Infokommunikáció 2023

Az egyes hacker generációk támadási szokásai és aktuális támadási trendek fejlődése a 2000-es évektől napjainkig

Busa Attila József
MH KIMK, Képzési- és Gyakorlattámogató Osztály,
Kiber Képzési Alosztály
kibervédelmi tanácsos

BRU Infosec Kft.
alapító tag, ügyvezető

Óbudai Egyetem, Biztonságtudományi Doktori Iskola,
1.éves doktorandusz hallgató

2023.11.20.

Vázlat

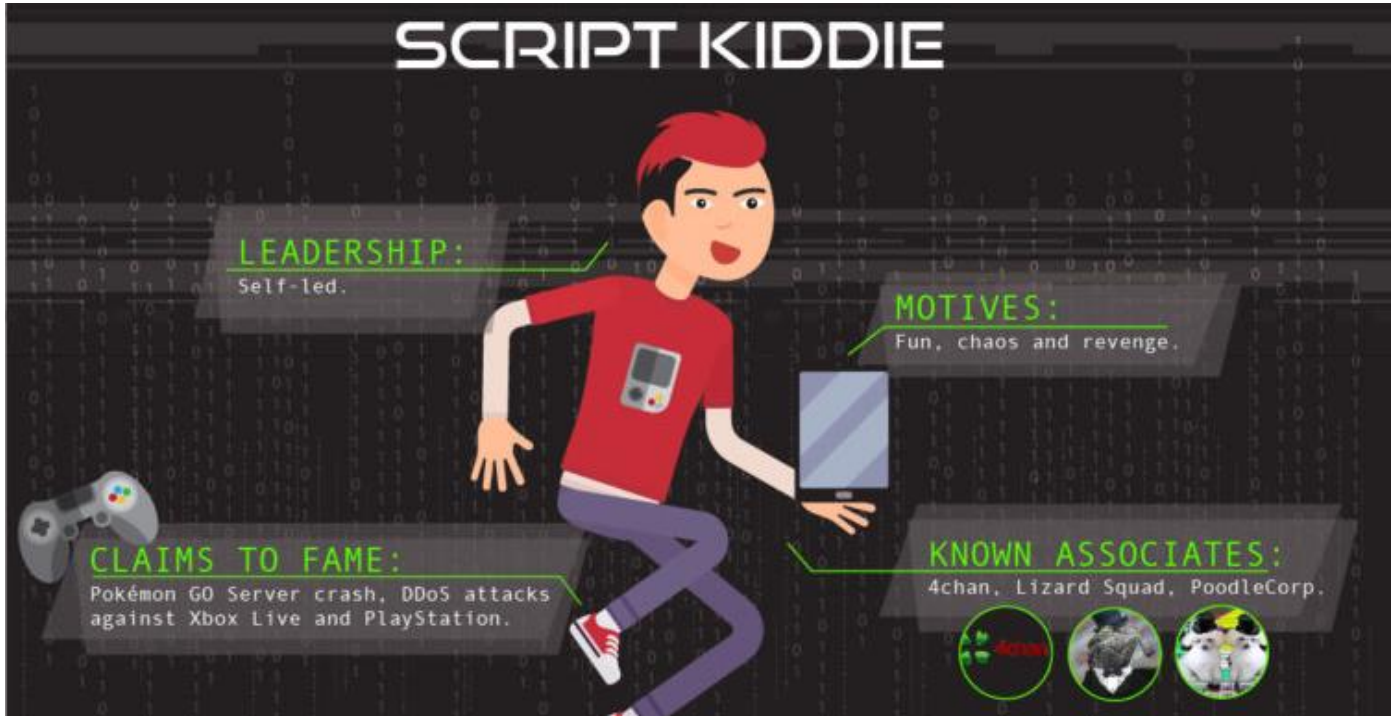
- hacker generációk fejlődésének bemutatása;
- a kialakult kibertámadási lánc;
- ajánlott védekezési javaslatok;
- összegzés;
- kérdések / válaszok

1. Generáció avagy a „hackerek” megjelenése

A 2000-es évek elején a közhiedelemben ők úgy jelentek meg, mint tinédzserek, akik sötét, nyirkos pincékben vírusokat írnak, hogy hírnevet szerezzenek, és megmutassák a világnak, hogy képesek rá.

