

Evidence of persistence mechanisms:

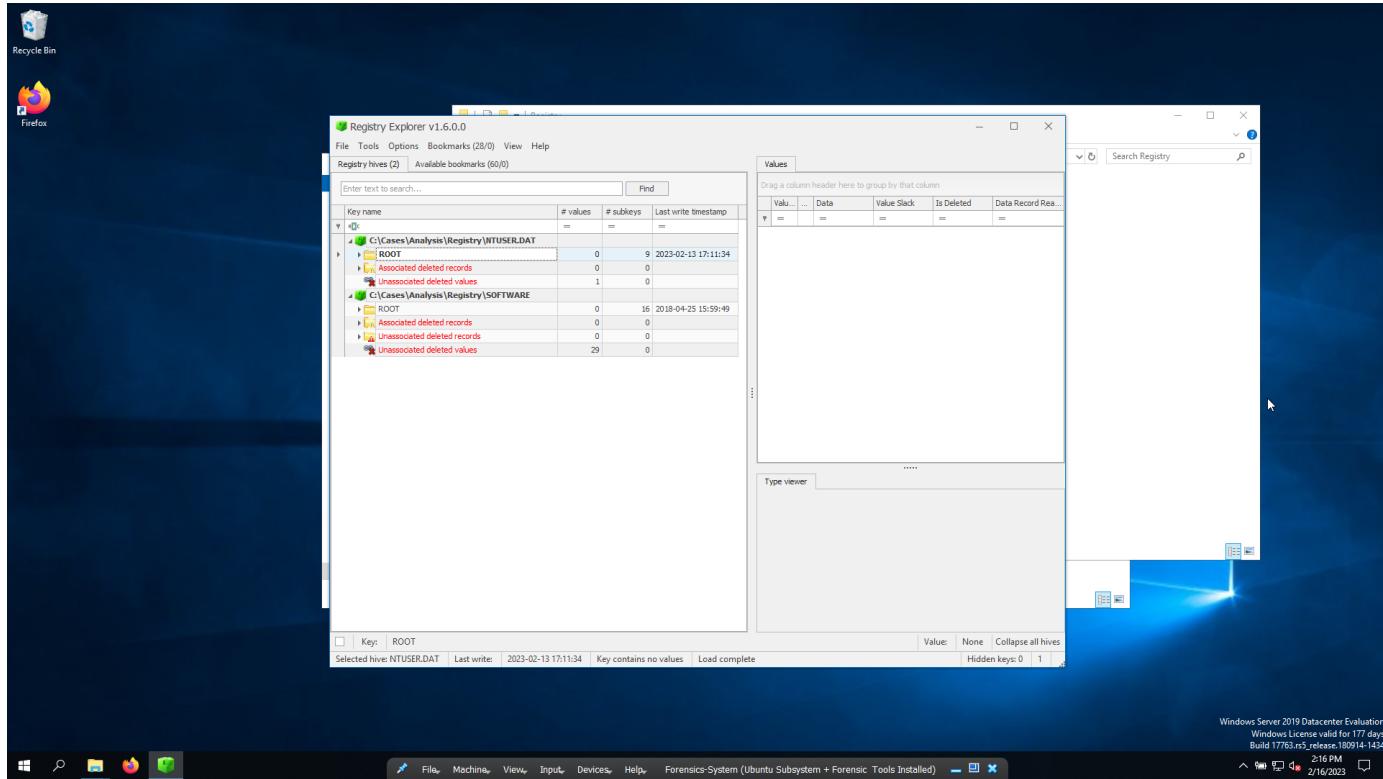
- Windows run keys
 - Startup Folders
 - Windows Services
 - Scheduled tasks
 - Sysinternals autoruns
- Find:
- Full path of AtomicService.exe that has been added to run keys.
 - Name of suspicious file in StartUp folder.
 - Time installation of atomic service.
 - What tasks did IEUser created, and what is the creation time.
 - How many times did they execute.

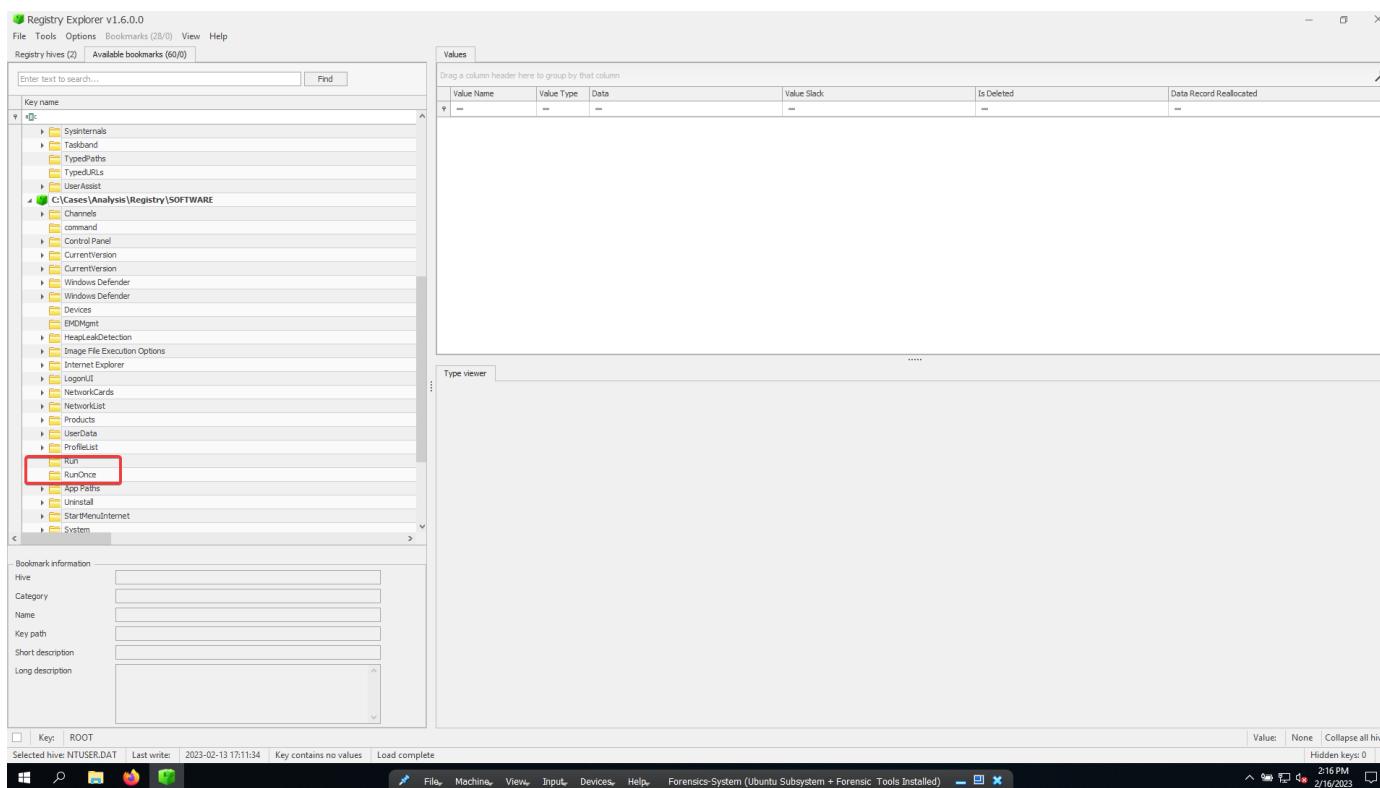
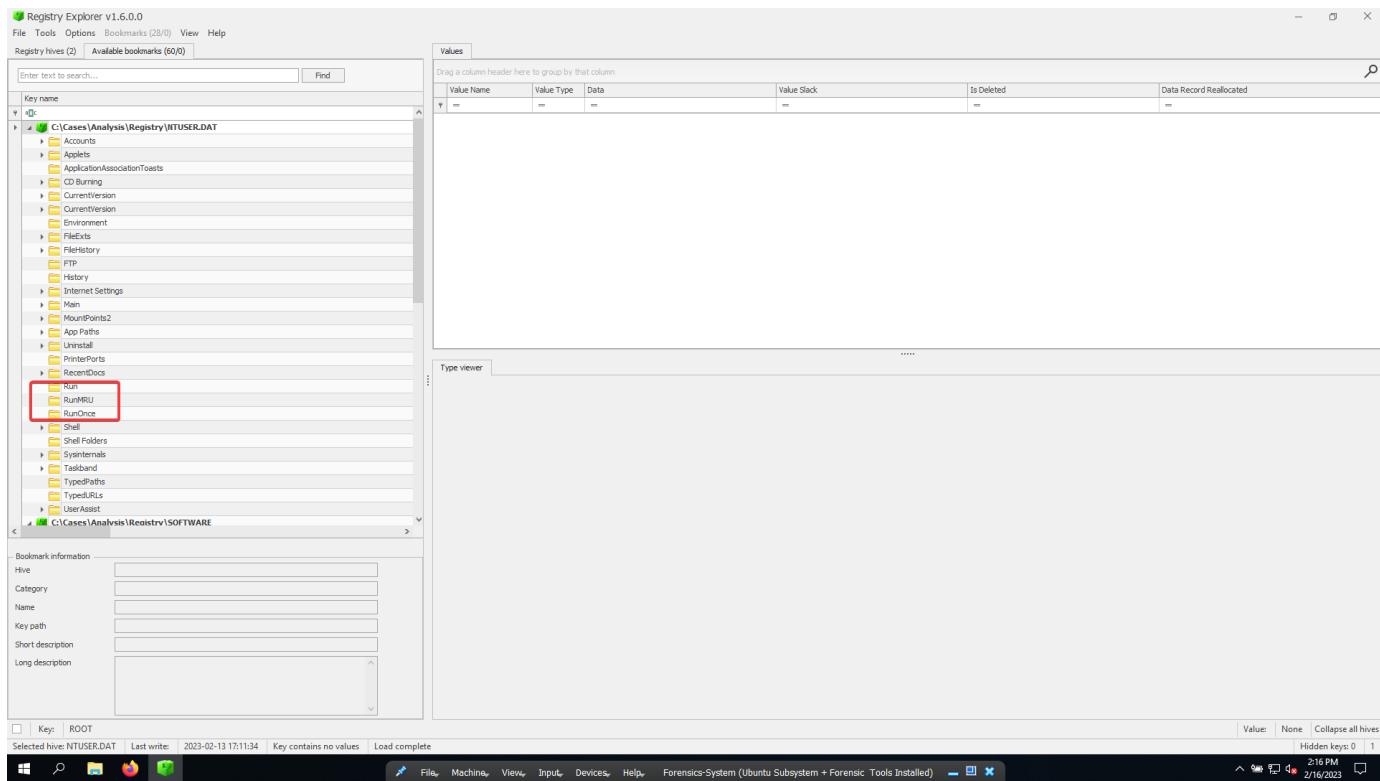
Windows run keys

- Location of the registries artifacts:
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
 - HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce
 - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
 - HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce

- In these registries, windows automatically loads, when boots up, those applications that are referenced in this subkeys.
- HKEY_CURRENT_USER: User specific run keys (Loads when the user logs in into the system)
- HKEY_LOCAL_MACHINE: System specific run keys (Loads anyway, does not depend on what user logs in)

- Investigate NTUSER.DAT and SOFTWARE hives:





- SOFTWARE hive:

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (28/0) View Help

Registry hives (2) Available bookmarks (60/0)

Enter text to search... Find

Key name: C:\Cases\Analysis\Registry\SOFTWARE\Run

Values

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
SecurityHealth	RegExpandSz	%ProgramFiles%\Windows Defender\MSASCUL.exe	00-00	<input type="checkbox"/>	<input type="checkbox"/>
VBoxTray	RegExpandSz	%SystemRoot%\system32\BoxTray.exe	00-00-00-00-00-00	<input type="checkbox"/>	<input type="checkbox"/>
bgrinfo	RegSz	C:\BgrInfo\bgrinfo.exe\acceptfile\jci\bgrinfo\bgrinfo...	73-5C-65-6E-2D-55	<input type="checkbox"/>	<input type="checkbox"/>

Type viewer Slack viewer Binary viewer

Value name: SecurityHealth

Value type: RegExpandSz

Value: %ProgramFiles%\Windows Defender\MSASCUL.exe

Raw value: 25-00-50-00-72-00-6F-00-67-00-72-00-61-00-6D-00-46-00-69-00-6C-00-65-00-73-00-25-00-5C-00-57-00-69-00-6E-00-64-00-6F-00-77-00-73-00-20-00-44-00-65-00-66-00-6E-00-64-00-65-00-72-00-5C-00-4D-00-53-00-41-00-53-00-43-00-75-00-9-00-4C-00-2E-00-65-00-78-00-65-00-00-00

Slack: 00-00

Bookmark information

Hive: C:\Cases\Analysis\Registry\SOFTWARE

Category: Autoruns

Name: Run

Key path: Microsoft\Windows\CurrentVersion\Run

Short description: Run key

Long description: Used to automatically start programs

Selected hive: NTUSER.DAT Last write: 2/13/2023 5:11:38 PM +00:00 3 of 3 values shown (100.00%) Value: SecurityHealth Collapse all hives Hidden keys: 0 1

File Machine View Input Devices Help Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) 2:18 PM 2/16/2023

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (28/0) View Help

Registry hives (2) Available bookmarks (60/0)

