Jegyzőkönyv

Biztonság és védelem az informatikában c. tárgy

2. feladat

Készítette:

Csomor Bence, TVIK4I

2021.02.24.

**Bot, Worm, behatoló detektálása**

**Elmélet:**

*PID:* (Process Identifier) Folyamat azonosító, hibakeresés során használatos sok helyen.

*Protocol:* A protokoll egy szabvány, ami leírja, hogy a hálózat résztvevői hogyan tudnak kommunikálni egymással. Nagyrészt kapcsolatfelvétel, továbbítás és kommunikáció.

*Local Address:* Magánhálózat, amely privát IP-címtartományt használ.

*Local Port:* A helyi port a helyi számítógép port száma.

*Remote Address:* A távoli cím annak a távoli számítógépnek az IP-címe, amelyhez a kapcsolat csatlakozik.

*Remote Port:* A távoli port a távoli számítógép port száma.

**State:** (TIME\_WAIT, LISTENING, ESTABLISHED, CLOSE\_WAIT):

*TIME\_WAIT:* Azt jelzi, hogy a helyi végpont (ezen az oldalon) lezárta a kapcsolatot.

*LISTENING:* Az aljzat csatlakozására vár.

*ESTABLISHED:* Jelzi, hogy jelenleg ott van egy kapcsolat.

*CLOSE\_WAIT:* Azt jelzi, hogy a távoli végpont (a kapcsolat másik oldala) lezárta a kapcsolatot.

*Sent Packets:* A csomag egy kis mennyiségű adat, amelyet hálózaton, például LAN-on vagy az Interneten keresztül küldenek.

*Sent Bytes:* Az elküldött bájtok/sec az az arány, amellyel a bájtokat minden hálózati adapteren keresztül elküldik, beleértve a keretező karaktereket.

*Rcvd Packets:* Amikor a csomagok eljutnak rendeltetési helyükhöz, azokat egyetlen fájlba vagy más összefüggő adatblokkba állítják össze.

*Rcvd Bytes:* Bájt fogadott/sec az az arány, amellyel a bájtokat minden hálózati adapteren keresztül fogadják, beleértve a keretező karaktereket is.

**Process Explorer:**

*CPU:* Az utolsó másodpercben a CPU-idő aránya százalékosan.

*Private Bytes:* Csakis a programhoz rendelt memória mennyisége.

*Working Set:* A Windows által a programhoz rendelt memóriának mennyisége.

*PID:* Az adott folyamat azonosítója.

*Description:* Az alkalmazás leírása (ha rendelkezik vele).

*Company Name:* Ez nagyon hasznos. Ha valaminek nincs igaza, kezdje el a Microsoft által nem használt folyamatok keresését.

*I/O Reads:* A folyamat által generált olvasási bemeneti / kimeneti műveletek száma, beleértve afájl, a hálózat és az eszköz I/O-kat.

*I/O Writes:* A folyamat által generált írási bemeneti / kimeneti műveletek száma, beleértve a fájl, a hálózat és az eszköz I/O-kat.

**Auto Runs:**

*Everything:* Az Autoruns első futtatásakor automatikusan megnyílik a „Minden” fül, és látjuk, hogy mindenféle „automatikus futtatással” kezd feltöltődni. Itt minden letiltható (a Winsock kivételével) vagy teljesen törölhető.

*Logon:* Ez a bejegyzés a szokásos automatikus indítási helyek, például az aktuális felhasználó és az összes felhasználó Startup mappájának, a Futtatási rendszerkulcsok és az alkalmazás szabványos indítási helyeinek vizsgálatát eredményezi.

*Explorer:* Az Explorer olyan funkciók meghívására is alkalmas, amelyek nem feltétlenül szeretnének aktívak lenni a rendszerben.

*Internet Explorer:* Ez a bejegyzés megjeleníti a Böngésző segítő objektumokat, az Internet Explorer eszköztárakat és bővítményeket.

*Scheduled Tasks:* Feladatütemező feladatok konfigurálása indításkor vagy bejelentkezéskor kezdődik.

*Services:* Megmutatja az összes Windows-szolgáltatást, amelyek úgy vannak beállítva, hogy automatikusan elinduljanak, amikor a rendszer elindul.

*Drivers:* Ez megjeleníti a rendszeren regisztrált összes kernelmódú illesztőprogramot, kivéve azokat, amelyek le vannak tiltva.

*Codecs:* Az automatikus futtatáson keresztül kodekek végezhetők, amelyeket általában a multimédiás tartalom dekódolásához és kódolásához használnak. A kodekek és / vagy a DirectShow szűrők létfontosságúak a DirectShow alapú multimédia lejátszók, például a Windows Media Player számára.

