HOW TO FIND MALWARE USING SYSINTERNAL SUITE

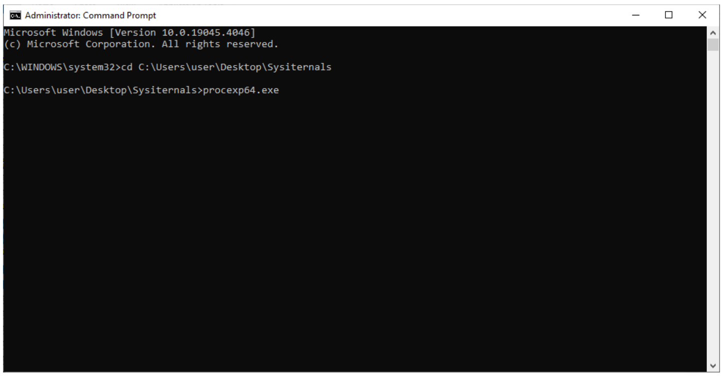
What to look for when analyzing the processes for malware:

- Processes that have no name
- Processes with no icon/image
- Processes with no description or company name
- Unsigned images
- Processes residing in the Windows directory or User profile
- Packed executables
- Suspicious URLs
- Processes with open TCP/IP connections
- Suspicious DLLs or services hosted by processes

Starting the Process

1. Run Process Explorer:

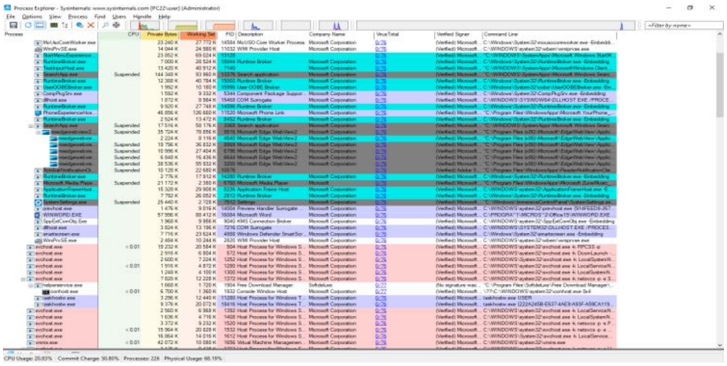
Open `procex64.exe` application located in the Sysinternals Suite folder. Alternatively, launch `procex64.exe` from the command prompt using the correct path to the file.



```
Microsoft Windows [Version 10.0.19045.4046]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd C:\Users\user\Desktop\Sysiternals

C:\Users\user\Desktop\Sysiternals>procexp64.exe
```



Process Explorer - Sysinternals: www.sysinternals.com [PC22\user] (Administrator)
File Options View Process Find Users Handle Help
<Filter by name>
Process CPU Private Bytes Working Set PID Description Company Name VirusTotal Verified Signer Command Line
CPU Usage: 20.83% Commit Charge: 30.80% Processes: 228 Physical Usage: 68.19%

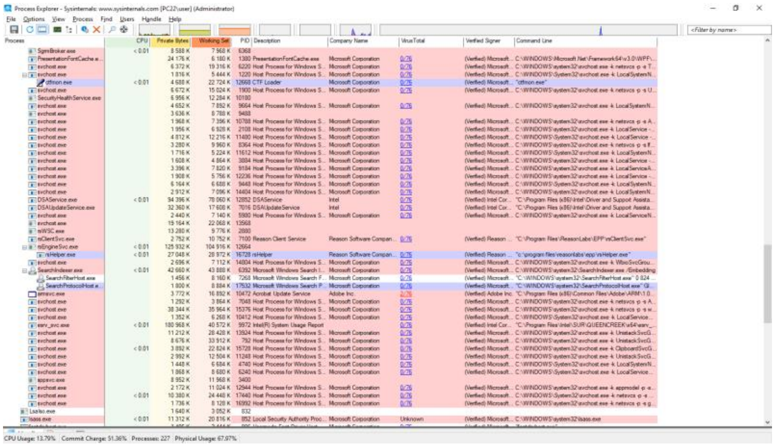
2. Options → Verify Image Signature:

Verify image signatures of processes. Missing signatures indicate potential red flags.