Enter text to search... Find

Key name: C:\Cases\Analysis\Registry\SOFTWARE\RunOnce

Values

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
—	—	—	—	—	—

Type viewer

Bookmark information

Hive: C:\Cases\Analysis\Registry\SOFTWARE

Category: Autoruns

Name: RunOnce

Key path: Microsoft\Windows\CurrentVersion\RunOnce

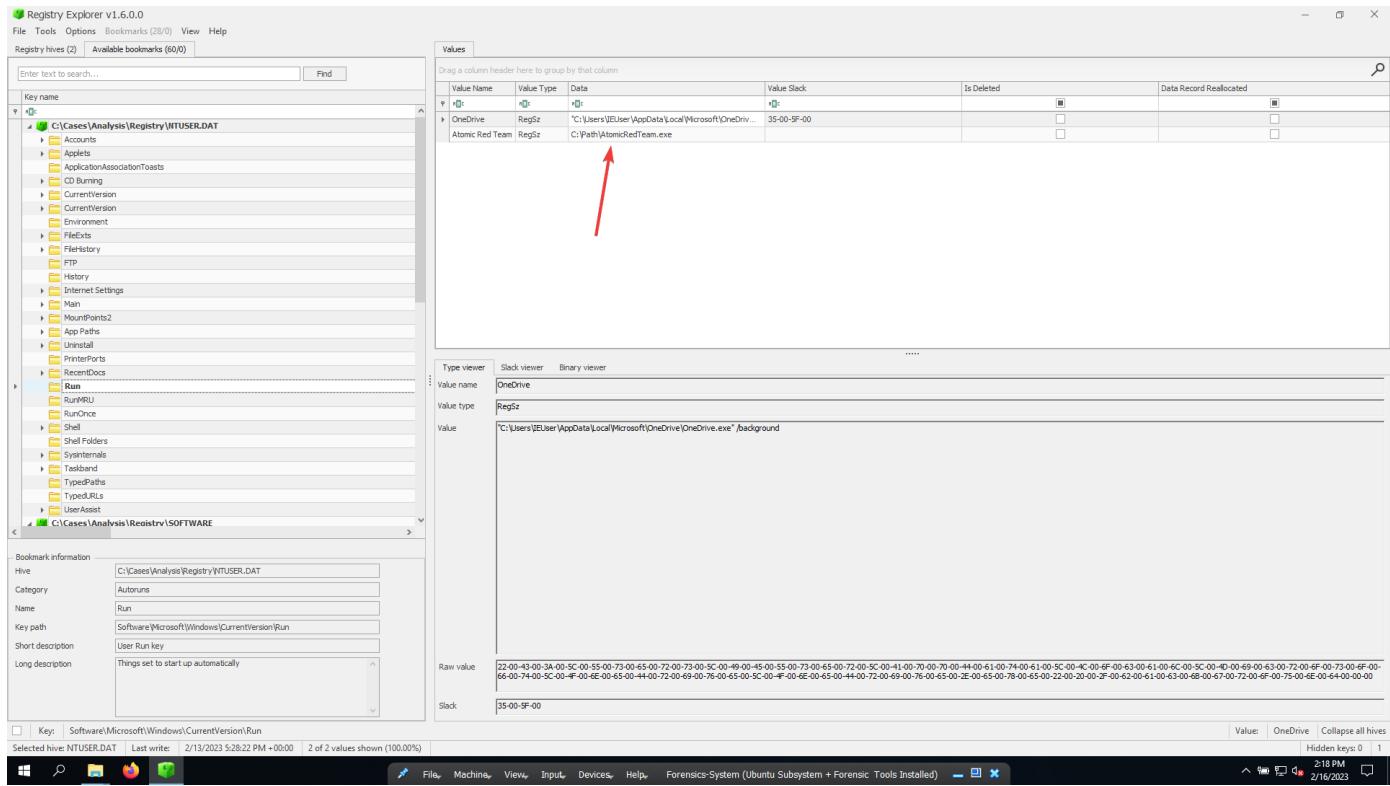
Short description: RunOnce (SOFTWARE)

Long description: RunOnce identifies programs that run only once at startup and can be assigned to a specific user account or to the machine

Selected hive: NTUSER.DAT Last write: 4/25/2018 4:00:17 PM +00:00 Key contains no values Value: None Collapse all hives Hidden keys: 0 1

File Machine View Input Devices Help Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) 2:18 PM 2/16/2023

- Nothing special, moving to NTUSER.DAT hive:



- Full path of AtomicService.exe that has been added to run keys.

C:\Path\AtomicRedTeam.exe

- This particular file, we cannot retrieve it or recover it , because it might have been deleted

- Search based on registry keys:

C:\Cases\Analysis\Registry\SYSTEM.mht - Notepad++ [Administrator]

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

Software SECURITY SYSTEM

140 0000000b 03e842e000100000 000a0000000000000000 Microsoft.XboxGameCallableUI cw5nh2ttxyewy neutral

141 00000009 000100015be00000 000a0000027410000 8664 Microsoft.NET.Native.Runtime.i.1.1 Swekyb3d8bbwe

142 00000009 a000a00042ee0001 000a00033900000 8664 Microsoft.ECApp Swekyb3d8bbwe

143 00000009 000a000042ee0001 000a0000000000000000 8664 Microsoft.Windows.SecureAssessmentBrowser cw5nh2ttxyewy neutral

144 C:\Windows\system32\sysmain.exe 2018-04-11 23:34:19

145 C:\Program Files\Avast\Avast\avast.exe 2015-01-14 02:39:11

146 00000008 000a000042ee0001 000a00003390000 8664 Microsoft.AsyncTextService Swekyb3d8bbwe

147 00000009 a000a2d8a4300000 000a00042800000 8664 Microsoft.ZuneVideo Swekyb3d8bbwe

148 00000009 000100061470000 000a000027410000 8664 Microsoft.NET.Native.Runtime.i.6 Swekyb3d8bbwe

149 C:\Windows\system32\mpaint.exe 2018-04-11 23:34:19

150 C:\Users\LEADER\AppData\Local\Microsoft\OneDrive\StandaloneUpdater\MicrosoftEdgeWebView2Setup.exe 2023-02-13 17:08:44

151 C:\Users\LEADER\AppData\Local\Temp\{F976CAF8-2F12-4069-BBC8-EAF7770C871}\MsSigStub.exe 2018-04-11 23:34:12

152 C:\Windows\System32\wcmcons.exe 2018-04-11 23:34:37

153 C:\Users\LEADER\AppData\Local\Microsoft\EdgeUpdate\MicrosoftEdgeUpdate.exe 2023-02-13 17:08:44

154 C:\ProgramData\Microsoft\Windows Defender\platform\4.16.17613.18039-0\MpCmdRun.exe 2018-04-25 15:57:31

155 C:\Windows\system32\svcsvc.exe 2018-04-11 23:34:40

156 C:\Windows\system32\OneDriveSetup\OneDriveSetupStub.exe 2023-02-13 17:05:16

157 C:\Windows\system32\wupshost.exe 2018-04-11 23:34:38

158 00000009 3e537f4534600000 000a00042ee0001 8664 Microsoft.windowscommunications Find

159 00000009 000100076b150000 000a000027410000 8664 Microsoft.NET.Native.Fx2 Find

160 C:\Users\LEADER\AppData\Local\Microsoft\OneDrive\StandaloneUpdater\OneDriveSetup.exe Find

161 00000009 a000a0003540000 000a00004610000 8664 Microsoft.DesktopAppInst Find

162 00000009 000100032200000 000a000078a0000 8664 Microsoft.Xaml.2.3 Find

163 00000009 000a00003660000 000a00004610000 8664 Microsoft.SkypeApp kf8f Find

164 C:\Windows\sys\KWN64\yezsvr32.exe 2018-04-11 23:35:00

165 C:\Windows\system32\unrempg2.exe 2018-04-11 06:39:00

166 SIGN.MEDIA=1\$FF7FVBxWindowAdditions-anded4.exe 2018-02-26 15:08:47

167 SIGN.MEDIA=SACACAmcacheParser.exe 2023-02-11 11:30:09

168 C:\Windows\system32\sysmain.exe 2018-04-11 23:34:22

169 C:\Windows\system32\lmsvc.exe 2018-04-11 23:34:17

170 C:\Users\LEADER\AppData\Local\Microsoft\OneDrive\17.3.6516.0313\FileSyncConfig.exe

171 00000009 a000a6a25c90000 000a0003fa0000 8664 Microsoft.GetHelp Swek

172 C:\Windows\system32\MDMAgent.exe 2018-04-11 23:34:41

173 00000008 a000a00042ee0001 000a000042ee0001 8664 Microsoft.Windows.Capture

174 00000008 0002a00000000000 000a000042ee0001 8664 Microsoft.UI.Xaml.2.4

175 C:\Windows\system32\wbinddeploy.exe 2018-04-11 23:34:34

176 C:\Windows\System32\RuntimeBroker.exe 2018-04-11 23:34:06

177 C:\Acumatica\Team\AcumaticaT1543.003\bin\AcumaticaService.exe 2022-04-28 01:14:47

178 C:\Windows\System32\Speech_OneCore\Common\SpeechRuntime.exe 2018-04-11 23:34:17

179 00000009 000200273480000 000a000027410000 8664 Microsoft.NET.Native.Fx2

180 C:\Windows\system32\wcmcons.exe 2018-04-11 23:34:49

181 C:\Windows\system32\cmd.exe 2018-04-11 23:34:49

182 00000009 000a00042ee0001 000a00003fa0000 8664 Microsoft.Windows.SeHealthUI cw5nh2ttxyewy

183 SIGN.MEDIA=1\$FC541VBxWindowAdditions.exe 2023-01-11 14:38:18

184 00000008 000a00000203e8 000a000042ee0001 8664 windows.immersivecontrolpanel cw5nh2ttxyewy neutral

185 C:\Windows\System32\WScript.exe 2018-04-11 23:34:13

186 C:\Windows\system32\7zip\7z.dll 2018-04-11 23:34:09

187 C:\Windows\sys\KWN64\cmd.exe 2018-04-11 23:34:49

188 C:\Windows\system32\SgrmBroker.exe 2018-04-11 23:34:04

189 C:\Users\LEADER\AppData\Local\Microsoft\EdgeUpdate\1.1.731.45\MicrosoftEdgeUpdateCore.exe 2023-02-13 17:08:45

190 00000009 a000a00042ee0001 000a000042ee0001 8664 Microsoft.Windows.PeopleExperienceHost cw5nh2ttxyewy neutral

191 C:\Windows\system32\onecoreui.exe 2018-04-11 23:34:12

192 C:\Windows\system32\desigconhost.exe 2018-04-11 23:34:22

193 00000008 03e842e000100000 000a0002580000 8664 Microsoft.AAD.BrokerPlugin cw5nh2ttxyewy neutral

194 C:\Windows\system32\MSched.exe 2018-04-11 23:34:43

195 C:\Users\LEADER\AppData\Local\Temp\{F976CAF8-2F12-4069-BBC8-EAF7770C871}\MsSigStub.exe 2018-04-25 15:58:43

196 00000009 000a06a90040000 000a0002800000 8664 Microsoft.Advertising.Xaml Swekyb3d8bbwe

