagini hanno ricostruito uno scenario ben più esteso e severo: gli inquirenti parlano tranquillamente «di cyberwar e di materiale strategico con finalità militari». Perché Leonardo non costruisce soltanto parti di velivoli civili come Boeing o Atr ma anche radar e sistemi di gestione di apparecchiature per la sicurezza e difesa del Paese. Gli inquirenti hanno capito che, per quasi due anni (tra maggio 2015 e gennaio 2017), Leonardo è stata colpita da un attacco mirato e persistente (noto come Advanced persistent threat o Apt), poiché «realizzato con l'installazione nei sistemi, nelle reti e nei Pc-bersaglio, di un codice malevolo finalizzato alla creazione e al mantenimento di canali di comunicazione attivi e idonei a consentire l'esfiltrazione silenziosa di rilevanti quantitativi di dati e informazioni classificati di rilevante valore aziendale».

Il software malevolo si comportava come un trojan di nuova ingegnerizzazione, inoculato mediante l'inserimento di chiavette usb nei Pc spiati, e permetteva di intercettare quanto digitato sulla tastiera delle postazioni infettate e catturare i fotogrammi di ciò che risultava visualizzato sugli schermi. Faceva in sostanza, quel che facciamo a volte

tutti noi con i nostri smartphone, uno screen shot dello schermo, solo a livelli molto più elevati. Tanto che la cyber-spia collegandosi al centro di comando e controllo del sito web "fujinama", dopo aver scaricato i dati carpiti, cancellava da remoto ogni traccia sulle macchine compromesse. Sono 33 le postazioni di lavoro hackerate alla Leonardo di Pomigliano d'Arco. «Su tali postazioni — afferma la Procura — erano configurati molteplici profili utente in uso a dipendenti, anche con mansioni dirigenziali. In totale risultano sottratti, dai 33 Pc-bersaglio, 10 gigabyte di dati, pari a circa 100 mila file, riguardanti la gestione amministrativo-contabile, l'impiego delle risorse umane, l'approvvigionamento e la distribuzione dei beni strumentali, nonché la progettazione di componenti di aeromobili civili e di velivoli militari destinati al mercato interno e internazionale».

Una tegola sul capo di Leonardo, azienda quotata in Borsa e unanimemente riconosciuta al top nel sistema industriale italiano. «Leonardo — si legge in una nota del management — è ovviamente parte lesa in questa vicenda, ha fornito fin dall'inizio e continuerà a fornire la massima collaborazione agli inquirenti per fare chiarezza sull'accaduto e a propria tutela. Si precisa infine che dati classificati ossia strategici sono trattati in aree segregate e quindi prive di connettività e comunque non presenti nel sito di Pomigliano».