Ecco come gli hacker russi minacciano il settore hotel: 3 consigli per tenerli a bada

FireEye, azienda di Intelligence Led Security, questa estate ha rilevato una campagna **malware** che ha avuto come obiettivo il settore dell'Hospitality. L'azienda americana di security ritiene che questa campagna possa essere attribuita al gruppo di hacker russi noto come APT28.

FireEye, a seguito delle sue indagini, ha scoperto un documento di spear **phishing** che è stato inviato nella posta elettronica di molte aziende del settore hospitality, compresi hotel in almeno sette paesi europei e uno del Medio Oriente all'inizio di luglio. L'esecuzione del documento infetto avrebbe comportato l'installazione del malware Gamefish che, una volta ottenuto l'accesso ai computer connessi alle reti Wi-Fi aziendali e degli ospiti, diffonde Responder, uno strumento che spinge il computer della vittima ad inviare il nome utente e la password alla macchina controllata dall'attaccante.

L'attività di spionaggio informatico contro l'industria alberghiera è in genere focalizzata sulla raccolta di informazioni su o dagli ospiti dell'hotel piuttosto che sull'industria alberghiera stessa, anche se gli attori possono raccogliere informazioni direttamente sull'hotel come mezzo per facilitare altre operazioni.

I nuovi attacchi rilevati delineano un nuovo vettore di infezione utilizzato dal **gruppo APT28, che sta sfruttando le reti Wi-Fi meno sicure degli hotel per rubare le credenziali.**

Per questo i viaggiatori devono sempre essere consapevoli delle minacce possibili durante i viaggi, specialmente all'estero, e prendere le dovute precauzioni per proteggere i loro sistemi e i loro dati. Allo stesso modo gli albergatori devono fare tutto il possibile per garantire un servizio wifi a prova di hacker.

Abbiamo chiesto a **Marco Rottigni**, Consulting System Engineer Southern Europe di FireEye, alcuni consigli per rendere la rete wifi dell'albergo il più sicura possibile:

"Offrire un accesso pubblico in hotel tramite rete Wi-Fi - spiega Rottigni - significa offrire un servizio ai vostri ospiti, non una minaccia o un pericolo di infezione. Diventa quindi importante che le catene alberghiere implementino **soluzioni per rilevare traffico malevolo** proprio come se la WiFi degli ospiti fosse una delle proprie reti interne. I viaggiatori spesso si fidano dei livelli di sicurezza dell'Hotel, specialmente se offerti da catene alberghiere importanti e note, quindi è essenziale garantire una

qualità della security pari a quella degli altri servizi offerti agli ospiti".
"In secondo luogo - prosegue - **La cultura e l'informazione sui rischi informatici è fondamentale** per evitare compromissioni via mail di *phishing* e altre minacce basate sulla "debolezza del fattore umano". Una buona soluzione sarebbe di contribuire a diffondere tale cultura mettendo in ogni stanza un opuscolo che riassuma i pericoli come il *phishing* e i rischi di prendere la security sottogamba, così come una raccomandazione all'utilizzo delle VPN aziendali quando ci si connette alla rete WiFi alberghiera per motivi di business".
"Per finire - conclude l'esperto di sicurezza aziendale - Il reparto Security dell'Hotel dovrebbe **monitorare la rete WiFi pubblica come controlla le proprie reti interne**, avvisando proattivamente gli utenti in caso venisse rilevato traffico malevolo o infezioni in corso".