Normal text file length: 364,933 lines: 6,970 Ln:157 Col:55 Sel:2|1 Windows (CR LF) UTF-8 INS

```

C:\Cases\Analysis\Registry\SOFTWARE.txt - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
[Software.dat] [Security.txt] [Default.txt] [NTUSER.DAT.txt] [SAM.txt] [UserClasses.dat.txt] [bam.p1] [SYSTEM.txt]

39781 pologging.v.00200515
39782 (NTUSER.DAT, Software) Extracts PowerShell logging settings
39783
39784 Software\Policies\Microsoft\Windows\PowerShell not found.
39785 Policies\Microsoft\Windows\PowerShell not found.
39786 -----
39787 run v.20200511
39788 (Software, NTUSER.DAT) [Autostart] Get autostart key contents from Software hive
39789
39790 Microsoft\Windows\CurrentVersion\Run
39791 LastWrite Time 2023-02-13 17:11:39Z
39792 VBoxTray = %SystemRoot%\system32\VBoxTray.exe
39793 SecurityHealth = %ProgramFiles%\Windows Defender\MSASCuIL.exe
39794 bginfo = C:\BInfo\BgInfo.exe /accepteula /i:c:\bginfo\bgconfig.bgi /timer:0
39795
39796 Microsoft\Windows\CurrentVersion\Run has no subkeys.
39797
39798 Microsoft\Windows\CurrentVersion\RunOnce
39799 LastWrite Time 2018-04-25 16:00:17Z
39800 Microsoft\Windows\CurrentVersion\RunOnce has no values.
39801 Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.
39802
39803 Microsoft\Windows\CurrentVersion\RunServices not found.
39804
39805 Wow6432Node\Microsoft\Windows\CurrentVersion\Run
39806 LastWrite Time 2018-04-11 23:40:34Z
39807

Search results: (35 hits)
Search "CurrentVersion\Run" (35 hits in 3 files of 8 searched)
C:\Cases\Analysis\Registry\SOFTWARE.txt (16 hits)
Line 39791: Microsoft\Windows\CurrentVersion\Run
Line 39792: Microsoft\Windows\CurrentVersion\Run has no subkeys.
Line 39793: Microsoft\Windows\CurrentVersion\RunOnce
Line 39794: Microsoft\Windows\CurrentVersion\RunOnce has no values.
Line 39795: Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.
Line 39796: Microsoft\Windows\CurrentVersion\RunServices not found.
Line 39797: Wow6432Node\Microsoft\Windows\CurrentVersion\Run
Line 39798: Microsoft\Windows\CurrentVersion\Run has no values.
Line 39799: Wow6432Node\Microsoft\Windows\CurrentVersion\Run has no subkeys.
Line 39800: Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce
Line 39801: Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce has no values.
Line 39802: Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.
Line 39803: Microsoft\Windows\CurrentVersion\Run not found.
Line 39804: Microsoft\Windows\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Run not found.
Line 39805: Microsoft\Windows\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\RunOnce not found.
Line 39806: Microsoft\Windows\CurrentVersion\RunOnceEx
Line 39807: Microsoft\Windows\CurrentVersion\RunOnceEx has no subkeys.

C:\Cases\Analysis\Registry\DEFAULT.txt (9 hits)
C:\Cases\Analysis\Registry\NTUSER.DAT.txt (10 hits)
Line 691: Software\Microsoft\Windows\CurrentVersion\Run
Line 692: Microsoft\Windows\CurrentVersion\Run has no subkeys.
Line 693: Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run not found.
Line 694: Software\Microsoft\Windows\CurrentVersion\RunOnce
Line 695: Microsoft\Windows\CurrentVersion\RunOnce has no values.
Line 696: Microsoft\Windows\CurrentVersion\RunOnceEx
Line 697: Microsoft\Windows\CurrentVersion\RunServices not found.
Line 698: Software\Microsoft\Windows\CurrentVersion\RunServices not found.
Line 699: Software\Microsoft\Windows\CurrentVersion\RunOnce
Line 700: Microsoft\Windows\CurrentVersion\RunOnce has no values.
Line 701: Software\Microsoft\Windows\CurrentVersion\RunOnceEx has no subkeys.
Line 702: Software\Microsoft\Windows\CurrentVersion\RunServices not found.

Search results: (86 hits)
Search "CurrentVersion\Run" (85 hits in 3 files of 8 searched)
C:\Cases\Analysis\Registry\SOFTWARE.txt (16 hits)
Line 39791: Microsoft\Windows\CurrentVersion\Run
Line 39792: Microsoft\Windows\CurrentVersion\Run has no subkeys.
Line 39793: Microsoft\Windows\CurrentVersion\RunOnce
Line 39794: Microsoft\Windows\CurrentVersion\RunOnce has no values.
Line 39795: Microsoft\Windows\CurrentVersion\RunOnceEx
Line 39796: Microsoft\Windows\CurrentVersion\RunServices not found.
Line 39797: Microsoft\Windows\CurrentVersion\Run
Line 39798: Microsoft\Windows\CurrentVersion\Run has no values.
Line 39799: Microsoft\Windows\CurrentVersion\Run has no subkeys.
Line 39800: Microsoft\Windows\CurrentVersion\RunOnce
Line 39801: Microsoft\Windows\CurrentVersion\RunOnce has no values.
Line 39802: Microsoft\Windows\CurrentVersion\RunOnceEx
Line 39803: Microsoft\Windows\CurrentVersion\RunServices not found.
Line 39804: Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.
Line 39805: Microsoft\Windows\CurrentVersion\Run not found.
Line 39806: Microsoft\Windows\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Run not found.
Line 39807: Microsoft\Windows\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\RunOnce not found.
Line 39808: Microsoft\Windows\CurrentVersion\RunOnceEx
Line 39809: Microsoft\Windows\CurrentVersion\RunServicesOnce not found.
Line 39810: Software\Microsoft\Windows\CurrentVersion\RunOnceEx has no subkeys.

C:\Cases\Analysis\Registry\DEFAULT.txt (10 hits)
Line 691: Software\Microsoft\Windows\CurrentVersion\Run
Line 692: Software\Microsoft\Windows\CurrentVersion\Run has no subkeys.
Line 693: Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run not found.
Line 694: Software\Microsoft\Windows\CurrentVersion\RunOnce
Line 695: Microsoft\Windows\CurrentVersion\RunOnce has no values.
Line 696: Software\Microsoft\Windows\CurrentVersion\RunOnceEx
Line 697: Microsoft\Windows\CurrentVersion\RunServicesOnce not found.
Line 698: Software\Microsoft\Windows\CurrentVersion\RunServicesOnceEx has no subkeys.
Line 699: Software\Microsoft\Windows\CurrentVersion\RunServices not found.
Line 700: Software\Microsoft\Windows\CurrentVersion\RunServicesOnce not found.
Line 701: Software\Microsoft\Windows\CurrentVersion\Run not found.

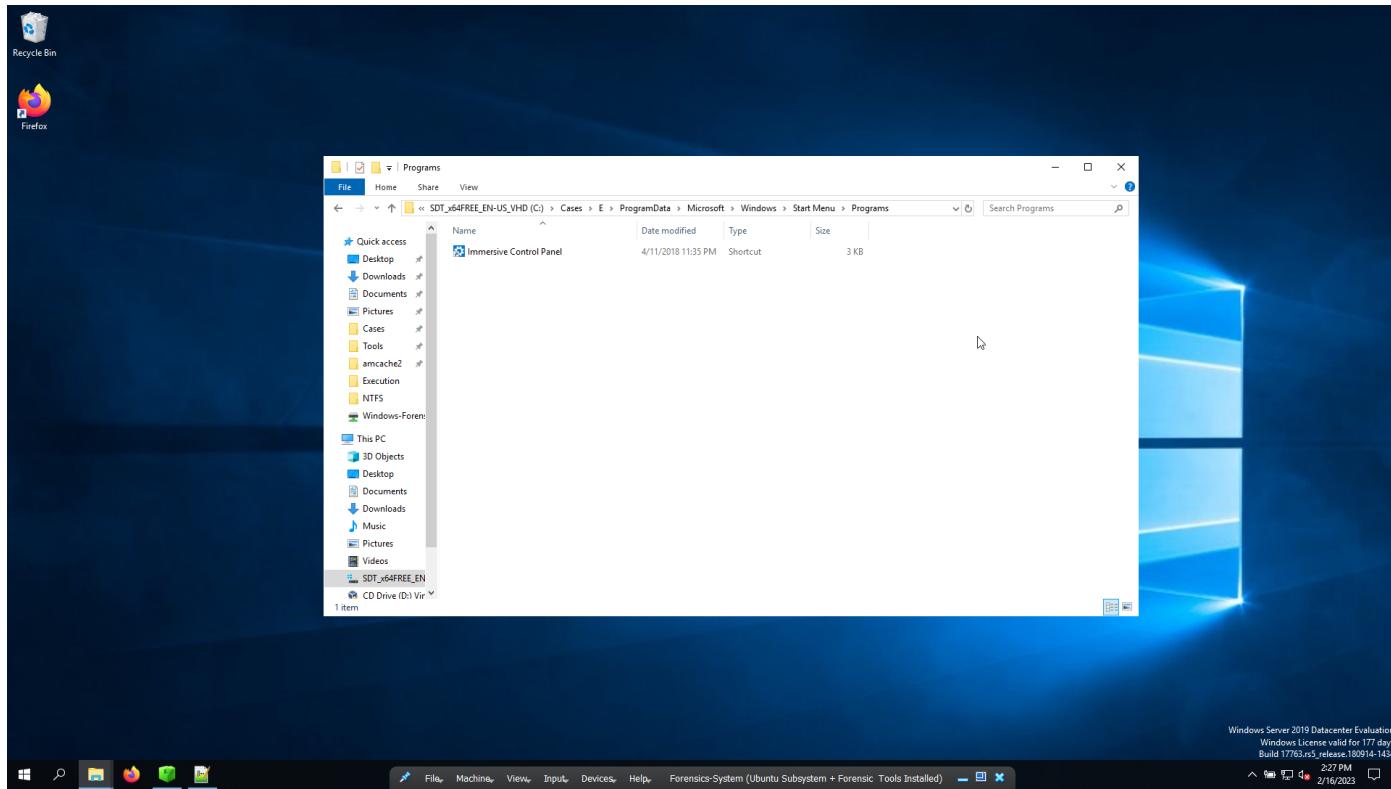
C:\Cases\Analysis\Registry\NTUSER.DAT.txt (10 hits)
Line 691: Software\Microsoft\Windows\CurrentVersion\Run

```

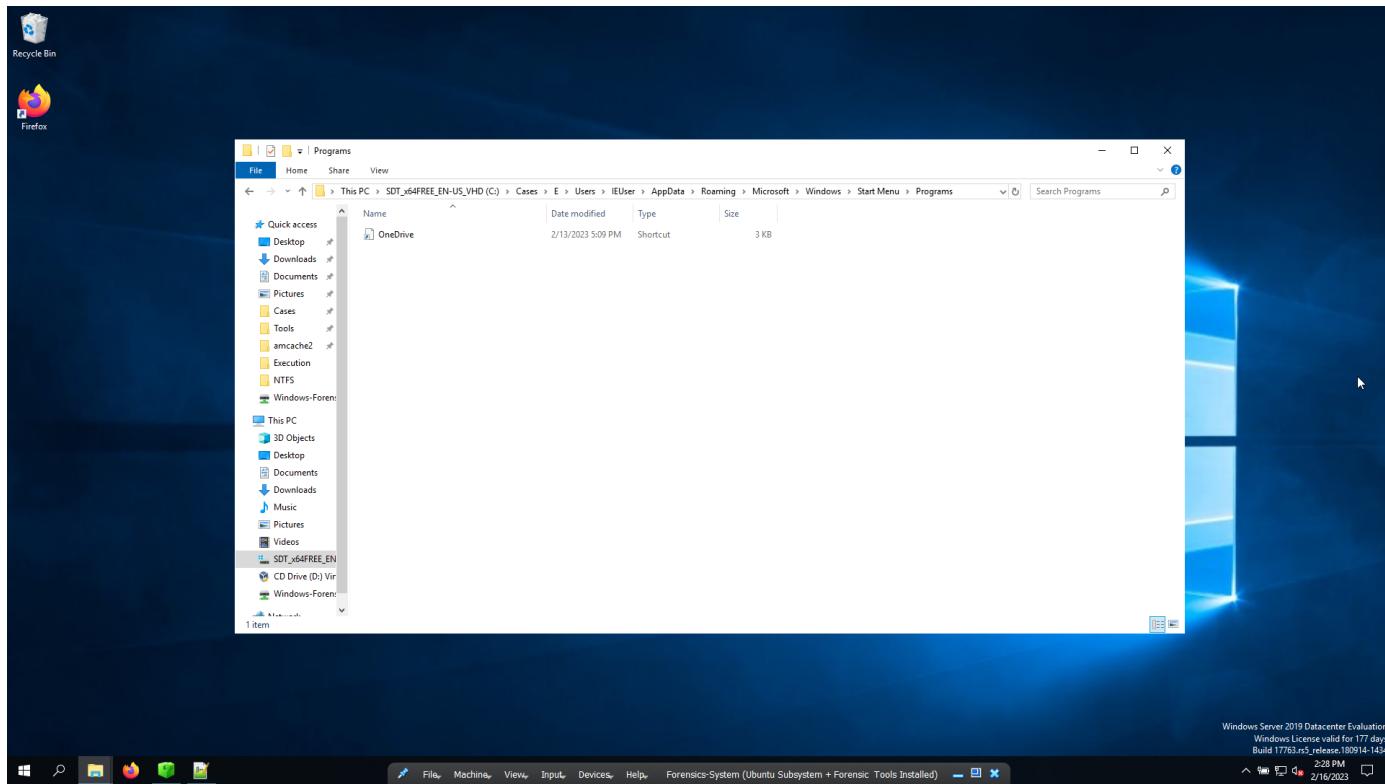
Startup Folders

- Locations:

- C:\Users\’username’\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
- C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp
- Placing an executable in each of this paths, the windows will execute them at startup.
- We will search in these folders, and hope to find something:



- Nothing. Moving on.



- Nothing as well.
- Lets search for the file paths in the MFT with ubuntu subsystem.
- Change directory to the NTFS folder, for the MFT file:

```
forensic@WIN-90HAJ6CQHQH:~$ cd /mnt/c/Cases/Analysis/NTFS
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 4.4.0-17763-Microsoft x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

System information as of Thu Feb 16 14:29:54 DST 2023

System load: 0.52      Processes: 7
Usage of /home: unknown  Users logged in: 0
Memory usage: 31%      IPv4 address for eth0: 10.0.2.15
Swap usage: 1%

1 update can be applied immediately.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

This message is shown once a day. To disable it please create the
/home/forensic/.hushlogin file.
forensic@WIN-90HAJ6CQHQH:~$ cd /mnt/c/Cases/Analysis/NTFS/
forensic@WIN-90HAJ6CQHQH:~/mnt/c/Cases/Analysis/NTFS$
```

- Search in the MFT for the Startup.

```
forensic@WIN-90HAJ6CQHQ: /mnt/c/Cases/Analysis/NTFS
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 4.4.0-17763-Microsoft x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

System information as of Thu Feb 16 14:29:54 DST 2023

System load: 0.52      Processes: 7
Usage of /home: unknown  Users logged in: 0
Memory usage: 31%      IPv4 address for eth0: 10.0.2.15
Swap usage:  1%

1 update can be applied immediately.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

This message is shown once a day. To disable it please create the
/home/forensic/.hushlogin file.
forensic@WIN-90HAJ6CQHQ: ~$ cd /mnt/c/Cases/Analysis/NTFS/
forensic@WIN-90HAJ6CQHQ: /mnt/c/Cases/Analysis/NTFS$ grep StartUp MFT.csv -
```

- Interesting file:

- Name of suspicious file in StartUp folder.

batstartup.bat

- Mount the .vhdx and search for the file.

```

forensic@WIN-90HAJ6CQHQH:/mnt/c/Cases/Analysis/NTFS
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 4.4.0-17763-Microsoft x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

System information as of Thu Feb 16 14:29:54 DST 2023

System load: 0.52 Processes: 114
Usage of /home: unknown Users logged in: 1
Memory usage: 31% IPv4 address(es):
Swap usage: 1% 

1 update can be applied immediately.
To see these additional updates run: apt update

The list of available updates is more than 1 day old.
To check for new updates run: sudo apt update

This message is shown once a day. To disable it, log in as root and run:
echo "0" | sudo tee /etc/hushlogin

Forensic@WIN-90HAJ6CQHQH:/mnt/c/Cases/Analysis/NTFS$ cd /mnt/c/Cases/Analysis/NTFS
Forensic@WIN-90HAJ6CQHQH:/mnt/c/Cases/Analysis/NTFS$ ls
1446_1,True,1440_1,.\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
29218_1,True,1446_1,.\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
batstartup.bat
Forensic@WIN-90HAJ6CQHQH:/mnt/c/Cases/Analysis/NTFS$ 

28:25.2699863,2018-04-25 16:43:54
16:44:10.5578661,2018-04-11 23:3
3.0000000,2023-02-13 17:28:25.269

Forensic@WIN-90HAJ6CQHQH:/mnt/c/Cases/Analysis/NTFS$ 

```

This screenshot shows a Windows File Explorer window displaying the contents of a mounted Linux file system (Local Disk (E)). The directory structure includes subfolders like 'AtomicRedTeam', 'BGInfo', 'PerfLogs', 'Program Files', 'Program Files (x86)', 'ProgramData', 'Users', and 'Windows'. A red arrow points from the left margin to the 'Startup' folder in the navigation pane.

- Search the startup folder path in the mounter image:

```

forensic@WIN-90HAJ6CQHQH:/mnt/c/Cases/Analysis/NTFS
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 4.4.0-17763-Microsoft x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

System information as of Thu Feb 16 14:29:54 DST 2023

System load: 0.52 Processes: 114
Usage of /home: unknown Users logged in: 1
Memory usage: 31% IPv4 address(es):
Swap usage: 1% 

1 update can be applied immediately.
To see these additional updates run: apt update

The list of available updates is more than 1 day old.
To check for new updates run: sudo apt update

This message is shown once a day. To disable it, log in as root and run:
echo "0" | sudo tee /etc/hushlogin

Forensic@WIN-90HAJ6CQHQH:/mnt/c/Cases/Analysis/NTFS$ cd /mnt/c/Cases/Analysis/NTFS
Forensic@WIN-90HAJ6CQHQH:/mnt/c/Cases/Analysis/NTFS$ ls
1446_1,True,1440_1,.\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
29218_1,True,1446_1,.\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup
batstartup.bat
Forensic@WIN-90HAJ6CQHQH:/mnt/c/Cases/Analysis/NTFS$ 

28:25.2699863,2018-04-25 16:43:54
16:44:10.5578661,2018-04-11 23:3
3.0000000,2023-02-13 17:28:25.269

Forensic@WIN-90HAJ6CQHQH:/mnt/c/Cases/Analysis/NTFS$ 

```

This screenshot shows a Windows File Explorer window displaying the contents of a mounted Linux file system (Local Disk (E)). The directory structure includes subfolders like 'AtomicRedTeam', 'BGInfo', 'PerfLogs', 'Program Files', 'Program Files (x86)', 'ProgramData', 'Users', and 'Windows'. A red arrow points from the left margin to the 'batstartup.bat' file in the main content area.

E:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\b startup.bat - Notepad++ [Administrator]

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

SOFTWARE [] SECURITY [] DEFAULT [] NTUSER.DAT [] SAM.bk [] UserClass.dat.bk [] User.ppl [] SYSTEM [] batstartup.bat []

```
1 echo " T1547.001 Hello World Bat"
2
```

Search results - (35 hits)

Search "CurrentVersion\Run" (35 hits in 3 files of 8 searched)

C:\Cases\Analysis\Registry\SOFTWARE.txt (16 hits)

Line 39791: Microsoft\Windows\CurrentVersion\Run
Line 39792: Microsoft\Windows\CurrentVersion\Run has no subkeys.
Line 39795: Microsoft\Windows\CurrentVersion\RunOnce
Line 39801: Microsoft\Windows\CurrentVersion\RunOnce has no values.
Line 39802: Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.
Line 39804: Microsoft\Windows\CurrentVersion\RunOnceServices not found.
Line 39805: Wow6432Node\Microsoft\Windows\CurrentVersion\Run
Line 39806: Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce
Line 39808: Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.
Line 39809: Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.
Line 39811: Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce
Line 39813: Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce has no values.
Line 39814: Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.
Line 39815: Microsoft\Windows\CurrentVersion\RunOnce not found.
Line 39822: Microsoft\Windows\NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\RunOnce not found.
Line 39833: Microsoft\Windows\CurrentVersion\RunOnceEx
Line 39834: Microsoft\Windows\CurrentVersion\RunOnceEx has no subkeys.

C:\Cases\Analysis\Registry\DEFAULT.txt (9 hits)

C:\Cases\Analysis\Registry\SYSTEM.txt (10 hits)

Line 680: Software\Microsoft\Windows\CurrentVersion\Run
Line 681: Software\Microsoft\Windows\CurrentVersion\Run has no subkeys.
Line 684: Software\Microsoft\Windows\CurrentVersion\RunOnce
Line 696: Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run not found.
Line 698: Software\Microsoft\Windows\CurrentVersion\RunOnce
Line 700: Software\Microsoft\Windows\CurrentVersion\RunOnce has no values.
Line 701: Software\Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.
Line 702: Software\Microsoft\Windows\CurrentVersion\RunServices not found.
Line 703: Software\Microsoft\Windows\CurrentVersion\RunServicesOnce not found.
Line 707: Software\Microsoft\Windows\NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Run not found.

Windows Services

- Registry location : HKLM\SYSTEM\CurrentControlSet\Services
 - View the registry hive with registry explorer:

Registry Explorer V1.6.0.0

File Tools Options Bookmarks (28/0) View Help

Registry hives (3) Available bookmarks (88/0)

Values Services

Name	Description	Display Name	Start Mode	Service Type	Name Key Last Write	Parameters Key Last.	Group	Image Path	Service DLL	Required Privileges
.NET CLR Data			=	Adapter	2023-02-13 17:17:38					
.NET CLR Networking			=	Adapter	2023-02-13 17:17:38					
.NET CLR Networking 4.0.0.0			=	Adapter	2018-04-11 23:38:44					
.NET Data Provider for Oracle			=	Adapter	2018-04-11 23:38:44					
.NET Data Provider for SQLServer			=	Adapter	2018-04-11 23:38:44					
.NET Memory Cache 4.0			=	Adapter	2018-04-11 23:38:44					
.NET Framework 1394hd	@1394.inf %PCI\CC_00000000\1394%1394 OHCI Compliant Host Controller	Manual		KernelDriver	2018-04-11 23:38:04			\SystemRoot\System32\drivers\1394hd.sys		
3ware			Boot	KernelDriver	2018-04-25 15:46:30	2018-04-11 23:38:04	SCSI import	\System32\drivers\3ware.sys		
ACPI	@acpi.inf \ACPI\Device\Microsoft ACPI Driver	Boot		KernelDriver	2023-02-14 03:11:05	2018-04-25 15:47:47	Core	\System32\drivers\ACPI.sys		
AcpDev	@AcpDev.inf %AcpD\ev\Sv\Device\%Acp\Devices driver	Manual		KernelDriver	2018-04-11 23:38:04		Extended Base	\SystemRoot\System32\Drivers\AcpDev.sys		
apex	Microsoft ACPI\Ex Driver	Boot		KernelDriver	2018-04-25 15:46:30	2018-04-25 15:47:47	Boot Bus Extender	\System32\Drivers\apciex.sys		
apipag	@apipag.inf %AcpD\ext\%ACPI Processor Aggregator Driver	Manual		KernelDriver	2018-04-11 23:38:11			\SystemRoot\System32\Drivers\apipag.sys		
AcpPm	@acpm.inf %AcpP	Manual		KernelDriver	2018-04-11 23:38:02			\SystemRoot\System32\Drivers\acpm.sys		

Total rows: 639

Type viewer

Bookmark information

Hive: C:\Cases\Analysis\Registry\SYSTEM

Category: Operating system

Name: Services

Key path: ControlSet001\Services

Short description: Service definitions and parameters

Long description:

Selected hive: NTUSER.DAT Last write: 2/13/2023 5:56:59 PM +00:00 Key contains no values

Value: None Collapse all hives

Hidden keys: 1

- Search the registry hive with text file with 2 plugins:
- First.

C:\Cases\Analysis\Registry\SYSTEMmbt - Notepad+ [Administrator]

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

Software.txt DEFAULT.txt NTUSER.DAT.txt SAMER.txt User.dat.txt bmm.txt SYSTEM.txt startup.txt

```

853 ControlSet001\Services\Tcpip\Parameters\PersistentRoutes
854 LastWrite: 2018-04-11 23:38:42
855
856 ControlSet001\Services\Tcpip\Parameters\PersistentRoutes has no values.
857 -----
858 Launching securityproviders v.20200526
859 (System) Gets SecurityProvider value from System hive
860
861 LastWrite: 2018-04-11 23:39:26
862
863 SecurityProviders = credssp.dll
864 -----
865 services\20181024
866 (System) Lists services/drivers in Services key by LastWrite times
867
868 ControlSet001\Services
869 Lists services/drivers in Services key by LastWrite times
870
871 Tue Feb 14 03:11:26 2023 Z
872 Name = BasicDisplay
873 Display = BasicDisplay
874 ImagePath = \SystemRoot\System32\drivers\BasicDisplay.sys
875 Type = Kernel driver
876 Start = System Start
877 Group = Video
878
879 Name = monitor
Search results: (35 hits)
Search "CurrentVersion\Run" (35 hits in 3 files of 8 searched)
C:\Cases\Analysis\Registry\SOFTWARE.txt (15 hits)
Line 39791: Microsoft\Windows\CurrentVersion\Run
Line 39791: Microsoft\Windows\CurrentVersion\Run has no subkeys.
Line 39792: Microsoft\Windows\CurrentVersion\RunOnce
Line 39792: Microsoft\Windows\CurrentVersion\RunOnce has no values.
Line 39800: Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.
Line 39801: Microsoft\Windows\CurrentVersion\RunServices not found.
Line 39801: Wow6432Node\Microsoft\Windows\CurrentVersion\Run
Line 39801: Wow6432Node\Microsoft\Windows\CurrentVersion\Run has no values.
Line 39802: Wow6432Node\Microsoft\Windows\CurrentVersion\Run has no subkeys.
Line 39811: Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.
Line 39811: Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.
Line 39821: Microsoft\Windows\NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Run not found.
Line 39821: Microsoft\Windows\NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\RunOnce not found.
Line 39831: Microsoft\Windows\CurrentVersion\RunOnceEx
Line 39831: Microsoft\Windows\CurrentVersion\RunOnceEx has no subkeys.
C:\Cases\Analysis\Registry\NTUSER.DAT.txt (9 hits)
C:\Cases\Analysis\Registry\NTUSER.DAT.txt (10 hits)
Line 691: Software\Microsoft\Windows\CurrentVersion\Run
Line 691: Software\Microsoft\Windows\CurrentVersion\Run has no subkeys.
Line 692: Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run not found.
Line 693: Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run has no subkeys.
Line 701: Software\Microsoft\Windows\CurrentVersion\RunOnce has no values.
Line 701: Software\Microsoft\Windows\CurrentVersion\RunOnce has no subkeys.
Line 703: Software\Microsoft\Windows\CurrentVersion\RunServices not found.
Line 703: Software\Microsoft\Windows\CurrentVersion\RunServicesOnce not found.
Line 703: Software\Microsoft\Windows\NT\CurrentVersion\Terminal Server\Install\Software\Microsoft\Windows\CurrentVersion\Run not found.

```

Find Replace Find in Files Find in Projects Mark

Find what: services.v

Find Next Count Find All in Current Document

In selection Find All in Opened Documents Close

Search Mode Normal Extended (v, V, t, T, \w, \W) Regular expression matches newline

Transparency On losing focus Always

length: 364,933 lines: 6,970 Ln: 865 Col: 12 Sel: 11 | 1 Windows (CR LF) UTF-8 INS

C:\Case\Analysis\Registry\SYSTEM.txt - Notepad - [Administrator]

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

SOFTWARE.txt DEFAULT.TXT NTUSER.DAT.TXT SAM.TXT UseClass.dat.txt bam.p.txt SYSTEM.txt bootstrap.bell.txt

```
1141 Name = Wdf01000
1142 Display = %SystemRoot%\system32\drivers\Wdf01000.sys,-1000
1143 ImagePath = system32\drivers\Wdf01000.sys
1144 Type = Kernel_driver
1145 Start = Boot_Start
1146 Group = WdfHeadGroup
1147
1148 Tue Feb 14 03:04:33 2023 Z
1149 Name = VBoxVideoW8
1150 Display =
1151 ImagePath = %SystemRoot%\system32\DRIVERS\VBoxVideoW8.sys
1152 Type = Kernel_driver
1153 Start = Manual
1154 Group = Video
1155
1156 Mon Feb 13 17:30:47 2023 Z
1157 Name = BITS
1158 Display = %SystemRoot%\system32\qmgr.dll,-1000
1159 ImagePath = %SystemRoot%\System32\svchost.exe -k netsvcs -p
1160 Type = Share_Process
1161 Start = Auto_Start
1162 Group =
1163
1164 Mon Feb 13 17:28:30 2023 Z
1165 Name = AtomicCfesService_CMD
1166 Display =
1167 ImagePath = C:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.exe
1168 Type = Own_Process
1169 Start = Manual
1170 Group =
1171
1172 Mon Feb 13 17:25:13 2023 Z
1173 Name = Symmon
1174 Display = Symmon
1175 ImagePath = C:\Windows\Symmon.exe
1176 Type = Own_Process
1177 Start = Auto_Start
1178 Group =
1179
1180 Name = SymmonDrv
1181 Display = SymmonDrv
1182 ImagePath = SymmonDrv.sys
1183 Type = Kernel_driver
1184 Start = Boot_Start
1185 Group =
1186
1187 Mon Feb 13 17:17:38 2023 Z
1188 Name = .NET CLR Data
1189 Display =
1190 ImagePath =
1191 Type =
1192 Start =
1193 Group =
1194
1195 Name = .NET CLR Networking
1196 Display =
1197 ImagePath =
```

Normalized file

length: 364,933 lines: 6,970 Ln: 865 Col: 12 Sel: 11 | 1 Windows (CR LF) UTF-8 2:41 PM 2/16/2023

- Second.

File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?

Software List SECURITY DEFAULT NTUSER.DAT SAM UsClass.dat bam.pl SYSTEM.txt batstartup.bat

