

Paragon: la vicenda dello spyware Graphite, i chiarimenti del Garante Privacy e il ruolo dell'ACN



Paragon Solutions ltd., società israeliana specializzata in strumenti *cyber offensive*, ha conquistato nelle ultime settimane un posto di rilievo nella cronaca nazionale e internazionale.

Vediamo in dettaglio come si sia sviluppata la vicenda, in merito alla quale si è recentemente pronunciato anche il Garante italiano per la Protezione dei dati personali.

Paragon Solutions: la società israeliana dietro allo spyware Graphite

Fondata nel 2019 da alcuni ex membri dell'esercito israeliano (IDF), tutti esperti in raccolta di informazioni e *intelligence* militare, la Paragon si è sempre più specializzata nello sviluppo di strumenti di *Signal Intelligence* (SIGINT).

Alla fine del 2024 la società è stata acquisita, per circa un miliardo di dollari, da un fondo di *private equity* statunitense. Dalle notizie trapelate sembra che verrà fusa con altre aziende già in forza al Dipartimento della Difesa di Washington, entrando a far parte delle risorse di *cyber intelligence* targate USA.

Sul piano dell'offerta commerciale una delle principali

soluzioni di Paragon è lo *spyware* Graphite, un *trojan* creato per intercettare le comunicazioni su app di messaggistica istantanea o via email, installandosi sui dispositivi tramite attacchi “*zero-click*”.

E lo scorso 31 gennaio è stata proprio una piattaforma di messaggistica, Whatsapp, a denunciare l'uso del software Graphite per spiare decine di suoi utenti – inclusi giornalisti, attivisti e rappresentanti di varie ONG – in 24 paesi, fra i quali l'Italia.

Paragon e Pegasus: il ruolo ambiguo degli spyware nello scacchiere internazionale

Dopo l'annuncio di Meta-Whatsapp, basato anche sulle ricerche condotte dal Citizen Lab dell'Università di Toronto, è emerso come i clienti italiani di Paragon fossero due enti istituzionali, in particolare un'agenzia di *intelligence* e un corpo di polizia.

La notizia ha rapidamente scalato le cronache nazionali ed estere, suscitando reazioni e prese di posizione; l'uso di software-spia riveste infatti un ruolo complesso nel diritto vigente, ponendo delicate questioni di bilanciamento tra difesa della sicurezza e tutela dei diritti individuali.

Dal canto suo Paragon sostiene di attuare un “*minimal use of invasion of privacy*”, sottolineando che tra le caratteristiche di Graphite non rientra l'accesso a fotocamere o microfoni dei dispositivi su cui è in esecuzione.

Afferma, inoltre, di vendere i propri prodotti solo ai governi democratici e con esclusive finalità di supporto alle indagini in ambito criminale o ad attività di prevenzione e contrasto del terrorismo. In questo modo si contrappone strategicamente alla *competitor* NSO, creatrice del noto *spyware* Pegasus, al centro di numerose inchieste per il suo impiego contro giornalisti e politici di tutto il mondo.

Sebbene il governo italiano abbia negato ogni coinvolgimento nelle intercettazioni, Paragon avrebbe scelto di sospendere l'operatività dei propri prodotti nel nostro Paese e di rescindere il relativo accordo commerciale.

Il motivo risiederebbe nella violazione dei termini contrattuali, che formalmente escludono l'impiego di Graphite contro soggetti non coinvolti in alcuna ipotesi di reato.

A breve la vicenda sarà oggetto di un'audizione presso il Comitato parlamentare per la sicurezza della Repubblica (Copasir), dalla quale potrebbero emergere nuovi sviluppi; in corso anche una procedura di *due diligence* condotta in collaborazione tra Servizi e Agenzia per la Cybersicurezza Nazionale (ACN).

L'avviso del del Garante Privacy: l'uso di spyware può violare la normativa italiana

Lo scorso 14 febbraio, il Garante per la Protezione dei dati personali ha emesso una nota in merito alla vicenda.

Il comunicato si rivolge, senza ulteriori specificazioni, a *“tutti coloro che dovessero utilizzare lo spyware “Graphite” della società israeliana Paragon Solutions ltd, o sistemi analoghi, o dovessero utilizzare le informazioni raccolte tramite questi software”*.

Come ricorda il Garante *“tali attività, svolte al di fuori degli usi consentiti dalla legge, violano il Codice privacy e possono comportare l'applicazione di una sanzione amministrativa fino a 20 milioni di euro o al 4% del fatturato”*.

L'Autorità ribadisce, più in generale, che *“le intercettazioni di comunicazioni elettroniche che non rientrano nelle finalità*

di sicurezza della Repubblica e di prevenzione, indagine, accertamento e perseguimento di reati, devono rispettare la normativa in materia di protezione dei dati personali”.

Mentre si attende l'esito delle verifiche condotte dall'ACN, è già evidente come la vicenda Paragon – analogamente al caso Pegasus – imponga una riflessione troppo a lungo rimandata sull'ammissibilità di includere il ricorso agli *spyware*, nonché ad altri strumenti di sorveglianza digitale, tra le risorse che un paese democratico può utilizzare contro i propri stessi cittadini.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/notizie/paragon-spyware-cyber/>