„Social engineering” már az alapoktól jelen volt és a telefonos csalásokkal (vishing) kezdtek, amik a manapság is nagyon elterjedtek.

„Script kiddie”-k megjelenése.



2. Generáció (2000-es évek közepe)

Olyan férgeket kezdtek alkalmazni, amelyekkel adathordozók és e-mailek segítségével képesek voltak megfertőzni munkaállomásokat.

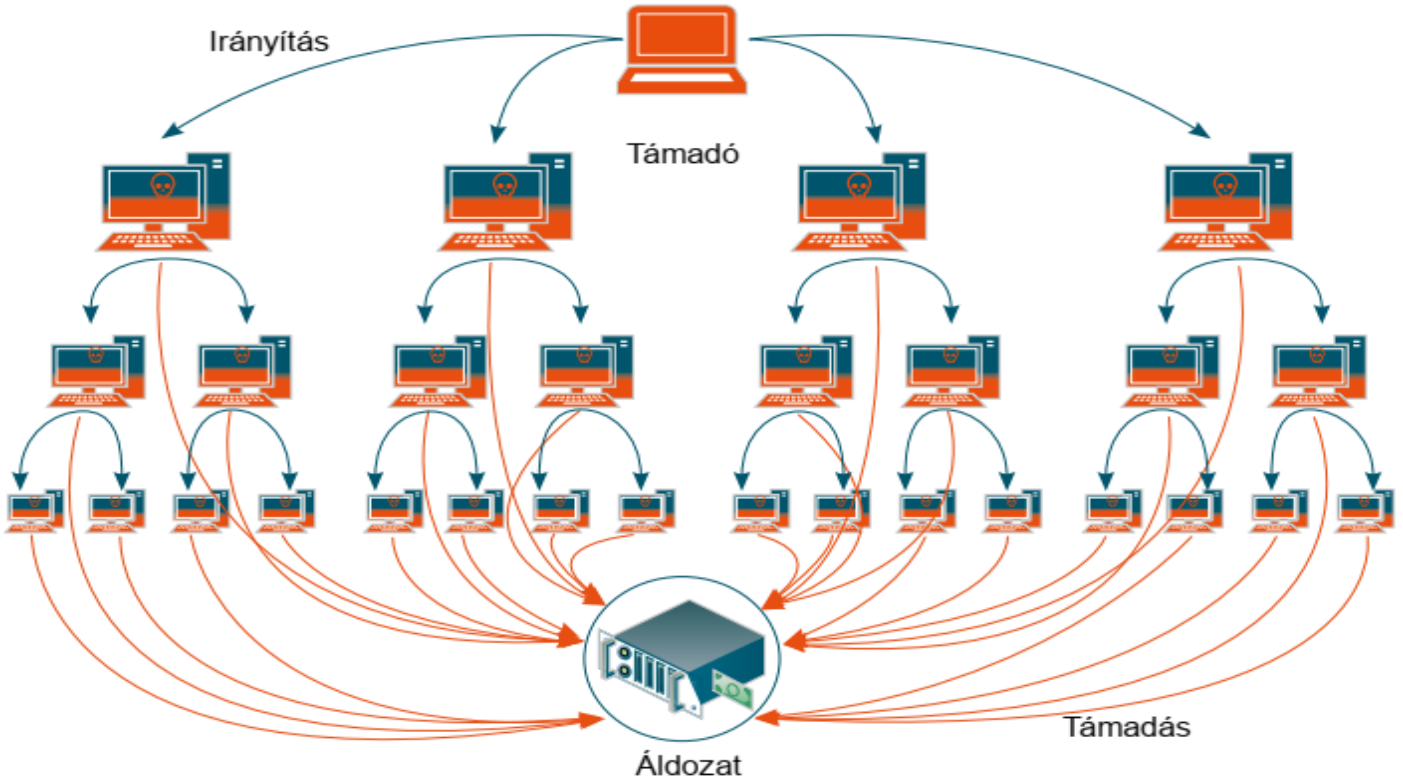
Pl.:

- Sasser (2004) – Olykor a PC-k leállítását, újraindítását blokkolta Ms. Windows XP és Ms. Windows 2000-es gépeken.
- NetSky (2000-es évek) – Tömeges e-mailekben küldte szét magát az áldozatoknak valamint a szükségtelen hálózati forgalommal lassították vagy blokkálták a kommunikációt.

Cél: többnyire káresemény okozás, infokommunikáció hátráltatása.

3. Generáció (2010-s évek eleje)

Ennél a generációnál már a motiváció az elismerésről a díjazás felé mozdult el. Megjelentek a botnetek, melyeket már DDOS támadásokra is alkalmaztak. A bevetett programkódok már jóval fejlettebbek voltak, mint a korábbi generációk által használt programsorok, azonban még mindig könnyen beazonosíthatónak és kivédhetőnek számítottak.

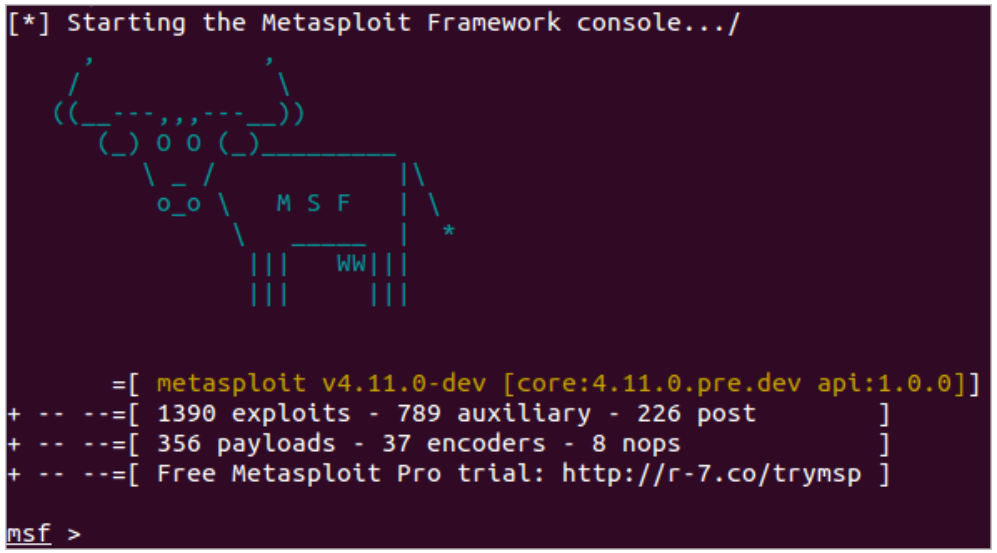


4. Generáció (2010-es évek közepe)

A kiberbűnözés professzionális szintre lépett. A kiberűnözők a rosszindulatú szoftvereket elkezdték elrejteni, és egyre jobban megszervezték csoportjaikat. Tapasztalt programozói tudással rendelkeztek, ami sokkal jobb minőségű malware-eket eredményezett. A támadók többnyire saját maguk módosították egyedivé a payload-ot, pontosan tudták, hogy a támadást elősegítő programkód hogyan épül fel és hogyan működik. Egyre nagyobb célpontokat vettek célba, ahonnan több pénzt lehet ellopni. Ez az időszak, amikor a hagyományos maffiák is bekapcsolódtak a játékba.

