

IT BIZTONSÁG

4. forduló



A kategória támogatója: EURO ONE
Számítástechnikai Zrt.

Ismertető a feladathoz

A 4. forduló után elérhetőek lesznek a helyezések %-os formában: azaz kiderül, hogy a kategóriában a versenyzők TOP 20% - 40% -60% -ához tartozol-e!

Szeretnénk rá felhívni figyelmedet, hogy a játék nem Forma-1-es verseny! Ha a gyorsaságod miatt kilököd a rendesen haladó versenyzőket, kizárást vonhat maga után!

Kártékony kód visszafejtés

Ajánlott programok: Windows, [VSCode](#) vagy hasonló kódszerkesztő

Felhasznált idő: 00:00/40:00

Elért pontszám: 0/23

Indítás utáni csatolmányok

1. feladat 0/0 pont

A céges levélszűrőn fennakadt egy érdekes levél, ami egy gyanús csatolmányt tartalmaz. A feladat kielemezni ezt a csatolmányt, és megállapítani, hogy mit csinál.

Miért van ISO fájlba becsomagolva?

Válasz

- ☐ Megnehezíti a visszafejtést
- ☐ Jobban tömörül így a csatolmány
- ☒ Elkerüli ezzel az "internetről letöltött" jelzést
Ez a válasz helyes, de nem jelölted meg.
- ☐ Nincs rá különösebb indok

Magyarázat

Kedves Versenyzők!

A feladatot 0 pontosra állítottuk:

Habár a feladat írásakor ez még így volt, legfrissebb Windows rendszeren a helyesnek jelölt állítás már nem igaz.

Köszönjük megértéseket!

(2022.11.11.)

Elkerüli ezzel az "internetről letöltött" jelzést: Windows esetében az internetről letöltött fájlok kapnak egy speciális attribútumot, így az operációs rendszer képes korlátozni a működését (például Office fájlok esetén védett nézetet alkalmaz, vagy exe futtatása előtt figyelmezteti a felhasználót). Azáltal, hogy a vírus egy ISO-ba van csomagolva, a benne lévő fájlok nem kapják meg ugyanezt a jelölést, ezzel megkerülve egy védelmi mechanizmust.

2. feladat 0/3 pont

Hogyan indul el a kártékony kód?

Válasz

- ☐ Az ISO csatolásakor automatikusan lefut a vírus
- ☒ A "Csatolmányok" mappa megnyitásakor indul el a vírus
Ez a válasz helyes, de nem jelölted meg.
- ☐ Nem tartalmaz vírust ez a fájl

Magyarázat

A "mappa" valójában egy parancsikont, ami elindítja a vírus fájlt.

3. feladat 0/4 pont

Melyek a kártékony kód futásának lépései?

Válasz

- ☒ cmd.exe -> powershell -> Javascript
Ez a válasz helyes, de nem jelölted meg.
- ☐ cmd.exe -> powershell
- ☐ powershell -> cmd.exe -> VBScript
- ☐ powershell -> cmd.exe

Magyarázat

A parancsikont elindítja a cmd.exe-t, ami ezután meghívja a powershell-t egy speciális paranccsal, hogy rejtett maradjon az ablak. A powershell ezután csript segítségével futtat egy Javascript fájlt (pontosabban JScript fut le, ami ugyanúgy Javascript).

4. feladat 0/6 pont

Mivel kommunikál a kártékony kód?

Válasz

- ☐ Google szerverekkel
- ☒ Localhost-tal
Ez a válasz helyes, de nem jelölted meg.
- ☐ Észak-Koreával
- ☐ A vírus nem próbál meg sehova se kapcsolódni

Magyarázat

Localhost (127.0.0.1), erre próbál meg elküldeni egy kérést.

Ez a cím a "rick" nevű tömbben található, hexadecimálisan kódolva.

5. feladat 0/8 pont

A kártékony kód futása során milyen egyedi azonosítót szerez meg a gépről?

Válasz

- ☒ MAC cím
Ez a válasz helyes, de nem jelölted meg.
- ☐ Windows UUID
- ☐ Felhasználónév
- ☐ Windows licenc kulcs

Magyarázat

A "rick" nevű tömbben található a "MACAddress" változó, ami erre utal. Valamint az alábbi szöveg található még meg:

Select * from Win32_NetworkAdapter where physicaladapter=true

Ez egy WMI parancs, amivel le lehet kérdezni a számítógépen található hálózati adaptereket.

6. feladat 0/2 pont

Ez a legjobb módja a számítógép egyedi azonosításának?

Válasz

- ☐ igen
- ☒ nem
Ez a válasz helyes, de nem jelölted meg.

Magyarázat

Nem. Egy számítógépnek több MAC címe is lehet, és a MAC cím nem biztos, hogy valódi hálózati kártyához tartozik, valamint szoftveres és hardveres változtatások miatt könnyedén megváltozhat ez az érték.



[Legfontosabb tudnivalók](#)  [Kapcsolat](#)  [Versenyszabályzat](#)  [Adatvédelem](#) 

© 2023 Human Priority Kft.

KÉSZÍTETTE 

Megjelenés

 Világos 