Due gruppi hacker nella trappola della Polizia postale

"New generations" è l'operazione conclusa questa mattina dalla Polizia postale con cui ha individuato due gruppi criminali responsabili, negli ultimi giorni, di attacchi a sistemi informatici, a siti istituzionali e ad aziende private del Paese.

Sono 15 le persone denunciate con l'accusa di danneggiamento di sistemi informatici, interruzione illecita di comunicazioni informatiche e telematiche, accesso abusivo a sistemi informatici, e per danneggiamento di dati e programmi informatici utilizzati dallo Stato o altro Ente pubblico o di pubblica utilità.

Si tratta di 14 giovani, alcuni minorenni e un 40enne che si celavano dietro i nomi delle crew "Anonymous Iag" e "THC Squad".

I due gruppi hanno agito secondo uno schema ben preciso e collaudato: dopo aver individuato gli obiettivi ed attaccato i siti acquisendo le credenziali di accesso, si introducevano all'interno dei web server e dei database, copiando i dati personali degli utenti e modificando il contenuto delle pagine web. I dati sottratti venivano poi diffusi sui più noti social network, quali Twitter o Facebook .

Tra i siti attaccati figurano il portale della stessa Polizia Postale commissariatodips.it, i siti delle Camere del lavoro in Lombardia, della UIL e della FIOM, i siti esercito.difesa.it, dps.tesoro.it, urp.cnr.it e quello dell'Agenzia del Territorio.

Le azioni criminose portate a termine dalle crew si possono distinguere sostanzialmente in tre tipologie:

-attacchi di tipo ddos, rendono irraggiungibile per un determinato periodo di tempo il sito bersaglio dell'attacco;

-attacchi di tipo sql injection, sottrae informazioni sensibili memorizzate sul database preposto alla gestione dei contenuti di un sito web;

-defacement, sostituisce la homepage originale del sito con un'altra pagina creata ad hoc, spesso con contenuti di rivendicazione diretta.

Nel corso delle perquisizioni, che hanno interessato 10 regioni italiane, sono stati sequestrati numerosi computer e altri dispositivi con cui gli hacker sono riusciti a portare a termine gli attacchi.

Le indagini del Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (C.N.A.I.P.I.C.) e del Compartimento polizia postale di Perugia, si sono basate in particolare su attività di osint (open source intelligence) svolte su fonti aperte. Si è trattato di una vera e propria attività di ricerca nella rete finalizzata al rintraccio di indizi ed elementi che hanno permesso l'effettiva identificazione degli hacker.

15/07/2015