

Phishing “in volo”: 100 milioni di attacchi contro le compagnie aeree

2008-09-18 16:34:10



Gli ultimi giorni d'estate ci hanno messo in luce una nuova trovata della criminalità informatica. Dopo finte banche, finti avvocati, finte fatture, e finte lotterie (vittoriose, s'intende) è stata finalmente la volta delle **finte compagnie aeree che comunicano via e-mail i dettagli dell'avvenuto acquisto di biglietti per voli low cost**. L'insidia è nascosta in un allegato al messaggio di posta elettronica nel quale dovrebbero trovarsi i dettagli dell'acquisto.

Tuttavia *questo nuovo caso di phishing "volante" si caratterizza per due significative differenze rispetto ai classici attacchi contro le finte banche* che da alcuni anni abbiamo imparato – si spera – a riconoscere, seppur non ancora – purtroppo- a debellare o ad arginare. Innanzitutto il messaggio è in inglese, quindi ben si attaglia ad una platea decisamente planetaria, non limitata agli angusti confini nazionali. *Se questo da un lato è un vantaggio per gli utenti abituati a cestinare immediatamente ogni comunicazione elettronica non espressa nella lingua di Dante, tuttavia non consente di verificare immediatamente le improbabilità grammaticali del messaggio e potrebbe indurre in errore coloro che effettivamente abbiano eseguito degli acquisti on line di biglietti aerei pochi giorni prima.*

Tenuto conto che la potenziale platea di truffati è di diverse centinaia di milioni di utenti (e non poche decine come il mercato italiano dell'home banking) le possibilità di pescare vittime diventano numericamente significative. La seconda caratteristica è data dal fatto che il messaggio fraudolento non ci invita a collegarci con finti portali truffaldini per indurci a consegnare i nostri dati (come nella subdola versione del phishing bancario), ma si "limita" (si fa per dire) semplicemente a farci aprire un allegato che, lungi dall'essere la nostra fattura d'acquisto, è in realtà un pericoloso programma eseguibile che installa un cavallo di troia nel nostro computer che consente ad esterni malintenzionati di prenderne possesso a nostra insaputa.

Per la precisione si tratta di un virus di tipo **trojan denominato: Trojan.Agent-43132**. L'allegato si presenta sottoforma di file compresso (nell'esempio: eTicket_N832.zip) che contiene il file infetto; il file infetto ha estensione .exe e cliccandovi sopra scatena l'installazione del trojan. I falsi messaggi inviati dalle compagnie aeree indicano anche un numero di biglietto elettronico nell'oggetto, per convincere gli utenti a cliccare sul link trappola. Non si sono fatti attendere gli interventi delle associazioni di consumatori:

“Chi credeva che il fenomeno del Phishing si fermasse all'attacco delle banche si sbagliava” ha affermato Massimo Penco, presidente dell'associazione Cittadini di Internet “Lo avevamo già affermato molti mesi fa, e i fatti continuano a darci ragione: i criminali informatici sono sempre più organizzati e continuano a setacciare il mercato alla ricerca di ogni possibilità che permetta loro di frodare i “Cittadini di Internet” con calcolata precisione. In tempo di ferie, l'interesse dei navigatori si sposta sulle vacanze e il settore diventa così appetibile”.

Anti-Phishing Italia: il portale contro le truffe on-line

Phishing “in volo”: 100 milioni di attacchi contro le compagnie aeree

Il testo dell'email truffa tradotto dall'inglese dagli esperti de "Cittadini" è il seguente: "Ti ringraziamo per aver usato il nostro sistema on-line per l'acquisto dei biglietti. Nel nostro sito web XXX, potrai entrare nella tua prenotazione digitando il codice XXX e la password XXX. Abbiamo addebitato sulla tua carta di credito l'importo di \$ XXX. Ti ricordiamo che ogni volta che acquisterai biglietti aerei nel nostro sito web riceverai lo sconto del 10%. Inclusa in questo messaggio troverai la fattura del biglietto da te acquistato, stampala e sarai pronto per volare con noi. Cordiali saluti, nome della compagnia aerea".

Per consultare i messaggi che stanno ricevendo le vittime l'associazione "Cittadini di Internet" ha messo a disposizione la seguente risorsa Web

[https://www.cittadininternet.org/articoli.asp?stampa=Security Alert](https://www.cittadininternet.org/articoli.asp?stampa=SecurityAlert)

Ulteriori informazioni: [PcWord](#)

Fonte: Anti-Phishing Italia – www.anti-phishing.it