Távoli asztal kapcsolat feltörésének elemzése

Investigation of an RDC attack

Dr. HORNYÁK Olivér

egyetemi docens.
Miskolci Egyetem, Informatikai Intézet
Miskolc-Egyetemváros, Magyarország, +36 46 565-111, www.uni-miskolc.hu

Abstract

This paper gives an overview on malware types. An attack against Remote Desktop Protocol is investigated. A detailed overview is given on analyzing event logs for brute force attack. A script is provided to detect failed connection attempts of the Remote Desktop Connection and reveal the attackers IP address in order to block it.

Keywords: remote desktop connection, attack, security, computer, malware

Kivonat

Ez a cikk áttekinti a leggyakoribb rosszindulatú szoftver típusokat. A cikk írásának motivációja egy esettanulmány, egy kibertámadás kivizsgálása, és a további támadások megakadályozása. Ez a cikk bemutatja, hogyan lehet megvizsgálni az eseménynapló bejegyzésit. A cikk második része egy olyan módszert ír le, amely lehetővé teszi a rendszergazdának, hogy a távoli asztali kapcsolat feltörési kísérleteit észlelje, , a támadó IP címét kizárja.

Kulcsszavak: távoli asztal kapcsolat, támadás, biztonság, malware. számítógép

1. BEVEZETÉS

Malicious software, malware, malicious code vagy malcode – az angol nyelvű irodalom így nevezi azokaz a szoftvereket, amelyek arra tervetek, hogy rosszat, kártékonyat, akaratunkkal ellenkezőt csináljanak például:

- lopjanak,
- kárt okozzanak,
- törvénytelen dolgot műveljenek,
- megzavarjanak,
- felhasználják az erőforrásainkat (memória., processzor, háttértár),
- stb.

Az alábbi osztályokba sorolhatjuk ezeket:

- vírusok,
- férgek,
- trójaiak,
- botok.
- botok.

A számítógépes vírus lemásolja magát és beszúrja magát valamelyik programba, részévé válik annak. A vírusok egy része csupán valami bosszantó dolgot tesz. Van, ami az adataidban okoz kárt. és van, amelyik szolgáltatásmegtagadási támadásokat (Denial-of-Service, DOS) okoz. A legtöbbször a vírus egy végrehajtható állományban bújik meg. A megfertőződött gazdaprogram akár továbbra is működőképes maradhat. Van olyan vírus is, amelyik elpusztítja a gazdaprogramját. Hogyan kerül a vírus a számítógépre? A legtöbbször az alábbi módokon:

- hálózat,
- külső memória,
- fájlmegosztás,
- e-mail melléklet,

- rendszerfrissítés,
- diszk.

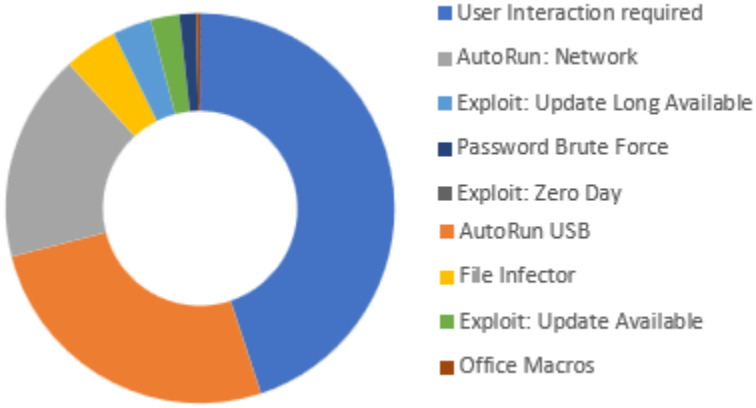
A számítógép féreg is képes lemásolni magát másik számítógépre és így képes terjedni. A féreg egy különálló program. Nem kell neki gazdafájl a terjeszkedéshez. A féreg gyakran a számítógép valamiyen sebezhetőségét kihasználva jut be a rendszerbe. A trójaiak a görög faló után kapta a nevét. Általában valami trükk segítségével jutnak be a rendszerbe. A trójaiak károkozási listáján szerepel az adatlopás, adatok lekódolása, hátsó ajtók kinyitása más kártékony kód számára. A trójaiak nem másolják le magukat. A számítógépes botok neve a robot szóból egyszerűsödött ki. Ezek automatikus eljárások. Összekapcsolódnak más hálózati szolgáltatásokkal. A robotok jelszavakat lophatnak, információkat gyűjthetnek, billentyűleütéseket naplózhatnak, spam üzeneteket továbbíthatnak.

