Polizia di Stato

Bologna: fermato tentativo di phishing ai Salesiani

Il 28 febbraio scorso personale amministrativo dell'Opera Salesiana del Sacro Cuore di Bologna segnalava di aver verificato delle operazioni sospette di bonifici on-line per un importo di 60.000 € effettuate sul conto corrente postale dell'istituto religioso, alimentato per lo più dai versamenti dei fedeli bolognesi. Le indagini, avviate immediate, permettevano di tracciare la destinazione finale del denaro, il quale dopo essere stato inviato ad un conto corrente di una filiale Bancaria della Capitale, era già stato oggetto di ulteriore dispersione, verso rapporti accesi presso altre banche, su carte prepagate connesse al predetto rapporto e verso un altro conto corrente postale. Dopo una complessa attività investigativa, il personale operante riusciva a recuperare la somma di 50.000 €, procedendo al sequestro preventivo delle somme individuate, poco prima che venisse dato corso alle già disposte operazioni di prelievo del denaro disponibile sui conti destinatari delle rimesse. Le indagini avviate permettevano di fermare tre pregiudicati ucraini, residenti a Roma, i quali risultano aver falsificato anche alcune fatture per operazioni in favore della predetta struttura religiosa, quali intestatari dei conti correnti bancari, e un cittadino italiano residente in provincia di Piacenza intestatario del conto corrente postale. Nelle prime ore del 5 marzo, in collaborazione con il Compartimento omologo competente per il Lazio, sono stati eseguiti i provvedimenti di perquisizione domiciliare e locale disposti dal Pubblico Ministero Antonella SCANDELLARI, del pool reati informatici della Procura della Repubblica di Bologna che coordina le indagini, per i reati di cui agli artt. 615 ter e 640 ter c.p. a carico degli indagati. Le operazioni delegate hanno portato al rinvenimento e sequestro di materiale utile alle indagini e pertinente le operazioni illecite compiute. Solitamente questa particolare forma di "pesca" si concretizza in attacchi massivi ai conti di innumerevoli correntisti sconosciuti dai quali si cerca di prelevare somme contenute; nel caso di specie, l'aggressione è stata mirata al conto corrente dei religiosi (conto alimentato dalle offerte dei fedeli).

Il Phishing (pesca di dati sensibili) rientra nelle eventualità previste dal reato di frode informatica di cui all'art. 640 ter c.p.; si tratta di una attività illegale che sfrutta una tecnica di ingegneria sociale finalizzata ad entrare in possesso delle credenziali in uso ai sottoscrittori di conti corrente aventi anche operatività on-line (c.d. home banking). La prima denuncia prodotta da un correntista di un istituto di credito vittima di phishing (risalente all'anno 2005) è stata presentata a Bologna. Metodologia delittuosa email esca (1° versione). L'autore del reato (phisher) spedisce al malcapitato e ignaro utente un messaggio email "ingannevole"che riproduce fedelmente quello di una istituzione nota al destinatario (per esempio la sua banca, il suo provider web, un sito on line a cui è iscritto). L'email invita il destinatario ad utilizzare un link presente nel messaggio per collegarsi al sito di chi lo ha contattato che in realtà è un clone. Il collegamento fornito, allocato su un server controllato dal phisher rimanda, invece, ad una pagina web utilizzata per catturare le informazioni riservate. Il criminale utilizza i dati carpiti per trasferire somme di denaro, acquistare beni o per ulteriori operazioni fraudolente. Per concludere l'attività delittuosa gli autori del reato necessitano di conti correnti "di appoggio" su cui far transitare il denaro illecitamente sottratto. Questi ultimi vengono recuperati mediante false offerte di lavoro presentate da fantomatiche società, che richiedono per la prestazione di lavoro le coordinate bancarie di conti aventi operatività on line, con lo scopo di ricevere l'accredito di somme di denaro che verranno poi trasferite a terze persone, a mezzo money transfert (es. Western Union), previo storno di una percentuale che si aggira dal 5 al 10 % di cui beneficerà il titolare del c/c che ha prestato i propri dati (quest'ultimo rischia l'incriminazione per il reato di riciclaggio ex art. 648 bis. c.p.). Per l'invio delle email, si è potuto constatare che i server utilizzati vengono di solito ospitati in paesi dell'est europeo o del Sud America. Metodologia delittuosa malware (2° versione/evoluzione). L'evoluzione criminale del fenomeno prevede anche l'utilizzo di virus informatici che, infettando le macchine d'ignari utenti di servizi web, catturano i soli dati relativi alle credenziali di accesso ai conti correnti on line, inoltrandoli, poi, agli ideatori del reato, per il futuro loro indebito utilizzo. Il fenomeno criminale del phishing, su base nazionale, registra un modesto aumento (20% circa); dato assolutamente coerente rispetto alla straordinaria diffusione delle possibilità di collegamento agli strumenti di gestione on line dei rapporti bancari ed alle policy del sistema creditizio. Anche in Emilia Romagna si registra un aumento analogo (14% circa); tuttavia il numero complessivo dei reati registrati in regione corrisponde a meno del 2% di tutti i reati registrati sul territorio nazionale. Il dato è di particolare soddisfazione per la Polizia Postale e delle Comunicazioni ed in particolare per il Reparto di Bologna e può trovare ragione nello storico impegno dell'ufficio nel contrastare tale forma di reato (che, si ricorda, venne registrato per la prima volta in questo Capoluogo nel 2005), nell'elevato livello di sicurezza dei sistemi automatici di protezione predisposti dai maggiori istituti di credito ma, soprattutto, nell'elevato livello culturale nell'impiego dei sistemi evoluti di comunicazione raggiunto dagli utenti. Il tal senso la Polizia di Stato, nella sua azione di prevenzione e nella sua funzione di

"polizia di prossimità" ha svolto e continua ad assicurare un'insistente opera d'informazione nei confronti delle varie categorie di utenti (in particolare le più deboli). Al fine di rendere ancor più incisiva la propria azione, la Polizia delle Comunicazioni ha recentemente realizzato un innovativo sistema per il contrasto dei cyber crime incentrato sulla condivisione di informazioni con il sistema bancario, OF2CEN (Online Fraud Cyber Center and Expert Network). Frutto di una costante opera di sensibilizzazione che ha portato l'intero sistema bancario a porre a fattor comune il concetto stesso di sicurezza nel nuovo mondo delle transazioni on line, il sistema si pone come strumento di collaborazione operativa e di interscambio informativo tra la Polizia e le principali aziende private del settore, quali istituti di credito, società di emissione di dispositivi di monetica, intermediari e fornitori di infrastrutture telematiche a supporto di transazioni finanziarie elettroniche. Allestito con il supporto delle più importanti banche italiane, il sistema mira ad abbattere tutte le barriere burocratiche e tecniche di ostacolo per una concreta ed efficace attività di prevenzione e contrasto del crimine on line. Ispirato alla realizzazione delle più avanzate sinergie tra settore pubblico e privato il progetto vede interessate unitamente alla Polizia quindici tra le principali realtà bancarie italiane rappresentate dall'ABI (Associazione Bancaria Italiana).

14/03/2014