

L'aeroporto di Heathrow esposto ad attacchi Hacker

Inviato da Michael Dogali

L'aeroporto di Heathrow e' considerato uno degli aeroporti internazionali piu' sicuri del mondo.

Negli ultimi tempi le crescenti minacce terroristiche, che ne fanno uno dei bersagli ad alto rischio, hanno reso ancora piu' severa la policy di sicurezza in vigore, con procedure di imbarco molto accurate e una continua vigilanza all'interno dell'intero perimetro aeroportuale.

Di fatto, la soglia di attenzione per tutto cio' che riguarda la sicurezza fisica e' massima, non cosi' invece pare essere il controllo delle strutture telematiche e la sicurezza informatica.

Un nostro utente ha recentemente fatto una scoperta molto interessante al riguardo ed ha scelto di raccontarlo a RedOracle.com perche' attraverso il nostro sito si porti a conoscenza un caso emblematico di negligenza informatica.

Recentemente Honest (questo e' il nick del nostro affezionato utente) ha casualmente scoperto che il sistema telematico a fruizione del pubblico dell'aeroporto londinese non e' affatto cosi' sicuro, tanto che e' facilmente vulnerabile ad attacchi Hacker (nel senso letterale del termine e non in quello abusato e malinterpretato di uso mediatico).

Ma andiamo per ordine.

Pochi giorni fa Honest mi contatta per chiedermi se fossimo interessati a pubblicare un articolo su quello che lui ha definito uno "scoop" del settore informatico.

{mosgoogle right}Ovviamente questo suscita subito la mia curiosita' e quindi Honest inizia a raccontarmi come ha scoperto, del tutto casualmente, che alcune postazioni telematiche dell'aeroporto di Heathrow siano facilmente esposte al rischio di violazioni esterne.

Difatti, continua, su queste postazioni (che con ogni probabilita' sono installate in comodato d'uso da societa' fornitrici esterne) chiunque potrebbe condurre diversi tipi di attacchi informatici che mirino a prendere il controllo della macchina e trasformarla in una sonda piuttosto che ponte con l'esterno, con grave rischio per la sicurezza informatica di chi ha utilizzato la macchina e lasciato magari dati sensibili.

Queste postazioni infatti sono dedicate al pubblico per navigare a pagamento su internet tramite l'utilizzo di carta di credito.

E' facile, quindi, immaginare che ogni utente inserisca i propri dati di conto, acceda al proprio account di posta, digiti password di accesso e cosi' via; dati sensibili che, data la scarsa protezione della macchina, potrebbero essere facilmente carpiri e utilizzati per scopi non legittimi.

Honest mi assicura di poter fornire tutti i riscontri necessari per dimostrare quanto detto.

Premetto che io non conosco personalmente Honest e prima di quest'occasione non abbiamo siamo mai stati in contatto.

Di lui so solo cio' che lui stesso mi ha confidato: Honest e' italiano e si occupa di sicurezza informatica. Per cui non ho ritenuto attendibile la sua informazione nell'immediato, o per lo meno mi sono concesso il beneficio del dubbio chiedendo al nostro informatore di darmi maggiori dettagli.

Honest quindi mi da il link di un'immagine su un server estero che rappresenta uno screenshot della macchina incriminata; naturalmente questo non e' sufficiente per poter dare pieno credito al suo racconto, che comunque necessita di una dovuta verifica.

{mosgoogle left}Ma nello specifico, come ha scoperto Honest questa falla informatica del sistema telematico di uno dei piu' importanti aeroporti al mondo?

Nella maniera piu' "banale", direi: Honest, di passaggio nello scalo londinese, decide di utilizzare uno dei terminali per navigare su internet e per caso riesce ad accedere ad una finestra di Internet Explorer, semplicemente perche' il software dopo un errore genera un PopUp non previsto, bypassando cosi' il portale dedicato, che dovrebbe inibire l'esecuzione di altri programmi presenti sul PC.

Da qui in poi la curiosita' di Honest ha subito preso il sopravvento: inizia cosi' a verificare tutta una serie di condizioni; al termine della sua "esplorazione" rimane assolutamente sorpreso dal livello di esposizione di una macchina che puo' arrecare un notevole danno alla sicurezza informatica di Heathrow.

Certo, la macchina non sara' di proprieta' dell'aeroporto ma molto probabilmente di una societa' esterna (<http://www.spectruminteractive.co.uk/>) che ne vende il servizio, ma questo non cambia la responsabilita' di chi propone questo servizio al pubblico dei frequentatori dell'aeroporto (viaggiatori e dipendenti).

Honest, infatti, ci chiarisce che sulla macchina da lui utilizzata e' possibile non solo "aggirare" l'accesso, navigando gratuitamente invece che a pagamento, ma anche installare diversi tipi di software, accedere a tutti i file di sistema, trasformarlo in una sonda per intercettare traffico IP o sniffare le credenziali di accesso o trasformarlo in un punto di accesso dall'esterno.

