Böngészőbiztonság 101 – avagy az információtolvajok babérkoszorúja

Kocsis Tamás – OSCP, OSWP, ISO 27001 LA, WTF, BGP, PING, DIR

2021.05.19

A probléma

- **A böngészők helytelen használata biztonsági kockázatot jelent**
  - Privacy sérülése (alacsony kockázat)
  - Malware fertőzés (magas kockázat)
  - Adatszivárgás (kritikus kockázat)

- **A vállalatok többnyire nem menedzselik központilag a böngészőket**

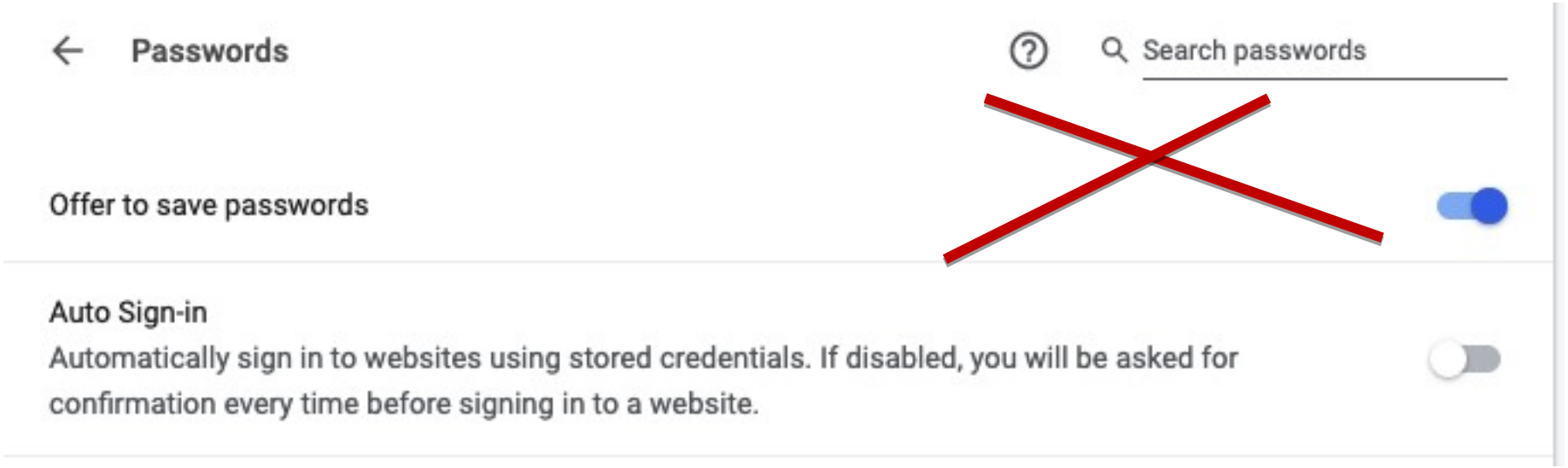
- **Nincs szabályozva a böngészőhasználat** (sem)

- **Többnyire a kockázatokkal sincsenek tisztában**

- **Jelszómentés a böngészőben (#1)**
  - Alapértelmezett, felajánlja, menti
  - Kiolvashatók a jelszavak
  - Helyi adatbázis (pl. Chrome – SQLite)
  - Elvileg titkosított (Windows CryptProtectData),
  - A gyakorlatban kiolvasható, visszaállítható

- **Kockázat**
  - Jogosulatlan hozzáférés és visszaállítás
  - Malware is képes kiolvasni, visszaállítani
  - Insecure jelszótárolás

