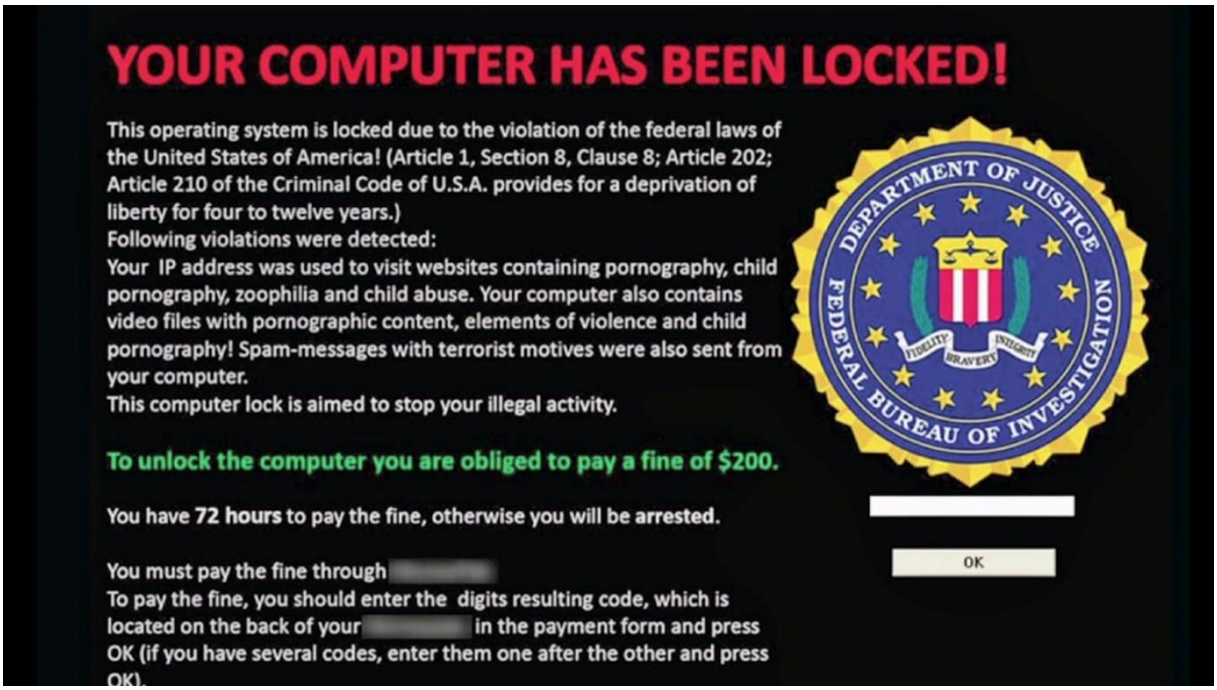
https://wigner.hu/szhk/ransomware-elleni-vedelem-windows-rendszereken

RANSOMWARE ELLENI VÉDELEM WINDOWS RENDSZEREKEN

1. Mi a ransomware?

Napjainkban megnövekedett az úgynevezett ransomware programok terjedése. Ezek a rosszindulatú programok használhatatlanná teszik a számítógépet, titkosítják a rajta található adatokat. Általában fenyegetéssel próbálnak pénzhez jutni a felhasználóktól, a támadók váltságdíj fejében állítják vissza az adatokat.



2. Hogyan védekezzünk ellene?

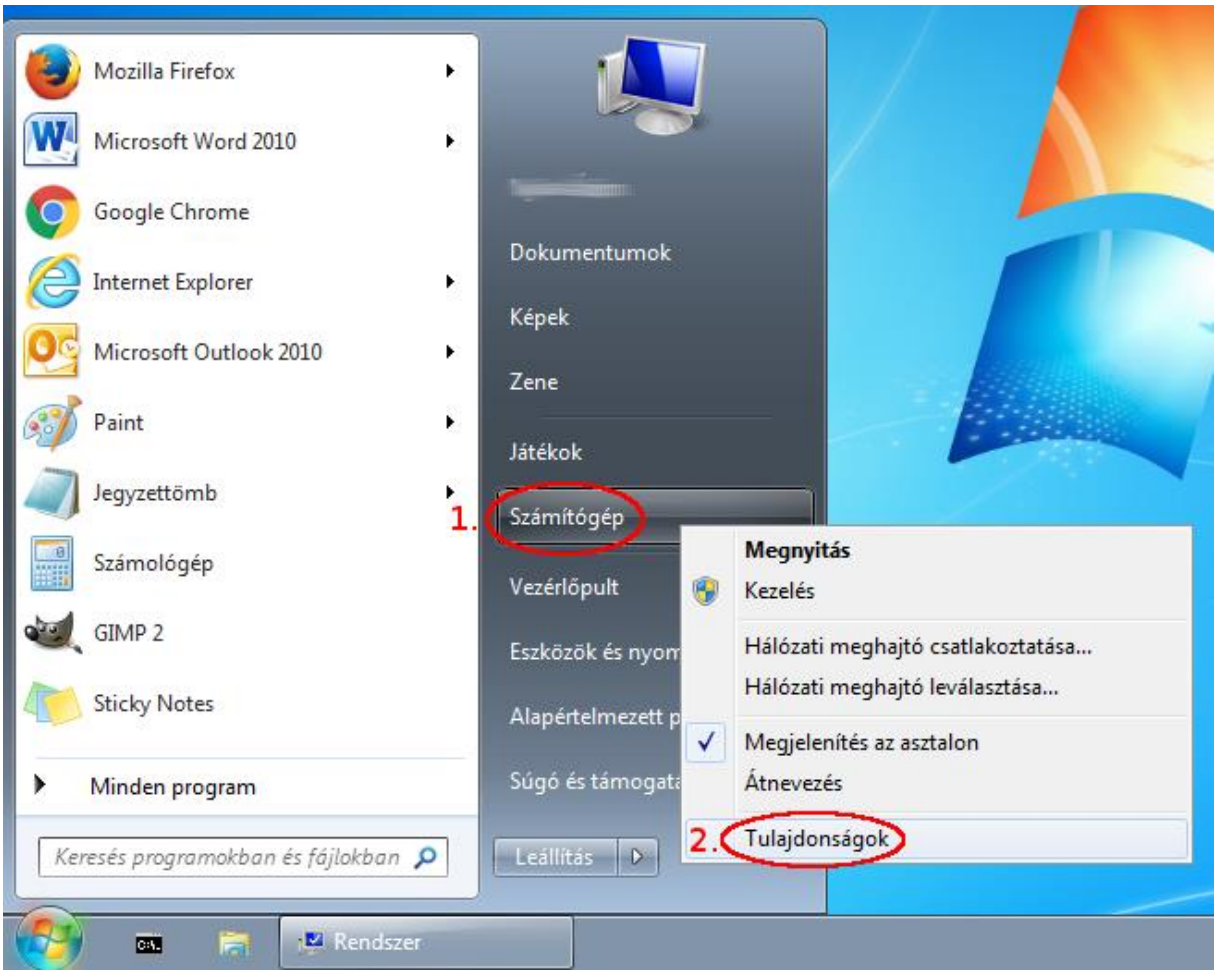
I. Operációs rendszer rendszeres frissítése: az elavult operációs rendszerek fokozottabban vannak kitéve a ransomware támadásoknak, ezért elengedhetetlen, hogy rendszeresen frissítse szoftvereit és operációs rendszerét számítógépének védelme érdekében.
II. Korlátozott hozzáférésű fiók: amennyiben lehetséges, ne használjunk Rendszergazda fiókot a rendszerünkön. Csak azon alkalmazásoknak engedélyezzük az emelt jogosultságú futtatást, amelyek ezt igénylik, és megbízunk bennük!