A támadás fázisait angol nyelven 5 p betűs szóval szokás leírni [2]:

1. ábra. *A számítógépes rendszereket ért támadás fázisai*

- Probe – Puhatolózás: a célpontok azonosítása
- Penetrate – Behatolás: - rosszindulatú kód továbbítása a célpontjához
- Persist – Ragaszkodás: a rosszindulatú programok megpróbálnak a rendszerben maradni
- Propagate – Kiterjesztés: kiterjesztés más rendszerekre
- Paralyze – Paralizálás: - a rosszindulatú programok kárt okoznak

Számítások szerint 2021-ben a kiberbűnözés okozta kár 6,000,000,000,000 USD (hattrillió $), és minden másodpercben 12 ember válik áldozattá. Security Intelligence Report [4] statisztikái alapján a rosszindulatú kód elterjedése az alábbi módokon valósul meg:



2. ábra. *A számítógépes rendszereket ért támadás fázisai*

A [4] áttekintést ad a rosszindulatú támadásokról. Érdekes látni, hogyan fejlődtek a rosszindulatú programok az elmúlt években [11]. A rosszindulatú programok első generációja (DOS vírusok) főként emberi tevékenység segítségével replikálódott. A második generációs kártevők önreplikálódnak segítség nélkül, egyébként az első generáció jellemzőivel rendelkeznek. Fájlokon és a médián keresztül terjednek. A harmadik generáció már az internet lehetőségeit használja ki a továbbterjedéshez. Ez nagy lökést adott a vírusok terjedésének. A negyedik generációval megjelennek a szervezet-specifikusabb, és a kereskedelmi forgalomba hozott rosszindulatú kódok. Megjelenik a vírusirtó szoftverek vagy rendszerek megtámadása, kiiktatása. Az ötödik generáció jellemzője a rosszindulatú programok kiberhadviselésben való használata, illetve megjelenik a malware as service (kártevő szolgáltatásként) fogalma.

Egyre nagyobb volumenben jelennek meg a dolgok internete (Internet of Things, IOT) célzott támadásai [1].

2. A VÉDEKEZÉS LEHETŐSÉGEI

A védekezés módszereit a legtöbbször a következőkben felsorolt szabályok betartása és betartatása jelenti:

1. A védekezés kulcsa a megelőzés.
   a. Légy óvatos, kerüld az ismeretlen ingyenes szoftvereket és a kalóz szoftvereket.
   b. kerüld a privilegizált (pl.: admin, root) fiókokat, ha nem szükséges.
   c. alkalmazz biztonságos konfigurációkat.
   d. tartsd naprakészen a géped. Alkalmazd a biztonsági frissítéseket a böngésző, az e -mail kliens és az operációs rendszer számára.
   e. különítsd el a frissíthetetlen számítógépeket.
   f. használj fokozott védelmet böngészőhöz és e -mailjei klienshez, használj biztonságos e -mail átjárót.
   g. használj rosszindulatú programok elleni eszközöket.
   h. a hálózati védelem legyen valós idejű.
   i. tanítsd a felhasználókat gyanakvásra.
2. Legyenek a hozzáférések szabályozva
   a. Használd a szükséges legkevesebb jogosultságot.
   b. Szegmentáld a hálózatot.
   c. Legyél óvatos, amikor engedélyeket adsz az alkalmazásoknak.
   d. Az alkalmazásokat megbízható helyekről töltsd le, például az App Store -ból.
   e. Erős felhasználói korlátozási szabályokat használj az alkalmazások futtatásakor.
   f. Használj listát a megbízható az alkalmazásokról.
3. Használj biztonsági mentést.
   a. Fontos, hogy legyen automatikus biztonsági mentés.
   b. Használhatsz online szolgáltatásokat.
   c. Győződj meg arról, hogy a kritikus adatokat tartalmazó biztonsági másolat nem megsemmisíthető.
   d. Legyen biztonsági mentések készítésének házirendje.
   e. A biztonsági másolatokat legalább két különböző típusú tárhelyen tárold, amelyek közül az egyik külső.

