PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 24 - numero 5158 di Venerdì 06 maggio 2022

Molti lettori conoscono il phishing, ma quanti conoscono il vishing?

Nel continuo confronto tra l'attività dei malviventi e quelli delle persone oneste, purtroppo spesso i malviventi acquistano una posizione di vantaggio, elaborando sempre più sofisticate tecniche truffaldine. Una delle ultime è il vishing.

Il vishing, o voice phishing, è una nuova forma di attacco informatico che cerca di ingannare le vittime, chiedendo informazioni sensibili, come numeri di carte di credito, dettagli di conto corrente bancario e parole chiave, usando il telefono come mezzo di comunicazione tra l'attaccante e la vittima.

Anche se questa tecnica può sembrare già ben nota, in realtà i malviventi hanno recentemente raffinato questo strumento, rendendolo decisamente temibile.

Vediamo come funziona.

Il truffatore avvia il procedimento, per solito cercando di agganciare on-line la sua vittima, grazie un messaggio di posta elettronica. Questo tipo di attacco è già ben noto e si chiama phishing.

L'obiettivo di questa prima fase dell'attacco è quello di individuare il numero telefonico della vittima potenziale, in modo da poterlo chiamare, impersonando un tecnico informatico oppure un responsabile della sicurezza.

L'attenzione prestata dai malviventi a questa fase è dimostrata anche dal fatto che l'analisi dei numeri telefonici, da cui sembra provenire la chiamata, porta ad una apparenza di completa legittimità.

Il chiamante, che ad esempio impersona un responsabile antifrode di una banca o di una azienda, emittente carte di credito, cerca di imprimere al contenuto delle telefonate una immagine di grande urgenza, per mettere in apprensione il chiamato ed indurlo a rispondere alle richieste dell'attaccante, senza avere a disposizione troppo tempo per meditare sulla legittimità della richiesta.

Una volta che il chiamante ha ottenuto le informazioni personali desiderate, egli può utilizzarle per commettere frodi finanziarie, effettuare acquisti non autorizzati o perfino prelevare somme dal conto corrente del soggetto chiamato.

Come individuare tempestivamente questa tecnica di attacco.

È evidente che il fatto che un soggetto preso di mira possa individuare tempestivamente degli elementi, che possano far sospettare che una frode sia in corso, rappresenta un elemento di protezione oltremodo efficace.

A questo proposito, tutte le istituzioni finanziarie proclamano, in mille modi, il fatto che nessun loro dipendente o soggetto autorizzato possa effettuare chiamate per acquisire dati personali e dati finanziari di un loro cliente.

Purtroppo, anche se questi messaggi vengono visualizzati con estrema frequenza e chiarezza, un abile malvivente può fare leva su aspetti psicologici, legati ad esempio all'urgenza di un intervento, mirato a bloccare una carta di credito clonata, che può far dimenticare al chiamato di adottare le appropriate precauzioni.

Un altro trucco frequente nasce dal fatto che il malvivente è venuto a conoscere alcuni elementi afferenti ad un incidente stradale, in cui il chiamato è rimasto coinvolto; a questo punto, il chiamante dichiara di rappresentare la compagnia di assicurazione di essere pronto ad una rapida transazione, a favore del chiamato (evidentemente!).

Egli chiede i dati personali e finanziari necessari per attivare il bonifico. In questi casi è evidente che l'atteggiamento più cautelativo è quello di chiamare direttamente la compagnia di assicurazione coinvolta, per appropriati controlli incrociati.

Un'altra tecnica, che negli ultimi tempi si è diffusa rapidamente, fa sì che il chiamante dichiari di essere un tecnico di help desk, che ha rilevato la presenza di un virus nel computer del chiamante. Fortunatamente, i sofisticati apparati presenti presso lo help desk permettono di neutralizzare il virus a distanza, senza quindi doversi recare fisicamente presso il computer coinvolto. A seconda della risposta ricevuta, la frode può attuarsi, chiedendo una somma per la ripulitura del computer, oppure può comportare l'istallazione di uno spyware sul computer della vittima.

Infine, il chiamante può spacciarsi per un addetto all'agenzia delle entrate, o ente similare, segnalando che vi è una posizione esposta del chiamato, che richiede un immediato intervento, per evitare che si attivino salate sanzioni per ritardato pagamento.

Un atteggiamento proattivo è sempre efficace.

Ecco un elenco di qualche misura che si può adottare, per rendere inefficace questa tipologia di attacco:

- evitare di rispondere a chiamate provenienti da numeri non conosciuti, lasciando che si attivi la segreteria telefonica; avrete così elementi per effettuare ulteriori approfondimenti;
- non comunicare mai a soggetti ignoti dati personali o finanziari, via telefono; ancora una volta, occorre ricordarsi che le aziende che operano in modo corretto mai richiedono queste informazioni per telefono;
- se, durante la telefonata, e per un qualunque motivo, i vostri sospetti circa una telefonata fraudolenta vengono attivati, agganciate immediatamente e, se del caso, richiamate voi stessi il numero in questione;
- riferite immediatamente alla polizia postale della vostra località qualsiasi evento, che possa far sospettare che un fenomeno di vishing è in corso.

Se tutti gli utenti segnalassero sempre alla polizia postale questi eventi, la polizia avrebbe a disposizione un quadro di riferimento, che permetterebbe di avviare immediate ed approfondite indagini e, nel contempo, mettere in guardia altre possibili vittime.

Adalberto Biasiotti