III. Vírusirtó, biztonsági csomag telepítése, tűzfal: Windows rendszereken elengedhetetlen a vírusirtó, és más biztonsági megoldások használata. Vírusirtó gyanánt használja a Csillebérci telephelyen működő kutatóintézetekben dolgozók számára letölthető vírusirtó csomagot. A tűzfalat tartsa bekapcsolva a rendszerén. Ezen felül fontolja meg a BitDefender ingyenes, ransomware elleni programjának
telepítését: http://download.bitdefender.com/am/cw/BDAntiRansomwareSetup.exe
A Microsoft szintén biztosít ingyenes biztonsági megoldást ransomware ellen, a szoftvercsomag neve EMET, mely a következő hivatkozáson tölthető le: https://www.microsoft.com/en-us/download/details.aspx?id=50766
Fontos: *Biztonsági szoftverekből (vírusírtó, tűzfal, ransomware elleni program), mindig csak egyet-egyet használjon! Ne legyen például 2 db ransomware elleni program a gépen, mert ez a helyes rendszerműködés rovására mehet, azaz többet árt mint használ!*
IV. Kerülje a gyanús e-mailek megnyitását, ismeretlen fájlok letöltését: a ransomware programok nagy százalékban e-mailben, vagy internetes hivatkozások (URL) útján jutnak be a számítógépre. Ne nyisson meg olyan fájlokat, amiket nem ismer, küldője ismeretlen, netán ismeri az illetőt, de idegen nyelven ír Önnek.
V. Rendszeres biztonsági mentés készítése: kapcsolja be a biztonsági mentés funkciót az összes meghajtóra. Készítsen biztonsági mentést egy külső adathordozóra (külső diszk, pendrive, CD/DVD). A műveletek elvégzéséhez segítségére lehet a lentebbi tutorialok egyike.
VI. Megfelelő registry beállítások: a támadások megelőzése végett elérhetővé tettünk egy letölthető .reg (registry - Windows Regisztrációs Adatbázis) fájlt, ami a következő beállításokat importálja rendszerébe:
- Rejtett fájlok, könyvtárak, meghajtók mutatása
- Rejtett fájlkiterjesztések mutatása
- Automatikus lejátszás kikapcsolása az összes meghajtón
- Rendszer-visszaállítás opció elérhetővé tétele (ha azt group policy tiltja) - ez még nem jelent bekapcsolást!
- UAC (User Account Control) engedélyezése, alapbeállítások betöltése
- Távoli Asztali Kapcsolat letiltása
- Scripting Host letiltása
- Word, Excel, Project makrók futtatásának tiltása

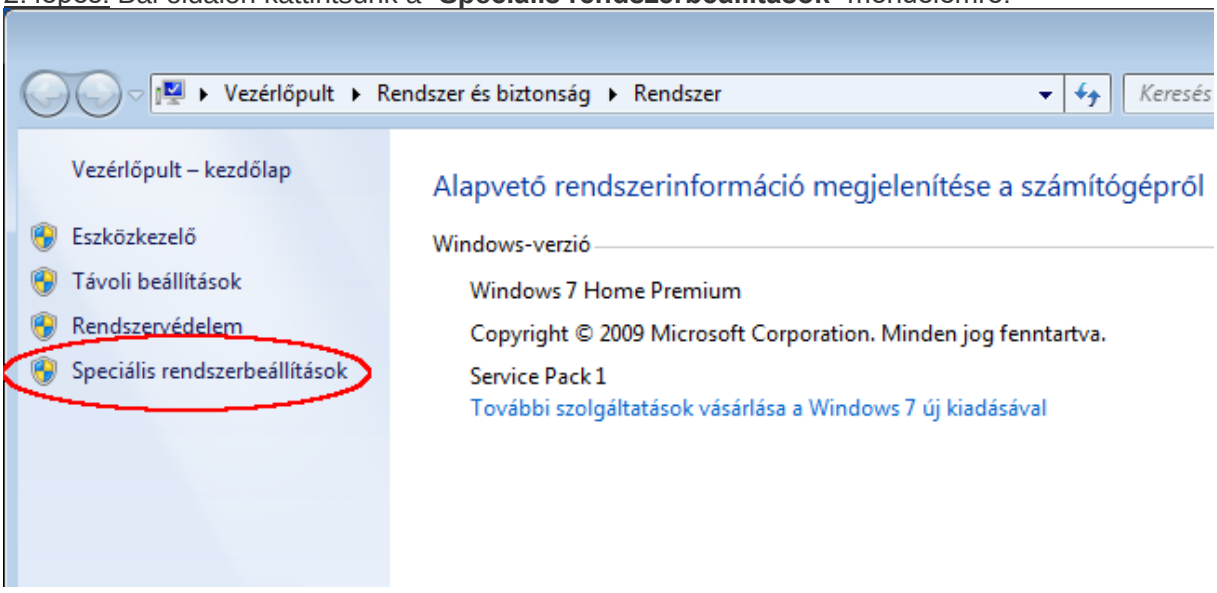
Figyelem: *Bizonyos beállítások csak a jelenlegi felhasználóra vonatkoznak (HKEY_CURRENT_USER ág)! Minden használt fiókon futtassa le a .reg fájlt!*
A .reg fájl letölthető innen: against_ransomware_settings.reg

VII. Biztonsági mentés bekapcsolása minden meghajtón, rendszer-helyreállító lemez készítése: Windows frissítések, programtelepítések előtt, valamint változó időközönként, alapértelmezetten a rendszer automatikus biztonsági mentéseket (rendszer-visszaállítási pontokat) készít. Ezeket erősen ajánlott bekapcsolni minden meghajtóra, ha ez nem így lenne.

