ECHO

www.echonetwork.eu

A COVID-19 járványhoz kapcsolódó hacker-gondolkodásmód

ECHO FEHÉR KÖNYV #1

ISSUED: 2020 ÁPRILIS 8.

Funded by the European Union's Horizon 2020
Research and Innovation Programme, under Grant Agreement №830934

Absztrakt

Figyelemmel kísérve a kiberbiztonsági környezetet és a COVID-19 járvány következtében a kiberbiztonsági szakértők és a bűnüldöző szervek által világszerte jelentett növekvő kiberbűnözési eseteket, az ECHO kiberbiztonsági központ hálózata egyesítette erőit a COVID-19 kibervédelmi szövetség létrehozásának érdekében. Célja minden olyan kezdeményezés támogatása, amely az EU tagállamainak, a kulcsfontosságú szolgáltatásoknak és a kritikus infrastruktúráknak a számítógépes támadásokkal szembeni védelmét szolgálja.

Innovatív ötletekkel, gyakorlati útmutatásokkal és megoldási lehetőségek kidolgozásával az ECHO hozzájárul a COVID-19 kiberbiztonsági fenyegetettségek megelőzéséhez és az Európai Unió, a tagállamok vállalkozásai, valamint az állampolgárok kiberbiztonságának megerősítéséhez.

Ez a fehér könyvből készült kivonat az első eredménye annak az együttes erőfeszítésnek, amely elsősorban a hackerek COVID-19 járvánnyal kapcsolatos gondolkodásmódját mutatja be.

2020. április 6-án 15 tagállam ECHO szakértőinek két csoportja online hackathon keretében megvizsgálta a hackerek gondolkodásmódját a COVID-19 járvány szemszögéből. A fő következtetésük az, hogy ez a világjárvány egyedülálló lehetőségeket kínál a kiber bűnözők számára a meglévő támadási technikák kiaknázására. Ezeknek az a célja, hogy visszaéljenek az otthonról dolgozó munkavállalók és diákok - saját megosztott eszközeik nem biztonságos használatából adódó - sérülékenységével.
Függetlenül a hackerek motivációjától (profitszerzés vagy társadalmi zavarkeltés) a bűncselekmények sikeres lebonyolításához ma már rengeteg lehetőség és módszer áll rendelkezésre a COVID-19 világjárvány következtében.

Kulcsszavak: kiberbiztonság, COVID-19, támadási mutatók, támadók profiljai, keresztirányú kérdések, enyhítő intézkedések.

Fő megállapítások

Általános észrevételek

Az ECHO szakértőinek általános következtetése az, hogy jelenleg a hackerek által alkalmazott megközelítések és eszközök nagyrészt megegyeznek a korábbiakkal. Két különbség fedezhető fel (van azonban); egyrészt, (először is) a hirtelen áttérés az online munkavégzésre és az online oktatásra, amellyel könnyen a hackerek célpontjává válunk, másrészt, (másodszor) a hackerek most kihasználják az emberek sebezhetőségét, amely nagyobb, mint korábban. Félünk attól, hogy megbetegszünk, aggódunk a családunk és a barátaink miatt, és sok időnk van arra, hogy az Interneten információk után kutassunk a világjárványról. Ez az aggodalom, az elkeseredettség és az (észlelt) információhiány befolyásolhatja az óvatosságunkat, például ha egy linkre kattintunk, letöltünk egy fájlt, telepítünk egy alkalmazást, vagy személyes adatokat adunk meg egy weboldalon. Hajlamosak vagyunk elfogadni a magasabb számítógépes kockázatot a COVID-19 világjárvány miatt, ezért kiszolgáltatottabbá válunk, amelyet a hackerek azonnal kihasználnak.

A támadók jellemzői

A potenciális fenyegetés szereplőinek három profilja azonosítható: a hacker bűnözők, a hacktivisták, és az állam által támogatott hackerek csoportja. A terrorista hacker a hacktivista vagy az állami hacker altípusokba tartozik.

A hacker bűnözők fő célja különféle formákban a profitszerzés: közvetlenül fizetett bitcoin, vagy pl.: a nemzeti vámügyi adatbázisokhoz való hozzáférés. A COVID-19 világjárvány eredményeként az online munkavégzés és tanulásra való

Funded by the European Union's Horizon 2020
Research and Innovation Programme, under Grant Agreement №830934

átállás a hacker bűnözők számára új lehetőségeket kínál a személyes, valamint a kis-, közép- és nagyvállalati hálózatok megtámadására.

