Il Phishing

Il phishing è un tipo di truffa via Internet attraverso la quale un aggressore cerca di ingannare la vittima convincendola a fornire informazioni personali sensibili.Si tratta di una attività illegale che sfrutta una tecnica di ingegneria sociale: attraverso l'invio casuale di messaggi di posta elettronica che imitano la grafica di siti bancari o postali, un malintenzionato cerca di ottenere dalle vittime la password di accesso al conto corrente, le password che autorizzano i pagamenti oppure il numero della carta di credito. Tale truffa può essere realizzata anche mediante contatti telefonici o con l'invio di SMS (SMISHING)La prima menzione registrata del termine phishing è sul newsgroup di Usenet alt.online-service.america-online il 2 gennaio 1996, malgrado il termine possa essere apparso precedentemente nell'edizione stampata della rivista per hacker 2600. Il termine phishing è una variante di fishing (letteralmente "pescare" in lingua inglese), probabilmente influenzato da phreaking e allude all'uso di tecniche sempre più sofisticate per "pescare" dati finanziari e password di un utente.

Metodo di attacco

Il processo standard delle metodologie di attacco di phishing può riassumersi nelle seguenti fasi:

1. l'utente malintenzionato (phisher) spedisce al malcapitato e ignaro utente un messaggio email che simula, nella grafica e nel contenuto, quello di una istituzione nota al destinatario (per esempio la sua banca, il suo provider web, un sito di aste online a cui è iscritto).
2. l'e-mail contiene quasi sempre avvisi di particolari situazioni o problemi verificatesi con il proprio conto corrente/account (ad esempio un addebito enorme, la scadenza dell'account, ecc.) oppure un'offerta di denaro.
3. l'e-mail invita il destinatario a seguire un link, presente nel messaggio, per evitare l'addebito e/o per regolarizzare la sua posizione con l'ente o la società di cui il messaggio simula la grafica e l'impostazione (Fake login).
4. il link fornito, tuttavia, non porta in realtà al sito web ufficiale, ma a una copia fittizia apparentemente simile al sito ufficiale, situata su un server controllato dal phisher, allo scopo di richiedere e ottenere dal destinatario dati personali particolari, normalmente con la scusa di una conferma o la necessità di effettuare una autenticazione al sistema; queste informazioni vengono memorizzate dal server gestito dal phisher e quindi finiscono nelle mani del malintenzionato.
5. il phisher utilizza questi dati per acquistare beni, trasferire somme di denaro o anche solo come "ponte" per ulteriori attacchi.

Casi giudiziari e prime condanne penali

Nel 2007 con sentenza del Tribunale di Milano si è avuta, per la prima volta in Italia, la condanna di membri di una associazione transnazionale dedita alla commissione di reati di phishing. Tale sentenza è stata confermata in Cassazione nel 2011.Nel 2008, con sentenza del Tribunale di Milano, si è invece pervenuti per la prima volta in Italia alla condanna per riciclaggio di soggetti che, quali financial manager, si erano prestati alla attività di incasso e ritrasferimento di somme di denaro provento dei reati di phishing a danno dei correntisti italiani.Queste due sentenze hanno dunque indicato quali norme possono essere applicate a questo nuovo fenomeno criminale, dal momento che in Italia il phishing non è ancora specificatamente regolamentato, a differenza di altre legislazioni - prima fra tutte quella americana - che possiedono norme penali incriminatrici ad hoc