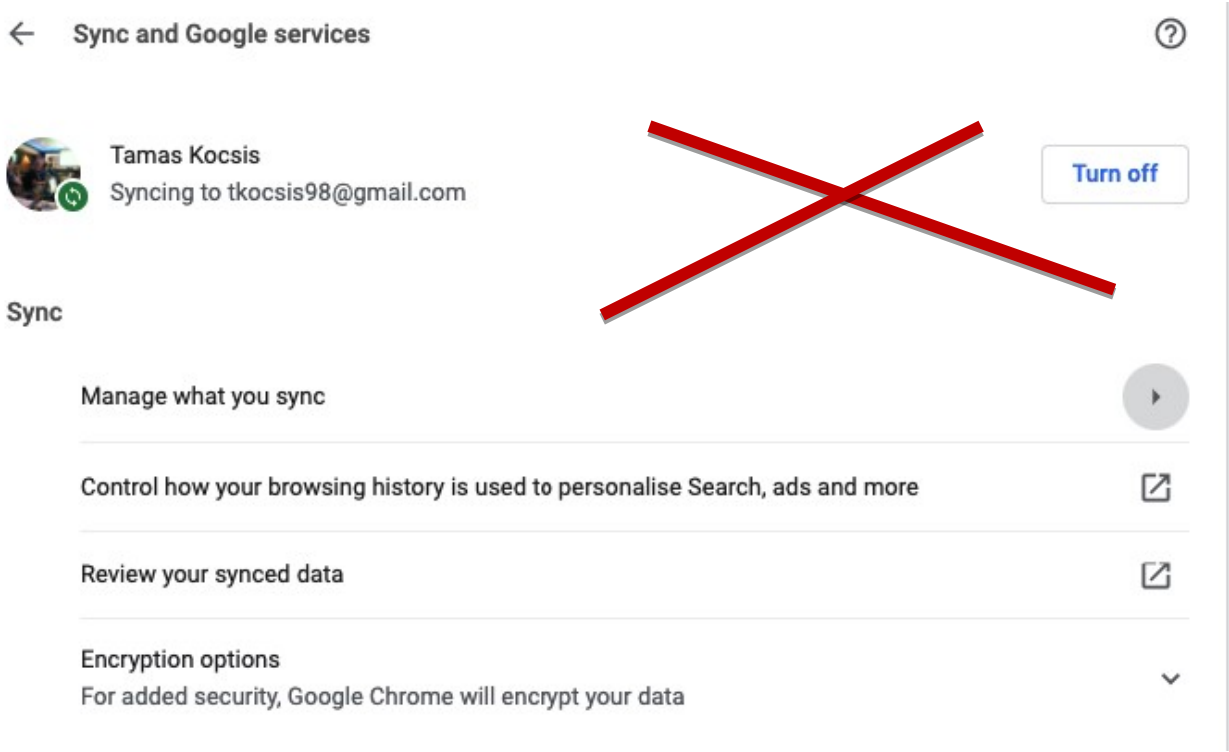
- **Jelszómentés a böngészőben (#1)**



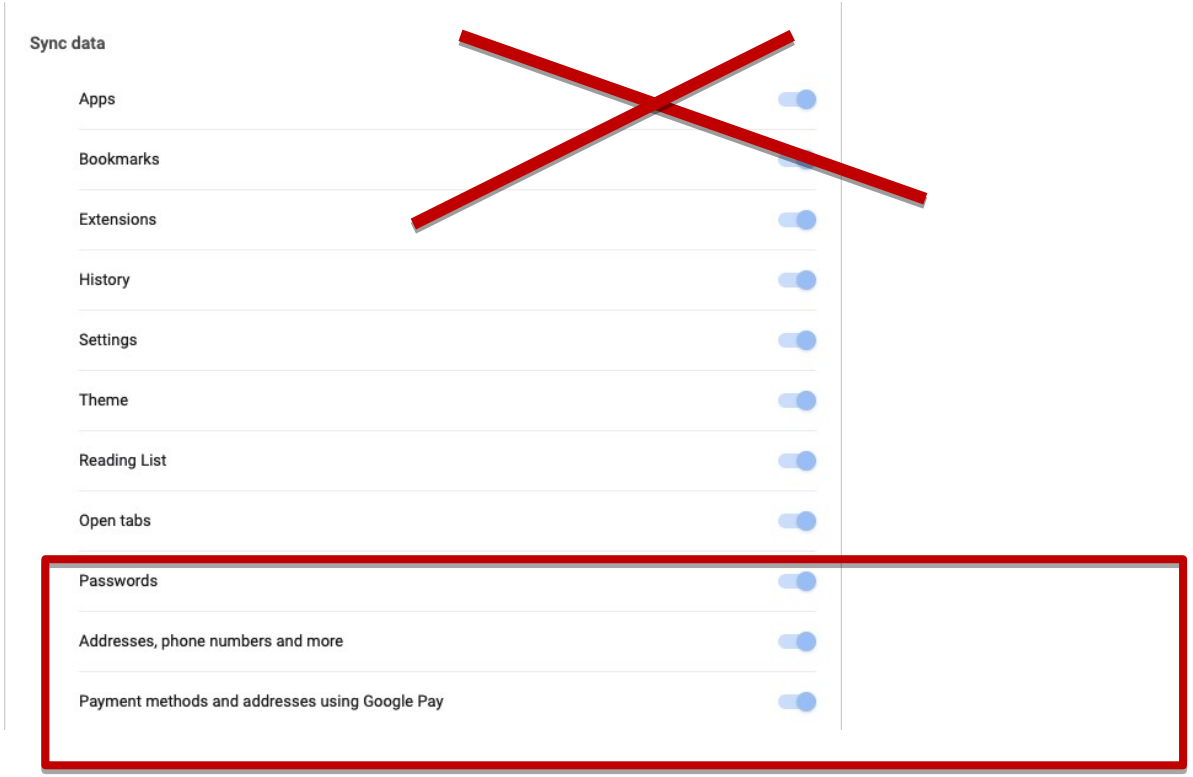
- **Böngésző szinkronizáció (#2)**
  - Alapértelmezett
  - A böngésző a felhőn keresztül (Chrome, Firefox) a szervezettől idegen eszközre szinkronizál (otthoni gép)
  - Mennek az elmentett adatok, jelszavak, bővítmények, sütik, stb.

