TLP:CLEAR
Szabadon terjeszthető!

Tájékoztatás
Technikai támogatásnak álcázott online csalások

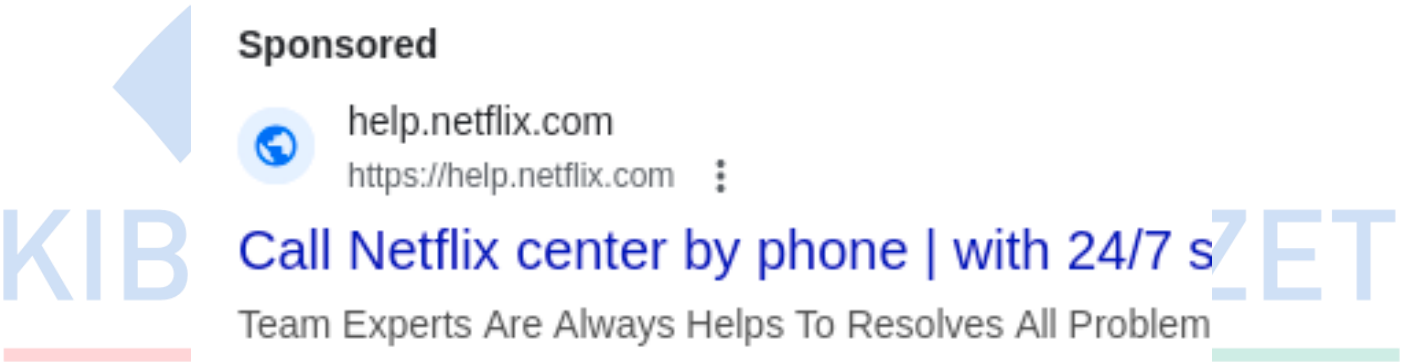
A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) tájékoztatót ad ki a technikai támogatásnak álcázott csalások újabb formájának megjelenésével kapcsolatban.

A Malwarebytes kutatásokért felelős igazgatója által feltárt valós esetek alapján **a csalók hamis keresési találatokkal élnek vissza**, kihasználva a felhasználók bizalmát az ismert márkák – például az Apple, a Microsoft, a Facebook, a Netflix, a Bank of America vagy a PayPal – iránt.

A támadás folyamata

A támadók **fizetett hirdetést jelenítenek meg a Google keresési találatai között**, amely első ránézésre hivatalosnak tűnik. A hirdetés vagy **egy hamis weboldalra, vagy egy valódi oldal „Súgó" felületére irányítja** a felhasználót, azonban ott a csalók által **beágyazott hamis telefonszám** jelenik meg.

Mivel **a böngésző címsora a valódi domaint mutatja**, a felhasználó gyanútlan marad (1. ábra). A hívás során **a csalók a cég ügyfélszolgálatának adják ki magukat**, hogy személyes vagy banki adatokat szerezzenek meg, illetve távoli hozzáférést szerezzenek az áldozat eszközéhez.



1. ábra Szponzorált hirdetés forrás: Malwarebytes

A támadás technikai háttere

A módszer neve: „search parameter injection attack". A támadó egy olyan URL-t hoz létre, amely az eredeti weboldal legitim keresési funkciójába ágyaz be hamis adatokat, például egy telefonszámot. Ez a technika (reflected input vulnerability) egy olyan bemeneti sebezhetőséget használ ki, ahol a felhasználótól érkező adat azonnal megjelenik a weboldal válaszában, mindenféle szűrés vagy ellenőrzés nélkül. A felhasználó így hiteles megjelenésű, de megtévesztő tartalommal találkozik.

Hogyan lehet kivédeni a technikai támogatásnak álcázott csalásokat?

- **Figyeljünk az URL-re:** ha a böngésző címsorában telefonszám jelenik meg, az gyanúra adhat okot.
- **Gyanús keresési kifejezések:** kerüljük az olyan találatokat, amelyekben „Hívjon most" vagy „Azonnali támogatás" jellegű szöveg szerepel!
- **Szokatlan karakterek:** az URL-ben megjelenő kódolt jelek, mint a *%20* (szóköz) vagy *%2B* (+ jel) telefonszámokkal együtt szintén árulkodóak lehetnek.
- **Valótlan keresési eredmények:** ha a weboldal már akkor megjeleníti az eredményeket, mielőtt bármit beírtunk volna, az a keresési funkció manipulációjára utal.
- **Sürgető hangnem:** ha a weboldal szövege nyomást gyakorol ránk („Fiók felfüggesztve", „Hívjon most!"), legyünk különösen óvatosak!
- **Böngésző figyelmeztetései:** ne hagyjuk figyelmen kívül a biztonsági szoftver vagy a böngésző által megjelenített csalásra utaló riasztásokat!
- **Ellenőrizzük a telefonszámot:** mielőtt bárkit felhívnánk, keressük elő a hivatalos elérhetőséget a vállalattal korábban folytatott kommunikációból (pl. e-mail, közösségi média), és hasonlítsuk össze a keresési eredménnyel. Ha eltérés van, ellenőrizzük alaposabban!
- **Személyes és banki adatok védelme:** ha a telefonbeszélgetés során olyan adatokat kérnek, amelyek nem kapcsolódnak közvetlenül az ügyintézéshez, szakítsuk meg a hívást!

Hivatkozások:

https://www.malwarebytes.com/blog/news/2025/06/scammers-hijack-websites-of-bank-of-america-netflix-microsoft-and-more-to-insert-fake-phone-number?utm_source=chatgpt.com

Nemzetbiztonsági Szakszolgálat
Nemzeti Kibervédelmi Intézet
Telefon: +36-1-336-4833