Reti WiFi pubbliche: come usarle in sicurezza grazie a Panda Security

- Ultima modifica: Giovedì, 30 Settembre 2021 10:19
Pubblicato: Giovedì, 30 Settembre 2021 10:19
Scritto da Laura Benedetti

Le reti WiFi pubbliche sono spesso bersaglio di attacchi informatici, grazie ad alcune vulnerabilità e all'ingenuità degli utilizzatori. Panda Security, che ha identificato le principali minacce, offre importanti consigli per proteggersi.

A volte le strade più pericolose sono quelle più conosciute e battute, perché con il passare del tempo si abbassa la guardia e si è esposti agli attacchi dei criminali, che invece non smettono mai di cercare nuove vulnerabilità. È ciò che è capitato al **Wi-Fi**, il protocollo di trasmissione di dati wireless che tutti utilizzano a casa e al lavoro, e ormai anche in moltissimi spazi pubblici delle città.

Proprio le **reti pubbliche** sono spesso le porte di ingresso dei "pirati informatici". Le stesse caratteristiche che rendono le reti Wi-Fi gratuite appetibili agli utenti le rendono interessanti anche agli hacker: si tratta banalmente della possibilità di **connettersi aggirando una prima autenticazione.** Data la diffusioni delle reti pubbliche (ristoranti, locali, hotel, aeroporti, librerie e persino in alcuni negozi) ormai gli hacker riescono con estrema facilità a **carpire dati da smartphone, tablet o laptop** quando gli utenti sono connessi a questo tipo di reti.

Phoca PDF

Ma quali sono gli attacchi più diffusi tramite le reti pubbliche? **Panda Security** ha rilevato le principali minacce, a cui ci si espone in caso di connessione WiFi pubblica:

- **Attacco Man-in-the-Middle (MitM):** le comunicazioni quotidiane tramite Wi?Fi possono condurre ad una violazione quando un criminale informatico intercetta e altera segretamente conversazioni legittime
- **Evil twin:** i criminali informatici utilizzano in modo doloso il proprio access point per imitare un vero access point alla rete Wi?Fi e un indirizzo hardware univoco. Gli utenti rischiano di perdere documenti e credenziali private, che possono contenere informazioni sensibili, a causa di ladri informatici che intercettano i dati inviati tramite la rete
- **Errata configurazione dell'access point:** l'implementazione di access point senza seguire le best practice di sicurezza Wi?Fi può portare involontariamente a configurazioni errate, che spesso comportano un rischio per la sicurezza
- **Access point falsi:** non vi è nulla che impedisca fisicamente ai criminali informatici di attivare un access point esterno nella vostra rete e invitare vittime ignare a eseguire l'accesso. Gli utenti che cadono vittima dell'access point falso possono facilmente subire un furto di dati e credenziali o un'iniezione di codice dannoso che spesso passa inosservata
- **Uso sconveniente e illegale:** le organizzazioni che offrono reti Wi?Fi guest rischiano di ospitare presso di sé una vasta gamma di comunicazioni illegali e potenzialmente dannose. I contenuti riservati agli adulti o di stampo estremista possono risultare offensivi per gli utenti vicini e i download illegali di file multimediali protetti possono esporre l'organizzazione a cause legali per violazione del copyright
- **Spoofing dell'indirizzo MAC dell'access point**: i criminali informatici che realizzano violazioni della sicurezza Wi?Fi generalmente tentano di mascherare i loro access point dannosi come access point legittimi o noti mediante lo spoofing degli indirizzi MAC
- **Attacco Karma:** dopo più di dieci anni dalla sua invenzione, questo attacco dilaga ancora oggi. Gli access point dannosi ascoltano le richieste dei probe client alla ricerca di nomi di rete Wi?Fi ai quali sono stati connessi in precedenza, quindi trasmettono tali nomi connettendo le vittime all'access point dannoso per rubare dati, credenziali e altre informazioni sensibili
- **Violazione della crittografia WPA/WPA2 (KRACK):** tramite il KRACK, lo streaming di dati su reti Wi?Fi crittografate WPA/WPA2, come password e dati personali, può essere intercettato, decifrato e modificato all'insaputa dell'utente. Questa falla nella sicurezza significa che, per i client e gli access point vulnerabili, il traffico Wi?Fi crittografato WPA e WPA2 è potenzialmente esposto.

Data la natura non mirata di un attacco, spesso gli hacker non hanno interesse a forzare dei dispositivi protetti e si concentrano unicamente su bersagli facili. Questo consente di **potersi difendere** anche con poco impegno in reti pubbliche complesse, ma è necessario avere

Phoca PDF

maggiore protezione se si usufruisce di reti condivise di ambienti più piccoli.

Spesso in seguito al rilevamento di alcune vulnerabilità, i produttori di dispositivi e reti hanno rilasciato degli **aggiornamenti di sicurezza** che mettono a riparo da molte problematiche. Per cui, il primo consiglio fondamentale è di assicurarsi che i dispositivi ed i sistemi operativi siano sempre aggiornati. In secondo luogo, data la natura degli attacchi di aggregazione e frammentazione, ecco **i consigli di Panda Security** per proteggere la tua connessione Wi-Fi:

- Installare un programma di cybersicurezza completo e impostare gli aggiornamenti automatici. Un buon **antimalware e antivirus** è la difesa migliore contro la maggior parte dei malware su cui si basano molti attacchi informatici
- Quando ci si connette tramite una connessione non sicura è indispensabile utilizzare una **connessione VPN (Virtual Private Network).** Anche se un hacker riuscisse a intromettersi nella connessione, intercetterebbe dati protetti tramite una crittografia avanzata
- Non inserire mai i propri dati personali su siti web che non utilizzano il **protocollo HTTPS**, con la S finale (e non solo http). Per verificarlo, basta guardare la barra degli indirizzi del browser e controllare che l'URL inizi appunto con "https". Inoltre, per i siti sicuri che hanno ottenuto il certificato SSL, il browser mostra anche un'icona a forma di lucchetto proprio a sinistra del nome del sito
- Moltissimi attacchi comprendono una tattica di phishing, ovvero di contraffazione di informazioni e inganno dell'utente in modo da convincerlo a condividere i propri dati di accesso a un account online. È importante **mantenersi informati** per conoscere le campagne di phishing in corso e le ultime novità di sicurezza informatica. A tal proposito consigliamo di seguire il blog di Panda Security.

Proprio come per le minacce, anche le **misure di sicurezza più efficaci** sono spesso quelle più comuni e sottovalutate, seguire queste semplicissime norme di sicurezza può far risparmiare tempo, denaro e tanti problemi.

Phoca PDF