CYBER KILL CHAIN

MIMIKATZ

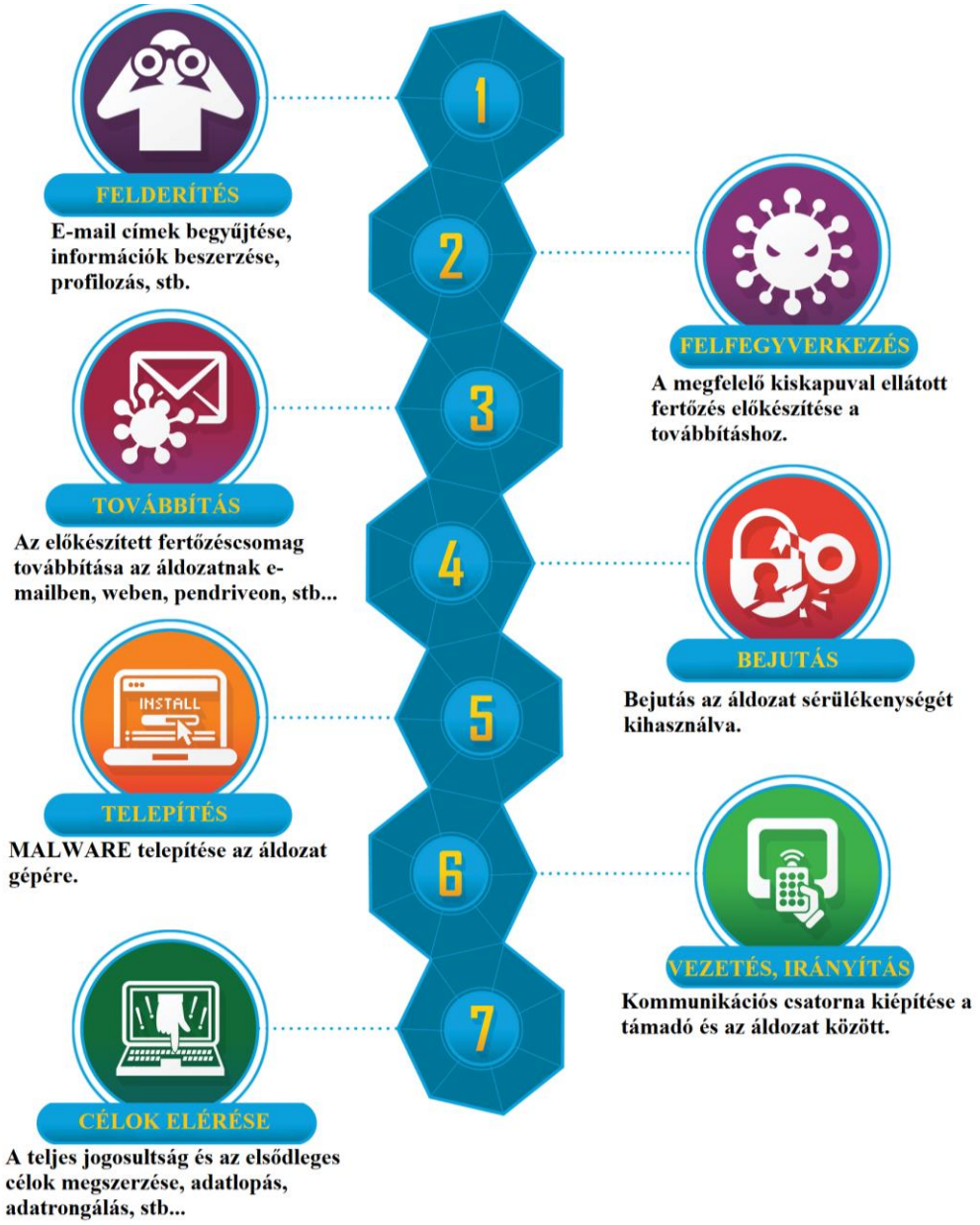


5. Generáció (2010-es évek végétől napjainkig)

Az ötödik és jelenlegi generáció gyakran előre elkészített eszközöket (toolokat) használ a kibertámadásokhoz azért, mert ezek könnyen használhatók, idő- és erőforrástakarékosak, lehetővé teszik gyors támadásokat és tömeges célpontokat, valamint lehetővé teszik a specializációt az adott területeken. Programozói tudásuk nem olyan fejlett, mint a 4. generációnak. Minden támadás típusra megvannak a kifinomult eszközcsomagjuk. Ha valami nem működik, nehezebben rögtönöznek.

