Polizia di Stato

Roma. operazione contro il cybercrime

La Polizia di Stato, sotto la direzione della Procura di Roma, ha portato a termine una della più articolate attività di indagine nel settore del cybercrime, l'Operazione PEOPLE 1.Centinaia di credenziali di accesso a dati sensibili, migliaia di informazioni private contenute in archivi informatici della pubblica amministrazione, relativi a posizioni anagrafiche, contributive, di previdenza sociale e dati amministrativi appartenenti a centinaia di cittadini e imprese del nostro Paese: è quanto è stato scoperto dagli investigatori specializzati del Servizio Polizia Postale e delle Comunicazioni, che hanno dato esecuzione ad un' ordinanza di custodia cautelare in carcere e proceduto ad eseguire 6 decreti di perquisizione sul territorio nazionale; destinatarie anche diverse agenzie investigative. Il principale sospettato, R.G., cittadino italiano di anni 66 originario della provincia di Torino, residente in Sanremo con un know how informatico di altissimo livello e numerosi precedenti penali e di polizia, è stato posto in arresto su provvedimento del GIP presso il Tribunale di Roma. I numerosi indizi raccolti durante le indagini indicano il soggetto come il principale responsabile di ripetuti attacchi ai sistemi informatici di numerose Amministrazioni centrali e periferiche italiane, attraverso i quali sarebbe riuscito ad intercettare illecitamente centinaia di credenziali di autenticazione (userID e password). Dapprima attaccando i sistemi informatici di alcuni Comuni italiani, il sospettato è riuscito ad introdursi in banche dati di rilievo istituzionale, appartenenti ad Agenzia delle Entrate, INPS, ACI ed Infocamere, veri obiettivi finali dell'attività delittuosa, da questi esfiltrando preziosi dati personali di ignari cittadini ed imprese italiane. Denunciati a piede libero, per le medesime violazioni, 6 complici dell'arrestato, tutti a vario titolo impiegati all'interno di note agenzie investigative e di recupero crediti operanti in varie città d'Italia. Questi, in particolare, commissionavano a R.G. gli accessi abusivi ed il furto delle preziose credenziali, per poi farne uso nelle rispettive attività professionali di investigazione privata, in tal modo riuscendo a profilare illecitamente, a loro insaputa, centinaia di cittadini e imprese. L'attività investigativa condotta dagli uomini del CNAIPIC ha permesso di ricostruire come R.G., nel corso degli anni, avesse ingegnerizzato un vero e proprio sistema di servizi, tra cui il portale illecito "PEOPLE1", commercializzato clandestinamente ed offerto alle agenzie interessate, le quali, pagando una sorta di canone, potevano istallare il software con una semplice pen-drive USB, e riuscire così a connettersi clandestinamente alle banche dati istituzionali e fare interrogazioni dirette. Per ottenere l'accesso clandestino a tali banche dati, il gruppo criminale utilizzava sofisticati virus informatici, con i quali infettava i sistemi degli Uffici pubblici riuscendo ad ottenere le credenziali di login degli impiegati. La tecnica utilizzata a tal proposito prevedeva, anzitutto, il confezionamento di messaggi di posta elettronica (phishing), apparentemente provenienti da istituzioni pubbliche, ma in realtà contenenti in allegato pericolosi malware. I messaggi arrivavano a migliaia di dipendenti di Amministrazioni centrali e periferiche, in particolare a quelli dei piccoli Comuni e dei patronati, che venivano, con l'inganno, portati a cliccare sull'allegato malevolo aprendo così la porta al sofisticato virus informatico che, in poco tempo, consentiva agli hacker di assumere il controllo dei computer. A questo punto il gruppo criminale, potendo contare su una rete vastissima di computer infettati, li metteva in rete sommandone le potenze di calcolo, costruendo quella che, tecnicamente, è definita una BOTNET, controllata da remoto dall'indagato R.G. grazie ad una centrale (cosiddetta Command and Control) che egli aveva installato su server all'estero. La potente rete di computer infetti veniva quindi utilizzata dall'indagato per sferrare gli attacchi informatici massivi, compromettere i database delle Amministrazioni pubbliche ed esfiltrare i dati personali dei cittadini. La persistenza delle attività illecite era in particolare assicurata dallo stesso malware, che arrivava a modificare le chiavi di registro in modo da eseguire automaticamente, all'avvio della macchina infettata, specifici programmi in grado di autoinstallarsi sul computer della vittima e registrare, tra l'altro, i caratteri digitati sulla tastiera (keylogging) tra i quali, appunto, le credenziali di autenticazione alle banche dati centralizzate. I dati venivano poi inviati su una serie di server all'estero, principalmente in Canada, Russia, Ucraina ed Estonia, direttamente gestiti, come dimostrato nel corso di complesse attività di intercettazione telematica e telefonica, da R.G., e quindi utilizzati per accedere abusivamente alle banche dati di interesse pubblico ed eseguire la profilazione di imprese e privati cittadini. Tale stabile infrastruttura informatica rappresenta il core della complessa piattaforma realizzata dal sodalizio criminale, che consentiva migliaia di illeciti accessi nelle banche dati istituzionali, detentrici di informazioni sensibili. Target finale dell'attacco erano, ovviamente, i cittadini e le Pubbliche amministrazioni, le cui banche dati istituzionali, il cui accesso deve essere strettamente riservato a funzionari autorizzati, rappresentano uno strumento indispensabile per il corretto funzionamento dei servizi resi alla collettività grazie ai moderni sistemi di e-government. Il destinatario della misura cautelare si è avvalso nel corso della sua attività criminale anche della "consulenza" di hacker freelance stranieri ingaggiati all'interno del Darkweb, allo stato in fase di identificazione. Gli hacker, dietro pagamento, sviluppavano righe di comando attraverso le quali la piattaforma veniva implementata proprio per aggirare le misure di sicurezza delle piattaforme

