AGENȚIA DE APĂRARE CIBERNETICĂ

Wi-Fi

PUBLIC WI-FI

BEST SECURITY PRACTICES

Introducere

Utilizarea unei conexiuni Wi-Fi publice expune utilizatorul la mai multe amenințări severe de securitate. În prezent, Internetul este fără îndoială o necesitate în viața de zi cu zi a fiecărei persoane, iar punctele de Wi-Fi publice prezente aproape peste tot sunt ceea ce actuala generație de utilizatori are nevoie. Navigarea în Internet prin Wi-Fi-ul de acasă nu reprezintă o problemă, accesul fiind ușor, facil și rapid. Cu toate acestea, atunci când navigarea în Internet se realizează printr-un punct Wi-Fi public, lucrurile se schimbă.

Cum funcționează Wi-Fi-ul public ?

Un punct Wi-Fi public reprezintă un punct de acces gratuit către Internet. Modul de funcționare a Wi-Fi-ului public constă în accesarea Internetului prin conectarea dispozitivelor personale, precum smartphone, tabletă sau laptop la un dispozitiv de rețea (router sau access point), viteza de trafic și puterea semnalului oscilând în funcție de distanța fizică dintre utilizator și dispozitivul de rețea. Multe orașe sau companii oferă acces gratuit la Wi-Fi, ceea ce ajută utilizatorii să beneficieze de conexiuni mult mai rapide la Internet comparativ cu utilizarea datelor mobile.

Cu toate acestea riscurile asociate utilizării unei astfel de conexiuni sunt majore. Iată câteva sfaturi pentru îmbunătățirea securității și evitarea riscului de a deveni victima unei înșelăciuni.

Cum exploatează atacatorii rețelele Wi-Fi publice ?

Nu sunt necesare cunoștințe de specialitate pentru a asigura protecția datelor sensibile împotriva persoanelor rău-intenționate. Tot ce trebuie făcut este înțelegerea riscurilor și a metodelor utilizate de aceștia. Iată câteva metode folosite de atacatori:

- ***Rogue access points*** - sunt puncte de acces în Internet deținute de către persoane rău-intenționate, similare ca denumire cu rețeaua legitimă. La conectarea la o rețea publică necunoscută este recomandată verificarea cu atenție a datelor acesteia.
- ***Wi-Fi pineapple*** - reprezintă un dispozitiv fizic portabil conceput pentru auditarea unui segment de rețea pentru a verifica configurarea acesteia. Cu toate acestea, persoanele rău-intenționate îl folosesc pentru a seta un punct de acces fals și a lansa atacuri de tip ”*man-in-the-middle*[1]”.
- ***Peeping toms*** - rețelele publice sunt accesate de o mulțime de persoane, iar unele dintre ele nu au întotdeauna intenții bune. Atunci când un atacator accesează o rețea publică, în lipsa unor măsuri de securitate adecvate, acesta poate intercepta informațiile transmise de ceilalți utilizatori ai rețelei și lansa atacuri de tip ”*man-in-the-middle*”.
- ***Alerte de actualizare*** - Este recomandată actualizarea periodică a dispozitivului cu condiția ca aceasta să se desfășoare în cadrul unei rețele de încredere. Majoritatea oamenilor nu acordă suficientă atenție mesajelor de tip alertă care solicită o actualizare urgentă a dispozitivului. În cadrul unei rețele publice, afișarea unui mesaj de actualizare poate fi similar unui cal troian, alerta fiind de fapt un malware deghizat transmis de către atacatori.

Wi-Fi Pineaplle

[1] Man-in-the-middle - metodă de atac cibernetic în care atacatorul se poziționează între utilizator și aplicație, având posibilitatea de a intercepta și chiar modifica traficul de rețea, fără ca utilizatorii să observe. Un astfel de atac poate compromite date sensibile precum informații personale, credențiale sau date bancare.

