Polizia di Stato

Polizia di Stato: Operazione "New Generation" - 2 hacker nella trappola

Nelle ultime ore la Polizia di Stato ha portato a termine un'articolata operazione, che ha permesso di individuare i componenti di due gruppi criminali responsabili di decine di attacchi ai danni dei sistemi informatici di infrastrutture critiche, siti istituzionali e aziende private del paese. In totale sono 15 le persone denunciate dalla Polizia Postale e delle Comunicazioni, nel corso delle attività coordinate dalle Procure della Repubblica di Roma, Perugia e di quelle presso il Tribunale per i minorenni sempre del capoluogo umbro. Il reato: concorso nel danneggiamento di sistemi informatici, nell'interruzione illecita di comunicazioni informatiche e telematiche, per accesso abusivo a sistemi informatici, e per danneggiamento di dati e programmi informatici utilizzati dallo Stato o altro Ente pubblico o di pubblica utilità. Nel corso delle perquisizioni, che hanno interessato 10 regioni italiane, sono stati sequestrati numerosi personal computer e altri dispositivi utilizzati per portare a compimento gli attacchi. Determinante, in tale contesto, è stato il ruolo del Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (C.N.A.I.P.I.C.) del Servizio Polizia Postale e delle Comunicazioni e del Compartimento Polizia Postale di Perugia, titolari delle indagini, impegnati per mesi in complesse attività investigative finalizzate all'identificazione dei soggetti che si celavano dietro i nomi delle crew "Anonymous Iag" e "THC Squad". Un prezioso apporto nelle attività investigative è stato fornito inoltre dai Compartimenti regionali della Specialità di Lazio, Lombardia, Emilia-Romagna, Campania, Marche, Veneto, Friuli, Piemonte, Puglia e Abruzzo, con il supporto operativo delle rispettive articolazioni provinciali.Le indagini: all'alba di oggi si è conclusa l'operazione "*New generations*" che ha riunito due articolate indagini coordinate rispettivamente dai Sostituti Procuratori Francesco Polino e Eugenio Albamonte della Procura di Roma e da quelli della Procura della Repubblica di Perugia e di quella presso il Tribunale per i minorenni del capoluogo umbro, e condotte dal personale specializzato del Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (C.N.A.I.P.I.C.) del Servizio Polizia Postale e delle Comunicazionie del Compartimento Polizia Postale di Perugia. I provvedimenti sono stati eseguiti nei confronti di quattordici giovani, alcuni minorenni e un 40enne con diversi precedenti penali. Le indagini 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, con i doverosi riscontri dati da tradizionali attività investigative. Il primo filone di indagine, seguito e portato a conclusione dal personale del C.N.A.I.P.I.C., riguarda la *crew* nota come *anonymous iag,* nata presumibilmente nel settembre del 2012 e formata da cinque sedicenti hacktivisti dediti ad attacchi informatici nei confronti di istituzioni ed infrastrutture critiche. 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. Il gruppo prende il nome dal più grande e noto collettivo *anonymous*, con l'aggiunta dell'acronimo "iag" che sta per "italian anonymous group". Il fondatore, e figura apicale della crew, che celava la propria identità sotto i nickname *anondb* e *aj3dx*, è un 40enne residente in provincia di Torino con precedenti per rapina, ricettazione, concorso in associazione per delinquere, lesioni personali, falso in scrittura privata, guida senza patente, porto abusivo di armi ed altri reati, risultato vicino a famiglie camorriste. E' da evidenziare la peculiare personalità autocelebrativa del soggetto che in passato ha rilasciato diverse interviste in cui si definiva come il capo della crew: nell'ultima in ordine di tempo, subito dopo la recente operazione "Unmask"*, aveva promesso addirittura azioni di ritorsione*. Spesso agli attacchi seguiva la pubblicazione dei dati sottratti, o parte di essi, e del comunicato di rivendicazione, la cui diffusione era solitamente effettuata per mezzo dei più noti social network, quali twitter o facebook, del noto sito pastebin.com e attraverso il blog ufficiale del gruppo www.anonymousiag.blogspot.it. Semplificando, le azioni criminose portate a termine dalle *crew* si possono distinguere sostanzialmente in tre tipologie: attacchi di tipo ddos, aventi lo scopo di rendere irraggiungibile per un determinato periodo di tempo il sito bersaglio dell'attacco; attacchi di tipo sql injection, con lo scopo di sottrarre informazioni sensibili memorizzate sul database preposto alla gestione dei contenuti di un sito web. L'attaccante enumera le tabelle del database ed effettua quello che in gergo viene detto dump, ovvero preleva, oltre ai nomi delle tabelle, anche il contenuto di ogni singola tabella costituente il database, tra cui solitamente è presente quella contenente le credenziali di accesso degli utenti (solitamente in forma cifrata), e quelle degli amministratori del sito, che l'attaccante può utilizzate per accedere ad aree riservate, con la possibilità di inviare, modificare o cancellare file. defacement, che consistono nel sostituire la homepage originale del sito con un'altra pagina creata ad hoc, spesso con contenuti di rivendicazione diretta. Il secondo filone d'indagine, condotto dal personale del Compartimento Polizia Postale di Perugia, riguarda la *crew thc squad.* Gli investigatori, dopo aver

verificato che i sistemi informatici di alcuni istituti scolastici perugini erano stati oggetto di intrusioni poste in essere con identiche modalità operative, decidevano di sottoporre a costante attività di monitoraggio i canali di comunicazione utilizzati dagli hackers.La corretta scelta investigativa e la elevata preparazione tecnica del personale addetto alle indagini consentivano di identificare l'intera *crew* nota con il nome di "*thc squad*". I soggetti individuati, tra cui emergono anche minorenni, risultano aver agito secondo uno schema ben preciso e collaudato: dopo aver attentamente individuato gli obiettivi ed attaccato i siti acquisendo le credenziali di accesso, si introducevano abusivamente all'interno dei web server e dei database, copiando i dati personali degli utenti e modificando il contenuto delle pagine web, sì da ostacolarne la normale e corretta successiva consultazione. Si evidenzia che gli attacchi rivendicati sono oltre 150 dello stesso tipo di quelli precedentemente descritti. I sistemi maggiormente colpiti sono risultati essere quelli attinenti al mondo dell'istruzione, tanto che la *crew* aveva messo in atto una vera e propria "operazione scuole", mossa dall'intento di introdursi abusivamente, sia singolarmente che in gruppo, nei siti di istituti scolastici, di università e di enti di ricerca, non disdegnando, in ogni caso, anche siti istituzionali di governo, regioni, comuni, associazioni di forze di polizia ed imprese private. Le perquisizioni, effettuate presso le abitazioni degli hacker tra le province di Roma, Monza, Milano, Napoli, Ancona, Torino, Modena, Verona, Udine, Brindisi, Teramo e Varese,hanno consentito di sottoporre a sequestro numerosi sistemi e supporti informatici, la cui analisi tecnica da parte dagli esperti della Polizia Postale consentirà, in sinergia con le competenti Autorità Giudiziarie sia di delineare esattamente i ruoli dei soggetti coinvolti e sia di ricostruire dettagliatamente tutte le modalità operative utilizzate nell'esecuzione del piano criminoso. Le indagini sui due gruppi sono state svolte di pari passo tenuto conto della contiguità tra le crew, tanto che alcuni membri facevano parte di entrambe. Ecco i nickname utilizzati dagli hacker: *anondb, aj3dx, guy fawkes, anonrvg, deathpower, dark_baba, anonhackoder, cyberghost, easter, snow, eagle, nerdology, william, king, syned, denon, d3417.*

15/07/2015