- **Kockázat**
  - A munkahelyi eszközön elmentett webes alkalmazások jelszavai a szervezettől idegen és védtelen eszközökön is letárolásra kerülnek
  - Az otthoni vagy más idegen gép jogosulatlan hozzáférése vagy malware fertőzése a szervezet rendszereit komprommitálja

- **Böngésző szinkronizáció (#2)**



- **Böngésző szinkronizáció (#2)**



- **Böngésző bővítmények (#3)**
  - Többezer kártékony bővítmény...
  - A felhasználók szabadon telepíthetnek bővítményeket
  - A bővítmények (bár „sandboxban”), de a felhasználó jogosultságával működnek

- **Kockázat**
  - A kártékony böngésző bővítmények malware-jellegű tevékenysége konkrét adatlopást valósíthat meg
  - Sérülékennyé teheti a böngészőt (pl. weboldalakkal összejátszva)
  - Backdoor

- **Böngésző bővítmények (#3)**

Four Malicious Google Chrome Extensions Affect 500K Users

ICEBRG Security Research team's finding highlights an often-overlooked threat.

The ICEBRG Security Research team discovered four malicious Google Chrome extensions during a routine investigation of anomalous traffic. More than 500,000 users, including workstations in major businesses around the world, have been affected.

Home > News > Security > Privacy > Smartphones > Android

Nearly 80 Chrome extensions caught spying -- how to protect yourself

By Nicholas Fearn 11 months ago

79 malicious browser extensions booted by Google from the Chrome Web Store

https://threatpost.com › Web Security

Google Yanks 106 'Malicious' Chrome Extensions | Threatpost

Jun 18, 2020 — Trojan **Chrome browser extensions** spied on users and maintained a foothold on the ... June 18, **2020** 4:49 pm ... While Google has long policed its **Chrome** Web Store for **rogue browser extensions**, what is unique about this ...

https://nakedsecurity.sophos.com › 2019/01/22 › rogue...

Rogue websites can turn vulnerable browser extensions into ...

Jan 22, 2019 — It's a blind spot: we might know that app permissions can be risky but when it comes to **extensions** for **browsers** such as **Chrome** and **Firefox** there ...

https://www.zdnet.com › Topic › Security

Three million users installed 28 malicious Chrome or Edge ...

Dec 17, 2020 — Below is the **list** of **Chrome extensions** that Avast said it found to contain **malicious** code: Direct Message for Instagram. DM for Instagram. Invisible mode for Instagram Direct Message. Downloader for Instagram. App Phone for Instagram. Stories for Instagram. Universal Video Downloader. Video Downloader for FaceBook™

- **Nézzünk konkrét példát**

  - Ügyfélkapu és gov.hu web alkalmazások
  - Rengeteg felhasználó (állampolgárok)
  - Jelszómentés, szinkronizáció
  - Malware fertőzés, a malware ellopta az adatokat

Több mint 20 ezer magyar állampolgár Ügyfélkapus és más, gov.hu webalkalmazás hitelesítési adatai kompromittálódtak...

