Polizia di Stato

Napoli: indagini attacco informatico a Leonardo Spa

All'esito di complesse attività d'indagine del Gruppo di lavoro sul *cybercrime* della Procura della Repubblica di Napoli, volte a definire i contorni di un grave attacco alle strutture informatiche della Divisione Aerostrutture e della Divisione Velivoli di Leonardo S.p.A. , il C.N.A.I.P.I.C. del Servizio Centrale della Polizia Postale e delle comunicazioni e il Compartimento campano del medesimo servizio hanno eseguito due ordinanze applicative di misure cautelari nei confronti di un *ex* dipendente e di un dirigente della predetta società, essendo gravemente indiziati, il primo, dei delitti di accesso abusivo a sistema informatico, intercettazione illecita di comunicazioni telematiche e trattamento illecito di dati personali (rispettivamente previsti dagli artt. 615-*ter*, commi 1, 2 e 3, 617*quater*, commi 1 e 4, c.p., e 167 d.lgs. 196/2003, in relazione all'art. 43 d.lgs. 51/2018) e, il secondo, del delitto di depistaggio (art. 375, comma 1, lett. a e b, e 2, c.p.). Nel gennaio 2017 la struttura di *cyber security* di Leonardo S.p.A. aveva segnalato un traffico di rete anomalo, in uscita da alcune postazioni di lavoro dello stabilimento di Pomigliano D'Arco, generato da un *software* artefatto denominato *"cftmon.exe"*, sconosciuto ai sistemi antivirus aziendali. Il traffico anomalo risultava diretto verso una pagina *web* denominata *"www.fujinama.altervista.org"*, di cui è stato richiesto e disposto, ed oggi eseguito, il sequestro preventivo. Secondo la prima denuncia di Leonardo S.p.A., 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. Infatti, le indagini hanno evidenziato che, per quasi due anni (tra maggio 2015 e gennaio 2017), le strutture informatiche di Leonardo S.p.A. erano state colpite da un attacco informatico mirato e persistente (noto come *Advanced Persistent Threat* o *APT*), poiché realizzato con installazione nei sistemi, nelle reti e nelle macchine bersaglio, di un codice malevolo finalizzato alla creazione ed il mantenimento di attivi canali di comunicazione idonei a consentire l'esfiltrazione silente di rilevanti quantitativi di dati e informazioni classificati di rilevante valore aziendale. In particolare, allo stato delle acquisizioni, risulta che tale grave attacco informatico è stato condotto da un addetto alla gestione della sicurezza informatica della stessa Leonardo S.p.A., nei confronti del quale il G.I.P. del Tribunale di Napoli ha disposto la misura della custodia cautelare in carcere. È emerso, infatti, che il *software* malevolo - creato per finalità illecite delle quali è in corso la compiuta ricostruzione - si comportava come un vero e proprio *trojan* di nuova ingegnerizzazione, inoculato mediante l'inserimento di chiavette USB nei PC spiati, in grado così di avviarsi automaticamente ad ogni esecuzione del sistema operativo. Risultava dunque possibile all'*hacker* intercettare quanto digitato sulla tastiera delle postazioni infettate e catturare i fotogrammi di ciò che risultava visualizzato sugli schermi (*screen capturing*). Dati aziendali riservati dello stabilimento di Pomigliano D'Arco di Leonardo S.p.a. erano così di fatto nel pieno controllo dell'attaccante, che, grazie alle proprie mansioni aziendali, era nel tempo in grado di installare più versioni evolutive del *malware*, con capacità ed effetti sempre più invasivi e penetranti. Le indagini hanno permesso, infine, di ricostruire l'attività di *antiforensic* dell'attaccante, che collegandosi al C&C (centro di comando e controllo) del sito *web* "*fujinama*", dopo aver scaricato i dati carpiti, cancellava da remoto ogni traccia sulle macchine compromesse. L'attacco informatico così realizzato, secondo la ricostruzione operata dalla Polizia delle Comunicazioni, è classificato come estremamente grave, in quanto la superficie dell'attacco ha interessato ben 94 postazioni di lavoro, delle quali 33 collocate presso lo stabilimento aziendale di Pomigliano D'Arco. Su tali postazioni erano configurati molteplici profili utente in uso a dipendenti, anche con mansioni dirigenziali, impegnati in attività d'impresa volta alla produzione di beni e servizi di carattere strategico per la sicurezza e la difesa del Paese. La gravità dell'incidente emerge anche dalla tipologia delle informazioni sottratte, tenuto conto che dalle 33 macchine bersaglio ubicate a Pomigliano d'Arco risulterano, allo stato, esfiltrati 10 Giga di dati, pari a circa 100.000 *files*, afferenti alla gestione amministrativo/contabile, all'impiego delle risorse umane, all'approvvigionamento e alla distribuzione dei beni strumentali, nonché alla progettazione di componenti di aeromobili civili e di velivoli militari destinati al mercato interno e internazionale. Accanto ai dati aziendali, sono state oggetto di captazione anche le credenziali di accesso ed altre informazioni personali dei dipendenti della Leonardo. Oltre alle postazioni informatiche dello stabilimento di Pomigliano D'Arco, sono state infettate 13 postazioni di una società del gruppo Alcatel, alle quali se ne sono aggiunte altre 48, in uso a soggetti privati nonché ad aziende operanti nel settore della produzione aerospaziale. Accanto agli accertamenti di natura informatica, sono state fondamentali le attività di indagine più tradizionali, che hanno permesso anche di ricostruire il percorso di formazione "cybercriminale" dell'indagato allo stato individuato come autore materiale dell'attacco, attualmente impiegato presso altra società operante nel settore dell'elettronica informatica.Ulteriori approfondimenti hanno consentito di raccogliere altresì convergenti indizi di colpevolezza riguardanti la commissione del reato di depistaggio da parte del responsabile del C.E.R.T. (*Cyber Emergency Readiness Team*) di Leonardo s.p.a., organismo

deputato alla gestione degli attacchi informatici subiti dall’azienda. Nei confronti di quest’ultimo, è stata applicata la misura cautelare della custodia domiciliare, risultando gravi indizi di colpevolezza con riferimento ad insidiose e reiterate attività di inquinamento probatorio, finalizzate a dare una rappresentazione falsa e fuorviante della natura e degli effetti dell’attacco informatico e ad ostacolare le indagini.

05/12/2020