




















































# Autorun

| Autorun Entry   | Description                         | Publisher                                   | Image Path                                 | Timestamp           | VirusTotal |
|---|-------------------------------------|---|--|---------------------|------------|
|  HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell         |                                     |   |  | 2019. 12. 07. 10:15 |            |
|  cmd.exe   | Windows Command Processor           | (Verified) Microsoft Windows                | c:\windows\system32\cmd.exe                | 1953. 12. 11. 3:58  |            |
|  HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run                    |                                     |   |  | 2021. 02. 21. 12:34 |            |
|  RTHDVCPL  | Realtek HD Audio Manager            | (Verified) Realtek Semiconductor Corp.      | c:\program files\realtek\audio\hda\vt...   | 2017. 01. 09. 8:46  |            |
|  HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run        |                                     |   |  | 2021. 02. 21. 12:50 |            |
|  Dropbox   | Dropbox                             | (Verified) Dropbox, Inc.                    | c:\program files (x86)\dropbox\client\...  | 1995. 02. 14. 6:37  |            |
|  SunJavaUpdateSched  | Java Update Scheduler               | (Verified) Oracle America, Inc.             | c:\program files (x86)\common files\...    | 2020. 12. 09. 16:36 |            |
|  TeamsMachineInstaller   | Microsoft Teams                     | (Verified) Microsoft Corporation            | c:\program files (x86)\teams installer\... | 2020. 08. 28. 19:30 |            |
|  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run                    |                                     |   |  | 2021. 02. 20. 20:53 |            |
|  com.squirrel.Teams.Teams  | Microsoft Teams                     | (Verified) Microsoft 3rd Party Applicati... | c:\users\veres\appdata\local\microso...    | 2020. 10. 02. 13:48 |            |
|  Discord   | Update                              | (Verified) Discord Inc.                     | c:\users\veres\appdata\local\discor...     | 2020. 06. 01. 21:58 |            |
|  Gajin.Net Updater   | Gajin.Net Updater                   | (Verified) Gajin Network LTD                | c:\users\veres\appdata\local\gajin\...     | 2020. 12. 03. 14:41 |            |
|  Steam   | Steam Client Bootstrapper           | (Verified) Valve                            | c:\program files (x86)\steam\steam.exe     | 2021. 02. 13. 0:23  |            |
|  HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components             |                                     |   |  | 2021. 02. 20. 19:10 |            |
|  Google Chrome   | Google Chrome Installer             | (Verified) Google LLC                       | c:\program files\google\chrome\appli...    | 2021. 02. 13. 0:08  |            |
|  Microsoft Edge  | Microsoft Edge Installer            | (Verified) Microsoft Corporation            | c:\program files (x86)\microsoft\edge...   | 2021. 02. 17. 4:41  |            |
|  n/a   | Microsoft .NET IE SECURITY REGIS... | (Verified) Microsoft Corporation            | c:\windows\system32\mscories.dll           | 2019. 10. 25. 4:45  |            |
|  HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components |                                     |   |  | 2021. 02. 05. 2:13  |            |
|  n/a   | Microsoft .NET IE SECURITY REGIS... | (Verified) Microsoft Corporation            | c:\windows\syswow64\mscories.dll           | 2019. 10. 25. 9:48  |            |
|  HKLM\SOFTWARE\Classes\Protocols\Filter                                |                                     |   |  | 2021. 02. 21. 8:31  |            |
|  text/xml  | Microsoft Office XML MIME Filter    | (Verified) Microsoft Corporation            | c:\program files\microsoft office\root\... | 2020. 12. 28. 23:39 |            |
|  HKLM\SOFTWARE\Classes\Protocols\Handler                               |                                     |   |  | 2021. 02. 21. 8:31  |            |
|  mso-minsb-roaming.16  | Microsoft Office component          | (Verified) Microsoft Corporation            | c:\program files\microsoft office\root\... | 2020. 12. 28. 23:33 |            |
|  mso-minsb.16  | Microsoft Office component          | (Verified) Microsoft Corporation            | c:\program files\microsoft office\root\... | 2020. 12. 28. 23:33 |            |
|  osf-roaming.16  | Microsoft Office component          | (Verified) Microsoft Corporation            | c:\program files\microsoft office\root\... | 2020. 12. 28. 23:33 |            |
|  osf.16  | Microsoft Office component          | (Verified) Microsoft Corporation            | c:\program files\microsoft office\root\... | 2020. 12. 28. 23:33 |            |
|  HKLM\Software\Classes\ShellEx\ContextMenuHandlers                     |                                     |   |  | 2021. 02. 21. 12:50 |            |
|  ANotepad++64  | ShellHandler for Notepad++ (64 bit) | (Verified) Notepad++                        | c:\program files (x86)\notepad++\vp...     | 2014. 05. 12. 10:49 |            |
|  DropboxExt  | Dropbox Shell Extension             | (Verified) Dropbox, Inc.                    | c:\program files (x86)\dropbox\client\...  | 1986. 10. 11. 2:15  |            |
|  WinRAR  | WinRAR shell extension              | (Verified) win.rar GmbH                     | c:\program files\winrar\warext.dll         | 2020. 12. 01. 19:00 |            |
|  HKLM\Software\Classes\Directory\ShellEx\ContextMenuHandlers           |                                     |   |  | 2021. 02. 21. 12:50 |            |
|  DropboxExt  | Dropbox Shell Extension             | (Verified) Dropbox, Inc.                    | c:\program files (x86)\dropbox\client\...  | 1986. 10. 11. 2:15  |            |