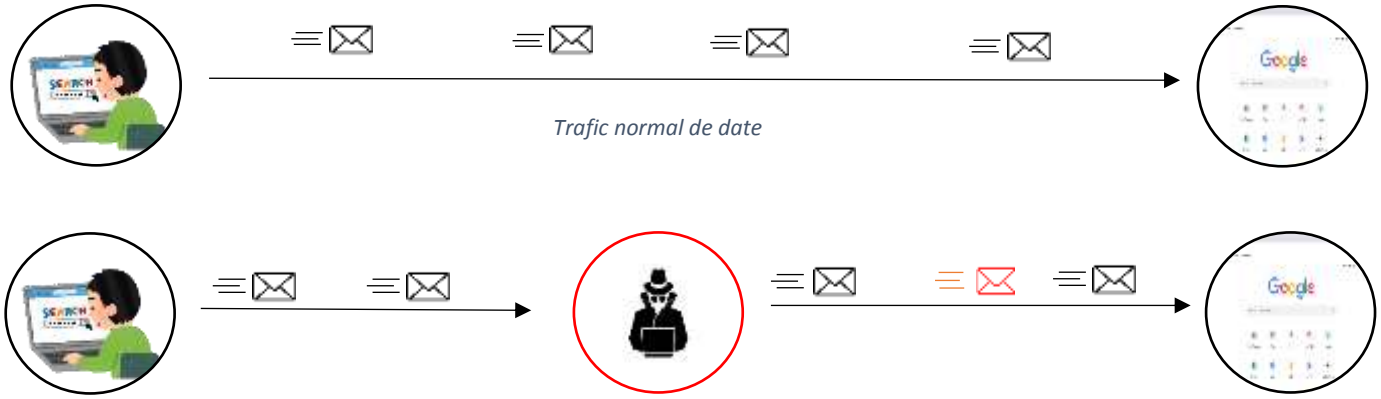
Riscurile utilizării unei rețele publice Wi-Fi

Pentru a fi accesată cât mai ușor de către toți utilizatorii, stabilirea unei conexiuni la Internet în cadrul unei rețele publice nu necesită autentificare. Prin urmare, aceasta este o oportunitate excelentă pentru atacatori de a accesa fără probleme orice dispozitiv nesecurizat conectat la rețea.

Iată câteva dintre cele mai comune pericole ale utilizării unei rețele Wi-Fi publice:

- ***Accesarea informațiilor personale***

Așa cum este menționat anterior, conectarea la o rețea publică nu necesită credențiale pentru autentificare, ceea ce înseamnă că rețeaua poate fi folosită de absolut oricine. Prin urmare, este o oportunitate tentantă pentru atacatori de a încerca accesarea sau sustragerea informațiilor personale ale utilizatorilor conectați. Una dintre cele mai des întâlnite modalități de intruziune este atacul de tip *man-in-the-middle*.



Trafic interceptat și modificat prin atacul Man-in-the-middle

- ***Infectarea dispozitivului cu malware***

Un alt risc major la care se expun utilizatorii unei rețele Wi-Fi publice este infectarea dispozitivului cu malware. Persoanele rău-intenționate pot folosi rețeaua ca mediu de infectare sau pentru a captura informațiile sensibile ale utilizatorilor. Spre exemplu, dacă funcția *sharing* este activă pe un dispozitiv conectat la o rețea publică, un atacator se poate conecta la dispozitivul respectiv și a-l compromite fără ca utilizatorul să observe.

Infectarea dispozitivului cu malware

- ***Interceptarea mesajelor și a traficului web***

În cadrul unei rețele publice atacatorii pot intercepta cu ușurință aplicațiile de mesagerie necriptate, precum și solicitările transmise către site-urile web. Deși majoritatea site-uri web folosesc protocoale de criptare a traficului, sunt încă multe site-uri care nu o fac, iar transmiterea de informații sensibile către un website nesecurizat prin intermediul unei rețele nesecurizate poate avea consecințe grave, precum furtul identității.