3. Options → VirusTotal → Check virustotal.com:

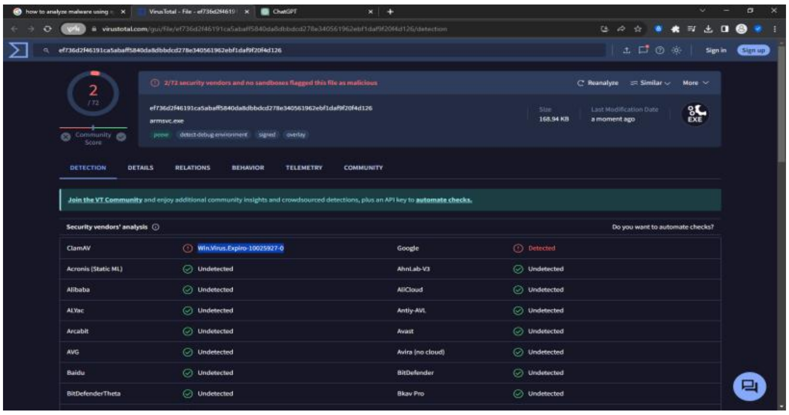
Click to check if running processes are legitimate. Pay attention to the numbers; they should ideally start with zero. Non-zero values may indicate suspicious activity.

Lets analyze the below process circles in red by clicking on the virus total number 2/72 to gain more info :



Process Explorer - Sysinternals: www.sysinternals.com [PC22\user] (Administrator)

CPU Usage: 13.79% Commit Charge: 51.36% Processes: 227 Physical Usage: 67.97%



virustotal.com/gui/file/ef736d2f46191ca5abaff5840da8dbbdcd278e340561962ebf1daf9f20f4d126/detection

ef736d2f46191ca5abaff5840da8dbbdcd278e340561962ebf1daf9f20f4d126

2/72 security vendors and no sandboxes flagged this file as malicious

ef736d2f46191ca5abaff5840da8dbbdcd278e340561962ebf1daf9f20f4d126
armsvc.exe

Size 168.94 KB
Last Modification Date a moment ago

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

ClamAV	Win.Virus.Expiro-10025927-0	Google	Detected
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected
Alibaba	Undetected	AliCloud	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avast	Undetected
AVG	Undetected	Avira (no cloud)	Undetected
Baidu	Undetected	BitDefender	Undetected
BitDefenderTheta	Undetected	Bkav Pro	Undetected

- 2/72 security vendors: This indicates that out of 72 different antivirus engines used by VirusTotal to scan the file, only 2 of them flagged it as potentially malicious. In other words, only 2 antivirus programs detected the file as a threat.

- No sandboxes flagged this file as malicious: Sandboxes are isolated environments used for safely executing and analyzing suspicious files without risking harm to the host system. In this case, none of the sandbox environments used by VirusTotal flagged the file as malicious. This could mean that the file doesn't exhibit obvious malicious behavior when executed in a controlled environment.

- ClamAV Win.Virus.Expiro-10025927-0 detected: ClamAV, an open-source antivirus engine, specifically detected the file as Win.Virus.Expiro-10025927-0. This indicates that ClamAV identified the file as a variant of the Expiro virus, which is a type of malware known for infecting executable files on Windows systems.

Overall, these results suggest that while one antivirus engine (ClamAV) flagged the file as malicious, the majority of antivirus engines did not detect it as a threat. However, it's essential to exercise caution with files that are flagged by any antivirus program, as they may still pose a risk to your system. You may want to further investigate the file and its source to determine whether it's safe to keep on your computer.