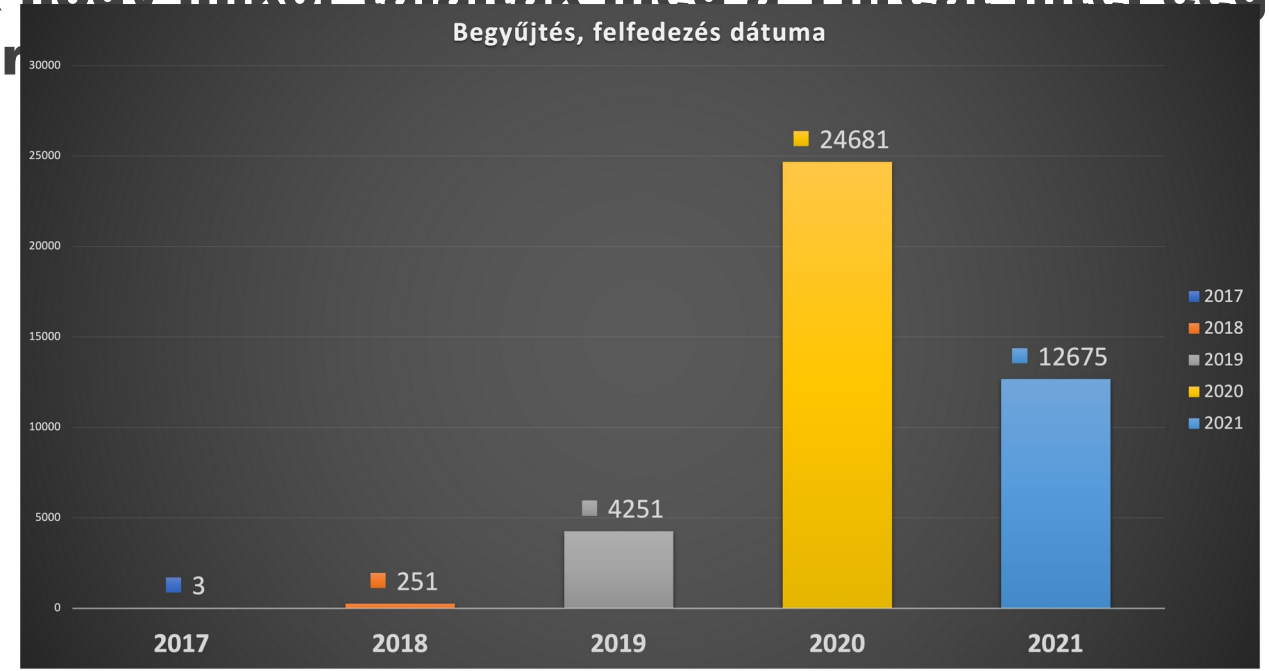
Egy patkó miatt...