5778 svc_v.20200525
(System) Lists Services key contents by LastWrite time (CSV)
5780
Time,Name, DisplayName, ImagePath\ServiceBinary, Type, Start, Kernel Driver, System, %SystemRoot%\system32\drivers\bam.sys,-101
5781 2023-02-13 03:11:06Z,BasicDisplay,inf,BasicDisplay.sys,Kernel driver,Kernel,0,%SystemRoot%\system32\drivers\basicdisplay.sys,-101
5782 2023-02-13 03:11:06Z,BasicMonitor,inf,BasicMonitor.sys,Kernel driver,Kernel,0,%SystemRoot%\system32\drivers\basicmonitor.sys,-101
5783 2023-02-13 03:11:07Z,mzmmbios,inf,Mzmmbios.inf,Microsoft Basic Monitor Class Function Driver Service,0,%SystemRoot%\system32\drivers\mzmmbios.sys,-101
5784 2023-02-13 03:11:07Z,mzmmbios,inf,Mzmmbios.inf,Microsoft Basic Monitor Class Function Driver Service,0,%SystemRoot%\system32\drivers\mzmmbios.sys,-101
5785 2023-02-13 03:11:06Z,Disk,inf,Disk.inf,Device\Disk,Driver,0,%SystemRoot%\system32\drivers\disk.sys,Kernel driver,Boot Start,,%SystemRoot%\system32\drivers\disktrck.dll,-300
5786 2023-02-13 03:11:06Z,EhStorClass,inf,EhStorClass.inf,Device\Disk,Driver,0,%SystemRoot%\system32\drivers\ehstorclass.sys,Kernel driver,Boot Start,,%SystemRoot%\system32\drivers\ehstorclass.sys,-101
5787 2023-02-13 03:11:06Z,fvevol1,inf,fvevol1.inf,Driver,0,%SystemRoot%\system32\drivers\fvevol1.sys,Kernel driver,Boot Start,,%SystemRoot%\system32\drivers\fvevol1.sys,-100
5788 2023-02-13 03:11:06Z,fvevol2,inf,fvevol2.inf,Driver,0,%SystemRoot%\system32\drivers\fvevol2.sys,Kernel driver,Boot Start,,%SystemRoot%\system32\drivers\fvevol2.sys,-100
5789 2023-02-13 03:11:06Z,partner,inf,partner.inf,Driver,0,%SystemRoot%\system32\drivers\partner.sys,Kernel driver,Boot Start,,%SystemRoot%\system32\drivers\partner.sys,-101
5790 2023-02-14 03:11:06Z,rdyboost,inf,rdyboost.inf,Driver,0,%SystemRoot%\system32\drivers\rdyboost.sys,Kernel driver,Boot Start,,ReadyBoost
5791 2023-02-14 03:11:06Z,volsnap,inf,volsnap.inf,Driver,0,%SystemRoot%\system32\drivers\volsnap.sys,Kernel driver,Boot Start,,%SystemRoot%\system32\drivers\volsnap.sys,-101
5792 2023-02-14 03:11:06Z,volume,inf,VVolumeService,Driver,0,%SystemRoot%\system32\drivers\volume.sys,Kernel driver,Boot Start,,%SystemRoot%\system32\drivers\volumen.sys,-101
5793 2023-02-14 03:11:06Z,ACPI,inf,ACPI.inf,Driver,0,%SystemRoot%\system32\drivers\acpi.sys,Kernel driver,Boot Start,,%SystemRoot%\system32\drivers\acpi.sys,-101
5794 2023-02-14 03:11:06Z,ACPI,inf,ACPI.inf,Driver,0,%SystemRoot%\system32\drivers\acpi.sys,Kernel driver,Boot Start,,%SystemRoot%\system32\drivers\acpi.sys,-101
5795 2023-02-14 03:11:06Z,atapi,inf,IDEchannel.Device,Driver,0,%SystemRoot%\system32\drivers\atapi.sys,Kernel driver,Boot Start,,%SystemRoot%\system32\drivers\atapi.sys,-101
5796 2023-02-14 03:11:06Z,BasicGender,inf,BasicGender.sys,Kernel driver,Boot Start,,%SystemRoot%\system32\drivers\basm.sys,-101
5797 2023-02-14 03:11:06Z,CAD,inf,CAD.inf,Driver,0,%SystemRoot%\system32\drivers\cad.sys,Kernel driver,Boot Start,,%SystemRoot%\system32\drivers\cad.sys,-101
5798 2023-02-14 03:11:06Z,CAD,inf,CAD.inf,Driver,0,%SystemRoot%\system32\drivers\cad.sys,Kernel driver,Boot Start,,%SystemRoot%\system32\drivers\cad.sys,-101
5799 2023-02-14 03:11:06Z,CdRom,inf,CdRom.inf,Driver,0,%SystemRoot%\system32\drivers\cdrom.sys,Kernel driver,Boot Start,,%SystemRoot%\system32\drivers\cdrom.sys,-101
5800 2023-02-14 03:11:06Z,CmBatt,inf,CmBatt.inf,Driver,0,%SystemRoot%\system32\drivers\cmbat.sys,Kernel driver,Boot Start,,%SystemRoot%\system32\drivers\cmbat.sys,-101
5801 2023-02-14 03:11:06Z,E10G,inf,E10G.inf,Driver,0,%SystemRoot%\system32\drivers\el10g.sys,Kernel driver,Boot Start,,%SystemRoot%\system32\drivers\el10g.sys,-102
5802 2023-02-14 03:11:06Z,F5/2,inf,F5/2.inf,Keyboard and Mouse Port Driver,0,%SystemRoot%\system32\drivers\f5_0404prt.sys,Kernel driver,Manual,Contains the undocumented video driver stacks to provide full
5803 2023-02-14 03:11:06Z,intelide,inf,IntelIDE.inf,Driver,0,%SystemRoot%\system32\drivers\intelide.sys,Kernel driver,Boot Start,,%SystemRoot%\system32\intelide.inf,-200
5804 2023-02-14 03:11:06Z,Kbdclass,inf,Kbdclass.inf,Keyboard Class Driver,0,%SystemRoot%\system32\drivers\kbdclass.sys,Kernel driver,Manual,,%SystemRoot%\system32\imron.dll,-2001
5805 2023-02-14 03:11:06Z,Kdmic,inf,Kdmic.inf,Driver,0,%SystemRoot%\system32\drivers\kdmic.sys,Kernel driver,Manual,,%SystemRoot%\system32\imron.dll,-2001
5806 2023-02-14 03:11:06Z,msmisdriv,inf,MSMisDrv.inf,Driver,0,%SystemRoot%\system32\drivers\msmisdrv.sys,Kernel driver,Boot Start,,%SystemRoot%\system32\drivers\msmisdrv.sys,-101
5807 2023-02-14 03:11:06Z,msmisdriv,inf,MSMisDrv.inf,Driver,0,%SystemRoot%\system32\drivers\msmisdrv.sys,Kernel driver,Boot Start,,%SystemRoot%\system32\drivers\msmisdrv.sys,-101
5808 2023-02-14 03:11:06Z,NdisVirtualBus,inf,NdisVirtualBus.inf,Driver,0,%SystemRoot%\system32\drivers\ndisvirtualbus.sys,-200,,%SystemRoot%\system32\drivers\ndisvirtualbus.sys,Kernel driver,Manual,,%SystemRoot%\system32\mprmag.dll,-32001
5809 2023-02-14 03:11:06Z,Pci,inf,Pci.inf,PCI Bus Driver,0,%SystemRoot%\system32\drivers\pci.sys,Kernel driver,Boot Start,,%SystemRoot%\system32\pcasvc.dll,-2
5810 2023-02-14 03:11:06Z,rdpbus,inf,rdpbus.inf,Driver,0,%SystemRoot%\system32\drivers\rdpbus.sys,Kernel driver,Manual,,%SystemRoot%\system32\rdpbus.sys,Kernel driver,Manual,,%SystemRoot%\system32\rdpbus.sys,-1001
5811 2023-02-14 03:11:06Z,sysecp,inf,Sysecp.inf,Spooler,Driver,0,%SystemRoot%\system32\drivers\sysecp.sys,Kernel driver,Manual,,%SystemRoot%\system32\sysecp.sys,-4
5812 2023-02-14 03:11:06Z,sysinfo,inf,sysinfo.inf,Driver,0,%SystemRoot%\system32\drivers\sysinfo.sys,Kernel driver,Manual,,%SystemRoot%\system32\sysinfo.sys,-10
5813 2023-02-14 03:11:06Z,svennum,inf,KSENNUM.SWDECS,Software Bus Driver,0,%SystemRoot%\system32\drivers\svennum.sys,Kernel driver,Manual,,%SystemRoot%\system32\swviser.sys,-10
5814 2023-02-14 03:11:06Z,umbus,inf,umbus.inf,UMBUS.inf,UMBUS Enumerator Driver,0,%SystemRoot%\system32\drivers\umbus.sys,Kernel driver,Manual,,%SystemRoot%\system32\agentservice.exe,-10
5815 2023-02-14 03:11:06Z,VBoxGuest,inf,VBoxGuest.inf,VirtualBox Guest House Service,0,%SystemRoot%\system32\DRIVERS\VBoxGuest.sys,Kernel driver,Boot Start,,%SystemRoot%\system32\vaultsvc.dll,-1004
5816 2023-02-14 03:11:06Z,VBoxHouse,inf,VBoxHouse.inf,VirtualBox Guest House Service,0,%SystemRoot%\system32\DRIVERS\VBoxHouse.sys,Kernel driver,Manual,,%SystemRoot%\system32\vaultv.dll,-1004
5817 2023-02-14 03:11:06Z,vdc,inf,vdc.inf,Driver,0,%SystemRoot%\system32\drivers\vdc.sys,Kernel driver,Manual,,%SystemRoot%\system32\windowsdefenderdesc.dll,-400
5818 2023-02-14 03:11:06Z,vdcroot,inf,vdcroot.inf,Driver,0,%SystemRoot%\system32\drivers\vdcroot.sys,Kernel driver,Boot Start,,%SystemRoot%\system32\windowsdefenderdesc.dll,-400
5819 2023-02-14 03:11:06Z,vdcroot,inf,vdcroot.inf,Driver,0,%SystemRoot%\system32\drivers\vdcroot.sys,Kernel driver,Boot Start,,%SystemRoot%\system32\windowsdefenderdesc.dll,-400
5820 2023-02-14 03:11:06Z,Wdf01000,inf,Wdf01000.inf,Driver,0,%SystemRoot%\system32\drivers\wdf01000.sys,Kernel driver,Boot Start,,%ProgramFiles%\Windows Defender\NpAesDesc.dll,-400
5821 2023-02-14 03:11:06Z,Wdf01000,inf,Wdf01000.inf,Driver,0,%SystemRoot%\system32\DRIVERS\Wdf01000.sys,Kernel driver,Manual,,Manages VM runtime information, time synchronization, remote sysprep execution and miscellaneous utilities for guest operating systems
5822 2023-02-14 03:11:06Z,Wmi,inf,Wmi.inf,Driver,0,%SystemRoot%\system32\drivers\wmi.sys,Kernel driver,Manual,,Manages VM runtime information, time synchronization, remote sysprep execution and miscellaneous utilities for guest operating systems
5823 2023-02-14 03:11:06Z,wmi,inf,wmi.inf,Driver,0,%SystemRoot%\system32\drivers\wmi.sys,Kernel driver,Manual,,Manages VM runtime information, time synchronization, remote sysprep execution and miscellaneous utilities for guest operating systems
5824 2023-02-14 03:11:06Z,wmi,inf,wmi.inf,Driver,0,%SystemRoot%\system32\drivers\wmi.sys,Kernel driver,Manual,,Manages VM runtime information, time synchronization, remote sysprep execution and miscellaneous utilities for guest operating systems
5825 2023-02-13 17:15:13Z,Syemon,inf,Syemon.inf,Driver,0,%SystemRoot%\system32\drivers\syemon.sys,Kernel driver,Boot Start,,System Monitor service
5826 2023-02-13 17:15:13Z,Symonrv,inf,Symonrv.inf,Driver,0,%SystemRoot%\system32\drivers\symonrv.sys,Kernel driver,Boot Start,,System Monitor driver
5827 2023-02-13 17:17:38Z,.NET CLR Data,.....
5828 2023-02-13 17:17:38Z,.NET CLR Networking,.....
5829 2023-02-13 17:17:38Z,Windows Firewall,inf,Windows Firewall.inf,Driver,0,%SystemRoot%\system32\drivers\fwctrl.sys,-2788
5830 2023-02-13 17:17:38Z,Windows Firewall 4.0.0.0.,inf,%SystemRoot%\system32\smrouter90c.dll,-10002
5831 2023-02-13 17:17:38Z,Windows Workflow Foundation 4.0.0.0.,inf,%ProgramFiles%\Windows Defender\UpdAesDesc.dll,-240
5832 2023-02-13 17:17:38Z,Windows Remediation Service,inf,Windows Remediation Service.inf,Driver,0,%SystemRoot%\system32\rempl\remdevc.exe,Own_Process,Auto Start,localSystem,,%SystemRoot%\system32\impmsg.dll,-32000
5833 2023-02-13 17:17:38Z,Windows Remediation Service,"C:\Program Files\rempl\remdevc.exe",Own_Process,Auto Start,localSystem,,Remediates Windows Update Components
Normal text file length: 364,933 lines: 6,970 Ln: 5,825 Col: 1 Sel: 174|1 Windows (CR/LF) UTF-8 24:38 9/16/2023

- Time installation of atomic service.

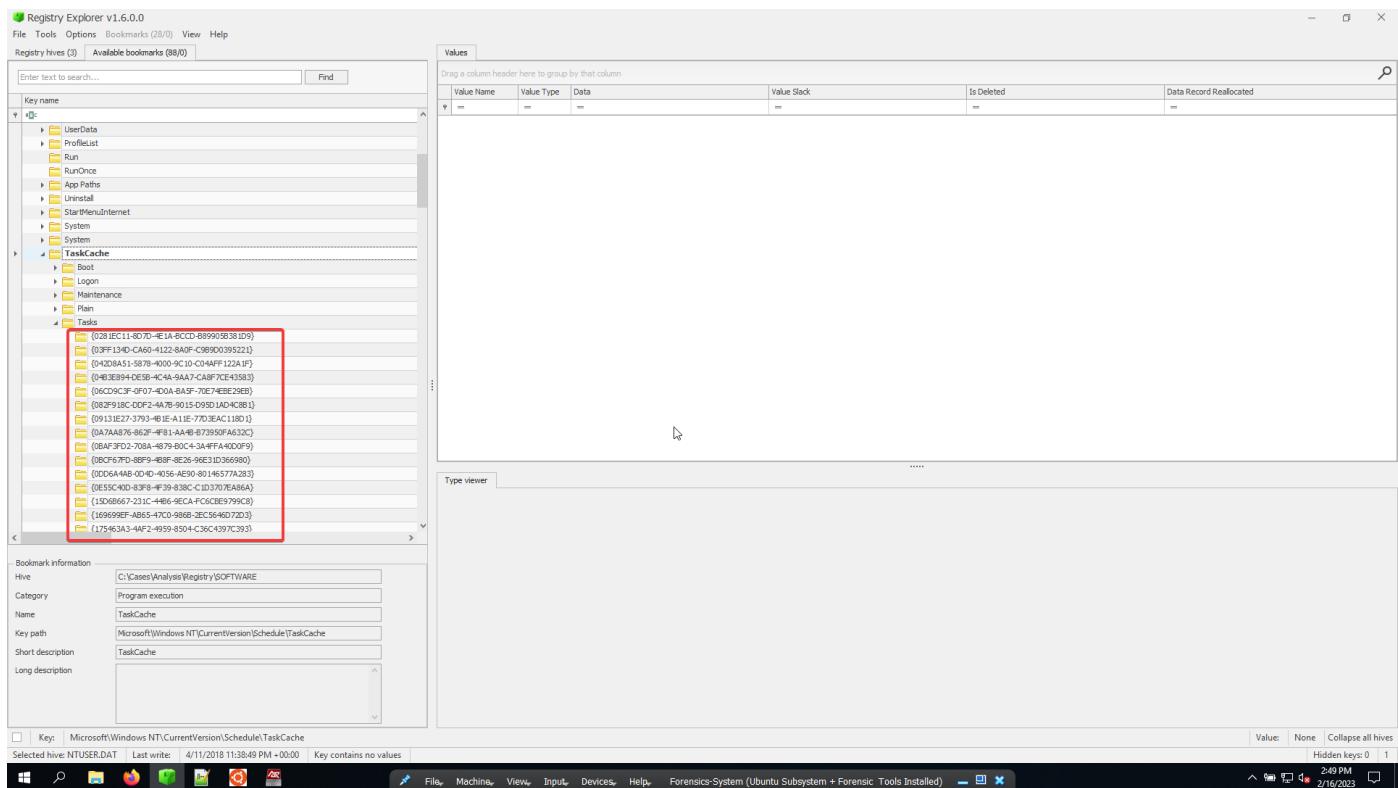
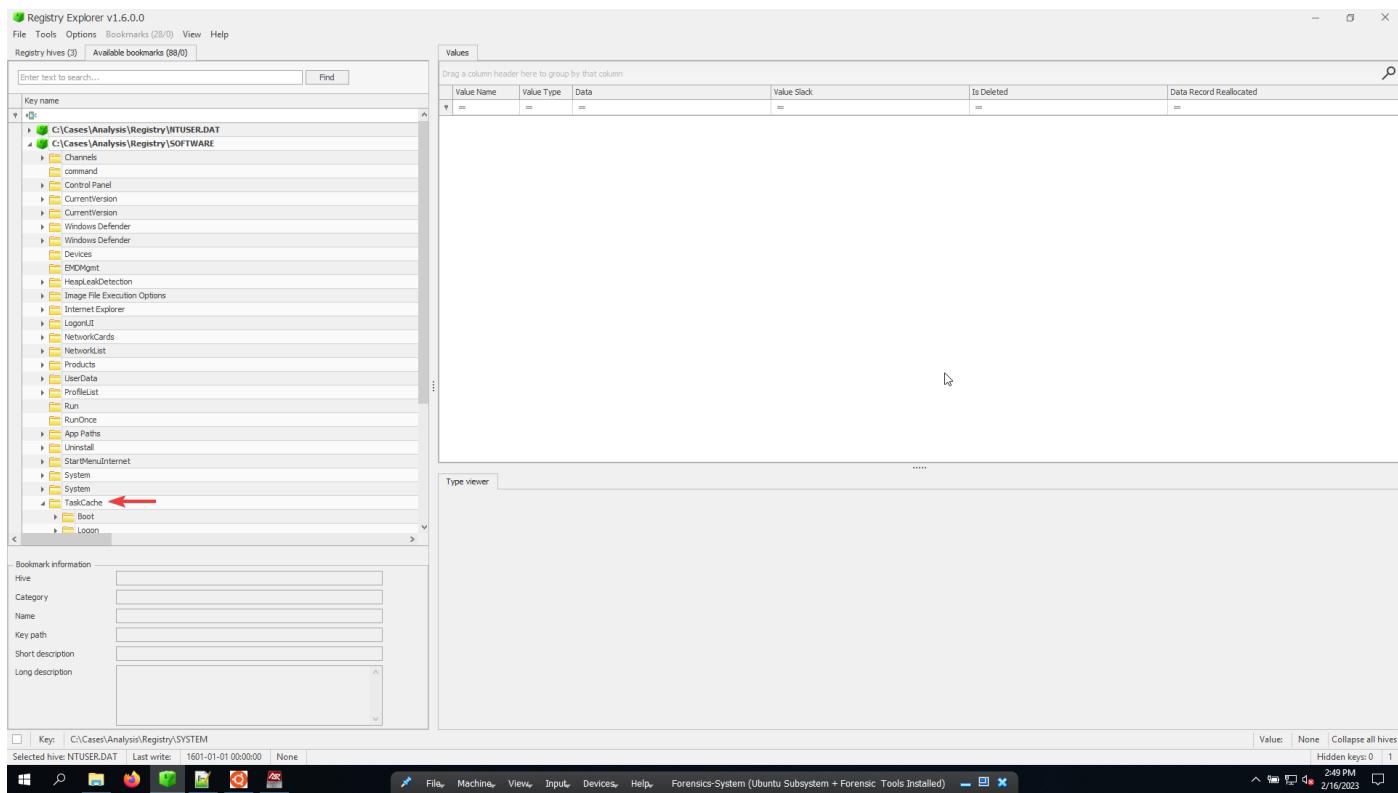
2023-02-13 17:28:30Z