*Boot Execute:* Natív képek, amelyek a rendszerindítási folyamat elején futnak.

*Image Hijacks:* Képfájl-végrehajtási lehetőségek és a parancssor automatikus indítása.

*AppInit:* Ennek során az Autoruns az alkalmazás inicializálási DLL-ként regisztrált DLL-eket mutatja.

*KnowDLLs:* Ez jelenti a DLL-ek helyét, amelyeket a Windows az őket hivatkozó alkalmazásokba tölt be.

*Winlogon:* Mutatja azokat a DLL-eket, amelyek regisztrálják magukat a Winlogon bejelentkezési eseményekről szóló értesítésére.

*Winsock Providers:* A regisztrált Winsock protokollokat mutatja, beleértve a Winsock szolgáltatókat is. A rosszindulatú programok gyakran telepítik magukat Winsock szolgáltatóként, mert kevés eszköz képes eltávolítani őket. Az automatikus futtatások letilthatják, de nem törölhetik őket.

*Print Monitors:* Megjeleníti a nyomtatási spooling szolgáltatásba betöltő DLL-eket. A rosszindulatú program ezt a támogatást használta az automatikus indításhoz.

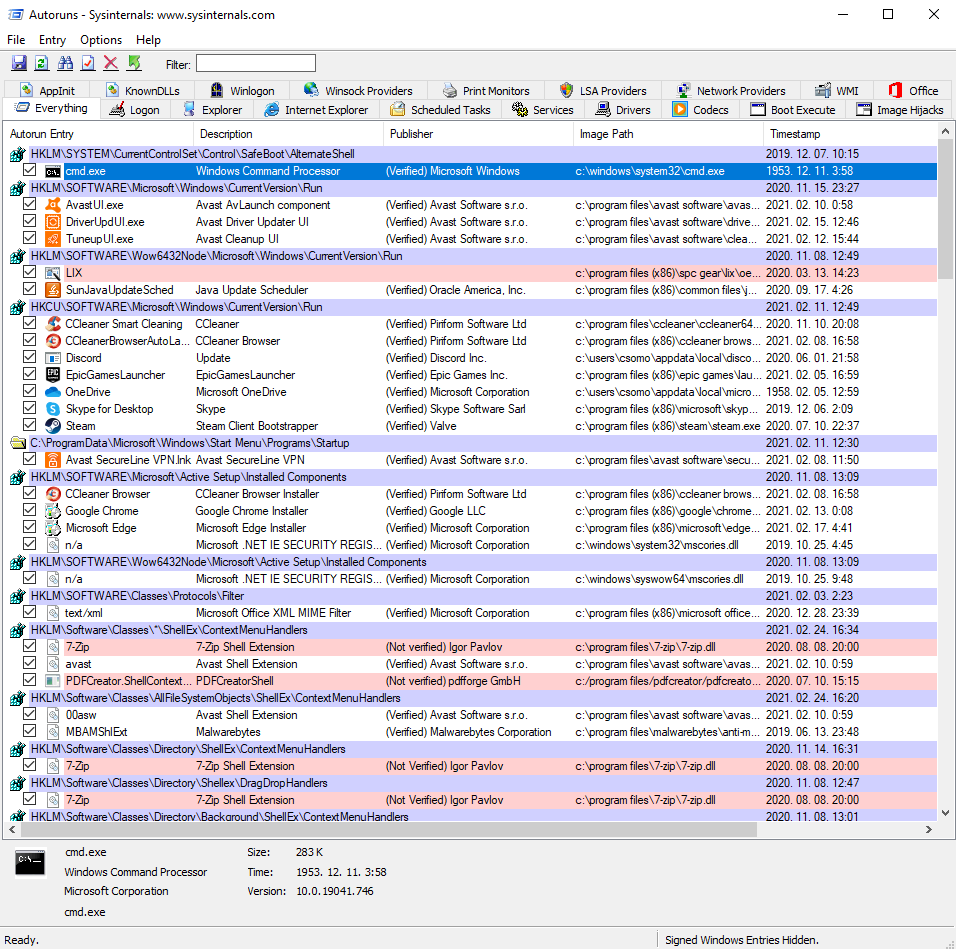
*LSA Providers:* Megmutatja a helyi biztonsági hatóság (LSA) hitelesítési, értesítési és biztonsági csomagjainak nyilvántartásait.