- ***Snooping & Sniffing***

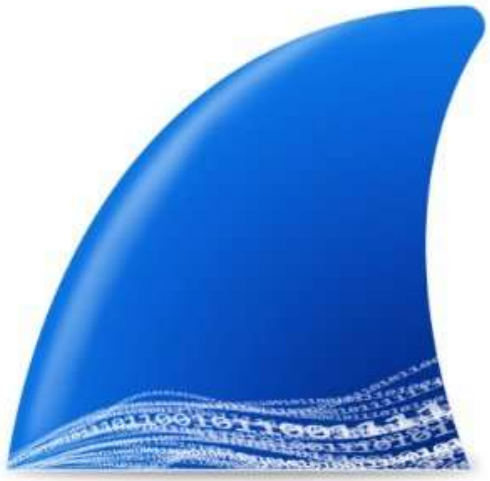
Cu ajutorul unor dispozitive și aplicații speciale, persoanele rău-intenționate pot intercepta traficul de rețea public. Utilizând tehnica *Snooping & Sniffing* aceștia pot vizualiza tot ceea ce utilizatorul accesează în mediul online, de la credențiale până la informațiile completate pe paginile web.

- ***Infectarea cu viermi***

Atacul cu viermi nu este un termen nou atunci când vine vorba de atacuri cibernetice. Un vierme de calculator este un tip de malware care se răspândește prin autoreplicare de la un sistem informatic la altul fără a fi necesară interacțiunea umană. În cadrul unei rețele publice se regăsesc o mulțime de dispozitive interconectate, iar dacă unul dintre acestea este infectat, și celelalte dispozitive sunt în pericol.

- ***Packet sniffing***

În mediul online se regăsesc gratuit o mulțime de instrumente de analiză a traficului, ex. Wireshark. Cu ajutorul acestora, o persoană rău-intenționată poate intercepta și analiza traficul de rețea pentru a obține credențiale sau alte informații sensibile ale utilizatorilor.



Logo Wireshark

- ***Sidejacking***

Cunoscută și sub denumirea de *session jacking*, este o tehnică bazată pe sniffing[2] și manipulare a cookie[3]-urilor transmise de utilizatori. Spre exemplu, dacă un atacator interceptează pachetele de date atunci când un utilizator dorește să își acceseze contul bancar, acesta are posibilitatea de a modifica cookie-urile transmise și de a se conecta ulterior la contul compromis fără ca banca să identifice incidentul.

- ***Shoulder surfing***

Uneori, persoanele rău-intenționate se poziționează strategic în zonele cu acces gratuit la Wi-Fi pentru a vedea numele de utilizator, parolele și celelalte informații sensibile ale utilizatorilor. Nu este recomandată lăsarea

[2] Sniffing - modalitate de interceptare a traficului de date prin intermediul unor aplicații sau dispozitive special concepute;
[3] Cookie - un modul cookie este un text special, deseori codificat, folosit pentru a urmări autentificarea și comportamentul utilizatorilor;

dispozitivelor nesupravegheate, chiar și pentru intervale scurte de timp, șansele de compromitere a dispozitivului cresc simțitor.

Ghid de protecție și bune practici pentru utilizarea rețelelor Wi-Fi publice

Pentru îmbunătățirea securității și mitigarea pericolelor, iată câteva recomandări:

- ***Instalarea unei soluții anti-malware și firewall pe dispozitive***

Toate dispozitivele informatice utilizate pentru a naviga în Internet ar trebui să aibă instalată o soluție anti-malware. Pe lângă aceasta, pentru o protecție completă, este recomandată și utilizarea unei soluții firewall.

- ***Utilizarea unei aplicații VPN***

Utilizarea unei conexiuni de tipul VPN[4] este fără îndoială cea mai bună metodă pentru a rămâne în siguranță atunci când sunt folosite rețele publice, dat fiind faptul că un VPN are rolul de a cripta integral traficul de date.