Egészen néhány évvel ezelőttig a kiberbűnözők erőfeszítéseiket a rosszindulatú programokra, az ezekkel végzett támadásokra összpontosították, mert ezek nyújtották a legnagyobb megtérülést. Újabban az adathalász támadásokra helyezték a hangsúlyt (~ 70%) azzal a céllal, hogy felhasználói adatokat gyűjtsenek [5]. Lépései a következők:

1. A bűnözők előkészítik infrastruktúrájukat pl.: kompromittált vagy hamis tartományokat (domaineket). Ezzel információt gyűjtenek a lehetséges célpontokról.
2. Rosszindulatú e -mail üzenetek küldése.
3. Az áldozatot a hamis tartományba irányítják.
4. Az áldozat hamis űrlapba írja be a hitelesítő adatokat, vagy az áldozat letölt egy rosszindulatú programot, amely hitelesítő adatokat gyűjt az eszközön.
5. A bűnözők hozzáférnek az áldozat hálózatához. A bűnözők ugyanazokat a hitelesítő adatokat használják más webhelyeken.

2. ábra. *A támadás egy lehetséges formája*

3. TÁVOLI ASZTAL KAPCSOLAT ALAPÚ TÁMADÁS ESETTANULMÁNYA

A [8] átfogó áttekintést ad a rosszindulatú programok észlelési technikáiról. Ezek magukban foglalják:

- Aláírás alapú rosszindulatú programok észlelése,
- Heurisztikus alapú rosszindulatú programok észlelése,
- Felhő alapú rosszindulatú programok észlelése.

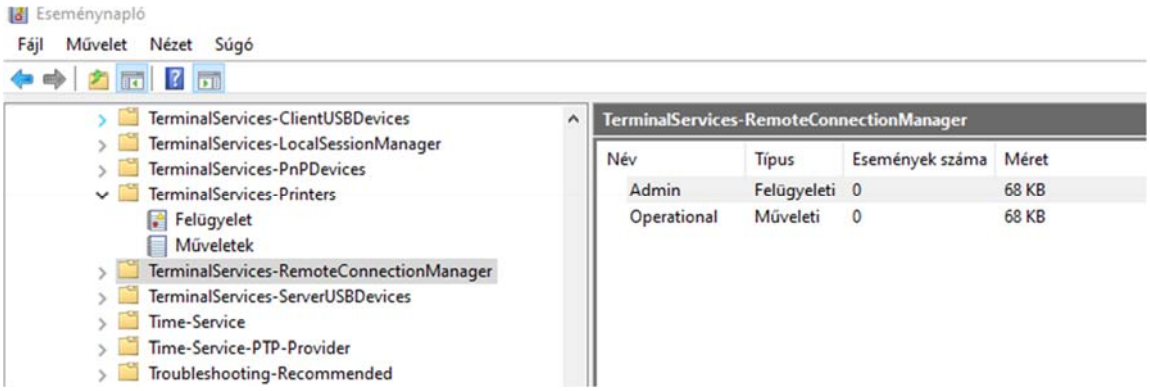
Vannak AI alapú technikák a rosszindulatú programok észlelésére. Egy másik áttekintés [10] szerint megkülönböztetünk

- host alapú,
- hálózati alapú és
- hibrid rosszindulatú programok észlelő rendszer.

Számos kereskedelmi rosszindulatú program-érzékelő rendszer létezik. Ha azonban a támadás időpontjában nem volt használatban, akkor is elemezhető, hogyan következett be a támadás. Ebben a fejezetben egy esettanulmányt kapunk, hogyan lehet megvizsgálni egy potenciális távoli asztali csatlakozási támadást.

Miután a támadók hozzáférést kaptak a célszámítógéphez, bejelentkezhetnek a Remote Desktop Connection (RDC) segítségével. A támadás nyomainak megkeresésére vizsgáljuk meg a Windows operációs rendszer eseménynaplóját. A távoli asztal kapcsolat felépítésének fő szakaszai:

- hálózati kapcsolat kiépítése,
- hitelesítés,
- bejelentkezés,
- munkamenetre való csatlakozás,
- kijelentkezés.