{mosgoogle right}E' importante sottolineare ancora una volta come la responsabilita' principale vada imputata in particolare alla spectrum interactive che ha fornito le macchine e che gestisce la manutenzione.

Questo articolo nasce da un'analisi condotta su alcune macchine presenti nell'aeroporto di Heathrow, per cui non e' detto che le vulnerabilita' riscontrate siano valide per tutte le macchine installate dello stesso e su tutte quelle degli altri clienti della Spectrum Interactive.

Di seguito e' riportata la scheda tecnica dell'analisi fatta da Honest con le rispettive evidenze che confermano le vulnerabilita' riscontrate:

File listing:

Attraverso il Browser Internet Explorer e' possibile accedere a tutti i files del computer.

Information Disclosure

Alcuni file utilizzati per il deploy del sistema contengono informazioni utili per condurre attacchi piu' sofisticati.

Command execution:

E' stato possibile eseguire comandi sulla macchina tramite la finestra MsDos.

Infatti e' stato possibile tramite una finestra di dialogo di Gmail per effettuare l'upload di file, modificare un collegamento presente sul Desktop in maniera da richiamare il file command.com.

Tramite la finestra MsDos e' stato possibile visualizzare diverse informazioni del computer:

Indirizzo IP

Nome Computer

Programmi Installati

Patch di Windows

Inoltre, sempre tramite l'utilizzo della finestra di dialogo di Internet explorer e' stato possibile installare programmi.

Nello specifico e' possibile tramite questa tecnica installare:

- Keyloggers
- Sniffer
- Back Door
- Malware
- Etc...

Remote Access:

L'indirizzo pubblico utilizzato da ogni macchina e' raggiungibile dall'esterno.

Cio' implica che e' possibile condurre attacchi dall'esterno, ed inoltre e' possibile utilizzare back door per garantire l'accesso ad utenti esterni.

Queste semplici vulnerabilita'

rendono queste postazioni completamente sotto il controllo di possibili utenti malintenzionati, e costituiscono un grosso problema per la privacy di tutti i fruitori del servizio internet all'interno dell'aeroporto.

Al momento della pubblicazione di questo articolo, i responsabili della sicurezza dell'aeroporto di Heathrow e la societa' che fornisce il Servizio all'aeroporto sono gia' stati allertati. Per cui probabilmente le postazioni saranno gia' state dismesse.

Morale:

Speriamo che dopo la pubblicazione di questo articolo, il management di Heathrow si rendera' conto che tutelare, anche dal punto di vista informatico, i propri utenti e' importante tanto quanto garantire la loro sicurezza fisica; inoltre speriamo vivamente che la Spectrum Interactive innalzerà il livello di attenzione nel distribuire i propri prodotti attuando controlli di sicurezza piu' accurati.

Abbiamo ritenuto importante pubblicare questo articolo con lo scopo quello di mettere in guardia tutti coloro che, tramite pc di cui non si conosce il grado di sicurezza, accedono alle proprie caselle e-mail o semplicemente introducono dati sensibili, come gli estremi della propria carta di credito, per usufruire della navigazione Internet o per effettuare transazioni online.

Infatti potreste aver immesso i vostri dati su un computer, come quelli presenti ad Heathrow, che forse sono gia' utilizzati da personaggi esperti di informatica e che conducono azioni assolutamente non legittime o addirittura illegali.

E' fondamentale che ognuno prenda coscienza delle problematiche relative alla sicurezza informatica e venga educato ad una maggiore attenzione proprio come accade per altre situazioni pericolose relative alla vita di tutti i giorni.

Il nostro ringraziamento va a Honest per la possibilita' che ci ha dato, attraverso il sito di RedOracle.com, di segnalare questa news e di poterla divulgare come informativa educativa.

{rokzoom title=|System Information| album=|heatrhov|}images/stories/BAA/sysinfo2.png{/rokzoom} {rokzoom title=|System Information| album=|heatrhov|}images/stories/BAA/sysinfo1.png{/rokzoom} {rokzoom title=|Network Information| album=|heatrhov|}images/stories/BAA/net1.png{/rokzoom} {rokzoom title=|File Listing and Information Disclosure| album=|heatrhov| }images/stories/BAA/filelisting.png{/rokzoom} {rokzoom title=|File Listing 2 and Information Disclosure| album=|heatrhov| }images/stories/BAA/filelisting2.png{/rokzoom} {rokzoom title=|File Listing 3 and Information Disclosure | album=|heatrhov| }images/stories/BAA/filelisting3.png{/rokzoom} {rokzoom title=|Information Disclosure| album=|heatrhov| }images/stories/BAA/info1.png{/rokzoom}