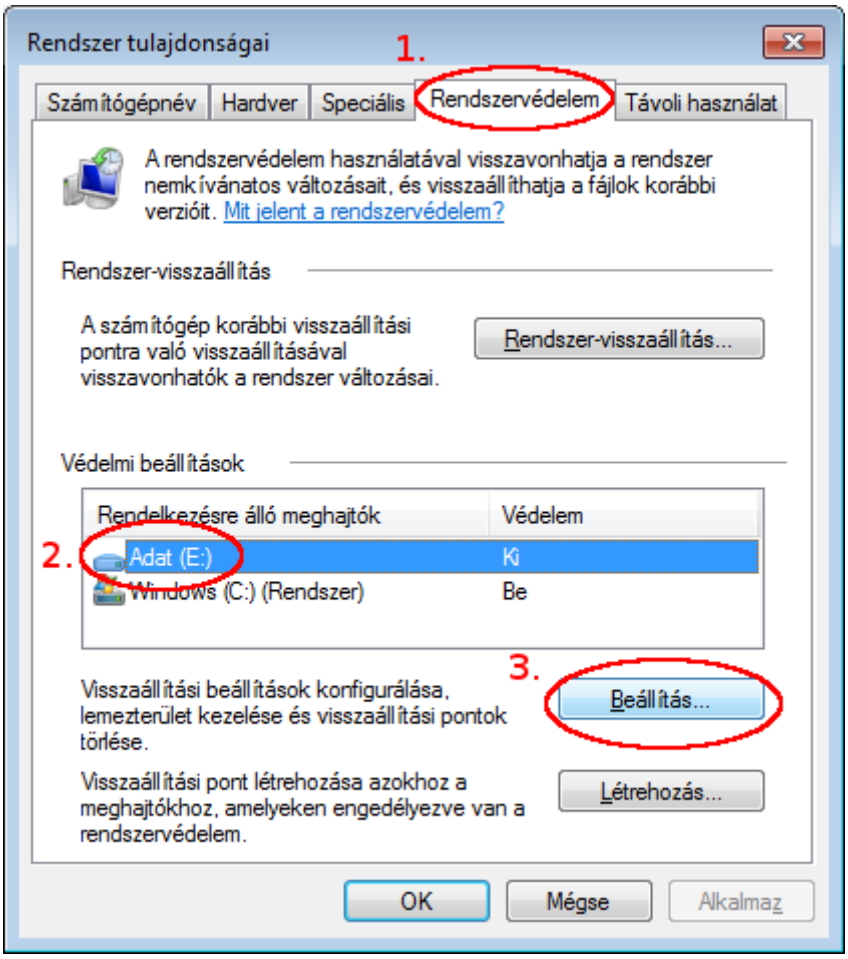
1. lépés:
Windows 7: a Start gombra kattintva a jobb oldali menüben láthatjuk a "**Számítógép**" menüpontot, ahol jobb egérgombbal kattintva a "**Tulajdonságok**" menüpontot kell kiválasztanunk.
Windows 8, 10: nyomjuk le a Windows gombot, majd keressünk a "**Rendszer**" kifejezésre (kezdjünk el gépelni). Nyomjunk "ENTER" billentyűt az első találat megnyitásához.



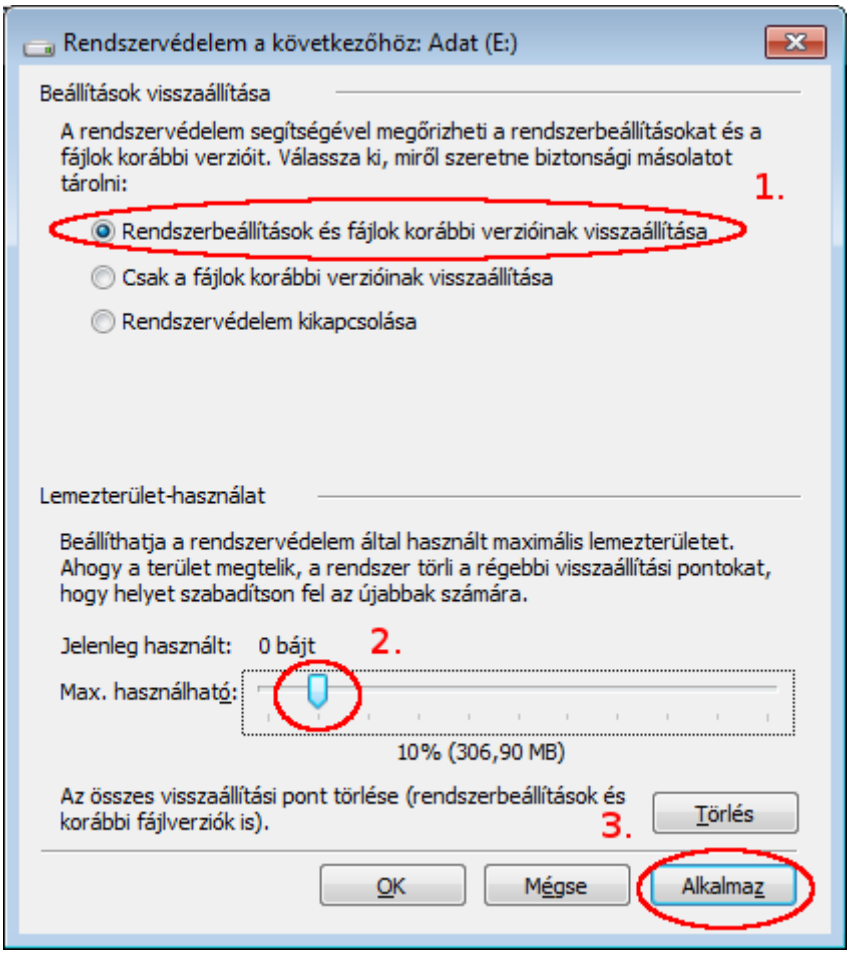
2. lépés: Bal oldalon kattintsunk a "**Speciális rendszerbeállítások**" menüelemre.



3. lépés: A "**Rendszervédelem**" fülön válasszuk ki azt a meghajtót, ahol ki van kapcsolva a rendszer-visszaállítás, majd a "**Beállítás**" gombra kattintsunk.



4. lépés: Kapcsoljuk be a rendszer-visszaállítást a képen látható módon. Adjunk meg 10% használható területet, majd alkalmazzuk a beállításokat.