Az ilyen előre elkészített eszközök elterjedése és nagy hatóereje miatt kiemelten fontos a számítógépes rendszerek hatékony védelme a kibertámadások ellen.

Lokheed Martin féle kibertámadási lánc



Védekezési javaslatok I.

1. szektor: Szerverek, amik az internetről láthatóak.

Az egyes szerverek egy alhálózatban vannak és kommunikálnak egymással. A bejutás többnyire egy létező rendszersérülékenység segítségével történik.

Javasolt megoldások:

- biztonsági dokumentációk elkészítése és betartatása;
- hálózati szegmentálás (nincs új a nap alatt);
- ellenőrzött operációs rendszer frissítések alkalmazása;
- logolás;
- képzett, személyzet (nem üzemeltetés a cél!!!);
- stb...

Védekezési javaslatok II.

2. szektor: Felhasználói szféra vagy üzemi terület

Külön alhálózatot képeznek a szerver szekcióval. A bejutás többnyire phising kampánnyal kezdődik. Ebben az esetben a támadónak mindenképpen el kell érnie, hogy a felhasználó hibázzon.

Javasolt megoldások:

- biztonsági dokumentációk elkészítése és betartatása;
- kiberbiztonsági tudatosító oktatások megtartása;
- stb...

Teljes biztonság nincs

Számos éles helyzetet szimuláló nemzetközi kibervédelmi gyakorlat van, amik segítenek felkészülni egy esetleges kibertámadásra.

<u>blue side:</u>

Pl.: Locked Shields, Cyber Coalition, EDA MilCert… stb.

<u>red side:</u>

pl.: Crossed Swords

Összefoglalás

A felnövekvő hacker generációkkal nagyon nehéz tartani a lépést a védelem oldalán, mert ez mindig egy macska-egér harc lesz a jövőben is. Azonban mindig nagyon hasznos megismerni hogyan épülhet fel egy valós kibertámadás, hogy felkészülhessünk az ellene való védelemre.

A kibervédelem szerepe nemzetközi és hazai szinten is kimagaslóan fontos. A védelmet azonban nem szabad csupán a szakemberekre hárítani. Minden felhasználónak tudatában kell lennie az őt érintő esetleges kiberfenyegetettségekkel és meg kell tennie mindent a tudatos kibertér használatának érdekében.

Források

- https://informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/ (letöltve: 2023.01.13.)
- A figyelemgazdaság átalakulása. Kitől kapjuk a kegyelemlökést? (Bíró Veronika), DigitalHungary, 2022. https://www.digitalhungary.hu/interjuk/A-figyelemgazdasag-atalakulasa-Kitol-kapjuk-a-kegyelemlokest/14003/ (letöltve: 2023.01.13.)
- Kibervédelem a bűnügyi tudományokban (Dornfeld L., Gyaraki R., Kiss T., Kovács Z., Nagy Z., Simon B.) Szerk.: Kiss Tibor, Budapest, 2020.
- MH KIMK – Cyber Academy: I. modul tananyag (Busa A. J., Rácz O., Umhauser B.), Szerk.: Busa A. J., Szentendre, 2022.
- Honvédelmi alapismeretek tankönyv (Almási L., Balog P., Berkecz G., Busa A. J., Drót L., dr. Eleki Z., Fekete A., dr. Kállai A., Kalmár I., Mihályi L., Nyulászi T., Szűcs P., dr. Tálas P. H., Tóth G., Zentai K.), Zrínyi Kiadó, Budapest, 2023.

Kérdések?

Köszönöm a figyelmet!