3. ábra. *Az eseménynapló vizsgálata*

A 3. ábra az eseménynapló nézegetőt ábrázolja az Alkalmazások és szolgáltatásnaplók → Microsoft → Windows → Terminal Services -RemotecConnectionManager → Operational című oldalon. Ha egy hálózati kapcsolat bekövetkezik, egy eseménynapló jön létre az EventID 1149 bejegyzéssel. Ez az esemény csak a kapcsolatot jelzi. A hitelesített eseményeknek két azonosítója van: 4624 azt jelzi, ha a fiók sikeresen bejelentkezett, vagy 4625 ha a fiók nem jelentkezett be. Az eseményleírás mezőben van egy mező, amely további információkat tartalmazhat:

A távoli aszta kapcsolódás részletei 1. táblázat

Belépés típusa	Leírás
2	Interaktív (jelszó manuális megadása)
3	Hálózati kapcsolat
4	Kötegelt – például egy taszk
5	Szolgáltatás indítása
7	Feloldás – például a képernyővédő jelszó megadása
8	Belépés kód nélkül
9	Nem használt
10	Távoli interaktív logon (Terminal Services, Remote Desktop or Remote Assistance)
11	Cached interaktív logon

Egy 4624 esemény például így néz ki:

```
An account was successfully logged on.

Subject:
```

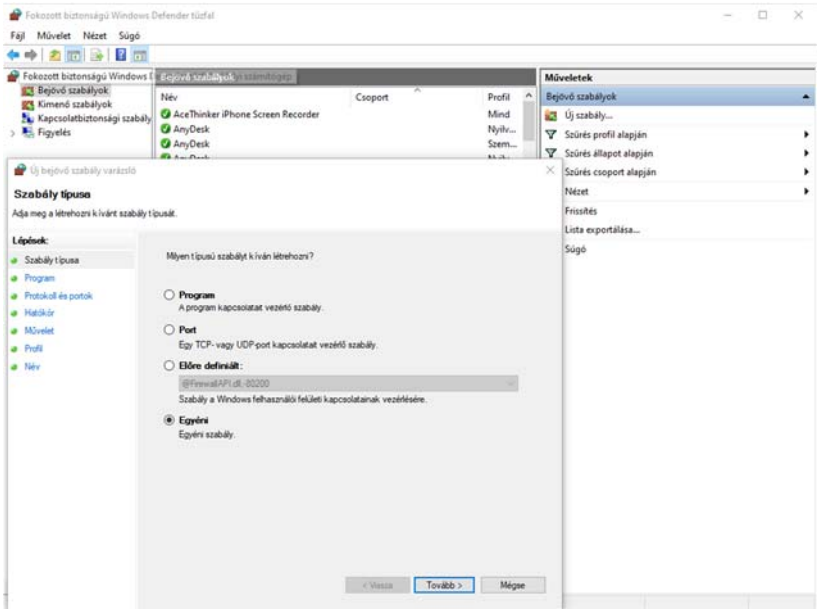
```
        Security ID: SYSTEM
        Account Name: DESKTOP- 5MRKQIP$
        Account Domain: LABOR
        Logon ID: 0x3E7

    Logon Information:
        Logon Type: 7
        Restricted Admin Mode: -
        Virtual Account: No
        Elevated Token: No

    Impersonation Level: Impersonation

    New Logon:
        Security ID: Oliver
        Account Name: oliver.hornyak@uni-miskolc.hu
        Account Domain: LABOR
        Logon ID: 0xFD5113F
        Linked Logon ID: 0xFD5112A
        Network Account Name: -
        Network Account Domain: -
        Logon GUID: {00000000-0000-0000-0000-000000000000}

    Process Information:
        Process ID: 0x30c
        Process Name: C:\Windows\System32\lsass.exe

    Network Information:
        Workstation Name: DESKTOP-5MRKQIP
        Source Network Address: -
        Source Port: -

    Detailed Authentication Information:
        Logon Process: Negotiat
        Authentication Package: Negotiate
        Transited Services: -
        Package Name (NTLM only): -
        Key Length: 0
```