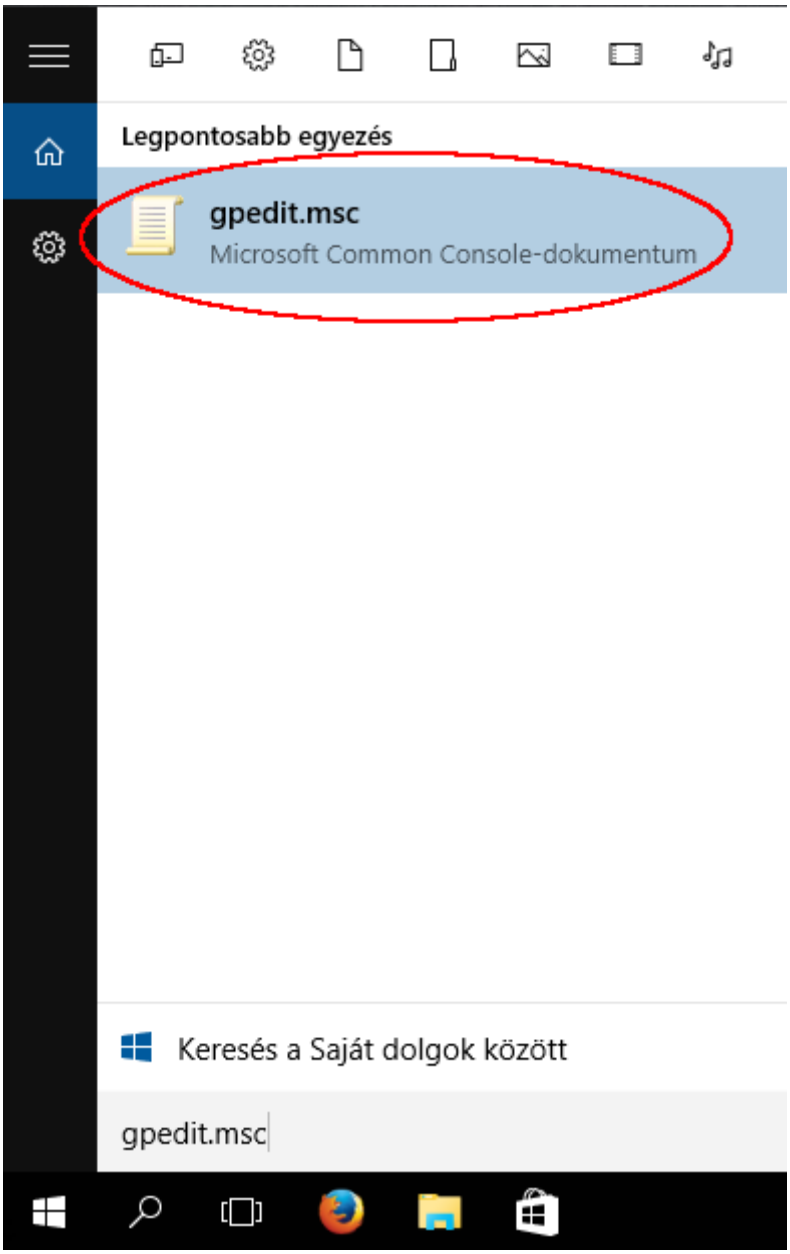


Rendszer-helyreállító lemez készítése: Windows rendszereken lehetőségünk van rendszer-helyreállító lemez készítésére. Ehhez helyezzünk egy CD/DVD lemezt (erre a célra vásárolhatunk újraiírható lemezt) a meghajtóba, majd a "Windows" gombot lenyomva keressünk a "**rendszer-helyreállító**" kifejezésre. Nyissuk meg a programot, válasszuk ki a meghajtót, majd kattintsunk a "**Lemez létrehozása gombra**".

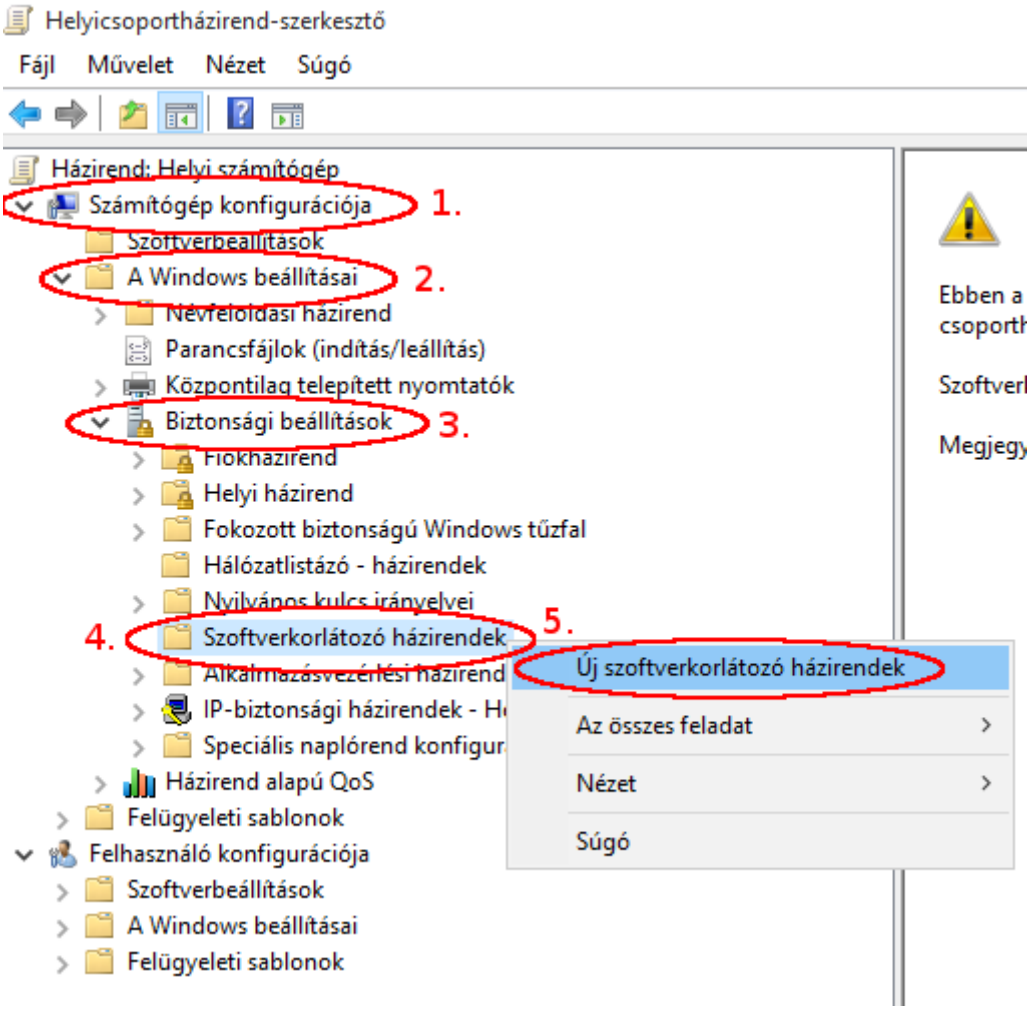
VIII. Programfuttatás letiltása a %AppData%, %LocalAppData%, %ProgramData%, %Temp% könyvtárakban:

A felsorolt könyvtárakban nagy a valószínűsége az ártalmas kód futtatásnak. Többnyire rejtett, vagy nehezen elérhetőek, így az átlag felhasználó elől rejtve maradnak. Ismert ransomware programok használják ezeket a könyvtárakat. A Group Policy Editor használatával (**gpedit.msc**), korlátozó szabályokat tudunk létrehozni a fertőzés megelőzésének érdekében. Windows 7 Starter, Home Basic és Home Premium rendszereken ez a funkció nem áll rendelkezésre.

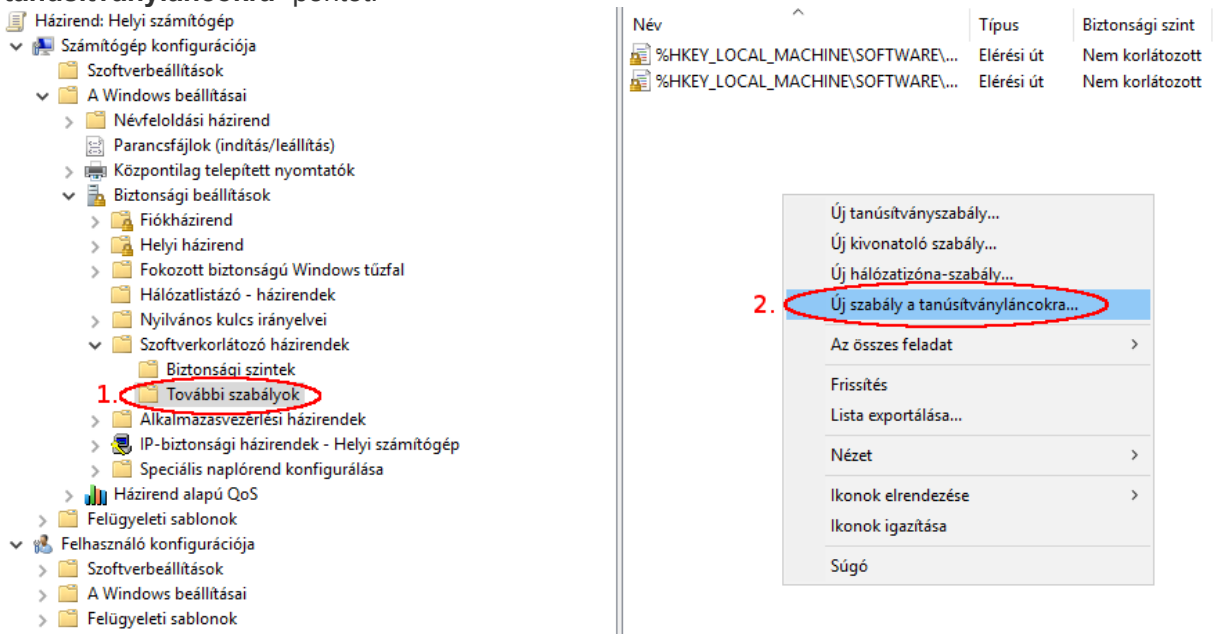
1. lépés: A Start menüben keressünk rá a "**gpedit.msc**" kifejezésre, majd nyissuk meg a programot.



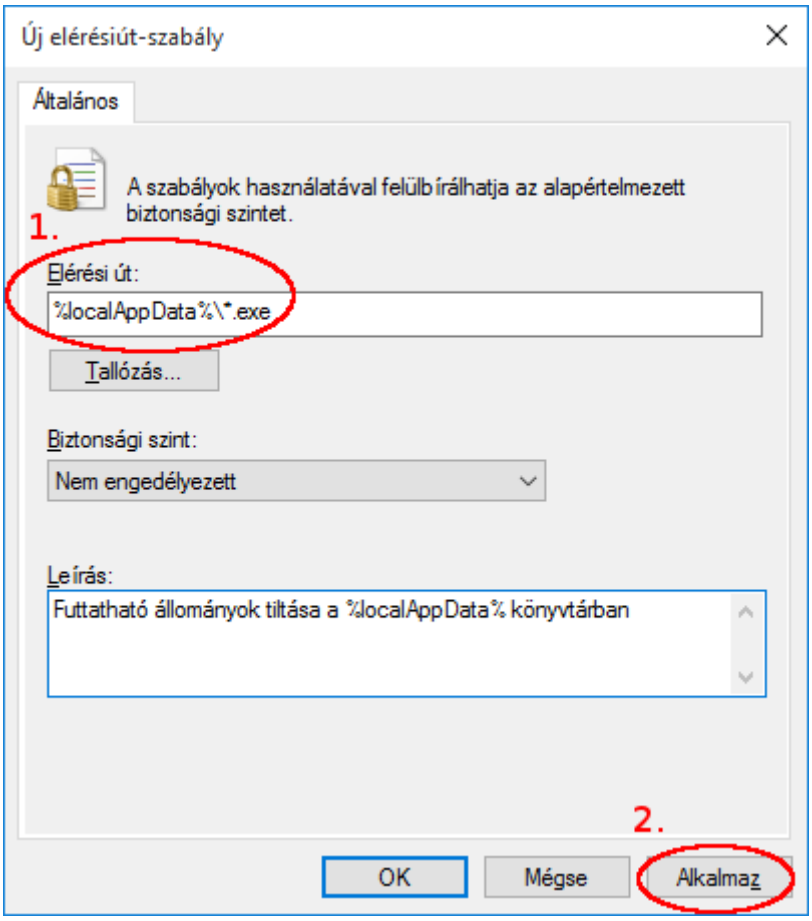
2. lépés: Navigáljunk a "**Számítógép konfigurációja**" >> "**Windows beállításai**" >> "**Biztonsági beállítások**" menü alatti "**Szoftverkorlátozó házirendek**" mappára, majd kattintsunk jobb klikkel, és válasszuk ki az "**Új szoftverkorlátozó házirendek**" pontot.



3. lépés: a "**Szoftverkorlátozó házirendek**" alatt ekkor megjelenik a "**További szabályok**" mappa, kattintsunk bele. Itt, a jobb klikkes menüben válasszuk az "**Új szabály a tanúsítványláncokra**" pontot.



