TLP:CLEAR
Szabadon terjeszthető!

Tájékoztatás

Simple egyes felhasználói fiókjai elleni támadásról
(2023. december 07.)

Tisztelt Ügyfelünk!

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) tájékoztatót ad ki az OTP Mobil Kft. által üzemeltetett Simple alkalmazás egyes felhasználói fiókjai elleni támadásról és digitális fiókvédelmi javaslatokról.

A Simple 2023.12.06-ai közleménye szerint:

„December 5-én este, más felület(ek)en eltulajdonított felhasználónév/jelszó kombinációkkal digitális adattolvajok több ezer Simple-felhasználó fiókjához fértek hozzá. Az illetéktelenek fizetési tranzakciót nem tudtak indítani, anyagi kár így nem történt. Az érintett fiókokat haladéktalanul blokkoltuk, a helyreállításról és a szükséges tájékoztatásról gondoskodtunk. A fiókok védelme érdekében a szükséges lépéseket megtettük. A bűnözők ellen hatósági intézkedést kezdeményezünk.”

A szolgáltató a támadásban érintett ügyfeleit tájékoztatta arról, hogy

- fiókjuk biztonsági okokból felfüggesztésre került,
- a helyreállításhoz **új jelszót** kell beállítaniuk egy **Simple-jelszó-módosító linket tartalmazó rendszeremail segítségével,**
- **ami javasolt, hogy a korábban, vagy más szolgáltatásban használttól eltérő.**

Az NBSZ NKI az eset kapcsán az alábbiakra szeretné felhívni a figyelmet:

1. **Amennyiben Ön érintett a Simple elleni kibertámadásban (erről a fentiek szerint értesítést kapott az alkalmazást üzemeltető OTP Mobil Kft.-től), és a feltört fiók jelszavát más szolgáltatásnál is alkalmazza, javasolt minden egyes ilyen szolgáltatásnál mielőbb lecserélnie a kiszivárgott jelszót, mert ezeket a fiókokat is támadás érheti.**

2. **A digitális felhasználói fiókok védelmében elengedhetetlen a szolgáltatásonként különböző, erős jelszavak használata. Az erős jelszó minimum 12 karakter hosszú, lehetőleg speciális karaktert (pl.: . # $) is tartalmaz. A témában ajánljuk az NBSZ NKI, „Kulcs a digitális élethez – a biztonságos jelszókezelésről” című tájékoztatóját, valamint a Kibertámadás! podcast adását, amelyben a jelszavak biztonságos tárolására adunk tanácsokat.**

3. **Ha egy szolgáltatás lehetőséget ad a többfaktoros hitelesítés használatára, azt javasolt aktiválni. (A Simple esetében bevezetés alatt áll a többtényezős hitelesítés.)**

4. **Mivel a támadók megszerezhették az érintett ügyfelek a SimplePay rendszerében regisztrált e-mail címeit, várhatóan meg fog szaporodni az ezekre érkező csaló, adathalász levelek száma, ezért az érintett fiókok tulajdonosainak javasolt fokozottan óvatosan kezelniük a hiperhivatkozást vagy csatolmányt tartalmazó üzeneteket.**
5. **A digitális csalásokról bővebb információért javasoljuk folyamatos tájékozódásra**
    - **a KiberPajzs együttműködés központi weboldalát: https://www.kiberpajzs.hu;**
    - **az NBSZ NKI weboldalát: https://nki.gov.hu;**
    - **valamint az NBSZ NKI Facebook oldalát: https://www.facebook.com/nki.gov.hu/.**

Nemzetbiztonsági Szakszolgálat
Nemzeti Kibervédelmi Intézet
Telefon: +36-1-336-4833
Incidensbejelentés: csirt@nki.gov.hu