4. View → Select Columns → Check "Show Command Line":**

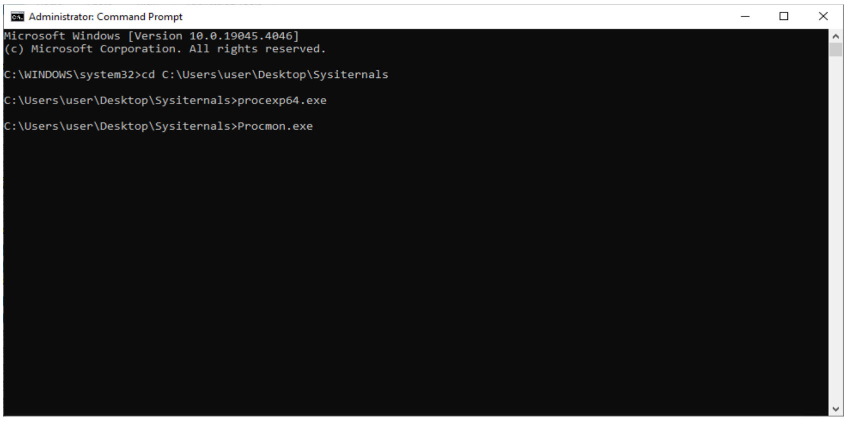
Enable the display of command-line information for processes.

5. Right-click on a Process → Properties:

- Explore additional information such as:
- Strings: Search for suspicious URLs.
- Image: Locate the folder where the process is running.
- TCP/IP: Check for open network connections.
- Threads: View information about process threads.
- Security: Examine process security settings.
- Environment: Review process environment variables.
- Performance: Analyze process performance metrics.

6. Run Process Monitor

Open Command Prompt and type procmon.exe, then press Enter.



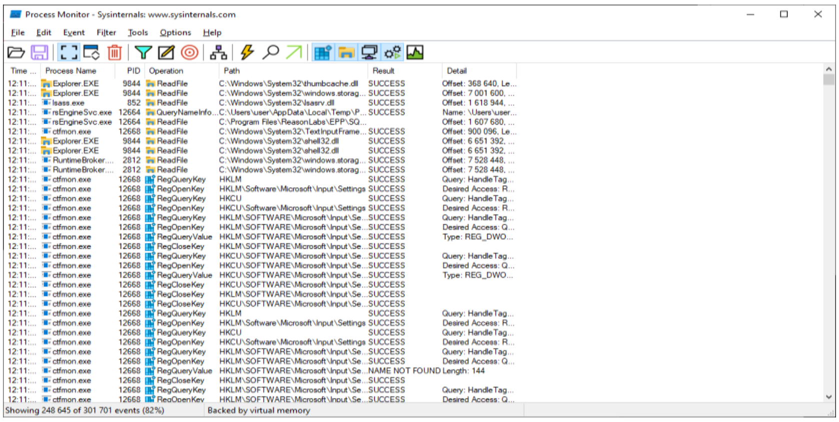
```
Microsoft Windows [Version 10.0.19045.4046]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd C:\Users\user\Desktop\Sysiternals

C:\Users\user\Desktop\Sysiternals>procexp64.exe

C:\Users\user\Desktop\Sysiternals>Procmon.exe
```