obiettivo dell’attività criminale. Le articolate e complesse indagini sono iniziate nel mese di maggio 2017, a seguito di una segnalazione della società di sicurezza informatica TS-WAY (che per prima ha individuato la minaccia sul territorio nazionale) nella quale veniva evidenziata una campagna di spear-phishing volta a diffondere codici malevoli ed avente quale primo obiettivo i sistemi informatici di numerose infrastrutture critiche italiane. Su delega della Procura della Repubblica di Roma, il CNAIPIC, grazie ad un’articolata attività di indagine sulla tipologia ed il funzionamento di tale virus e sulla provenienza delle suddette e-mail di spear phishing, resa possibile da servizi di intercettazione telematica attiva delle comunicazioni tra i componenti del sodalizio criminale, è riuscito infine a chiarire l’esatta portata e dinamica dei fatti, accertando le responsabilità penali della complessa infrastruttura informatica illegale scoperta. I cyber-investigatori della Postale, in tal modo, sono stati in grado di ricostruire e studiare il funzionamento della piattaforma utilizzata dagli indagati, i legami tra di essi, le metodologie di attacco ai sistemi informatici ed alle banche dati, le risorse ed i canali telematici attraverso i quali venivano gestiti e trasferiti i dati personali illecitamente acquisiti, nonché gli ingenti flussi finanziari ottenuti grazie a tali condotte delittuose. Le attività di indagine hanno reso inoltre necessario l’avvio di attività di cooperazione internazionale con numerosi Paesi esteri, in particolare con la polizia del Canada, il cui apporto indispensabile ha consentito di congelare e preservare il core della struttura informatica principale, sul quale si poggia la piattaforma illegale. L’attività, ancora in corso, ha consentito l’acquisizione degli elementi di prova informatica detenuti dalle società estere coinvolte nella fornitura dei servizi informatici al sodalizio criminale. Non si escludono, a questo punto, ulteriori sviluppi circa la completa ricostruzione della vasta rete di clienti del sodalizio criminoso (società di investigazione privata e di riscossione dei crediti). Ingenti i proventi dell’attività criminale, se si pensa alle decine di migliaia di interrogazioni illecite su commissione già accertate e che una singola interrogazione delle banche dati istituzionali veniva venduta a partire da 1 euro “a dato”, anche attraverso sistemi di pagamento evoluto e attraverso l’acquisto in modalità prepagata di “pacchetti di dati sensibili”. Per l’esecuzione dei provvedimenti restrittivi e di perquisizione, oltre che per l’espletamento della preliminare attività informativa, il CNAIPIC si è avvalso della collaborazione del personale dei Compartimenti di Polizia Postale di Roma, Milano, Napoli, Venezia, Genova e della Sezione di Imperia.

22/11/2019