- **41 ezer gov.hu breach rekord**
- **Több mint 20 ezer egyedi felhasználó**

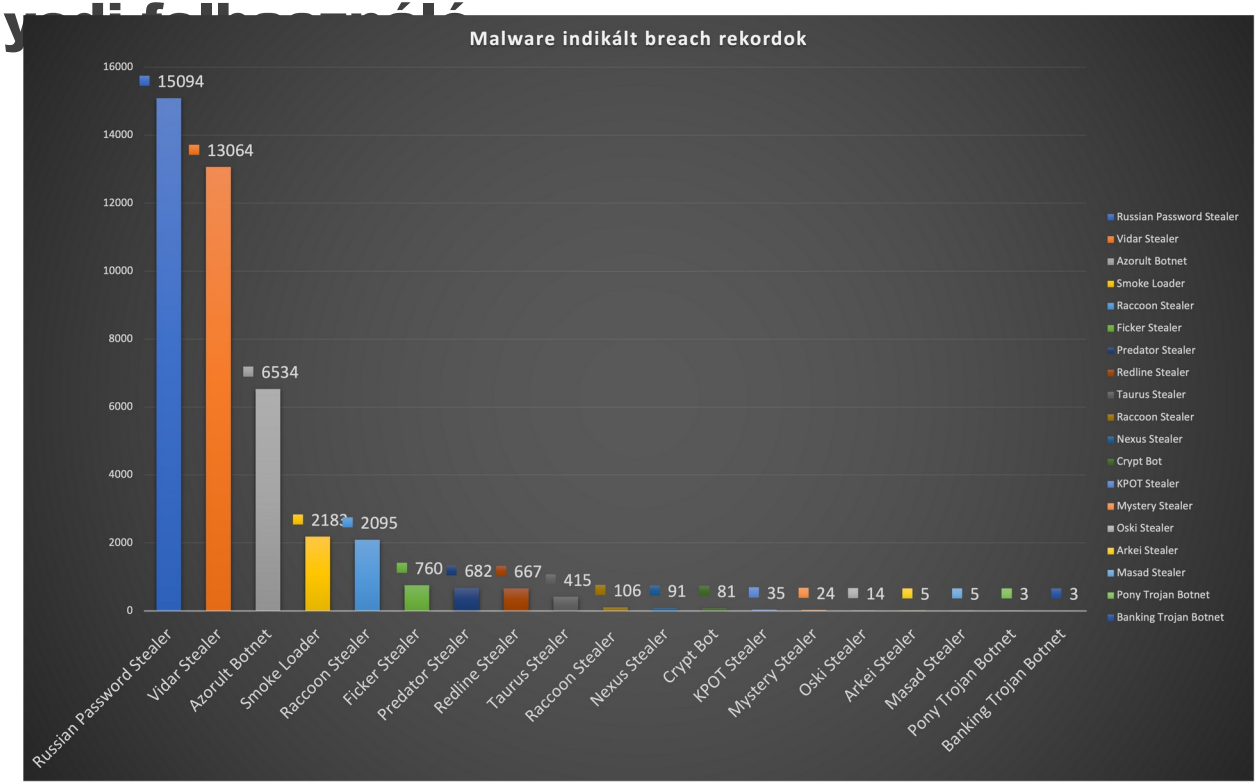
Breach Title	Username	Password	Target Domain	Severity
Azorult Botnet	szeles[redacted]	********	gov.hu	Critical
Redline Stealer	jord[redacted]	********	gov.hu	Critical
Redline Stealer	peter.[redacted]	********	gov.hu	Critical
Redline Stealer	szerencses[redacted]	********	gov.hu	Critical
Redline Stealer	meze[redacted]	********	gov.hu	Critical
Redline Stealer	[redacted]ton	********	gov.hu	Critical
Redline Stealer	kopasz[redacted]	********	gov.hu	Critical
Redline Stealer	tejfel[redacted]	********	gov.hu	Critical
Redline Stealer	lukacs[redacted]	********	gov.hu	Critical
Redline Stealer	[redacted]ngt	********	gov.hu	Critical

Showing 1 to 10 of 41,861 entries

- **Nem tudni pontosan mikor történtek a fertőzések és szivárgások**
- **Csak hogy mikor találták meg a Threat Intel cégek (kiber**



- **Egy kis statisztika – 41 ezer breach rekord, 20 ezer egyedi felhasználó**



- **Védekezés, javaslatok vállalatoknak**
  - **Központi böngészőmenedzsment!**
  - Chrome, Edge, IE, Firefox menedzselhető az Active Directory-ból
  - Minimum jelszómentés és szinkronizáció tiltása
  - Központi bővítménykezelés, engedélyezett bővítmények
  - Bővítmények tiltása

- **Védekezés, javaslatok vállalatoknak**

  - **Böngészőaudit + központi menedzsment + hardening**

  - Segédletek, hardening guideok

    - ❖ CIS Chrome Benchmark
    - ❖ CIS Mozilla Firefox Benchmarks
    - ❖ CIS Microsoft Internet Explorer Benchmarks
    - ❖ Security Baseline for Microsoft Edge
    - ❖ Chrome Browser Enterprise Security Configuration Guide

- **Köszönöm a figyelmet!**
- tamas.kocsis@alverad.hu
- www.alverad.hu

Kérdések?