Process monitor will open



Process Monitor - Sysinternals: www.sysinternals.com

```
Time ...  Process Name     PID    Operation       Path                                          Result          Detail
12:11:... Explorer.EXE     9844   ReadFile        C:\Windows\System32\thumbcache.dll            SUCCESS         Offset: 368 640, Le...
12:11:... Explorer.EXE     9844   ReadFile        C:\Windows\System32\windows.storag...         SUCCESS         Offset: 7 001 600, ...
12:11:... lsass.exe        852    ReadFile        C:\Windows\System32\lsasrv.dll                SUCCESS         Offset: 1 618 944, ...
12:11:... rsEngineSvc.exe  12664  QueryNameInfo...C:\Users\user\AppData\Local\Temp\P...         SUCCESS         Name: \Users\user...
12:11:... rsEngineSvc.exe  12664  ReadFile        C:\Program Files\ReasonLabs\EPP\SQ...                         Offset: 1 607 680, ...
12:11:... ctfmon.exe       12668  ReadFile        C:\Windows\System32\TextInputFrame...         SUCCESS         Offset: 900 096, Le...
12:11:... Explorer.EXE     9844   ReadFile        C:\Windows\System32\shell32.dll               SUCCESS         Offset: 6 651 392, ...
12:11:... Explorer.EXE     9844   ReadFile        C:\Windows\System32\shell32.dll               SUCCESS         Offset: 6 651 392, ...
12:11:... RuntimeBroker....2812   ReadFile        C:\Windows\System32\windows.storag...         SUCCESS         Offset: 7 528 448, ...
12:11:... RuntimeBroker....2812   ReadFile        C:\Windows\System32\windows.storag...         SUCCESS         Offset: 7 528 448, ...
12:11:... ctfmon.exe       12668  RegQueryKey     HKLM                                          SUCCESS         Query: HandleTag...
12:11:... ctfmon.exe       12668  RegOpenKey      HKLM\Software\Microsoft\Input\Settings        SUCCESS         Desired Access: R...
12:11:... ctfmon.exe       12668  RegQueryKey     HKCU                                          SUCCESS         Query: HandleTag...
12:11:... ctfmon.exe       12668  RegOpenKey      HKCU\Software\Microsoft\Input\Settings        SUCCESS         Desired Access: R...
12:11:... ctfmon.exe       12668  RegQueryKey     HKLM\SOFTWARE\Microsoft\Input\Se...           SUCCESS         Query: HandleTag...
12:11:... ctfmon.exe       12668  RegOpenKey      HKLM\SOFTWARE\Microsoft\Input\Se...           SUCCESS         Desired Access: Q...
12:11:... ctfmon.exe       12668  RegQueryValue   HKLM\SOFTWARE\Microsoft\Input\Se...           SUCCESS         Type: REG_DWO...
12:11:... ctfmon.exe       12668  RegCloseKey     HKLM\SOFTWARE\Microsoft\Input\Se...           SUCCESS
12:11:... ctfmon.exe       12668  RegQueryKey     HKCU\SOFTWARE\Microsoft\Input\Se...           SUCCESS         Query: HandleTag...
12:11:... ctfmon.exe       12668  RegOpenKey      HKCU\SOFTWARE\Microsoft\Input\Se...           SUCCESS         Desired Access: Q...
12:11:... ctfmon.exe       12668  RegQueryValue   HKCU\SOFTWARE\Microsoft\Input\Se...           SUCCESS         Type: REG_DWO...
12:11:... ctfmon.exe       12668  RegCloseKey     HKCU\SOFTWARE\Microsoft\Input\Se...           SUCCESS
12:11:... ctfmon.exe       12668  RegCloseKey     HKLM\SOFTWARE\Microsoft\Input\Se...           SUCCESS
12:11:... ctfmon.exe       12668  RegCloseKey     HKCU\SOFTWARE\Microsoft\Input\Se...           SUCCESS
12:11:... ctfmon.exe       12668  RegQueryKey     HKLM                                          SUCCESS         Query: HandleTag...
12:11:... ctfmon.exe       12668  RegOpenKey      HKLM\Software\Microsoft\Input\Settings        SUCCESS         Desired Access: R...
12:11:... ctfmon.exe       12668  RegQueryKey     HKCU                                          SUCCESS         Query: HandleTag...
12:11:... ctfmon.exe       12668  RegOpenKey      HKCU\Software\Microsoft\Input\Settings        SUCCESS         Desired Access: R...
12:11:... ctfmon.exe       12668  RegQueryKey     HKLM\SOFTWARE\Microsoft\Input\Se...           SUCCESS         Query: HandleTag...
12:11:... ctfmon.exe       12668  RegOpenKey      HKLM\SOFTWARE\Microsoft\Input\Se...           SUCCESS         Desired Access: Q...
12:11:... ctfmon.exe       12668  RegQueryValue   HKLM\SOFTWARE\Microsoft\Input\Se...           NAME NOT FOUND  Length: 144
12:11:... ctfmon.exe       12668  RegCloseKey     HKLM\SOFTWARE\Microsoft\Input\Se...           SUCCESS
12:11:... ctfmon.exe       12668  RegQueryKey     HKLM\SOFTWARE\Microsoft\Input\Se...           SUCCESS         Query: HandleTag...
12:11:... ctfmon.exe       12668  RegOpenKey      HKLM\SOFTWARE\Microsoft\Input\Se...           SUCCESS         Desired Access: Q...
Showing 248 645 of 301 701 events (82%)    Backed by virtual memory
```