- ***„Be your own hotspot"***

Utilizarea datelor mobile oferă un nivel de protecție mult mai ridicat comparativ cu rețelele publice. Deși poate implica costuri financiare, telefonul poate fi configurat ca punct de acces în Internet pentru celelalte dispozitive personale. De asemenea, anumite companii oferă posibilitatea contractării unui dispozitiv Wi-Fi portabil.

[4] VPN (Virtual Private Network) - rețea privată extinsă peste o rețea publică ce are ca scop creșterea securității conexiunii;

- ***Evitarea transmiterii de date personale prin intermediul unei rețele publice***

Trebuie conștientizat faptul că o rețea Wi-Fi publică poate fi în orice secundă compromisă. Tocmai de aceea, utilizatorilor nu li se recomandă accesarea sau transmiterea de date pe anumite platforme precum site-urile bancare.

- ***Actualizarea în permanență a aplicațiilor utilizate***

Această recomandare nu se aplică doar în cazul utilizării unei rețele publice. Pentru a fi protejat în permanență împotriva ultimelor amenințări din spațiul cibernetic este recomandată actualizarea periodică a sistemului de operare, a aplicațiilor și a soluțiilor utilizate.

- ***Deconectarea contului atunci când nu mai este necesară utilizarea acestuia***

Atunci când nu mai este necesară utilizarea unei anumite platforme, este recomandată deconectarea contului și evitarea memorării credențialelor în cadrul browser-elor.

- ***Utilizarea de parole unice și complexe***

Pentru un nivel de protecție ridicat este recomandată configurarea unor parole unice și complexe pentru fiecare cont în parte. Memorarea unor parole complexe poate fi dificilă tocmai de aceea utilizatorilor le este recomandată utilizarea unei aplicații de tip ”*password manager”*[5]. De asemenea, acolo unde este posibil, utilizatorilor le este recomandată implementarea autentificării multi-factor.[6]

[5] Password manager - aplicație ce permite generarea, stocarea și managementul parolelor pentru aplicațiile locale și serviciile online;

[6] Autentificare multi-factor - modalitate de autentificare bazată pe prezentarea a cel puțin 2 elemente din triada ”what you know, you have, you are”;

- ***Utilizarea extensiei ”HTTPS Everywhere”***

Este recomandată utilizarea unei extensii din browser precum ”HTTPS Everywhere”. Aceasta are rolul de a ”obliga” website-urile accesate să utilizeze protocolul HTTPS[7] în locul HTTP[8].

- ***Dezactivarea funcțiilor ”wi-fi”, ”sharing”, ”bluetooth” și ”tethering”***

Pentru a limita accesul neautorizat la dispozitivele personale, utilizatorilor le este recomandată dezactivarea funcțiilor wi-fi, sharing, bluetooth și tethering atunci când acestea nu sunt folosite. Totodată, funcția wi-fi ar trebui configurată astfel încât dispozitivul să nu se conecteze automat la rețelele descoperite.

Referințe

- https://www.freepik.com/premium-vector/wi-fi-network-icon-low-polygonal-abstract-wi-fi-sign_5651072.htm
- https://www.centurylink.com/home/help/internet/wireless/what-is-a-wi-fi-hotspot1.html
- https://privacysavvy.com/security/safe-browsing/public-wifi-dangers-and-how-to-protect/
- https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/risks-of-using-public-wi-fi
- https://www.nicepng.com/ourpic/u2q8r5i1a9a9r5i1_free-wifi-free-wifi-logo-in-png/
- https://ro.wikipedia.org/wiki/Cookie
- https://en.wikipedia.org/wiki/Sniffing_attack
- https://ro.wikipedia.org/wiki/Re%C8%9Bea_privat%C4%83_virtual%C4%83
- https://en.wikipedia.org/wiki/Password_manager

[7] HTTPS (HyperText Transfer Protocol Secure) - reprezintă protocolul HTTP încapsulat într-un flux SSL/TLS;
[8] HTTP (HyperText Transfer Protocol) - protocol de tip text ce permite accesarea informațiilor stocate în Internet;

Agenția de Apărare Cibernetică