DE IBK

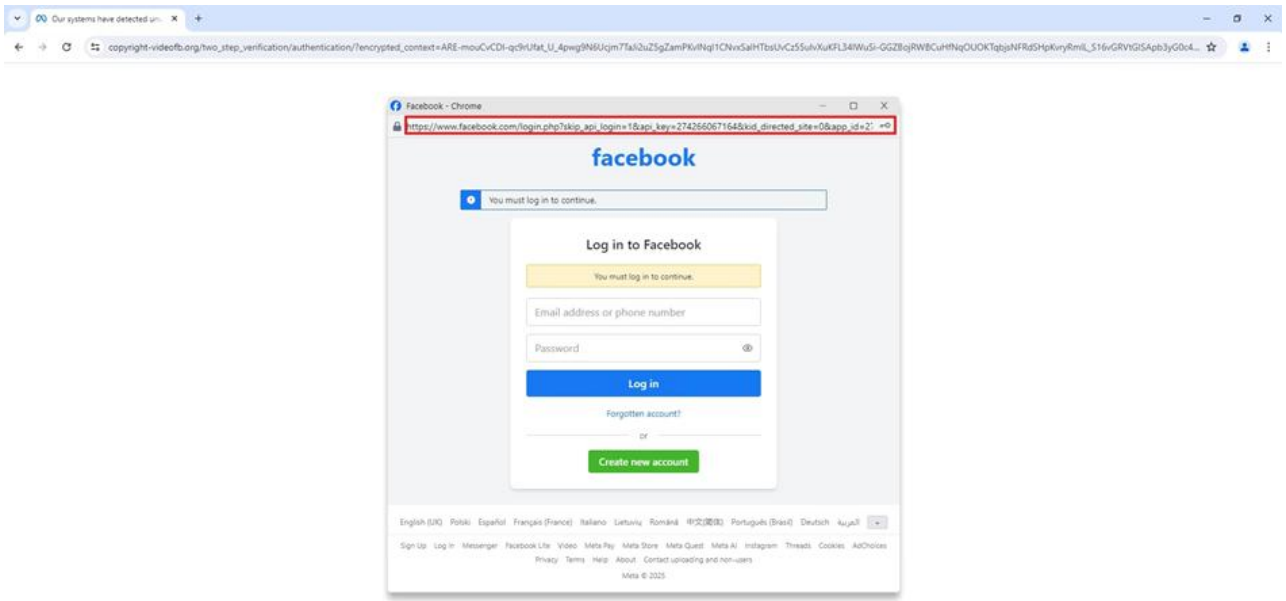
Hogyan védekezhetünk a böngésző a böngészőben támadás ellen?

A böngésző a böngészőben (browser-in-the-browser – BitB) támadás egy 2022-ben, akkor még csak elméleti síkon bemutatott adathalászati technika, amit a mr.d0x néven ismert kiberbiztonsági kutató fejlesztett ki. Néhány évvel később a technikát már széles körben használják a kiberbűnözők, de nézzük mitől is olyan különleges ez a módszer és hogyan lehet védekezni ellene.

Böngésző a böngészőben (BitB)

A BitB technika az adathalászat egy kifinomult módja. A támadók legitimnek tűnő, hamis weboldalakat hoznak létre, amelyeken a felhasználók csak bejelentkezés után tudnak bárminemű műveletet végrehajtani, például hozzászólásokat írni vagy vásárolni. A bejelentkezéshez használt felugró ablakban olyan népszerű szolgáltatások bejelentkezési oldalait másolják le a támadók, mint a Microsoft, a Google vagy a Facebook.

A támadás során a hamis weboldalon felugrik egy **hamis bejelentkezési ablak** egy népszerű, megbízhatónak tűnő szolgáltató nevében, ám a valódi bejelentkezési oldal helyett a felhasználó egy hamis űrlappal találkozik, ráadásul a bejelentkezési ablak címsorában az **URL cím is teljesen legitimnek tűnik.**



Mivel a támadók olyan URL címet jelenítenek meg a böngészőablakban, amilyet csak szeretnének, és ugyanez igaz a HTTPS kapcsolatot jelző SSL tanúsítvány szimbólumra (lakat) is, a BitB támadásokat kifejezetten nehéz észrevenni.

Facebook kampány

Egy Facebook hitelesítő adatok megszerzésére irányuló kampány során a csalók egy jogi iroda megszemélyesítésével, szerzői jogok megsértésének vádjával keresik fel e-mailben áldozataikat és fenyegetik meg őket a felhasználói fiókuk azonnal felfüggesztésével, ráadásul hamis biztonsági értesítéseket is küldenek a Meta nevében valójában nem létező, jogosulatlan bejelentkezésekről.

Hogyan védekezhetünk a BitB támadások ellen?

A legegyszerűbb védekezési módszer az ilyen jellegű támadások ellen a **jelszókezelők használata**.

Mikor a bejelentkezési adatok automatikus kitöltéséről van szó a jelszókezelők a valódi URL címet ellenőrzik, nem pedig azt, hogy mi került a címsorban megjelenítésre, így a legegyszerűbb szabály jelszókezelők használata mellett a következő:

> Ha a jelszókezelő felajánlja a bejelentkezési adatok automatikus kitöltését, akkor olyan weboldalon járunk, ahol korábban mentettünk el hitelesítő adatokat, így mindenképp gyanúra adhat okot, ha a jelszókezelő nem ajánlja fel a segítséget.

Ezen felül az adathalászat elleni általános védelmi megoldások érvényesek:

- Ahol csak módunkban áll **használjunk kétfaktoros azonosítást** (2FA)!
- Minden felhasználói fiókhoz **használjunk kellően hosszú, változatos karakterekből álló, egyedi jelszavakat**!
- **Ne nyissunk meg ismeretlen forrásból érkező** e-maileket és üzeneteket, továbbá **ne kattintsunk** az ily módon kapott hivatkozásokra sem!
- Mindig kezeljünk kellő gyanakvással az **érzelmeinkre ható** (pl.: sürgető, bűntudat- és pánik keltő) és **valamilyen interakciót** (pl.: válaszolás, linkre kattintás, űrlapkitöltés) kiváltani szándékozó megkereséseket!
- Hivatalosnak tűnő e-mailek és üzenetek esetén, mielőtt bármit is csinálnánk, érdemes felkeresni a megkeresésben feltüntetett **szervezetek hivatalos elérhetőségeinek** valamelyikét, és ott érdeklődni az üzenetek valódiságáról.
- Amennyiben úgy érezzük, hogy adathalász üzenettel van dolgunk, **jelentsünk** azt a platformok üzemeltetőinek, munkahelyi környezetben pedig a szervezet rendszergazdáinak!