Scheduled tasks

- Locations:
 - o HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks
 - o HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree
 - o C:\Windows\System32\Tasks

- Tasks can execute applications at any time based on specific triggers.

- Search for tasks subkey in registry explorer:



Registry Explorer V1.6.0.0

File Tools Options Bookmarks (28/0) View Help

Registry hives (3) Available bookmarks (88/0)

Enter text to search... Find

Key name

- NetworkCards
- NetworkList
- Products
- UserData
- profelist
- Run
- RunOnce
- App Paths
- Uninstall
- StartMenuInternet
- System
- TaskCache
- Tasks
- Tree
- Microsoft
- OneDrive Reporting Task-S-1-5-21-1058341133-2092417715-4019509128-1000
- OneDrive Standalone Update Task-S-1-5-21-1058341133-2092417715-4019509128-1000
- T1053_005_OnLogon
- T1053_005_OvStartup
- Trading
- VolumetricCache
- Windows Portable Devices
- Winlogon
- Trading
- Uninstall

Values TaskCache

Version	Key Name	Path	Created On	Last Start	Last Stop	Task State	Last Action Result	Source	Description	Author
3	{0281ECC11-BD70-4E1A-BCCD-889905B381D9}	\Microsoft\Windows\Power Efficiency\Graphics\AnalyzeSystem	2018-04-25 15:46:42	-	-	-	-	0	0 \${@%SystemRoot%\system32\energytask.dll,-602} \${@%SystemRoot%\system32\energytask.dll,-602}	0 \${@%SystemRoot%\system32\energytask.dll,-600}
3	{03FF134D-C460-4122-A0AF-C9890D395221}	\Microsoft\Windows\SHELL\Indexer\Automatic	2018-04-25 15:46:42	-	-	-	-	0	0 \${@%SystemRoot%\system32\srchadmin.dll,-1902}	0 \${@%SystemRoot%\system32\srchadmin.dll,-1901}
3	{0420DA51-5939-4000-9C10-C04A4F122AA1F}	\Microsoft\Windows\PowerDirectoryClient\HandleCommand	2018-04-25 15:46:42	-	-	-	-	0	0 \${@%SystemRoot%\system32\ProvTool.exe,-101}	0 \${@%SystemRoot%\system32\ProvTool.exe,-100}
3	{04B3E894-D5B-4C4A-A4AA-C4F2E424E83}	\Microsoft\Windows\Power\CellularProvision	2018-04-25 15:46:42	-	-	-	-	0	0 \${@%SystemRoot%\system32\pppdsvc.dll,-200}	0 \${@%SystemRoot%\system32\pppdsvc.dll,-1902}
3	{066DC0C3-F07-4000-8A5F-70E74BE2E291}	\Microsoft\Windows\AER\Verifier\VerifierDpiBlur	2018-04-25 15:46:41	-	-	-	-	0	0 \${@%SystemRoot%\system32\pppdsvc.dll,-200}	0 \${@%SystemRoot%\system32\pppdsvc.dll,-1902}
3	{083F918C-CDF2-447B-9015-09501A4C43B1}	\Microsoft\Windows\WOW64\High-Value\On	2018-04-25 15:46:42	-	-	-	-	0	0 \${@%SystemRoot%\system32\WofTasks.dll,-601}	0 \${@%SystemRoot%\system32\WofTasks.dll,-602}
3	{09131E27-3793-4B1E-A11E-7D03E4C18BD1}	\Microsoft\Windows\CloudService\WakeAndGo	2018-04-25 15:46:41	-	-	-	-	0	0 \${@%SystemRoot%\system32\ngtcskd.dll,-101}	0 \${@%SystemRoot%\system32\ngtcskd.dll,-102}
3	{0A4AA476-862F-4F8A-9A4B-873950FA632}	\Microsoft\Windows\Nlstart\WakeAndGo	2018-04-25 15:46:42	-	-	-	-	0	0 \${@%SystemRoot%\system32\pppdsvc.dll,-200}	0 \${@%SystemRoot%\system32\pppdsvc.dll,-1902}
3	{0BAF3FD2-708A-4B79-980C-434FFA4000F9}	\Microsoft\Windows\Start\StartCompon	2018-04-25 15:46:42	-	-	-	-	0	0 \${@%SystemRoot%\system32\WofTasks.dll,-601}	0 \${@%SystemRoot%\system32\WofTasks.dll,-602}
3	{0C5CF7FD-88F9-4B8F-F-8E26-96E31D36698}	\Microsoft\Windows\Sync\Sync	2018-04-25 15:46:42	-	-	-	-	0	0 \${@%SystemRoot%\system32\w32time.dll,-200}	0 \${@%SystemRoot%\system32\w32time.dll,-201}

Total rows: 172

Type viewer

File Machine View Input Devices Help Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) 25:00 2/16/2023

- Sort based on created on:

Registry Explorer V1.6.0.0

File Tools Options Bookmarks (28/0) View Help

Registry hives (3) Available bookmarks (88/0)

Enter text to search... Find

Key name

- NetworkCards
- NetworkList
- Products
- UserData
- profelist
- Run
- RunOnce
- App Paths
- Uninstall
- StartMenuInternet
- System
- TaskCache
- Tasks
- Tree
- Microsoft
- OneDrive Reporting Task-S-1-5-21-1058341133-2092417715-4019509128-1000
- OneDrive Standalone Update Task-S-1-5-21-1058341133-2092417715-4019509128-1000
- T1053_005_OnLogon
- T1053_005_OvStartup
- Trading
- VolumetricCache
- Windows Portable Devices
- Winlogon
- Trading
- Uninstall

Values TaskCache

Version	Key Name	Path	Created On	Last Start	Last Stop	Task State	Last Action Result	Source	Description	Author
3	{0281ECC11-BD70-4E1A-BCCD-889905B381D9}	\Microsoft\Windows\Power Efficiency\Graphics\AnalyzeSystem	2018-04-25 15:46:42	-	-	-	-	0	0 \${@%SystemRoot%\system32\energytask.dll,-602} \${@%SystemRoot%\system32\energytask.dll,-602}	0 \${@%SystemRoot%\system32\energytask.dll,-600}
3	{03FF134D-C460-4122-A0AF-C9890D395221}	\Microsoft\Windows\SHELL\Indexer\Automatic	2018-04-25 15:46:42	-	-	-	-	0	0 \${@%SystemRoot%\system32\srchadmin.dll,-1902}	0 \${@%SystemRoot%\system32\srchadmin.dll,-1901}
3	{0420DA51-5939-4000-9C10-C04A4F122AA1F}	\Microsoft\Windows\PowerDirectoryClient\HandleCommand	2018-04-25 15:46:42	-	-	-	-	0	0 \${@%SystemRoot%\system32\ProvTool.exe,-101}	0 \${@%SystemRoot%\system32\ProvTool.exe,-100}
3	{04B3E894-D5B-4C4A-A4AA-C4F2E424E83}	\Microsoft\Windows\Power\CellularProvision	2018-04-25 15:46:42	-	-	-	-	0	0 \${@%SystemRoot%\system32\pppdsvc.dll,-200}	0 \${@%SystemRoot%\system32\pppdsvc.dll,-1902}
3	{066DC0C3-F07-4000-8A5F-70E74BE2E291}	\Microsoft\Windows\AER\Verifier\VerifierDpiBlur	2018-04-25 15:46:41	-	-	-	-	0	0 \${@%SystemRoot%\system32\pppdsvc.dll,-200}	0 \${@%SystemRoot%\system32\pppdsvc.dll,-1902}
3	{083F918C-CDF2-447B-9015-09501A4C43B1}	\Microsoft\Windows\WOW64\High-Value\On	2018-04-25 15:46:42	-	-	-	-	0	0 \${@%SystemRoot%\system32\WofTasks.dll,-601}	0 \${@%SystemRoot%\system32\WofTasks.dll,-602}
3	{09131E27-3793-4B1E-A11E-7D03E4C18BD1}	\Microsoft\Windows\CloudService\WakeAndGo	2018-04-25 15:46:41	-	-	-	-	0	0 \${@%SystemRoot%\system32\ngtcskd.dll,-101}	0 \${@%SystemRoot%\system32\ngtcskd.dll,-102}
3	{0A4AA476-862F-4F8A-9A4B-873950FA632}	\Microsoft\Windows\Nlstart\WakeAndGo	2018-04-25 15:46:42	-	-	-	-	0	0 \${@%SystemRoot%\system32\pppdsvc.dll,-200}	0 \${@%SystemRoot%\system32\pppdsvc.dll,-1902}
3	{0BAF3FD2-708A-4B79-980C-434FFA4000F9}	\Microsoft\Windows\Start\StartCompon	2018-04-25 15:46:42	-	-	-	-	0	0 \${@%SystemRoot%\system32\WofTasks.dll,-601}	0 \${@%SystemRoot%\system32\WofTasks.dll,-602}
3	{0C5CF7FD-88F9-4B8F-F-8E26-96E31D36698}	\Microsoft\Windows\Sync\Sync	2018-04-25 15:46:42	-	-	-	-	0	0 \${@%SystemRoot%\system32\w32time.dll,-200}	0 \${@%SystemRoot%\system32\w32time.dll,-201}

Total rows: 172

Type viewer

File Machine View Input Devices Help Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) 25:00 2/16/2023

- Created date and author:

The screenshot shows the Registry Explorer interface with the 'TaskCache' tab selected. The left pane displays a tree view of registry keys under 'HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks'. A specific task, 'T1053_005_OnStartup', is expanded, showing its subkeys: 'RunOnce', 'Run', 'ProfileList', 'App Paths', 'Uninstall', 'StartMenuInternet', 'System', 'TaskCache', and 'Tree'. The right pane lists the tasks in the Task Cache:

Version	Key Name	Path	Created On	Last Start	Last Stop	Task State	Last Action Result	Source	Description	Author
3	(82D0187C-0468-49B9-A93C-193FD249BE60)	\T1053_005_OnStartup	2023-02-13 17:28:27	=	=	=	0	0		MSEdgeWin10\IEUser
3	(E0DE8EB8-4D0E-46B4-98E5-C7D6164DC190)	\T1053_005_OnLogon	2023-02-13 17:28:27	=	=	=	0	0		MSEdgeWin10\IEUser
3	(B860CC1F-4329-466B-B39D-60C4A629950)		2023-02-13 17:21:35				0	0	Periodic scan task.	
3	(C4D0964F-9514-47F3-8585-7952DFEB2A3)		2023-02-13 17:21:35				0	0	Periodic cleanup task.	
3	(D0019552-2CC4-47FC-C845-2F289F193016)		2023-02-13 17:21:35				0	0	Periodic maintenance task.	
3	(978AD0836-F203-4011-5-00F9-155D0E3E853)		2023-02-13 17:21:35				0	0	Periodic verification task.	
3	(FECDD653-3F81-4098-8-9383-9835A804269)		2023-02-13 17:19:24				0	0		
3	(6B8C041D-FE6E-46CE-E-8A0-8ECA8E87E78)		2023-02-13 17:13:32	2023-02-13 17:13:32	2023-02-13 17:13:55	0	1	Primary shell invocation for sediment pack	Sediment	

Total rows: 172

Type viewer

Selected hive: NTUSER.DAT Last write: 2/13/2023 5:28:27 PM +00:00 Key contains no values

File Machine View Input Devices Help Forensics-System (Ubuntu Subsystem + Forensic Tools Installed) 2/16/2023

- Using regripper output for the same problem:

The screenshot shows the Notepad++ interface displaying a text file with regripper output. The file contains several entries related to Task Cache tasks for the IEUser account. A search dialog is open in the foreground, showing the search term 'taskcache'.

```

39505 Path: file:///\\System Volume Information\\
39506 2 - LastWrite time: 2018-04-25 15:56:27Z
39507 Path: file:///C:\\{d0ladeff-47e1-48ca-a23e-54fad666c0f7}\\ProgramData\\Microsoft\\Windows\\Start Menu\\
39508
3 - LastWrite time: 2018-04-25 15:56:27Z
39509 Path: file:///C:\\{d0ladeff-47e1-48ca-a23e-54fad666c0f7}\\Users\\Default\\AppData\\
39510
4 - LastWrite time: 2018-04-25 15:56:27Z
39511 Path: file:///C:\\{d0ladeff-47e1-48ca-a23e-54fad666c0f7}\\Users\\IEUser\\AppData\\
39512
5 - LastWrite time: 2018-04-25 15:56:27Z
39513 Path: file:///C:\\{d0ladeff-47e1-48ca-a23e-54fad666c0f7}\\Users\\\\AppData\\
39514
6 - LastWrite time: 2018-04-25 15:56:27Z
39515 Path: file:///C:\\{d0ladeff-47e1-48ca-a23e-54fad666c0f7}\\Windows\\\\temp\\
39516
7 - LastWrite time: 2018-04-25 15:56:27Z
39517 Path: file:///C:\\{d0ladeff-47e1-48ca-a23e-54fad666c0f7}\\Users\\\\
39518
8 - LastWrite time: 2018-04-25 15:56:27Z
39519 Path: file:///C:\\{d0ladeff-47e1-48ca-a23e-54fad666c0f7}\\Windows..\\
39520
9 - LastWrite time: 2018-04-25 15:56:27Z
39521 Path: file:///\\RECYCLE.BIN\\
39522
39523 -----
39524 TaskCache v.20200427
39525 (Software) Checks TaskCache\\Tree root keys (not subkeys)
39526
39527 OneDrive Reporting Task-S-1-5-21-1058341133-2092417715-4019509128-1000
39528 LastWrite: 2023-02-13 17:10:49Z
39529 Id: (CB3FF708-D153-4221-9006-1BB3D37A740F)
39530 Task Reg Time: 2023-02-13 17:05:49Z
39531
39532 OneDrive Standalone Update Task-S-1-5-21-1058341133-2092417715-4019509128-1000
39533 LastWrite: 2018-04-25 15:51:26Z
39534 Id: (6006F9F1-4C31-408A-8045-536CB14A2781)
39535 Task Reg Time: 2018-04-25 15:51:26Z
39536 Task Last Run: 2023-02-13 17:07:05Z
39537 Task Completed: 2023-02-13 17:08:27Z
39538
39539 T1053_005_OnLogon
39540 LastWrite: 2023-02-13 17:28:27Z
39541 Id: (E0DE8EB8-4D0E-46B4-98E5-C7D6164DC190)
39542 Task Reg Time: 2023-02-13 17:28:27Z
39543
39544 -----
39545 tasks v.20200427
39546 (Software) Checks TaskCache\\Tasks subkeys
39547
39548 Path: \\Microsoft\\Windows\\Power Efficiency Diagnostics\\AnalyzeSystem
39549
39550 Normal text file length: 2,500,031 lines: 41,027 Ln: 39,981 Col: 10 Sel: 9|1 Windows (CR LF) UTF-8 2/16/2023

```

- What tasks did IEUser created, and what is the creation time.

