Tisztelt Partnerünk!

Ezúton tájékoztatjuk, hogy a Griffsoft Informatikai Zrt. informatikai rendszere 2021. november 9-én a hajnali órákban kifinomult kiberfegyverrel elkövetett támadás áldozata lett. Ennek egyik első lépéseként a támadók létrehoztak adminisztrátor felhasználót, amellyel képesek voltak

- a meglévő vírusmegoldásunkat deaktiválni a fertőzéshez,
- a szervereken a virtuális környezeteket leállítani és magát a teljes virtuális gépet elkódolni.

A behatolás során találtunk olyan felhasznált fájlokat is, amelyeket a víruskeresőnk nem ismert fel első körben, ezeket beküldtük további ellenőrzésre az ESET-nek.
A támadás zsarolóvírus (ransomware) telepítése érdekében történt, és az eddig lefolytatott vizsgálatok arra engednek következtetni, hogy levelezőrendszer sérülékenységét használták ki a támadók a bejutáshoz.

Az eddigi elemzések alapján azt állapítottuk meg, hogy a támadás a belső rendszer ellen irányult, nem tudunk adatszivárgásról, adatlopásról. Nem láthatók olyan nyomok sem, amelyek alapján arra következtethetnénk, hogy rajtunk keresztül másokat támadtak volna meg vagy a vírus tovább terjedt volna. A kibertámadás legjobb tudomásunk szerint csak cégünk rendszereiben okozott károkat.

Az észlelést követően azonnal megkezdtük a teljes rendszer izolálását, a gépeket és szervereket kikapcsoltuk, a hálózati és internet kapcsolatainkat megszűntettük. A rendszer vizsgálatában és biztonságos módon történő újraindításában és -építésében külsős IT biztonsági cég, a White Hat IT Security Kft. szakemberei segítségét kértük. A White Hat IT Security Magyarország egyik legnagyobb incidens-reagálási kapacitásával rendelkező kiberbiztonsági cég, amelynek szenior szakemberei mindegyike magyar Szigorúan Titkos! és EU-NATO Titkos! személyi biztonsági tanúsítvánnyal rendelkezik. A céget a NISZ Zrt. is megfelelően magas szakmai színvonalú külsős szakértőként jegyzi.

Az érintett gépek átvizsgálása offline és online módon is megtörtént, több egymástól független megoldással, amelyben a saját csapatunk és a külsős szakértők egyaránt részt vettek. A forráskódok és az Ügyfélkapun publikált binárisok sértetlenségének vizsgálatát több módszerrel, szintén saját erőforrással, a külsős szakértők által auditált folyamat során elvégeztük, annak érdekében, hogy ügyfeleinkhez sem rosszindulatú kód, sem a támadók által esetlegesen módosított kódrészlet ne kerülhessen ily módon.

A megtisztított, szükséges mértékben újratelepített és biztonsági műveleti központban folyamatosan felügyelt rendszer és az auditált forráskód-vizsgálat eredménye 2021.11.19-én pénteken bemutatásra került a NISZ Zrt. biztonsági csapatának, akik ez alapján a rendszer és az eszközökön történő fejlesztések felhasználók rendszereibe történő visszaengedését biztonságosnak minősítették.

Az esetleges kellemetlenségekért elnézésüket kérjük! Továbbra is megteszünk mindent az Önök rendszereinek hibamentes működtetése érdekében.

Budapest, 2021. november 22.

Tisztelettel:

Ferenczy Imre
GriffSoft Informatikai Zrt.
vezérigazgató

GriffSoft Informatikai Zrt.
1041 Budapest, Görgey Artúr u. 69-71.
Adószám: 12573936-2-41
Cégj.sz.: 01-10-049196
12

GriffSoft Informatikai Zrt.
1041 Budapest, Görgey Artúr utca 69-71.
Telefon: +36-1/450-2200, +36-62/549-100
Fax: +36-1/239-0056, +36-62/401-417
E-mail: info@griffsoft.hu, ugyfelszolgalat@griffsoft.hu
Web: www.griffsoft.hu