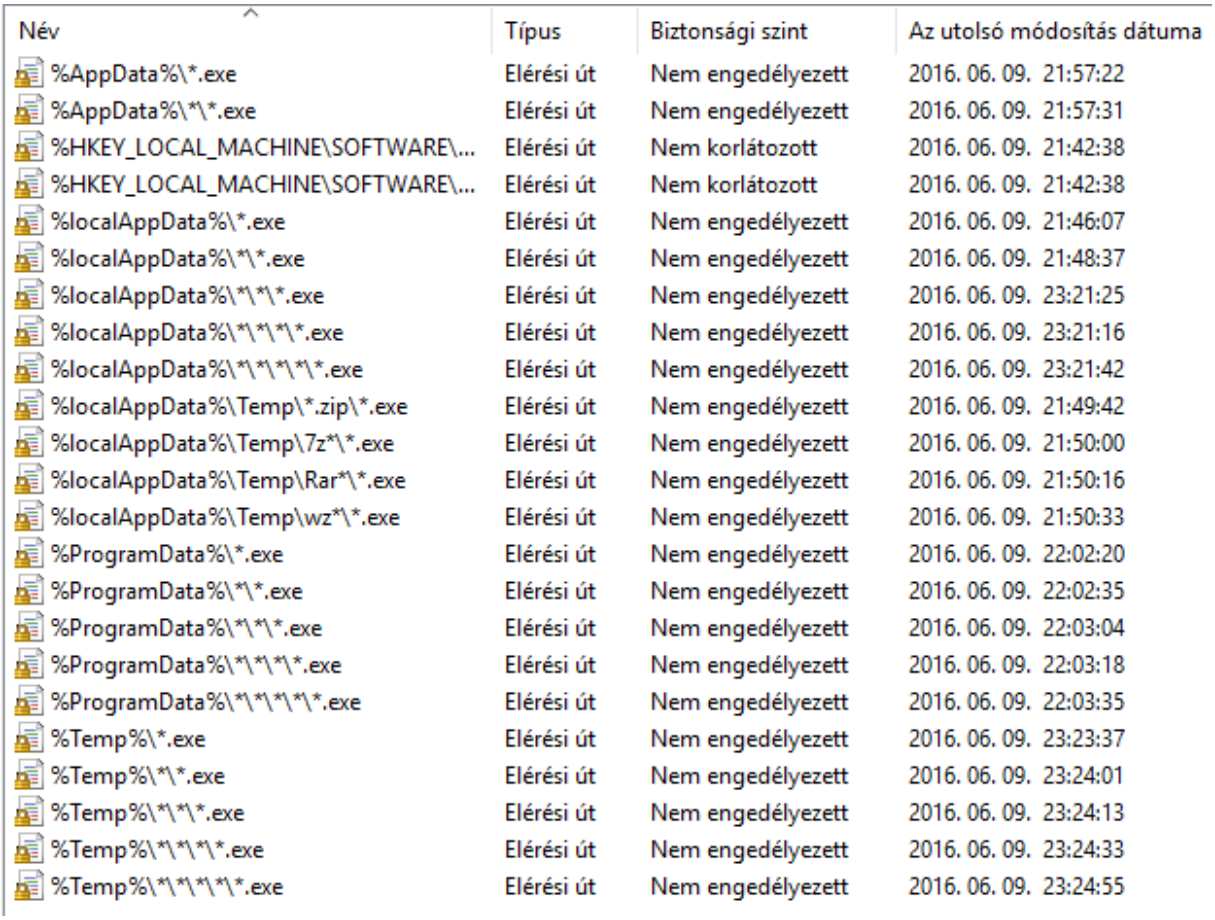
4. lépés: itt elérési útnak adjuk meg az alábbi paramétereket, majd alkalmazzuk a beállításokat.



5. lépés: egyesével végezzük el minden szükséges paraméter felvitelét:

%AppData%*.exe
%AppData%**.exe
%localAppData%*.exe
%localAppData%**.exe
%localAppData%***.exe
%localAppData%****.exe
%localAppData%*****.exe
%localAppData%\Temp*.zip*.exe
%localAppData%\Temp\7z**.exe
%localAppData%\Temp\Rar**.exe
%localAppData%\Temp\wz**.exe
%ProgramData%*.exe
%ProgramData%**.exe
%ProgramData%***.exe
%ProgramData%****.exe
%ProgramData%*****.exe
%Temp%*.exe
%Temp%**.exe
%Temp%***.exe
%Temp%****.exe
%Temp%*****.exe

A végeredménynek hasonlóképpen kell kinéznie:

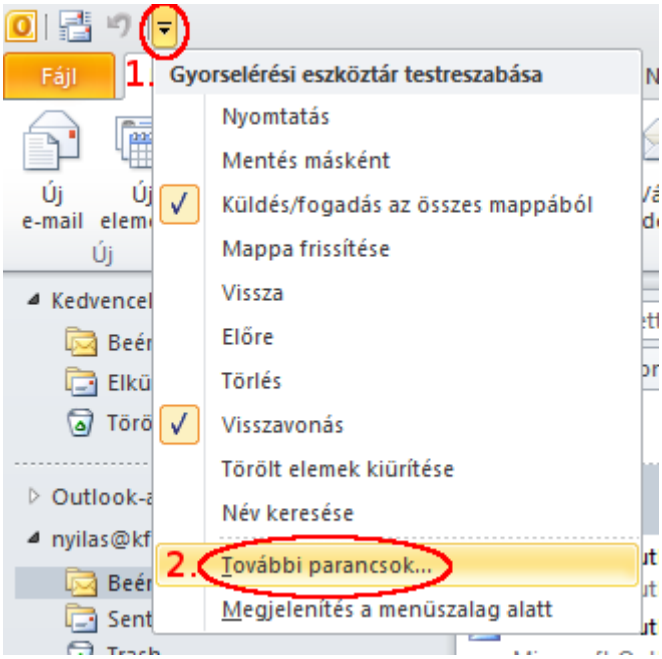


Név	Típus	Biztonsági szint	Az utolsó módosítás dátuma
%AppData%*.exe	Elérési út	Nem engedélyezett	2016. 06. 09. 21:57:22
%AppData%**.exe	Elérési út	Nem engedélyezett	2016. 06. 09. 21:57:31
%HKEY_LOCAL_MACHINE\SOFTWARE\...	Elérési út	Nem korlátozott	2016. 06. 09. 21:42:38
%HKEY_LOCAL_MACHINE\SOFTWARE\...	Elérési út	Nem korlátozott	2016. 06. 09. 21:42:38
%localAppData%*.exe	Elérési út	Nem engedélyezett	2016. 06. 09. 21:46:07
%localAppData%**.exe	Elérési út	Nem engedélyezett	2016. 06. 09. 21:48:37
%localAppData%***.exe	Elérési út	Nem engedélyezett	2016. 06. 09. 23:21:25
%localAppData%****.exe	Elérési út	Nem engedélyezett	2016. 06. 09. 23:21:16
%localAppData%*****.exe	Elérési út	Nem engedélyezett	2016. 06. 09. 23:21:42
%localAppData%\Temp*.zip*.exe	Elérési út	Nem engedélyezett	2016. 06. 09. 21:49:42
%localAppData%\Temp\7z**.exe	Elérési út	Nem engedélyezett	2016. 06. 09. 21:50:00
%localAppData%\Temp\Rar**.exe	Elérési út	Nem engedélyezett	2016. 06. 09. 21:50:16
%localAppData%\Temp\wz**.exe	Elérési út	Nem engedélyezett	2016. 06. 09. 21:50:33
%ProgramData%*.exe	Elérési út	Nem engedélyezett	2016. 06. 09. 22:02:20
%ProgramData%**.exe	Elérési út	Nem engedélyezett	2016. 06. 09. 22:02:35
%ProgramData%***.exe	Elérési út	Nem engedélyezett	2016. 06. 09. 22:03:04
%ProgramData%****.exe	Elérési út	Nem engedélyezett	2016. 06. 09. 22:03:18
%ProgramData%*****.exe	Elérési út	Nem engedélyezett	2016. 06. 09. 22:03:35
%Temp%*.exe	Elérési út	Nem engedélyezett	2016. 06. 09. 23:23:37
%Temp%**.exe	Elérési út	Nem engedélyezett	2016. 06. 09. 23:24:01
%Temp%***.exe	Elérési út	Nem engedélyezett	2016. 06. 09. 23:24:13
%Temp%****.exe	Elérési út	Nem engedélyezett	2016. 06. 09. 23:24:33
%Temp%*****.exe	Elérési út	Nem engedélyezett	2016. 06. 09. 23:24:55

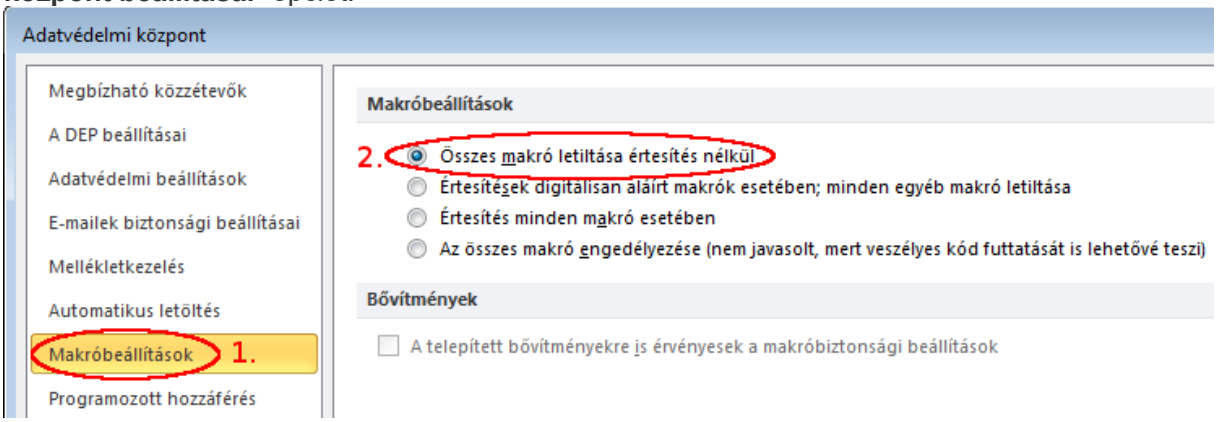
IX. Makrók futtatásának letiltása MS Outlook levelezőprogramban (és MS Office irodai programcsomagban):

A makrók nagy általánosságban automatizált feladatok elvégzésére írt scriptek. Ettől függetlenül rosszindulatú kódok futtatására is alkalmasak. Amennyiben nincs rájuk szükségünk, ajánlott őket letiltani. Az alábbi lépések a MS Office irodai csomagra is érvényesek, a menürendszer ugyanaz!

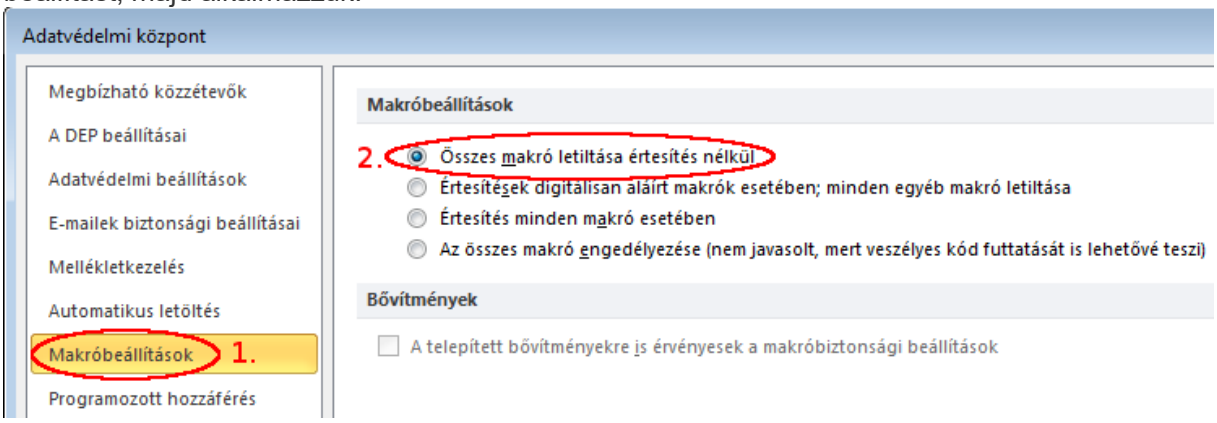
1. lépés: kattintsunk az ablak fejlécén található lefele mutató nyílra, majd a "**További parancsok**" menüpontra.



2. lépés: a megjelenő új ablakban válasszuk az "**Adatvédelmi központ**", majd az "**Adatvédelmi központ beállításai**" opciót.



3. lépés: a "**Makróbeállítások**" alatt kapcsoljuk be az "**Összes makró letiltása értesítés nélkül**" beállítást, majd alkalmazzuk.



