PaginaQ
Pisa
http://www.paginaq.it

Operazione anti hacker: due arresti, indagati e perquisizioni

Author : Redazione

Date : 20 maggio 2015

Perquisizioni e arresti a Torino, Sondrio, Livorno e Pisa nei confronti di un'organizzazione di hacker responsabile di attacchi contro sistemi informatici di infrastrutture nazionali e siti istituzionali, fra cui ultimi in ordine di tempo i sistemi informatici di **Expo 2015** e del **Ministero della Difesa** nell'ambito della campagna *Antimilitarist (#2)*, con pubblicazione di un corposo leak di materiale proprio nella giornata di ieri.

L'operazione denominata **Unmask**, coordinata dalla Procura della Repubblica di Roma, è stata portata a termine nelle scorse ore dalla Polizia di Stato. Ha permesso di individuare una cellula ritenuta responsabile di numerosi attacchi ai danni dei sistemi informatici di importanti infrastrutture critiche, siti istituzionali e di rilevanti realtà economiche del paese.

Due le persone messe ai domiciliari dalla Polizia Postale e delle Comunicazioni, un'altra denunciata per associazione a delinquere finalizzata al danneggiamento di sistemi informatici, all'interruzione illecita di comunicazioni informatiche e telematiche, all'accesso abusivo a sistemi informatici, alla detenzione e diffusione di codici di accesso a sistemi informatici.
Denunciate inoltre due persone per favoreggiamento personale.

Le perquisizioni hanno interessato diverse città del centro nord e numerosi personal computer e altri dispositivi utilizzati sono stati sequestrati.

Il personale 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 titolare delle indagini, è stato impegnato per mesi in complesse attività tecniche sotto copertura finalizzate all'identificazione dei soggetti nascosti dietro fantasiosi nickname che agivano con la sicurezza garantita dai vari servizi di anonimizzazione.

L'indagine
I provvedimenti cautelari, emessi dal GIP del Tribunale di Roma, sono stati eseguiti nei confronti di due cittadini italiani: **un livornese di 31 e un 27enne originario della provincia di Sondrio**, noti rispettivamente con i nickname ***aken*** e ***otherwise.***
Denunciati inoltre un 36enne originario della provincia di Torino (nickname ***h[a]te***) e due giovani originari della provincia di Livorno, un 27enne e un 31enne. A loro carico, nel corso dell'indagine, sarebbero stati acquisiti concreti elementi probatori che hanno permesso di ricostruire un complesso scenario in cui gli indagati si muovevano per portare a termine attacchi informatici ai sistemi di numerose amministrazioni pubbliche ed aziende private, dalle quali venivano illecitamente carpite credenziali di autenticazione (user id e password) ed altre informazioni sensibili, successivamente pubblicate sul web.

Le indagini effettuate dal C.N.A.I.P.I.C. hanno evidenziato come i nickname *otherwise* e *aken*, fossero già emersi nel corso di precedenti indagini.

Otherwise sarebbe stato il promotore della campagna nota come "oprevenge/optrasparenza" nell'ambito della quale il gruppo ha effettuato attacchi informatici a sistemi di enti istituzionali e di forze di polizia, nonché della cosiddetta "million mask march". Mentre ***aken*** sarebbe il fondatore e leader del "canale" di livello internazionale noto come "operation greenrights", ossia della campagna in cui sono stati riuniti gli attacchi di matrice ambientalista.

Gli investigatori hanno avuto modo di rilevare l'estrema accortezza dei due capi della cellula criminale nell'utilizzo delle utenze, nella navigazione in rete, grazie all'uso di sofisticate tecniche di anonimizzazione (vpn e reti tor) e addirittura di antenne direzionali in grado di sfruttare connessioni WIFI altrui, arrivando a dissimulare gergalità dialettali diverse, e particolare attenzione a non fornire il minimo particolare della propria vita reale.

L'esecuzione dei provvedimenti ha necessitato un particolare dispositivo operativo che ha permesso grazie al diretto coinvolgimento del personale impiegato in attività sotto copertura ed al coordinamento delle operazioni sul territorio, di sorprendere gli esperti hacker con i computer accesi, evitando quindi la cifratura dei contenuti.

I sistemi informatici attaccati
Corte Costituzionale, Presidenza del Consiglio, i Ministeri dell'Interno, della Giustizia, della Salute, dello Sviluppo Economico, la Procura della Repubblica ed il Tribunale di Torino, la Polizia di Stato, l'Arma dei Carabinieri, le Regioni Veneto, Calabria, Piemonte, Equitalia, i sindacati di Polizia COISP e SIULP e della Polizia Penitenziaria SAPPE ed OSAPP, ENI e Enel.

Recentemente l'attenzione degli hacker si rivolta ai sistemi informatici di EXPO 2015. Ieri infine sotto attacco sono finiti i sistemi della Difesa, da cui sono stati pubblicati dati sensibili o nell'ambito della campagna Antimilitarist(#2)

Le tre tipologie delle azioni
Attacchi di tipo ddos, che hanno lo scopo di rendere irraggiungibile per un determinato periodo di tempo il sito bersaglio dell'attacco, bloccandone quindi i servizi. Intrusioni informatiche, che hanno il duplice scopo di carpire dai database dei siti attaccati e dai sistemi di posta elettronica dati riservati e sensibili. Danneggiamento dei sistemi informatici come ad esempio nel caso del cosiddetto *defacement* con il quale viene effettuata la sostituzione della

homepage di un sito web con un messaggio di rivendicazione.

Le tecniche di attacco utilizzate
Il primo passo consiste nell'individuazione del sito target, oggetto di successive scansioni per la ricerca di vulnerabilità ed effettuate per mezzo di tool automatici. Successivamente, se il sito risulta essere vulnerabile, su canali privati irc vengono discusse le modalità con cui effettuare l'attacco.

La tipologia di attacco prediletta è la *sql injection*, tecnica che consente a chi attacca di sottrarre informazioni sensibili memorizzate sul database preposto alla gestione dei contenuti del sito web.

Chi attacca effettua cioè quello che in gergo viene detto il *dump* del contenuto di ogni singola tabella costituente il database del sito, tra cui solitamente è presente quella su cui sono memorizzate in forma criptata le credenziali di accesso (username e password) degli utenti accreditati, comprese quelle degli amministratori del sito.

Spesso chi attacca tenta di inviare al web server particolari file che consentono di avere il controllo completo da remoto della macchina oggetto di attacco. Un'ultima operazione che può essere fatta avendo ottenuto il controllo del server consiste nel sostituire l'originale homepage del sito con un'altra creata ad hoc, spesso con contenuti di rivendicazione diretta, effettuando quello che in gergo è chiamato defacement.
Segue infine la pubblicazione dei dati sottratti, o di parte di essi e del comunicato di rivendicazione. Infine troviamo la violazione di interi sistemi di posta elettronica, che ha portato alla pubblicazione in rete di corrispondenza elettronica e di documentazione anche di natura istituzionale.