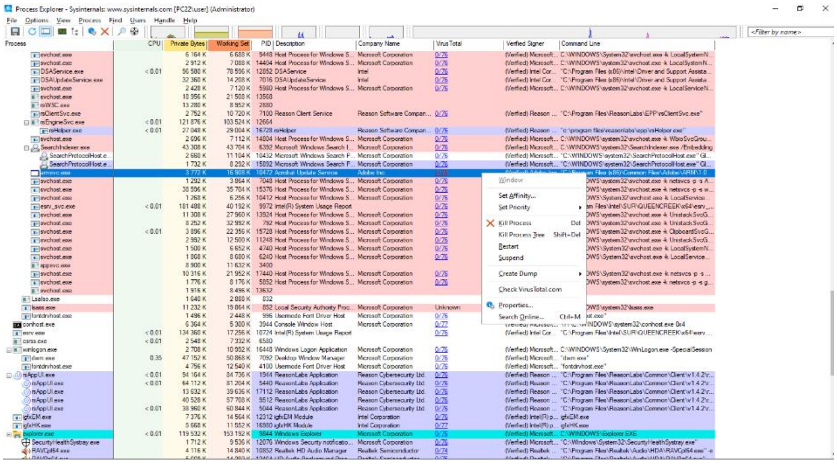
7. Filter Processes

- Use Process Monitor to filter processes that seem suspicious or those you want to monitor closely.
- Right-click on a row → Include, Exclude, etc. Click on Filtering icon for more complex filtering.
- Example: Category = Write only shows modification activity, where malware is likely to appear.

8. Suspend or kill Malicious Activity

Identify suspicious processes in Process Monitor.

Right-click on the process and choose an appropriate action such as suspending or killing the process.



