Hogyan akadályoz meg egy fejlesztő 14 karakterrel egy hackertámadást

Egy öltés jókor, megkímél nyolctól

HARDCORE IT

Márk Módly

HARDCORE IT

“Elképzelt” eset

A nem beadott ellenben teljesült banki átutalás

HARDCORE IT

- Nevezzük főhősünk **Xavér**nak röviden **X**
- **X** problémába ütközik a netbankba belépés után
  - a gyakori kérdések linkre kattintva **felugró ablakban** megjelenik az információs oldal
  - hősünk sokáig böngészi a kérdéseket, végül sikerrel jár
  - **X** visszalép az oldalra, **bejelentkező form fogadja** őt
  - amikor **bejelentkezik** először **hibaüzenetet kap**
  - a második **bejelentkezés sikeres**
- Furcsálja **X** a helyzetet,
  nem szokta elrontani a jelszavát

- Következő héten **X** telefonhívást kap
  - az állam által előírt **adategyeztetést** nem teljesítette
  - telefonon most lehetőséget kap **ha azonosítja magát**
  - azért hogy a hívó is biztosítsa kilétét, a **bejegyzett telefonra SMS-t küldenek melyből a kódot vissza kell olvasni**
  - **ellenőriznie kell a küldőt,**
    mert jeleztek már visszaéléseket

- **X** ellenőrzi, hogy **tényleg a szokásos helyről jött SMS**
  - visszaolvassa a kódot, majd **eldöntendő kérdések**et kap, melyek **mind helyes**ek
    (lakhely, számlaszám etc)
  - záráshoz az új (jó számról érkezett) kódot is beolvassa **X**

Bankszámla egyenleg

0 HUF

Mi történt?

Banki ügyfélszolgálat

- Kedves **X** mi azt látjuk, hogy Ön
  - hiba nélkül bejelentkezett
  - átutalást kezdeményezett
  - megadta a jóváhagyáshoz szükséges kódot
  - **azonnali átutalás teljesült**
  - kilépett a netbankjából

Mi történt *valójában*?

- A gyakori kérdések oldal megfertőződött
- Amikor a netbankból odaérkezett **X** a fertőzött oldal **az eredeti netbank ablak oldaláról egy *phising* oldalra irányította őt**
  - Hogyan lehetséges ez?
- **A megjelenő bejelentkezés egy adatgyűjtő oldal volt csupán**
- Az adatok elmentése után vissza irányította a felhasználót a valódi oldalra
- **X** valóban be tudott jelentkezni az eredeti oldalon

- A csaló
  - előkészítette a mentett adatokat
  - telefonhívás (***vhising***) közben a **két faktoros azonosítás kódját bekérte X-től** (SMS-ben érkező kód)
  - a **netbankon található információkra megerősítést** kért
  - **átutalást indított** az elérhető vagyonnal
  - a **megerősítő kódot** lezárásként **beolvastatta**

Reverse Tabnabbing

- JavaScript API segítségével lehetőség van az új ablakot megnyitó ablakot manipulálni, ha nincs explicit tiltva

```
<script>
 if (window.opener) {
    window.opener.location =
      "https://phish.tld";
 }
</script>
```

Explicit tiltás

```
rel="noopener"
```

Tanulság

- JavaScript lehetőséget ad a megnyitó ablak módosítására
- Nem mindenhol a default a biztonságos
- A gyakori kérdések oldalának megtörése nem lett volna ekkora probléma, ha a megfelelő tudás rendelkezésre állt volna

Felhasználóként

Nem adunk ki magunkról
érzékeny információt!

Borzalmas szóvicc

HARDCORE IT

Mi az adathalász Out of Office üzenete?

Gone Phising!

Kérem, hogy legalább azt vigyük magunkkal az előadásból, hogy a **nagy problémákat** kis részek alkotják, amiket **odafigyeléssel már a fejlesztés közben meg lehet akadályozni!**

HARDCORE IT

Találkozzunk a 30-án kezdődő **fejlesztőknek szóló biztonságos szoftverfejlesztés oktatáson**

info@hardcoreit.com