Attacco Hacker a Leonardo Spa, 2 arresti

Sono stati individuati e arrestati, dai poliziotti del Cnaipic e del compartimento della Polizia postale di Napoli, i responsabili degli attacchi alle strutture informatiche di Leonardo Spa.

I due, un ex dipendente e un dirigente della società, sono accusati dei delitti di accesso abusivo a sistema informatico, intercettazione illecita di comunicazioni telematiche e trattamento illecito di dati personali e di depistaggio.

Nella prima denuncia fatta nel 2017, la società Leonardo Spa segnalava un traffico anomalo di dati in uscita dallo stabilimento di Pomigliano D'Arco (Napoli). Il traffico anomalo risultava diretto verso una pagina web di cui è stato eseguito il sequestro preventivo. L'anomalia informatica sembrava circoscritta ad un numero ristretto di postazioni con una perdita di dati ritenuta non significativa.

Le successive indagini hanno ricostruito uno scenario ben piu? esteso. Infatti è emerso, per quasi due anni, tra maggio 2015 e gennaio 2017, le strutture informatiche di Leonardo Spa erano state colpite da un attacco informatico mirato e persistente (noto come Advanced Persistent Threat o APT), realizzato con installazione nei sistemi, nelle reti e nelle macchine bersaglio, di un codice malevolo finalizzato alla creazione ed al mantenimento di attivi canali di comunicazione idonei a consentire una perdita di dati lenta e continua di elevati quantitativi di dati e informazioni di importante valore aziendale.

Il responsabile di questo attacco è stato un addetto alla gestione della sicurezza informatica della stessa Leonardo Spa che è stato arrestato. Il software da lui creato, era stato inserito mediante chiavette Usb nei pc spiati, in grado cosi? 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 cio? che risultava visualizzato sugli schermi.

Su tali postazioni erano configurati profili utente in uso a dipendenti, anche con mansioni dirigenziali, impegnati in attività di carattere strategico per la sicurezza e la difesa del Paese.

Le informazioni sottratte, oltre 100mila file, riguardano, oltre i dati personali dei dipendenti, la progettazione di componenti di aeromobili civili e di velivoli militari destinati al mercato interno e internazionale.

Oltre alle postazioni informatiche dello stabilimento di Pomigliano D'Arco, sono state infettate 13 postazioni di una società del gruppo Alcatel e 48 di privati e aziende operanti nel settore della produzione aerospaziale.

Ulteriori approfondimenti hanno consentito di arrivare al responsabile del Cert (Cyber Emergency Readiness Team) di Leonardo, organismo deputato alla gestione degli attacchi informatici subiti dall'azienda.

Nei suoi confronti è stata applicata la misura cautelare della custodia domiciliare in quanto responsabile di aver falsato e minimizzato la natura e gli effetti dell'attacco informatico e, quindi, di aver ostacolato le indagini.

Donatella Fioroni

05/12/2020