Process Explorer - Sysinternals: www.sysinternals.com [PC22\user] (Administrator)

```
Process                    CPU     Private Bytes  Working Set  PID    Description                      Company Name               Virus Total  Verified Signer          Command Line
svchost.exe                        6 164 K        6 688 K      9448   Host Process for Windows S...    Microsoft Corporation      0/76         (Verified) Microsoft...  C:\WINDOWS\System32\svchost.exe -k LocalSystemN...
svchost.exe                        2 912 K        7 088 K      14404  Host Process for Windows S...    Microsoft Corporation      0/76         (Verified) Microsoft...  C:\WINDOWS\system32\svchost.exe -k LocalSystemN...
DSAService.exe             < 0.01  96 580 K       78 596 K     12852  DSAService                       Intel                      0/76         (Verified) Intel Cor...  "C:\Program Files (x86)\Intel\Driver and Support Assista...
DSAUpdateService.exe               32 360 K       14 208 K     7016   DSAUpdateService                 Intel                      0/76         (Verified) Intel Cor...  "C:\Program Files (x86)\Intel\Driver and Support Assista...
svchost.exe                        2 428 K        7 120 K      5980   Host Process for Windows S...    Microsoft Corporation      0/76         (Verified) Microsoft...  C:\WINDOWS\system32\svchost.exe -k LocalServiceN...
svchost.exe                        18 956 K       21 508 K     13568
rsWSC.exe                          13 280 K       8 952 K      2880
rsClientSvc.exe                    2 752 K        10 720 K     7100   Reason Client Service            Reason Software Compan...  0/76         (Verified) Reason ...    "C:\Program Files\ReasonLabs\EPP\rsClientSvc.exe"
rsEngineSvc.exe            < 0.01  121 876 K      103 524 K    12664
  rsHelper.exe             < 0.01  27 048 K       29 004 K     16728  rsHelper                         Reason Software Compan...  0/76         (Verified) Reason ...    "c:\program files\reasonlabs\epp\rsHelper.exe"
svchost.exe                        2 696 K        7 112 K      14804  Host Process for Windows S...    Microsoft Corporation      0/76         (Verified) Microsoft...  C:\WINDOWS\system32\svchost.exe -k WbioSvcGrou...
SearchIndexer.exe                  43 308 K       43 704 K     6392   Microsoft Windows Search I...    Microsoft Corporation      0/76         (Verified) Microsoft...  C:\WINDOWS\system32\SearchIndexer.exe /Embedding
  SearchProtocolHost.e...          2 660 K        11 104 K     10432  Microsoft Windows Search P...    Microsoft Corporation      0/76         (Verified) Microsoft...  "C:\WINDOWS\system32\SearchProtocolHost.exe" Gl...
  SearchProtocolHost.e...          1 732 K        8 292 K      15092  Microsoft Windows Search P...    Microsoft Corporation      0/76         (Verified) Microsoft...  "C:\WINDOWS\system32\SearchProtocolHost.exe" Gl...
armsvc.exe                         3 772 K        16 908 K     10472  Acrobat Update Service           Adobe Inc.                 0/76         (Verified) Adobe Inc.    "C:\Program Files (x86)\Common Files\Adobe\ARM\1.0...
svchost.exe                        1 292 K        3 864 K      7048   Host Process for Windows S...    Microsoft Corporation      0/76                                  ...OWS\system32\svchost.exe -k netsvcs -p -s A...
svchost.exe                        38 596 K       35 704 K     15376  Host Process for Windows S...    Microsoft Corporation      0/76                                  ...OWS\system32\svchost.exe -k netsvcs -p -s w...
svchost.exe                        1 268 K        6 256 K      10412  Host Process for Windows S...    Microsoft Corporation      0/76                                  ...OWS\System32\svchost.exe -k LocalService...
esrv_svc.exe               < 0.01  181 488 K      40 192 K     9972   Intel(R) System Usage Report                                0/76                                  ...am Files\Intel\SUR\QUEENCREEK\x64\esrv_...
svchost.exe                        11 308 K       27 960 K     13924  Host Process for Windows S...    Microsoft Corporation      0/76                                  ...OWS\system32\svchost.exe -k UnistackSvcG...
svchost.exe                        8 252 K        32 992 K     792    Host Process for Windows S...    Microsoft Corporation      0/76                                  ...OWS\system32\svchost.exe -k UnistackSvcG...
svchost.exe                < 0.01  3 896 K        22 356 K     15728  Host Process for Windows S...    Microsoft Corporation      0/76                                  ...OWS\system32\svchost.exe -k ClipboardSvcG...
