

FONTOS VÁLTOZÁS AZ FTP ELÉRÉSEKBEN

Megállj a jelszó lopásoknak!

Sajnos az elmúlt hónapokban egyre gyakoribb jelenséggé vált, hogy valamilyen kártékony program (vírus, spyware, malware stb.) a felhasználók FTP kliensén keresztül megszerzi az ftp felhasználónév / jelszó adatokat és elküldi azokat készítőjének. A honlap tulajdonosoknak ezzel jelentős kárt és bosszúságot okozhatnak, mert a megszerzett adatokkal elérik a weblap tartalmát képező állományokat és átírják azokat. Leggyakrabban olyan programkódot helyeznek el a honlap forrásában, amely a honlap megtekintésekor a látogató gépére egy távoli szerverről letölt valamilyen kártékony programot, amelyen keresztül a "támadók" a későbbiekben adatokat (pl. elmentett FTP jelszavakat) szerezhetnek meg a megfertőzött gépről, vagy más illegális célra (pl. spam küldésre) használhatják.

Az ilyen jellegű támadások esetén nem a weboldal fertőződik meg elsődlegesen, hanem a weboldalhoz hozzáféréssel rendelkező ügyfél számítógépe. Mivel az FTP kódolatlan csatornán kommunikál, ezért bejelentkezés közben az ügyfélgépen lévő vírus naplózza a bejelentkezési azonosítót és jelszót, majd ezt elküldi egy ismeretlen helyre. Pár nappal ezután általában megtörténik a tárhely feltörése, külföldi (többnyire orosz, brazil, japán) szerverekről módosítják a weboldal index és egyéb fájljait. Fontos tudni, hogy a weblap módosítását nem a fertőzött ügyfél-számítógép végzi, hanem mindig egy harmadik (külföldi) szerver.

Ez a jelenség sajnos a tárhelyszolgáltató részéről közvetlen módszerekkel nem kezelhető, hiszen a jelszó ellopása és felhasználása nem a szolgáltató szerverein és hálózatában történik. A probléma ellen a legjobb védekezés a jogtisztta, rendszeresen frissített operációs rendszer, és korszerű vírusvédelem használata.

Cégünk hatékony megoldást dolgozott ki az ilyen támadások megakadályozása érdekében. A szerveroldali védekezés lényege, hogy bár a jelszó ellopását nem tudjuk megakadályozni, a bejelentkezés ismeretlen IP tartományokból korlátozható. Így a külföldi (ismeretlen tartományból származó) szerverekről érkező FTP betörési kísérlet kockázata minimalizálható. Ha ez a beállítás Önnek nem felel meg, például nem .hu tartományból internetezik, vagy szeretne szigorítani a beállításokon akkor ezt írásban kérheti (levél, fax, email) az Ügyfélszolgálatunknál. A fenti intézkedéseket az indokolja, hogy a jelszólopó vírus bejelentkezése a tárhelyre jelenleg többségében külföldi szerverekről történik. Ezzel az intézkedéssel az ilyen jellegű betörési kísérlet nagymértékben gátolható.

Lehetőség szerint használja a csatlakozáshoz az FTP over SSL (ftps) üzemmódot, mert ekkor az adatok titkosított csatornán haladnak a szerverhez.

Amennyiben FTP jelszavait már megszerezték, és átírták a honlapját, kérjük az alábbi lépéseket tegye meg a javításhoz

Elhárítás, megelőzés:

1. Szüntesse meg a számítógépe internet kapcsolatát (UTP kábel kihúzása).
2. Ajánlott, hogy ezután törölje a nagy cache állományokat (pl.: Temporary Internet Files).
3. Végezzen a számítógépén teljeskörű vírus-, spyware-, malware stb. kártékony program ellenőrzést és irtást.
4. **Kérje a tárhelyhez tartozó jelszó módosítását.**
5. Törölje a fertőzött fájlokat a webszerverünkről.
6. Az érintett állományokat egy korábbi mentésből töltsse fel a webszerverre.
7. A továbbiakban szíveskedjen biztosítani számítógépe folyamatos védelmét a kártékony programoktól.
8. Ha tudomása van más olyan számítógépről, melyen ezt az ftp kapcsolatot létesítették vagy el vannak mentve ennek az ftp kapcsolódásnak az adatai, akkor végeztesse azon a gépen is vírus/spyware/malware irtást.
9. Ellenőrizze, hogy az operációs rendszerére, és a használt programokra (pl. MS Office) telepítve vannak-e az aktuális frissítések, és a rendszeres frissítés be van-e kapcsolva.
10. Ellenőrizze, hogy be van-e kapcsolva a számítógépén a tűzfal, és a "víruspajzs" alkalmazás, és ezek rendszeresen frissülnek-e.
11. ***Bármilyen módosítás után, vagy rendszeresen készítsen biztonsági másolatot a honlap fájljairól, amelyet nem a szerveren tárol, és amelyből bármikor vissza tudja állítani a "fertőzés" előtti állapotot.***
12. Az FTP kliensben (különösen ha Total Commandert használ) lehetőség szerint soha ne mentse el a felhasználóneveket, jelszavakat.
13. ***Biztonságosabb, SSL-izált FTP kapcsolaton keresztül csatlakozzon a szerverhez (ftps kapcsolat)***

Székesfehérvár, 2009. augusztus 1.