

Feltörték az oldalt

Szerző Admin
2011. október 25.

Sajnos ez is megtörtént.

Mint azt az elmúlt napokban tapasztalhattátok, az oldal nem volt elérhető.

Árme a magyarírat:

Múlt hét csütörtökén jött az első telefon, hogy az oldal (akkor még csak a fórum) megjelenésekor támadást jeleztek egyes vendégszoftverek.

Aznap már nem volt időm foglalkozni vele, de a fórum gyorsan le lett tiltva, ne okozzon gondot annak akinek nincs vendégszoftvere a rendszerében.

Fontos napra már a weboldal is fertőzött lett, így nem volt mit tenni azt is be kellett zárnunk.

Érdekesen telt a hétvégem.

Főtt a fejem rendesen.

A legnagyobb gondot az jelentette - és jelenti még most is - hogy a sajájt, programozásra használt gépem olyan szinten fertőzött, hogy még most sem sikerült letakarítani. Pedig fut rajta a NOD32, automatikusan frissített adatbázissal. Fut rajta tűzfal, telepítve van a SpyBot SD.

És mégis benyalta rendesen.

A támadás szelével kapcsolatban a következők derültek ki:

Vendégszoftverek, amik nem okoztak a támadást:

- AVG kártyánbázis
- Vipre
- NOD32

Vendégszoftverek, amik részben okoztak a támadást:

- Avast (XP-n jelzi a támadást, Windows7-en nem!)

Vendégszoftverek, amik okoztak a támadást:

- Eset Smart Security 5 (Windows7-en, és Vista-n is jelez. XP-n nem lett tesztelve)
- Eset Smart Security 4 (Windows7-en lett tesztelve)

A fenti szoftverek is csak a friss adatbázis esetén jelzik a támadást, ezért fontos, hogy mindenki figyeljen oda a frissítésre!

(A Smart Sec. 5-ös próbaverziója szeptemberi adatbázissal települ, és az még nem reagál a támadásra!!!)

Á

A fentiek miatt XP-s rendszerekre az Avast telepítését javaslom (ingyenes regisztráció után 1 évig frissít legálisan), jobb rendszerekre az Eset szoftvere lehet megoldás.

Mindenki gégezen egy teljes rendszerellenőrzést a gépén, és változtassa meg a weblapon a jelszavát!!! (felhasználói adataim másolására)

A vizsgálathoz megoldás még az Eset Online Scanner használata is (beírni a Google-ba, és megtalálod ;). Akár a megvédő víruskezelő ellenőrzésére is (sajnos saját tapasztalat alapján a rootkit-eket nem találja).

A weblapon a galéria és a fórum még nem működik, dolgozok rajta.

Ha a fentiekben valamilyen problémát tapasztaltok, akkor azt a klubos e-mail címemen (klub.lacetti@gmail.com) jelezzétek.