T1053_005_OnLogon

LastWrite: 2023-02-13 17:28:27Z

Id: {E0DE8EB5-4D0E-46B4-99E5-CD76164DC190}

Task Reg Time: 2023-02-13 17:28:27Z

T1053_005_OnStartup

LastWrite: 2023-02-13 17:28:27Z

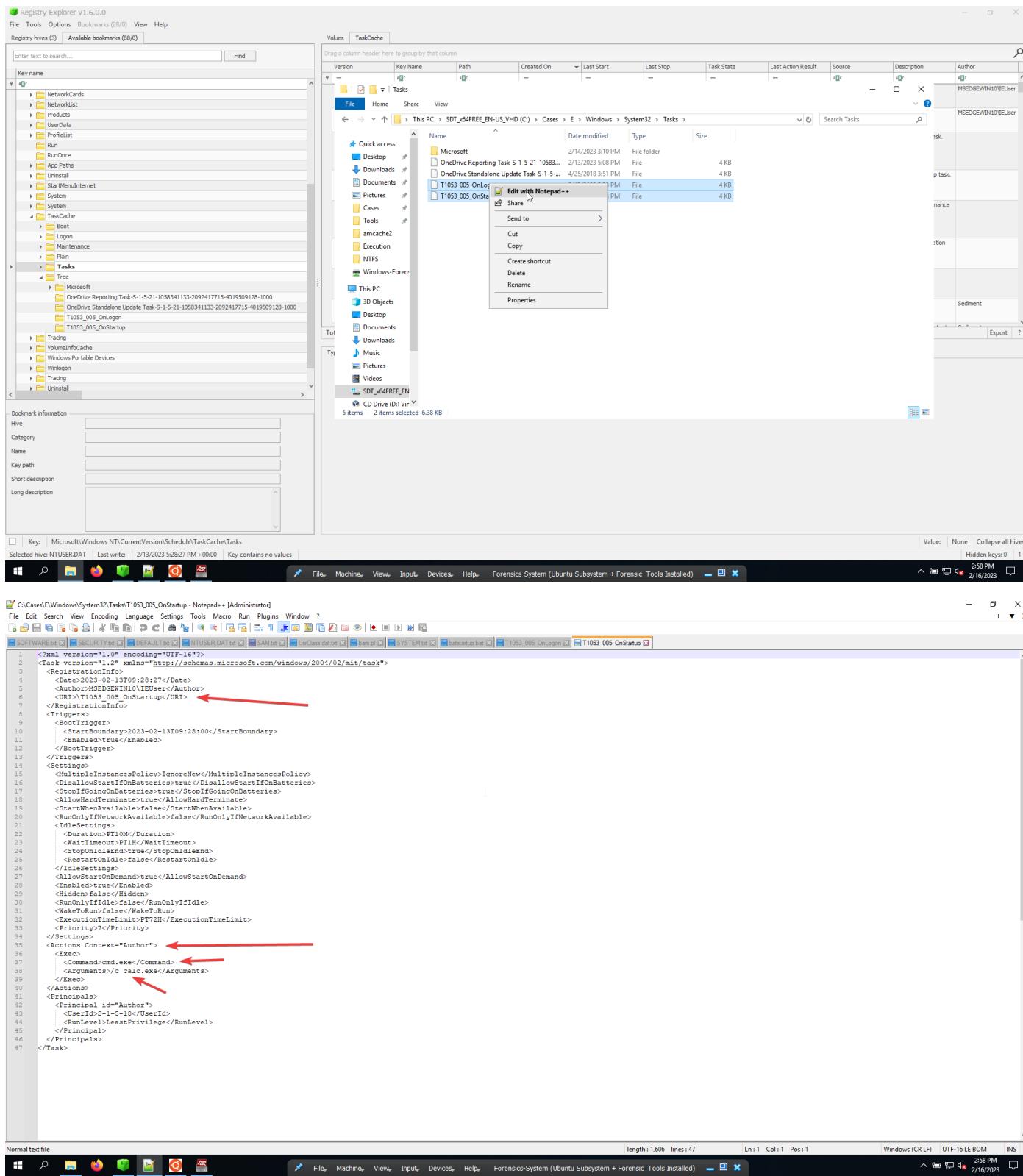
Id: {82DD187C-046B-45B9-A5C1-934FD249BE60}

Task Reg Time: 2023-02-13 17:28:27Z

- How many times did they execute.
 - The tasks didn't have time to execute, because of the lack of booting, or rebooting the system.

3	{82DD187C-046B-45B9-A5C1-934FD249BE60}	\T1053_005_OnStartup	2023-02-13 17:28:27			0	0		MSEdgeWin10\IEUser
3	{E0DE8EB5-4D0E-46B4-99E5-CD76164DC190}	\T1053_005_OnLogon	2023-02-13 17:28:27			0	0		MSEdgeWin10\IEUser

- You can see the information about tasks by opening them and view the XML code related to it.



Sysinternals autoruns

- Easier information gathering with Sysinternals Autoruns.

- Sysinternals Autoruns: <https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns>

```

1 <?xml version="1.0" encoding="UTF-16"?>
2 <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
3 <RegistrationInfo>
4 <StartBoundary>2023-02-13T09:28:27</StartBoundary>
5 <Author>MSDEGENIN10.IIEUser</Author>
6 <URI>T1053_005_OnStartup</URI>
7 </RegistrationInfo>
8 <Triggers>
9 <BootTrigger>
10 <StartBoundary>2023-02-13T09:28:00</StartBoundary>
11 <Enabled>true</Enabled>
12 </BootTrigger>
13 </Triggers>
14 <Settings>
15 <MultipleInstancesPolicy>TolerateNewMultiInstancePolicy</MultipleInstancesPolicy>
16 <DisallowStartIfBatteriesLow>true</DisallowStartIfBatteriesLow>
17 <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
18 <AllowHardTerminate>true</AllowHardTerminate>
19 <StartWhenAvailable>false</StartWhenAvailable>
20 <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
21 <RunOnlyIfIdle>false</RunOnlyIfIdle>
22 <Duration>T10H</Duration>
23 <WaitTimeout>PT1H</WaitTimeout>
24 <StopOnIdleEnd>true</StopOnIdleEnd>
25 <RestartOnFailure>false</RestartOnFailure>
26 <IdleSettings>
27 <AllowStartOnDemand>true</AllowStartOnDemand>
28 <Enabled>true</Enabled>
29 <Hidden>false</Hidden>
30 <RunOnlyIfIdling>false</RunOnlyIfIdling>
31 <WakeToRun>false</WakeToRun>
32 <ExecutionTimeLimit>PT2H</ExecutionTimeLimit>
33 <Priority>7</Priority>
34 </Settings>
35 <Actions Context="Author">
36 <Exec>
37 <Command>cmd.exe</Command>
38 <Arguments>/c calc.exe</Arguments>
39 </Exec>
40 </Actions>
41 <Principal>
42 <Principal id="Author">
43 <UserId>S-1-5-18</UserId>
44 <RunLevel>LeastPrivilege</RunLevel>
45 </Principal>
46 </Principals>
47 </Task>

```

Normal text file length: 1,606 lines: 47 Ln: 1 Col: 1 Pos: 1 Windows (CR LF) UTF-16 LE BOM INS 3:03 PM 2/16/2023

- Mount the image again and run the application as Administrator.

```

1 <?xml version="1.0" encoding="UTF-16"?>
2 <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">
3 <RegistrationInfo>
4 <StartBoundary>2023-02-13T09:28:27</StartBoundary>
5 <Author>MSDEGENIN10.IIEUser</Author>
6 <URI>T1053_005_OnStartup</URI>
7 </RegistrationInfo>
8 <Triggers>
9 <BootTrigger>
10 <StartBoundary>2023-02-13T09:28:00</StartBoundary>
11 <Enabled>true</Enabled>
12 </BootTrigger>
13 </Triggers>
14 <Settings>
15 <MultipleInstancesPolicy>TolerateNewMultiInstancePolicy</MultipleInstancesPolicy>
16 <DisallowStartIfBatteriesLow>true</DisallowStartIfBatteriesLow>
17 <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>
18 <AllowHardTerminate>true</AllowHardTerminate>
19 <StartWhenAvailable>false</StartWhenAvailable>
20 <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>
21 <RunOnlyIfIdle>false</RunOnlyIfIdle>
22 <Duration>T10H</Duration>
23 <WaitTimeout>PT1H</WaitTimeout>
24 <StopOnIdleEnd>true</StopOnIdleEnd>
25 <RestartOnFailure>false</RestartOnFailure>
26 <IdleSettings>
27 <AllowStartOnDemand>true</AllowStartOnDemand>
28 <Enabled>true</Enabled>
29 <Hidden>false</Hidden>
30 <RunOnlyIfIdling>false</RunOnlyIfIdling>
31 <WakeToRun>false</WakeToRun>
32 <ExecutionTimeLimit>PT2H</ExecutionTimeLimit>
33 <Priority>7</Priority>
34 </Settings>
35 <Actions Context="Author">
36 <Exec>
37 <Command>cmd.exe</Command>
38 <Arguments>/c calc.exe</Arguments>
39 </Exec>
40 </Actions>
41 <Principal>
42 <Principal id="Author">
43 <UserId>S-1-5-18</UserId>
44 <RunLevel>LeastPrivilege</RunLevel>
45 </Principal>
46 </Principals>
47 </Task>

```

Normal text file length: 1,606 lines: 47 Ln: 1 Col: 1 Pos: 1 Windows (CR LF) UTF-16 LE BOM INS 3:04 PM 2/16/2023

Registry Explorer V1.6.0.0

File Tools Options Bookmarks (28/0) View Help

Registry hives (3) Available bookmarks (88/0)

Enter text to search... Find

Key name

- NetworkCards
- NetworkList
- Products
- User Data
- Run
- RunOnce
- App Paths
- Uninstall
- StartMenu\Internet
- System
- Task Cache
- Tasks
- Tree
- Microsoft
- OneDrive Reporting
- OneDrive Standard
- T1053_005_OvLogon
- T1053_005_OvStart
- Trading
- Volumetric Cache
- Windows Portable Devices
- Winlogon
- Trading
- Uninstall

Values TaskCache

Drag a column header here to group by that column

Autoruns - Sysinternals www.sysinternals.com [Administrator] [WIN-9OHAJ6CQHQM]\Administrator

Offline System

Select the directories of the offline system:

System Root: E:\Windows User Profile: E:\Users\ElUser

OK Cancel Command Processor (Verified) Microsoft Windows C:\Windows\system32\cmd.exe Tue Feb 14 00:37:46 2023 Sat Sep 7 00:20:22 2019

30000 Windows Command Processor (Verified) Microsoft Windows C:\Windows\system32\cmd.exe Sat Sep 15 07:19:24 2018 Sat Sep 7 00:20:22 2019

HKEY_SOFTWARE\Microsoft\Active Setup\Installed Components n/a Microsoft .NET IE SECURITY REGISTRATION (Verified) Microsoft Corporation C:\Windows\System32\mscories.dll Sat Sep 7 00:17:18 2018 Sat Sep 15 07:11:57 2018

HKEY_SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components n/a Microsoft .NET IE SECURITY REGISTRATION (Verified) Microsoft Corporation C:\Windows\System32\mscories.dll Sat Sep 7 00:17:18 2018 Sat Sep 15 07:11:57 2018

HKEY_CLASSES\ShellEx\ContextMenuHandlers ANotepad+-64 ShellHandler for Notepad++ (64 bit) (Verified) Notepad++ C:\Program Files\Notepad+-\NppShell_06.dll Mon Feb 13 16:04:21 2023 Fri Jan 27 02:27:54 2023

Internet Explorer Scheduled Tasks

Microsoft.WindowsServerManager.CleanupOldPerfLogs Microsoft .Console Based Script Host (Verified) Microsoft Windows C:\Windows\system32\scriptc.exe Sat Sep 15 07:12:39 2018

Microsoft.WindowsSoftwareInventoryLoggingCollection Windows Command Processor (Verified) Microsoft Windows C:\Windows\system32\cmd.exe Sat Sep 7 00:20:22 2019

Microsoft.WindowsSoftwareInventoryLoggingConfiguration Windows Command Processor (Verified) Microsoft Windows C:\Windows\system32\cmd.exe Sat Sep 7 00:20:22 2019

Mozilla Firefox Background Update 30804680A4FA39CB The Background Update task checks for updates... (Verified) Mozilla Corporation C:\Program Files\Mozilla Firefox\firefox.exe Fri Jan 27 19:51:17 2023

Mozilla Firefox Default Browser Agent 30804680A4FA39CB The Default Browser Agent task checks... (Verified) Mozilla Corporation C:\Program Files\Mozilla Firefox\default-browser-agent.exe Fri Jan 27 19:51:17 2023