**Gyakorlat:**

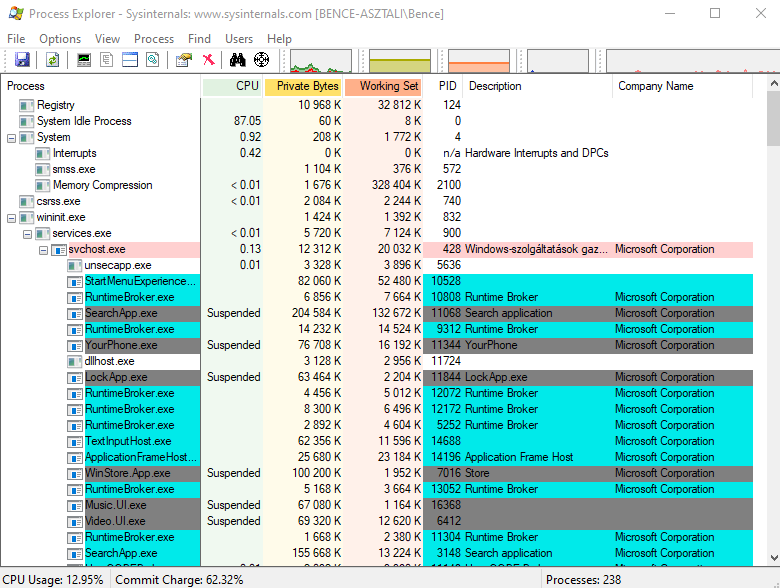
A <https://docs.microsoft.com/en-us/sysinternals/downloads/> Weboldalról leszedett programok segítségével az alkalmazások futás idejű tulajdonságait és hálózati forgalmát is analizálhatjuk. Ebben a megadott AutoRuns, ProcessExplorer, tcpView és a WindowsPortableApps lesz a segítségünkre.

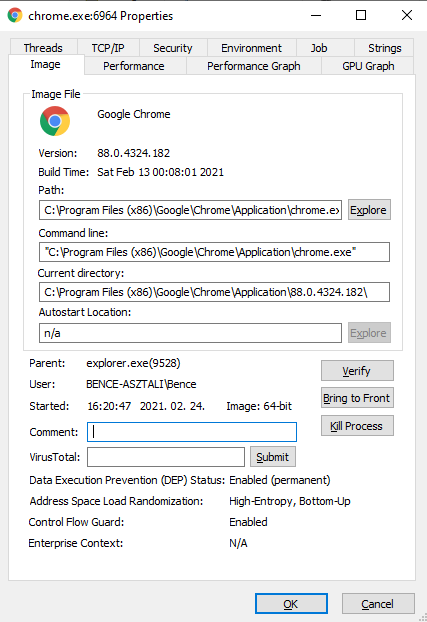
forrás: https://www.thewindowsclub.com/sysinternals-autoruns-windows

Az AutoRuns alkalmazással az éppen futó programokat lehet megfigyelni.

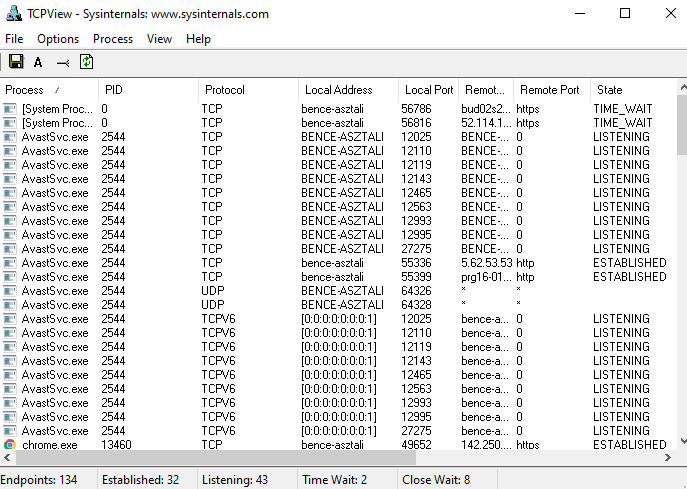


A ProcessExplorer segítségével részletesen ki lehet vizsgálni egy adott programot.



Megnyitva a Properties ablakot, az Image fülön láthatóak az adott program részletes adatai (verziószám, létrehozás időpontja, elérési útvonal, stb…). Továbbá lehetőségünk van a programokat elaltatni, elindítani, újraindítani és ha kell, teljesen leállítani.

A tcpView a harmadik program, amit letöltöttem, ezzel a hálózat használatát lehet megfigyelni az alkalmazásoknak.



Az utolsó alkalmazással, a WiresharkPortable-el a hálózaton küldött és fogadott adatokat is vissza lehet nézni, ha a Capture fülön a Start-ra nyomunk. Ezt egy kis futás után a Stoppal leállítva a rögzített adatokat elemezhetjük és le is menthetjük, szükség szerint.