4. A REMOTE DESKTOP KAPCSOLATOT ÉERINTŐ BRUTE FORCE TÁMADÁSOK KIVÉDÉSE

A támadók megkísérelhetnek egy úgynevezett brutális erő támadásra, amikor próbálgatják a jelszavakat a rendszerbe való belépéshez.. Ez folyamatos távoli asztali csatlakozási kísérleteket eredményez. A rendszergazda blokkolhatja a támadó IP -jét egy Windows tűzfal szabállyal [6]. A következő PowerShell szkript lekérdezi a sikertelen bejelentkezési kísérleteket (legalább 5 kísérlet ugyanabból az IP címről), és meghatározza a támadó IP -címét:

```
$timeFrame = [DateTime]::Now.AddHours(-12)
$failedRDPAttempts = Get-EventLog -LogName 'Security' -after
$timeFrame -InstanceId 4625 | ?{$_.Message -match 'logon type:\s+(3)\s'} | Select-
Object @{n='IpAddress';e={$_.ReplacementStrings[-2]} }
$attackerIP = $failedRDPAttempts | group-object -property IpAddress | where
{$_.Count -gt 5} | Select -property Name
```

Ezután a rendszer adminisztrátora beállíthat egy olyan tűzfal szabályt, amely blokkolja ezt az IP címet.



4. ábra. *Az IP cím bokkolása tűzfallal*

5. ÖSSZEFOGLALÁS

Ebben a cikkben áttekintést adta a Windows számítógép elleni leggyakoribb támadási típusokról. Bemutattam egy elemzőeszközt, amely képes felismerni a távoli asztali csatlakozási kísérleteket. Noha vannak kereskedelmi rosszindulatú programok elleni alkalmazások, ezek nem nyújtanak segítséget a támadás nyomainak megtalálásában és elemzésében. Részletesen ismertettem a távoli asztal támadás felderítésnek módszerét. A támadást követően a rendszergazdának meg kell akadályoznia a további támadásokat. Miután a támadó IP-címét meghatározta, a rendszergazda blokkolhatja ezeket az IP címeket egy tűzfalszabály segítségével. A javasolt módszer előnye, hogy ingyenes, csupán az alapvető rendszer-adminisztrációs ismeretek szükségesek hozzá.

IRODALMI HIVATKOZÁSOK

[1] Cayir, E. B., Ervural, B.: Overview of cyber security in the industry 4.0 era. Industry 4.0: managing the digital transformation. Springer, Cham, 2018. 267-284.

[2] Cox, K. J., Gerg, C.: Managing Security with Snort & IDS Tools: Intrusion Detection with Open Source Tools. O'Reilly Media, Inc., 2004.

[3] Which is the most popular malware propagation tactic https://www.zdnet.com/article/which-is-the-most-popular-malware-propagation-tactic/ (utolsó hozzáférés 2022. 08. 02)

[4] Microsoft Security Intelligence Report, https://clouddamcdnprodep.azureedge.net/gdc/gdc09FrGq/original (utolsó hozzáférés 2022. 10. 02)

[5] Microsoft Digital Defense Report | September 2020, https://www.microsoft.com/security/blog/2020/09/29/microsoft-digital-defense-report-2020-cyber-threat-sophistication-rise/ (utolsó hozzáférés 2022. 10. 02)

[6] http://woshub.com/rdp-connection-logs-forensics-windows/#h2_1

[7] Aslan, Ö. A, Refik S.: A comprehensive review on malware detection approaches. IEEE Access 8 (2020): 6249-6271.

[8] Ye, Y., Li, T., Adjeroh, D., Iyengar, S. S.: A survey on malware detection using data mining techniques. ACM Computing Surveys (CSUR) 50.3 (2017): 1-40.

[9] Ekta, G., Bansal, D. Sofat S.: Malware analysis and classification: A survey. Journal of Information Security 2014.

[10] Saeed, I. A., Selamat, A., Abuagoub, A. M. A.: A survey on malware and malware detection systems. International Journal of Computer Applications 67.16 (2013).

[11] Ligh, M. W., Hartstein, S. A., B., Richard, M.: Malware analyst's cookbook and DVD: Tools and Techniques for Fighting Malicious Code, ISBN 9780470613030, Wiley Pub., Inc, 2010