Task Scheduler

Microsoft.WindowsServerManager.CleanupOldPerfLogs Microsoft .Console Based Script Host (Verified) Microsoft Windows C:\Windows\system32\scriptc.exe Thu Feb 16 10:04:49 2023

Windows Task Scheduler

HKLM\System\CurrentControlSet\Services Services

File Home Share View Application Tools

Bookmark information

Hive Category Name Key path Short description Long description

Ready

Key: Microsoft.Windows NT\CurrentVersion\Schedule\TaskCache\Tasks

Selected hive: NTUSER.DAT Last write: 2/13/2023 5:28:27 PM +00:00 Key contains no values

Value None Collapse all hives Hidden keys: 0 1

3:00 PM 2/16/2023

Autoruns - Sysinternals www.sysinternals.com [Administrator] [WIN-9OHAJ6CQHQM]\Administrator

File Search Entry User Options Category Help

Quick Filter

LSA Providers Internet Explorer Scheduled Tasks Services... Drivers... Codec... Boot Execute Image Hijacks AppInit Known DLLs WinLogon Winsock Providers Print Monitors

Autoruns Entry Description Publisher Image Path Timestamp Virus Total

Logon

Atomic Red Team (highlighted with a red arrow)

HKEY_SOFTWARE\Microsoft\Windows\CurrentVersion\Run

OneDrive Microsoft OneDrive (Verified) Microsoft Corporation C:\Users\ElUser\AppData\Local\Microsoft\OneDrive\OneDrive.exe Mon Feb 13 17:09:03 2023

rdclip RDP Clipboard Monitor (Not Verified) Microsoft Corporation C:\Windows\system32\rdclip.exe Thu Apr 11 23:34:42 2018

HKEY_SOFTWARE\Microsoft\Windows\CurrentVersion\Run

binfo File not found: C:\Path\AtomicRedTeam.exe Mon Feb 13 17:28:22 2023

SecurityHealth Windows Defender notification icon (Not Verified) Microsoft Corporation C:\Program Files\Windows Defender\MSASClient.exe Wed Apr 11 23:33:58 2018

VBoxTray VirtualBox Guest Additions Tray Application (Not Verified) Oracle and/or its aff... C:\Windows\system32\VBoxTray.exe Wed Jan 11 07:20:56 2023

explorer.exe Windows Explorer (Not Verified) Microsoft Corporation C:\Windows\explorer.exe Wed Apr 11 23:34:44 2018

cmd.exe Windows Command Processor (Not Verified) Microsoft Corporation C:\Windows\system32\cmd.exe Wed Apr 11 23:34:14 2018

HKEY_SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Shell

userinit Windows Theme API (Not Verified) Microsoft Corporation C:\Windows\system32\themenui.exe Mon Feb 13 17:56:58 2023

C:\Windows\system32\userinit.exe Userinit Logon Application (Not Verified) Microsoft Corporation C:\Windows\system32\userinit.exe Wed Apr 11 23:34:22 2018

HKEY_SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\VmApplet

SystemPropertiesPerformance.exe/pagefile Change Computer Performance Settings (Not Verified) Microsoft Corporation C:\Windows\system32\SystemPropertiesPerformance.exe Mon Feb 13 17:56:58 2023

HKEY_SOFTWARE\Microsoft\Active Setup\Installed Components

Microsoft Windows Media Player Microsoft Windows Media Player Setup... (Not Verified) Microsoft Corporation C:\Windows\system32\unregmp2.exe Wed Apr 11 06:39:00 2018

Microsoft Windows Media Player Microsoft Windows Media Player Setup... (Not Verified) Microsoft Corporation C:\Windows\system32\unregmp2.exe Wed Apr 11 06:39:00 2018

n/a Microsoft .NET IE SECURITY REGISTRATION (Verified) Microsoft Corporation C:\Windows\System32\mscories.dll Wed Apr 11 23:33:56 2018

Themes Setup Windows Theme API (Not Verified) Microsoft Corporation C:\Windows\system32\themenui.exe Wed Apr 11 23:34:36 2018

Web Platform Customizations IE Per-User Initialization Utility (Not Verified) Microsoft Corporation C:\Windows\System32\ieuininit.exe Wed Apr 11 23:33:56 2018

Windows Desktop Update Windows Shell Common DLL (Not Verified) Microsoft Corporation C:\Windows\system32\shell32.dll Wed Apr 11 23:34:36 2018

HKEY_SOFTWARE\Microsoft\Windows NT\CurrentVersion\WindowsIconService.dll

IconCodeService.dll Converts a PNG part of the icon to a lega... (Not Verified) Microsoft Corporation C:\Windows\system32\IconCodeService.dll Wed Apr 11 23:34:25 2018

HKEY_SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components

Microsoft Windows Media Player Microsoft Windows Media Player Setup... (Not Verified) Microsoft Corporation C:\Windows\system32\unregmp2.exe Wed Apr 11 06:39:00 2018

Microsoft Windows Media Player Microsoft Windows Media Player Setup... (Not Verified) Microsoft Corporation C:\Windows\system32\unregmp2.exe Wed Apr 11 06:39:00 2018

n/a Microsoft .NET IE SECURITY REGISTRATION (Verified) Microsoft Corporation C:\Windows\SysWOW64\mscories.dll Wed Apr 11 23:33:56 2018

Internet Explorer

HKEY_SOFTWARE\Microsoft\Internet Explorer\UrlSearchHooks

Microsoft Url Search Hook Internet Browser (Not Verified) Microsoft Corporation C:\Windows\System32\ieframe.dll Wed Apr 11 23:33:56 2018

Scheduled Tasks

Boot Execute

HKEY_SOFTWARE\Microsoft\Internet Explorer\UrlSearchHooks

autocheck autochk * Auto Check Utility (Not Verified) Microsoft Corporation C:\Windows\System32\autochik.exe Tue Feb 14 08:11:25 2023

Image Hijacks

Scanning WinLogon... Done

File Machine View Input Devices Help Forensics-System (Ubuntu Subsystem + Forensic Tools Installed)

Press ESC to Cancel Offline scan: E:\Windows

3:09 PM 2/16/2023

Autorus - Sysinternals www.sysinternals.com (Administrator) [WIN-9OHAJ6CQHQ\administrator]

File Search Entry User Options Category Help

Quick Filter

LSA Providers Internet Explorer Scheduled Tasks Network Providers Services Drivers Codecs Boot Execute Image Hijacks WMI AppInit Known DLLs Office WinLogon Winsock Providers Print Monitors

Autorus Entry

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

Service Name	Description	Publisher	Image Path	Timestamp	Virus Total
AllJoynRouter	AllJoyn Router Service: Routes AllJoyn messages between devices.	(Not Verified) Microsoft Corporation	C:\Windows\System32\AllJoynRouter.dll	Mon Feb 13 17:56:59 2013	
ALG	Application Layer Gateway Service Provider	(Not Verified) Microsoft Corporation	C:\Windows\System32\alg.exe	Wed Apr 11 23:34:06 2018	
AppIDsvc	Application Identity: Determines and verifies the identity of applications.	(Not Verified) Microsoft Corporation	C:\Windows\System32\appidsvc.dll	Wed Apr 11 23:34:19 2018	
AppInfo	Application Information: Facilitates information exchange between applications.	(Not Verified) Microsoft Corporation	C:\Windows\System32\appinfo.dll	Wed Apr 11 23:34:06 2018	
AppMgmt	Application Management: Processes installed applications.	(Not Verified) Microsoft Corporation	C:\Windows\System32\appmgmt.dll	Thu Apr 12 09:19:31 2018	
AppReadiness	App Readiness: Gets apps ready for use through various mechanisms.	(Not Verified) Microsoft Corporation	C:\Windows\System32\appreadiness.dll	Wed Apr 11 23:34:52 2018	
AppClient	Microsoft App-V Client: Manages App-V packages.	(Not Verified) Microsoft Corporation	C:\Windows\system32\ApvClient.exe	Thu Apr 12 09:19:31 2018	
AppXDeployment	AppX Deployment Service (ApvxSVC): Provides deployment services for AppX packages.	(Not Verified) Microsoft Corporation	C:\Windows\system32\appxdpmnysvc.dll	Wed Apr 11 23:34:39 2018	
AppXSvc	AssignedAccessManager	(Not Verified) Microsoft Corporation	C:\Windows\System32\AssignedAccessManagerSvc.dll	Thu Apr 12 09:19:53 2018	
AssignedAccessManagerSvc	AssignedAccessManager	(Not Verified) Microsoft Corporation	C:\Windows\System32\AssignedAccessManagerSvc.dll	Thu Apr 12 09:19:53 2018	
AtomicsTestService_CMD	Atomics Test Service Command Line	(Not Verified) Microsoft Corporation	C:\Windows\System32\T1543.003\bin\AtomicService.exe	Thu Apr 12 09:19:53 2018	
AudioEndpointBuilder	Windows Audio Endpoint Builder: Manages audio for Windows.	(Not Verified) Microsoft Corporation	C:\Windows\System32\AudioEndpointBuilder.dll	Wed Apr 11 23:34:04 2018	
Audiosv	Windows Audio: Manages audio for Windows.	(Not Verified) Microsoft Corporation	C:\Windows\System32\Audiosv.dll	Wed Apr 11 23:34:04 2018	
BcastDVRUserService	Broadcast DVR User Service	(Not Verified) Microsoft Corporation	C:\Windows\System32\BcastDVRUserService.dll	Wed Apr 11 23:34:26 2018	
BDEsvc	BDE Service	(Not Verified) Microsoft Corporation	C:\Windows\System32\BdeSvc.dll	Wed Apr 11 23:34:04 2018	
BFE	Base Filtering Engine: The Base Filtering Engine.	(Not Verified) Microsoft Corporation	C:\Windows\System32\Bfe.dll	Wed Apr 11 23:34:12 2018	
BITS	Background Intelligent Transfer Service: Transfers files in the background.	(Not Verified) Microsoft Corporation	C:\Windows\System32\BITS.dll	Wed Apr 11 23:34:07 2018	
BluetoothUserService	Bluetooth User Support Service	(Not Verified) Microsoft Corporation	C:\Windows\System32\Bluetooth.UserService.dll	Wed Apr 11 23:34:02 2018	
BrokerInfrastructure	Broker Infrastructure	(Not Verified) Microsoft Corporation	C:\Windows\System32\BrokerInfrastructure.dll	Wed Apr 11 23:34:12 2018	
BTAGService	Bluetooth Audio Gateway Service: Service for audio.	(Not Verified) Microsoft Corporation	C:\Windows\System32\BTAGService.dll	Wed Apr 11 23:34:14 2018	
BtHvctpsvc	AV/CTP service: This is Audio Video Control.	(Not Verified) Microsoft Corporation	C:\Windows\System32\BtHvctpsvc.dll	Wed Apr 11 23:34:14 2018	
bthserv	Bluetooth Support Service: The Bluetooth Support Service.	(Not Verified) Microsoft Corporation	C:\Windows\System32\bthserv.dll	Wed Apr 11 23:34:14 2018	
camsv	Capability Access Manager Service: Provides access to capabilities.	(Not Verified) Microsoft Corporation	C:\Windows\System32\CapabilityAccessManager.dll	Wed Apr 11 23:34:06 2018	
CaptureService	CaptureService: OneCore Capture Service	(Not Verified) Microsoft Corporation	C:\Windows\System32\CaptureService.dll	Thu Apr 12 09:19:57 2018	
CDPSvc	Connected Devices Platform Service: This service manages connected devices.	(Not Verified) Microsoft Corporation	C:\Windows\System32\CDPSvc.dll	Wed Apr 11 23:34:06 2018	
CDPUserSvc	Connected Devices Platform User Service: Manages connected devices.	(Not Verified) Microsoft Corporation	C:\Windows\System32\CDPUserSvc.dll	Wed Apr 11 23:34:06 2018	
CertPropSvc	Certificate Propagation: Copies user certificates to other users.	(Not Verified) Microsoft Corporation	C:\Windows\System32\certprop.dll	Wed Apr 11 23:34:37 2018	
ClipSVC	Client License Service (ClipSVC): Provides client license management.	(Not Verified) Microsoft Corporation	C:\Windows\System32\ClipSVC.dll	Wed Apr 11 23:34:06 2018	
COMSysApp	COM+ System Application: Manages the COM+ system application.	(Not Verified) Microsoft Corporation	C:\Windows\System32\dllhost.exe	Wed Apr 11 23:34:22 2018	
CoreMessagingRegistrar	CoreMessaging: Manages communication between applications.	(Not Verified) Microsoft Corporation	C:\Windows\System32\coremessaging.dll	Wed Apr 11 23:34:19 2018	
CryptSvc	Cryptographic Services: Provides three cryptographic APIs.	(Not Verified) Microsoft Corporation	C:\Windows\System32\cryptsvc.dll	Wed Apr 11 23:34:20 2018	
CssService	Offline Files: The Offline Files service performs file operations.	(Not Verified) Microsoft Corporation	C:\Windows\System32\cssvc.dll	Thu Apr 12 09:19:49 2018	
DcomLaunch	DCOM Server Process Launcher: The DCOM server process launcher.	(Not Verified) Microsoft Corporation	C:\Windows\System32\rpcss.dll	Wed Apr 11 23:34:22 2018	
DefragSVC	Optimize drives: Helps the computer run faster.	(Not Verified) Microsoft Corporation	C:\Windows\System32\defragsvc.dll	Wed Apr 11 23:34:23 2018	
DeviceAssociationService	Device Association Service: Enables pairing of devices.	(Not Verified) Microsoft Corporation	C:\Windows\System32\des.dll	Wed Apr 11 23:34:12 2018	
DeviceInstall	Device Install Service: Enables a computer to install devices.	(Not Verified) Microsoft Corporation	C:\Windows\System32\umpnpmgr.dll	Wed Apr 11 23:34:15 2018	
DevicePickerUserSVC	DevicePicker: This user service is used for device picker.	(Not Verified) Microsoft Corporation	C:\Windows\System32\Windows.Devices.Picker.dll	Wed Apr 11 23:34:21 2018	
DevicesFlowUserSVC	DevicesFlow: Allows ConnectUX and PCs to communicate.	(Not Verified) Microsoft Corporation	C:\Windows\System32\DevicesFlowBroker.dll	Wed Apr 11 23:34:19 2018	

AtomicsTestService_CMD

Size: 4,096
Time: Thu Apr 28 01:14:48 2022
(Not Verified)
Version: 0.0.0.0
C:\AtomicRedTeam\atomics\T1543.003\bin\AtomicService.exe

Ready Offline scan: E:\Windows

File Machine View Input Devices Help Forensics-System (Ubuntu Subsystem + Forensic Tools Installed)

2:09 PM 2/16/2018