Az Autorun gyakorlatilag kilistázza hogy a Windows indításakor mely szolgáltatások indulnak el. Különféle kategóriák szerint szűrhetünk, az első képen minden ki van listázva. A másodikon csak a beütemezett folyamatok láthatóak

| Task Scheduler  |  |                                    |  |                     |  |
|---|--|------------------------------------|--|---------------------|--|
|  Microsoft Office\Office ... | Microsoft Office Click-to-Run Client   | (Verified) Microsoft Corporation   | c:\program files\common files\microso...   | 2021. 01. 30. 8:20  |  |
|  Microsoft Office\Office ... | Microsoft Office Click-to-Run Client   | (Verified) Microsoft Corporation   | c:\program files\common files\microso...   | 2021. 01. 30. 8:20  |  |
|  Microsoft Office\Office ... | Microsoft Office SDX Helper            | (Verified) Microsoft Corporation   | c:\program files\microsoft office\root\... | 2021. 02. 15. 20:20 |  |
|  Microsoft Office\Office ... | Microsoft Office SDX Helper            | (Verified) Microsoft Corporation   | c:\program files\microsoft office\root\... | 2021. 02. 15. 20:20 |  |
|  Microsoft Office\Office ... | Office Telemetry Dashboard Agent (O... | (Verified) Microsoft Corporation   | c:\program files\microsoft office\root\... | 2021. 01. 30. 8:26  |  |
|  Microsoft Office\Office ... | Office Telemetry Dashboard Agent (O... | (Verified) Microsoft Corporation   | c:\program files\microsoft office\root\... | 2021. 01. 30. 8:26  |  |
|  MSIAfterburner              | MSIAfterburner                         | (Verified) MICRO-STAR INTERNATI... | c:\program files (x86)\msi\afterburner...  | 2019. 10. 26. 12:05 |  |
|  NvBatteryBoostCheck...      | NVIDIA Container                       | (Verified) NVIDIA Corporation      | c:\program files\nvidia corporation\vn...  | 2020. 05. 06. 18:17 |  |
|  NvBroadcast_B2FE19...       | NVIDIA Broadcast                       | (Verified) NVIDIA Corporation      | c:\program files\nvidia corporation\vn...  | 2021. 01. 25. 17:38 |  |
|  NvDriverUpdateCheck...      | NVIDIA Container                       | (Verified) NVIDIA Corporation      | c:\program files\nvidia corporation\vn...  | 2020. 05. 06. 18:17 |  |
|  NVIDIA GeForce Exper...     | NVIDIA GeForce Experience              | (Verified) NVIDIA Corporation      | c:\program files\nvidia corporation\vn...  | 2021. 01. 27. 18:43 |  |
|  NvNodeLauncher_B2...        | NVIDIA nodes launcher                  | (Verified) NVIDIA Corporation      | c:\program files (x86)\nvidia corporati... | 2021. 01. 27. 18:19 |  |
|  NvProfileUpdaterDaily...    | NVIDIA driver profile updater          | (Verified) NVIDIA Corporation      | c:\program files\nvidia corporation\vn...  | 2021. 01. 20. 17:38 |  |
|  NvProfileUpdaterOnLo...     | NVIDIA driver profile updater          | (Verified) NVIDIA Corporation      | c:\program files\nvidia corporation\vn...  | 2021. 01. 20. 17:38 |  |
|  NvTmRep_CrashRepor...       | NVIDIA crash and telemetry reporter    | (Verified) NVIDIA Corporation      | c:\program files\nvidia corporation\vn...  | 2021. 01. 20. 17:49 |  |
|  NvTmRep_CrashRepor...       | NVIDIA crash and telemetry reporter    | (Verified) NVIDIA Corporation      | c:\program files\nvidia corporation\vn...  | 2021. 01. 20. 17:49 |  |
|  NvTmRep_CrashRepor...       | NVIDIA crash and telemetry reporter    | (Verified) NVIDIA Corporation      | c:\program files\nvidia corporation\vn...  | 2021. 01. 20. 17:49 |  |
|  NvTmRep_CrashRepor...       | NVIDIA crash and telemetry reporter    | (Verified) NVIDIA Corporation      | c:\program files\nvidia corporation\vn...  | 2021. 01. 20. 17:49 |  |
|  OneDrive Standalone ...     | Standalone Updater                     | (Verified) Microsoft Corporation   | c:\users\veres\appdata\local\microso...    | 1917. 03. 22. 7:46  |  |

Természetesen ezek szerkezhetőek, törölhetünk hozzáadhatunk folyamatokat, programokat ezen listákhoz.