svchost.exe                        2 992 K        12 500 K     11248  Host Process for Windows S...    Microsoft Corporation      0/76                                  ...OWS\system32\svchost.exe -k UnistackSvcG...
svchost.exe                        1 500 K        6 652 K      4740   Host Process for Windows S...    Microsoft Corporation      0/76                                  ...OWS\System32\svchost.exe -k LocalSystemN...
svchost.exe                        1 868 K        8 680 K      6240   Host Process for Windows S...    Microsoft Corporation      0/76                                  ...OWS\System32\svchost.exe -k LocalService...
appsvc.exe                         8 900 K        11 632 K     3400
svchost.exe                        10 316 K       21 952 K     17440  Host Process for Windows S...    Microsoft Corporation      0/76                                  ...OWS\System32\svchost.exe -k netsvcs -p -s ...
svchost.exe                        1 776 K        8 176 K      5852   Host Process for Windows S...    Microsoft Corporation      0/76                                  ...OWS\system32\svchost.exe -k netsvcs -p -s g...
svchost.exe                        1 916 K        8 496 K      13632
Lsalso.exe                         1 640 K        2 888 K      832
lsass.exe                          11 232 K       19 864 K     852    Local Security Authority Proc... Microsoft Corporation      Unknown                               ...OWS\system32\lsass.exe
fontdrvhost.exe                    1 496 K        2 448 K      996    Usermode Font Driver Host        Microsoft Corporation      0/76                                  ...st.exe"
conhost.exe                        6 364 K        5 300 K      3944   Console Window Host              Microsoft Corporation      0/77         (Verified) Microsoft...  ...INDOWS\system32\conhost.exe 0x4
esrv.exe                   < 0.01  134 360 K      17 256 K     10724  Intel(R) System Usage Report                                0/76         (Verified) Intel Cor...  "C:\Program Files\Intel\SUR\QUEENCREEK\x64\esrv....
csrss.exe                  < 0.01  2 548 K        7 332 K      6580
winlogon.exe                       2 708 K        10 992 K     16448  Windows Logon Application        Microsoft Corporation      0/76         (Verified) Microsoft...  C:\WINDOWS\System32\WinLogon.exe -SpecialSession
  dwm.exe                  0.35    47 152 K       50 868 K     7092   Desktop Window Manager           Microsoft Corporation      0/76         (Verified) Microsoft...  "dwm.exe"
  fontdrvhost.exe                  4 756 K        12 540 K     4100   Usermode Font Driver Host        Microsoft Corporation      0/76         (Verified) Microsoft...  "fontdrvhost.exe"
rsAppUI.exe                < 0.01  94 164 K       84 736 K     1944   ReasonLabs Application           Reason Cybersecurity Ltd.  0/76         (Verified) Reason ...    "C:\Program Files\ReasonLabs\Common\Client\v1.4.2\v...
  rsAppUI.exe              < 0.01  64 112 K       81 204 K     5440   ReasonLabs Application           Reason Cybersecurity Ltd.  0/76         (Verified) Reason ...    "C:\Program Files\ReasonLabs\Common\Client\v1.4.2\v...
  rsAppUI.exe                      13 632 K       39 636 K     17112  ReasonLabs Application           Reason Cybersecurity Ltd.  0/76         (Verified) Reason ...    "C:\Program Files\ReasonLabs\Common\Client\v1.4.2\v...
  rsAppUI.exe                      40 528 K       57 708 K     9512   ReasonLabs Application           Reason Cybersecurity Ltd.  0/76         (Verified) Reason ...    "C:\Program Files\ReasonLabs\Common\Client\v1.4.2\v...
  rsAppUI.exe              < 0.01  38 960 K       60 844 K     5044   ReasonLabs Application           Reason Cybersecurity Ltd.  0/76         (Verified) Reason ...    "C:\Program Files\ReasonLabs\Common\Client\v1.4.2\v...
igfxEM.exe                         7 376 K        14 564 K     12312  igfxEM Module                    Intel Corporation          0/76         (Verified) Intel(R) p... igfxEM.exe
igfxHK.exe                         5 668 K        11 552 K     16980  igfxHK Module                    Intel Corporation          0/77         (Verified) Intel(R) p... igfxHK.exe
explorer.exe               < 0.01  119 532 K      153 192 K    9844   Windows Explorer                 Microsoft Corporation      0/76         (Verified) Microsoft...  C:\WINDOWS\Explorer.EXE
  SecurityHealthSystray.exe        1 712 K        9 536 K      12076  Windows Security notificatio...  Microsoft Corporation      0/76         (Verified) Microsoft...  "C:\Windows\System32\SecurityHealthSystray.exe"
  RAVCpl64.exe                     4 116 K        14 840 K     10852  Realtek HD Audio Manager         Realtek Semiconductor      0/74         (Verified) Realtek ...   "C:\Program Files\Realtek\Audio\HDA\RAVCpl64.exe" -s
```