

Sajtóközlemény



Budapest, 2023. július 17.

A vállalkozások mobileszközeit célzó támadások ellen nyújt védelmet a Vodafone legújabb kiberbiztonsági szolgáltatása

A távmunka elterjedésével az okostelefonok elsődleges munkaeszközökké váltak, és ezt a támadók is tudják: csak a vishing (hangalapú adathalászat) visszaélések száma másfél év alatt több, mint hatszorosára ugrott 2022 második negyedévére.¹ A Vodafone vállalkozásoknak szóló szolgáltatása éppen a mobileszközöket célzó támadások ellen nyújt megoldást: a Lookout mobil kibervédelmi megoldás védelmet jelenthet a mobileszközöket fenyegető hálózat-, eszköz-, alkalmazás- és tartalomalapú kockázatok ellen.

A kibertámadások száma globális szinten folyamatosan emelkedik, 2022-ben megközelítőleg 5,5 milliárd ilyen támadást hajtottak végre világszerte. A támadásokkal okozott károk költségei 2022-ben 4,35 millió dollárra – több mint másfél milliárd forintra – emelkedtek, jelentős veszteségeket okozva ezzel az érintett cégeknek.² Noha az adathalász támadások egyetlen iparágat sem kerülnek el, 2022-ben a leginkább érintett területek a banki és az egészségügyi ágazatok mellett az energia- és közműszolgáltatások, a szállítás és a gyártás szektorok voltak³. Míg korábbi években a kibertámadások jelentősebb része Észak-Amerikát érintette, addig az utóbbi években megfigyelhető ennek a tendenciának az eltolódása az európai régió irányába.⁴

A legkomolyabb kockázatnak zsarolóvírusok tekinthetők, az előző évben több, mint 493 millió támadást indítottak világszerte különböző zsaroló technikákat alkalmazva.⁵ Emellett jelentősen elterjedt az adathalász technikák változatos kihasználása, például a vishing (hangalapú adathalászat), a smishing (SMS adathalászat) és a quishing (QR-kódos adathalászat) is egyre gyakoribban használt módszerek. A támadók számtalanszor ezeket kombinálva támadnak, ez az úgynevezett hibrid adathalászat, mellyel képesek akár a többfaktoros hitelesítés (MFA) kijátszására is. Csak a hangalapú visszaélések száma 2022 második negyedévében 625 százalékos növekedést mutatott, mióta 2021 első negyedévében elkezdtek rögzíteni ezen támadások jelenlétét.⁶ A megoldást a kiber-sebezhetőség csökkentése, valamint az adathalász támadások kivédése jelentheti – mely különösen kritikus a mobileszközök esetében.

¹ Lookout: The Global State of Mobile Phishing – 2023

² [Parachute: Cyber Attack Statistics](#) – 2023. április

³ Lookout: The Global State of Mobile Phishing – 2023

⁴ [Infographic - Mid-Year Update: 2022 SonicWall Cyber Threat Report](#)

⁵ [Latest Threat Intelligence Tracks Shifting Cyber Frontlines \(sonicwall.com\)](#)

⁶ Lookout: The Global State of Mobile Phishing – 2023

A mobil eszközök ugyanis számos érzékeny adatot tartalmaznak: hozzáférést biztosítanak az elektronikus levelezéshez, fényképekhez, a készülék kamerájához, GPS-koordinátákhoz, jelszavakhoz és kontaktlistákhoz. Emellett a távolról dolgozó alkalmazottak többségének gyakran engedélyezett a munkahelyük által, hogy olyan személyes eszközöket és hálózatokat is használjanak a munkájukhoz, amelyeket az IT nem tud megfelelően leellenőrizni. Mindez a vállalatok számára komoly biztonsági kockázatot jelent.

„A hazai és nemzetközi statisztikák alapján azt látjuk, hogy az adathalászat egyre növekvő fenyegetést jelent a vállalatoknak. A vállalkozások digitális támogatása elsődleges célunk, éppen ezért ezen a téren is partnereink segítségére leszünk, és olyan átfogó megoldást kínálunk, amely a hibrid munkavégzés és a saját mobil eszközök használata mellett is garantálja, hogy az érzékeny adatok ne kerüljenek illetéktelen kezekbe” – mondta el Dobó Mátyás, a Vodafone Magyarország vállalati szolgáltatások üzletág vezérigazgató-helyettese.

A Vodafone által kínált Lookout mobil kibervédelmi szolgáltatás védelmet biztosíthat a mobil eszközöket fenyegető hálózat-, eszköz-, alkalmazás- és tartalomalapú kockázatok ellen minden iOS, Android és Chrome OS mobil eszközön, továbbá megoldást nyújt a kockázatok felismeréséhez és kezeléséhez is.

A Lookout egy kimondottan mobil eszközökre fejlesztett szoftver, amely a mesterséges intelligencia segítségével elemzi a több, mint 200 millió eszközből és több, mint 120 millió alkalmazásból álló globális hálózat telemetriai adatait. A szokásostól eltérő viselkedés beazonosításával észleli és elhárítja a kényszerű behatolást, összegyűjti és elemzi a kompromittálásra utaló jeleket – ezzel megóvva az eszköz használatát a lehetséges fenyegetésektől. Működési elve rendkívül egyszerű: egy webes kezelőfelületből és egy könnyen átlátható mobil alkalmazásból áll, amelyhez magyar nyelvű támogatás is elérhető a felhasználók számára.

Noha az adathalász támadások egyetlen iparágat sem kerülnek el, 2022-ben a leginkább érintett területek a banki és az egészségügyi ágazatok mellett az energia- és közmuhszolgáltatások, a szállítás és a gyártás szektorok voltak⁷.

További információk:

sajto@vodafone.com

A Vodafone Magyarországról

A Vodafone Magyarország Zrt. Magyarország második legnagyobb telekommunikációs szolgáltatója. Konvergens szolgáltatóként (mobiltelefon, internet és TV) célunk, hogy a lakosság és a vállalkozások egyaránt élhessenek a digitális világ kínálta lehetőségekkel.

A Vodafone Magyarországnál mintegy 3000 kollégánk munkájának eredményeképp jelenleg több, mint 3 millió ügyfelet szolgálunk ki mobil szolgáltatásunkkal, míg vezetékes szolgáltatásunkat több, mint 800 ezer ügyfél veszi igénybe. A Vodafone Magyarország az elsők között van az IoT szolgáltatás területén is; országszerte több mint 600 ezer IoT kapcsolattal rendelkezünk.

Hiszünk abban, hogy az oktatás, az egészségügy, a mezőgazdaság és az ipar digitalizációja megkönnyíti a mindennapi életet, hozzájárul a közjóhoz, a gazdasági fejlődéshez és versenyképességhez, ahhoz, hogy jobb, zöldebb, digitálisabb jövőt teremtsünk.

Társadalmi felelősségvállalási politikánkban kiemelt szerepet kap az esélyegyenlőség megteremtése, a hátrányos helyzetű térségek felzárkóztatása, a digitális világ kínálta lehetőség minél szélesebb körnek való eljuttatása. Kiemelt célunk továbbá a saját és ügyfeleink környezeti hatásának csökkentése.

⁷ Lookout: The Global State of Mobile Phishing – 2023

A Vodafone Magyarország Zrt. a 4iG Csoport tagja.

További információk: www.vodafone.hu, [Vodafone Hungary Facebook](#)