A hactivista aggódik a kormányzat társadalom feletti hatalomgyakorlásának magasabb szintje miatt, a COVID-19 világjárvány terjedésének megakadályozására hozott intézkedések következtében. Ezt a lakosság feletti hatalom megszerzésének, illetve összeesküvésnek tekinti. A hactivista tevékenységének az a célja, hogy zavart okozzon a világjárvány közepette.

A (nemzet)állam által támogatott hackerek csoportjának érdeke egy másik (nemzet)állam működésének megzavarása, pl.: téves információk terjesztésével, így befolyásolva a polgárok és a nemzeti, valamint a nemzetek feletti kormányzati intézményekbe vetett bizalmat. A COVID járvány során kulcsfontosságú a polgárok és a hatóságok közötti bizalom megtartása a hatékony válságkezelés és a járvány lecsengése utáni gyors helyreállás érdekében. A téves információk terjedése lelassíthatja ezt a folyamatot, és akár a geopolitikai szövetségeket is befolyásolhatja. A nemzetállami hacker-csoportok szándékosan célozhatják meg a létfontosságú szolgáltatásokat is, hogy további káoszt és félelmet okozzanak a világjárvány közepette pl.: kórházakban vagy logisztikai ellátási láncokban. Előfordulhat, hogy beavatkoznak a kritikus infrastruktúrákba vagy kormányzati hálózatokba, későbbi felhasználás/profitszerzés/visszaélés céljából.

A támadások módja

Számos támadási vektort tárgyaltunk a hackerek különböző profiljával együtt.

- **E-mail**
- **SMS / WhatsApp üzenetek**
- **Távoli hozzáférés és saját eszköz használata során történő támadás**
- **Távoli hozzáférés és a kritikus infrastruktúrák szolgáltatóit érő támadás**
- **Orvosi eszközök használata során történő támadás**
- **COVID-19 mobil alkalmazások**

Transzverzális vagy ágazatközi felvetések

A transzverzális, illetve ágazatközi kérdéseket illetően megállapítottuk, hogy társadalmunk nagyban támaszkodik az alapvető ellátások (élelmiszer, közművek, orvosi ellátás, stb.) logisztikájára. Egy kikötő vagy repülőtér logisztikájának támadása azzal a céllal, hogy a rendszereket megsemmisítse zsarolóvírus vagy bármilyen más beavatkozás útján, potenciális célpont lehet a nemzetállami hackerek számára a káosz kialakításához.

Enyhítő intézkedések

Fontos a specifikus és könnyen megosztható üzenetek terjesztése, amelyek elmagyarázzák, hogy a hackerek hogyan tudják kihasználni a COVID-19 járványt. Az ECHO hálózat COVID-19 Kibervédelmi Szövetsége széles körű online kampányt indított ezekkel a lehetséges eszközökkel, hogy felhívja az állampolgárok figyelmét a kockázatokra.

Funded by the European Union's Horizon 2020
Research and Innovation Programme, under Grant Agreement №830934

Megelőzés szempontjából is fontos a COVID-19-specifikus korai figyelmeztető rendszerek (Early Warning Systems) fejlesztésének gyorsítása, hogy az állami, magán- és nem kormányzati szervezetek is biztonságosan megoszthassák egymással információikat.

Az ECHO projekt célja, hogy kifejlesszen egy rendszert tekintettel a COVID-19 kapcsán megjelenő kiber fenyegetésekre, amelynek béta verziója hamarosan tesztelésre kerül.

Konklúzió

Legfőbb megállapításunk, hogy a COVID-19 világjárvány egyedülálló lehetőségeket kínál a kiber bűnözők számára, a meglévő támadási technikák kiaknázására. Ezeknek célja, hogy visszaéljenek az otthonról dolgozó munkavállalók és diákok - saját megosztott eszközeik nem biztonságos használatából adódó - sérülékenységével.

Fontos most cselekednünk, hogy megakadályozzuk a digitális társadalom és az infrastruktúra rövid és középtávú sérülését.

A sokrétű, páneurópai kiberbiztonsági ECHO-hálózat továbbra is innovatív ötleteket, gyakorlati útmutatásokat és megoldásokat szándékozik kidolgozni a COVID-19 általi kiberbiztonsági fenyegetések kezelésére.

Ha további hasznos tanácsokat szeretne kapni, vagy érdekli az ECHO projekt és csatlakozna hálózatunkhoz, kérjük, vegye fel velünk a kapcsolatot: info@echonetwork.eu, vagy látogasson el weboldalunkra: https://echonetwork.eu/

A fehér könyv eredeti verziója honlapunkon található:

https://echonetwork.eu/wp-content/uploads/2020/04/20200408-ECHO-WhitePaper-Hackers-Mindset-FINAL.pdf

Funded by the European Union's Horizon 2020
Research and Innovation Programme, under Grant Agreement №830934