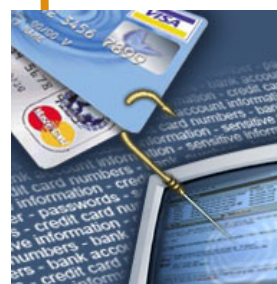
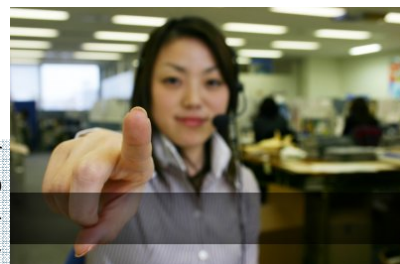


Lo scenario

Sono sempre più diffusi e pericolosi i casi di **phishing**, la tecnica utilizzata per ottenere l'accesso ad informazioni personali e riservate con la finalità del furto di identità mediante l'utilizzo di messaggi di posta elettronica fasulli, opportunamente creati per apparire autentici. Grazie a questi messaggi, l'utente è ingannato e portato a rivelare dati sensibili, come numero di conto corrente, nome utente e password, numero di carta di credito. Il processo standard di queste metodologie di attacco inizia con la spedizione di messaggi email che simulano nella grafica e nel contenuto quelli di istituzioni note al destinatario (ad es. la sua banca, il suo provider web, un sito di aste on-line a cui è iscritto). L'e-mail contiene spesso avvisi di particolari situazioni o problemi verificatisi con il proprio conto corrente/account (ad es. un addebito enorme, la scadenza dell'account, ecc.). Nella mail il destinatario è invitato 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. Il collegamento al sito web fornito NON porta in realtà al sito web ufficiale, ma ad un sito "trappola" costituito da pagine appositamente create per emulare il "Look and feel" del sito in oggetto e richiedere al 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 e finiscono nelle mani del phisher che le utilizza per acquistare beni, trasferire somme di denaro o anche solo come "ponte" per ulteriori attacchi.



Un'approccio all'Anti-phishing

Per contrastare il phishing abbiamo definito tre ambiti di intervento:

- Un ambito **reattivo**, originato da segnalazioni dei clienti, i quali, una volta ricevuta una comunicazione sospetta, hanno la possibilità di segnalarla all'organizzazione (es. la banca) su una casella di posta interna creata ad hoc.
- Un ambito **esplorativo**, attraverso la creazione di "e-mail civetta", iscrivendosi a diversi newsgroup su più siti Web considerati sospetti e suscettibili allo spamming che rimandano a siti phishing. In tal modo è possibile individuare tali siti da inserire così nell'archivio di quelli "trappola".
- Un ambito **proattivo**, non consistente quindi in una reazione ad attività di phishing, ma nell'individuazione preventiva di siti sospetti attraverso spiderizzazione di URL o semplicemente permutando gli elementi alfanumerici che compongono il nome del sito in oggetto.



La soluzione

Tutti gli ambiti elencati rendono necessaria un'attività di indagine che può essere gestita anche **manualmente**. Des in sinergia con Autonomy, con cui siamo partner e "Centro di Eccellenza" in Italia, attraverso una consolidata tecnologia già sperimentata nel campo del phishing su realtà come Deutsche Bank e HSBC, può rendere tali attività completamente **automatizzate**. Attraverso la piattaforma di "Phishing Detection" di Aungate, sarà possibile scovare tutti i tentativi di phishing grazie alla comprensione dei contenuti e del loro contesto, effettuando un monitoraggio completamente automatico non solo di testi, ma anche di immagini contenute all'interno delle comunicazioni e/o rappresentate sui siti "trappola". Forniamo le migliori soluzioni con una tecnologia che Autonomy ha già installato, solo per fare qualche nome, presso il Dipartimento della Difesa americano, la NASA, la DERA (Defense Evaluation and Research Agency) del Ministero della difesa inglese ed in altri ambiti anche bancari come ABN AMRO, Lloyds, Nomura Group....

La tecnologia, basata su sofisticati algoritmi di mappatura e accoppiamento concettuale, cattura miliardi di informazioni al giorno (spam-emails, host providers, domain registers...) da molteplici fonti e sistemi in tutto il mondo, comparandole e individuandone trasversalmente tutti i potenziali riferimenti, riuscendo così a segnalare all'organizzazione tutti i tentativi fraudolenti da parte di pericolosi phisher. Aungate si posiziona anche parallelamente ai server esistenti, intercettando tutto il traffico di rete. A compendio degli ambiti descritti, che sono da collocare all'interno dell'organizzazione, vi è un ulteriore approccio, che consiste nella possibilità di dotare gli utilizzatori (previa installazione sui propri PC) di un client SW per monitorare a livello locale tutte le comunicazioni e riconoscere potenziali tentativi di phishing, sulla base di una lista di siti web "trappola" spiderizzati, messi a disposizione dall'organizzazione di riferimento.



L'architettura