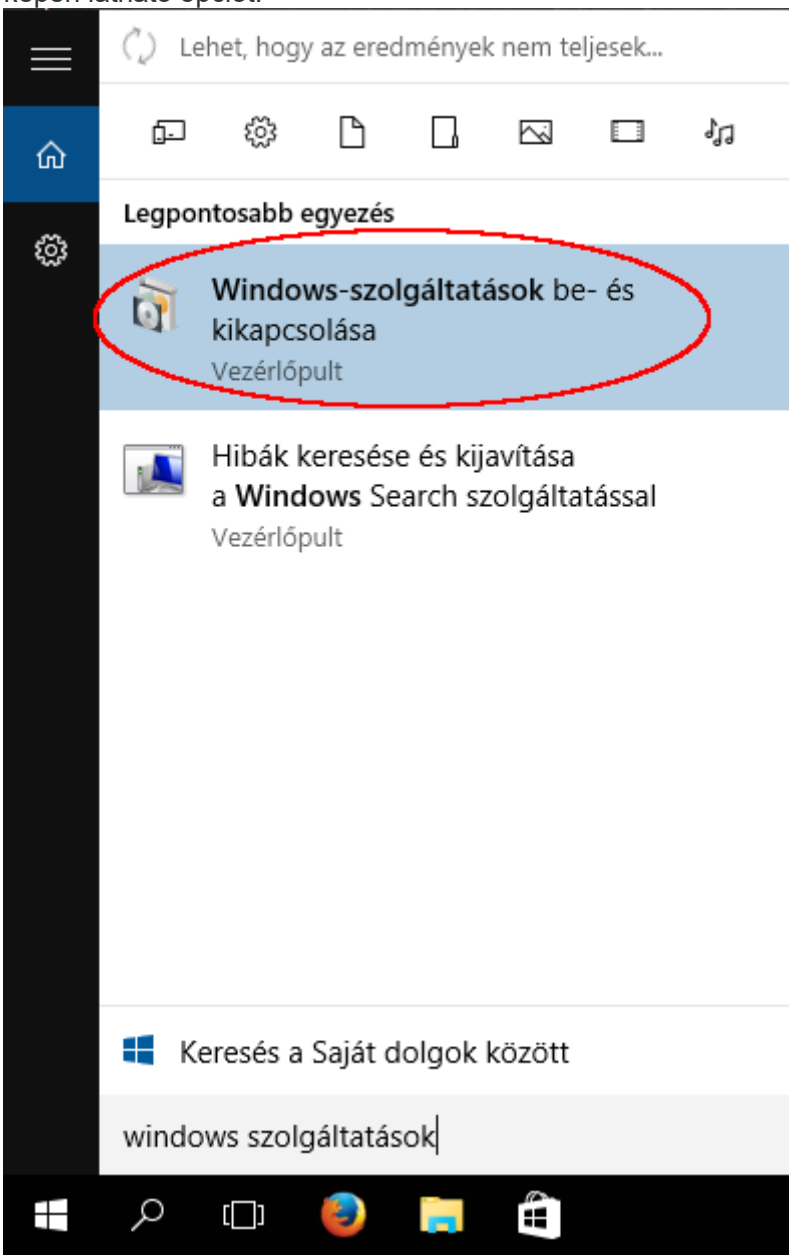
X. Powershell letiltása:

Az úgynevezett "PowerShell Shellcode injection" támadások ellen, védekezésképp letilthatjuk a PowerShell programot. Erre átlag felhasználónak vajmi kevés szüksége van.

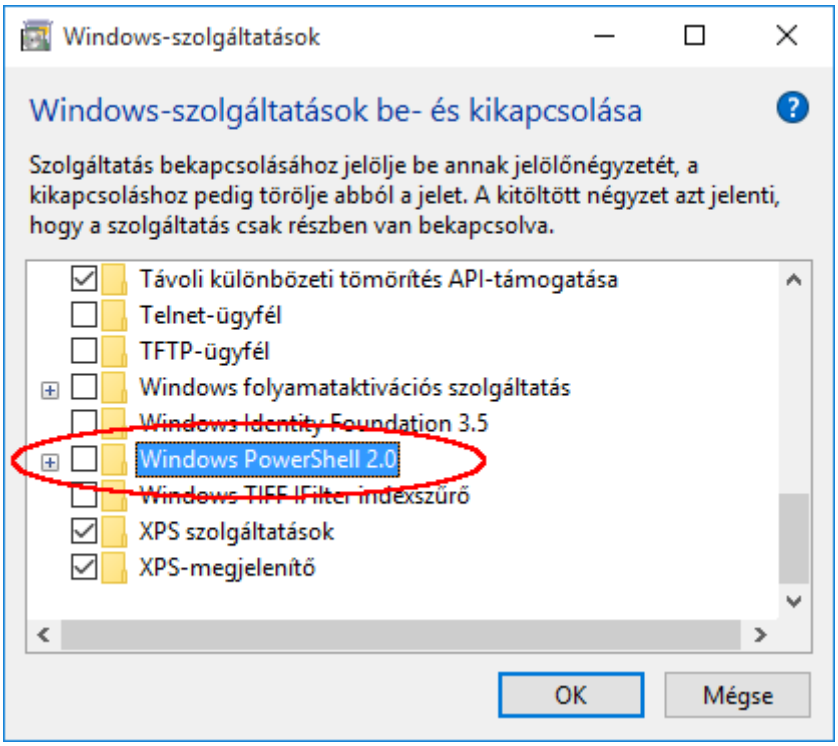
Windows 7: ezen rendszereken nem elérhető a PowerShell kikapcsolása. Bizonyos könyvtárak átnevezésével viszont elérhetetlenné tehetjük a kártékony programok számára a PowerShellt: Nyissuk meg a Parancssort, majd adjuk ki a következő parancsokat:

```
move C:\Windows\System32\WindowsPowerShell
C:\Windows\System32\WindowsPowerShellBackup
move C:\Windows\SysWOW64\WindowsPowerShell
C:\Windows\SysWOW64\WindowsPowerShellBackup
```

Windows 8, 10:
1. lépés: A Start menüben keressünk rá a "windows szolgáltatások" kifejezésre, majd válasszuk a képen látható opciót.



2. lépés: tekerjük le a csúszkát a megnyíló ablakban, majd vegyük ki a pipát a "Windows PowerShell 2.0" szolgáltatásból. Kattinsunk az "Ok" gombra.



3. lépés: a beállítások elvégzése után a Windows értesít bennünket, ekkor zárjuk be az ablakot.
XII. Teendők észlelt fertőzéskor: a ransomware programok képesek hálózati megosztásokat is titkosítani, így mindenféleképpen húzza le a gépét a hálózatról (vezetékes és WiFi egyaránt), vagy kapcsolja ki, majd szóljon a rendszergazdájának!