Dynamic Malware Analysis for IR CheatSheet

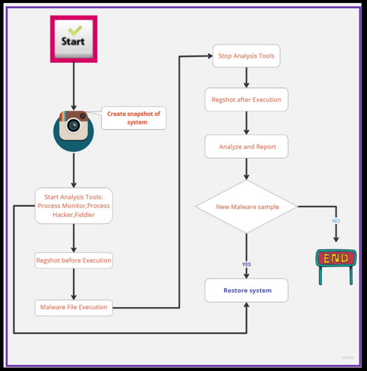
Dynamic Analysis

Dynamic malware analysis involves running potentially harmful code within a secure environment known as a sandbox. This isolated system allows security experts to observe the behavior of the malware without exposing their own system or corporate network to the risk of infection or unauthorized access.

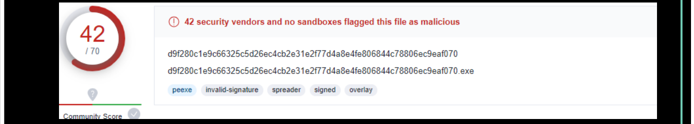
Approach

- Dynamic analysis requires programs to be executed in a closely
- monitored virtual environment.
- It uses a behavior-based approach for malware detection and analysis.
- Dynamic analysis involves API calls,Instruction traces,registry changes,
- network and system calls, memory writes and more.
- It is effective against all types of malware because it analyzes the sample
- by executing it.

Techniques



Malware Sample



42 / 70

42 security vendors and no sandboxes flagged this file as malicious

d9f280c1e9c66325c5d26ec4cb2e31e2f77d4a8e4fe806844c78806ec9eaf070

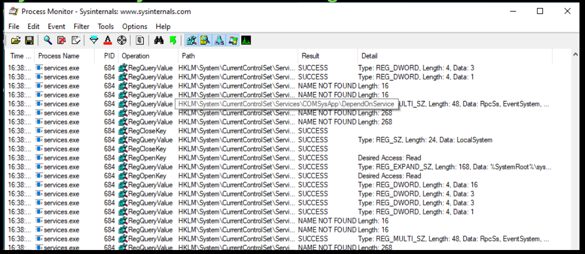
d9f280c1e9c66325c5d26ec4cb2e31e2f77d4a8e4fe806844c78806ec9eaf070.exe

peexe invalid-signature spreader signed overlay

Community Score

ProcMon

ProcMon is a Windows monitoring tool for capturing real-time system activity and troubleshooting.



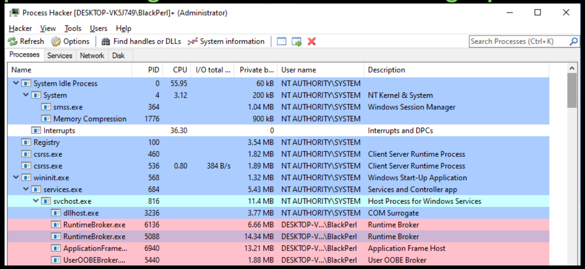
Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

```
Time ...  Process Name  PID  Operation      Path                                      Result           Detail
16:38:... services.exe  684  RegQueryValue  HKLM\System\CurrentControlSet\Servi...    SUCCESS          Type: REG_DWORD, Length: 4, Data: 3
16:38:... services.exe  684  RegQueryValue  HKLM\System\CurrentControlSet\Servi...    SUCCESS          Type: REG_DWORD, Length: 4, Data: 1
16:38:... services.exe  684  RegQueryValue  HKLM\System\CurrentControlSet\Servi...    NAME NOT FOUND   Length: 16
16:38:... services.exe  684  RegQueryValue  HKLM\System\CurrentControlSet\Servi...    NAME NOT FOUND   Length: 16
16:38:... services.exe  684  RegQueryValue  HKLM\System\CurrentControlSet\Services\COMSysApp\DependOnService  ULTI_SZ, Length: 48, Data: RpcSs, EventSystem, ...
16:38:... services.exe  684  RegQueryValue  HKLM\System\CurrentControlSet\Servi...    NAME NOT FOUND   Length: 268
16:38:... services.exe  684  RegQueryValue  HKLM\System\CurrentControlSet\Servi...    NAME NOT FOUND   Length: 268
16:38:... services.exe  684  RegCloseKey    HKLM\System\CurrentControlSet\Servi...    SUCCESS
16:38:... services.exe  684  RegQueryValue  HKLM\System\CurrentControlSet\Servi...    SUCCESS          Type: REG_SZ, Length: 24, Data: LocalSystem
16:38:... services.exe  684  RegCloseKey    HKLM\System\CurrentControlSet\Servi...    SUCCESS
16:38:... services.exe  684  RegOpenKey     HKLM\System\CurrentControlSet\Servi...    SUCCESS          Desired Access: Read
16:38:... services.exe  684  RegQueryValue  HKLM\System\CurrentControlSet\Servi...    SUCCESS          Type: REG_EXPAND_SZ, Length: 168, Data: %SystemRoot%\sys...
16:38:... services.exe  684  RegOpenKey     HKLM\System\CurrentControlSet\Servi...    SUCCESS          Desired Access: Read
16:38:... services.exe  684  RegQueryValue  HKLM\System\CurrentControlSet\Servi...    SUCCESS          Type: REG_DWORD, Length: 4, Data: 16
16:38:... services.exe  684  RegQueryValue  HKLM\System\CurrentControlSet\Servi...    SUCCESS          Type: REG_DWORD, Length: 4, Data: 3
16:38:... services.exe  684  RegQueryValue  HKLM\System\CurrentControlSet\Servi...    SUCCESS          Type: REG_DWORD, Length: 4, Data: 3
16:38:... services.exe  684  RegQueryValue  HKLM\System\CurrentControlSet\Servi...    SUCCESS          Type: REG_DWORD, Length: 4, Data: 1
16:38:... services.exe  684  RegQueryValue  HKLM\System\CurrentControlSet\Servi...    NAME NOT FOUND   Length: 16
16:38:... services.exe  684  RegQueryValue  HKLM\System\CurrentControlSet\Servi...    NAME NOT FOUND   Length: 16
16:38:... services.exe  684  RegQueryValue  HKLM\System\CurrentControlSet\Servi...    SUCCESS          Type: REG_MULTI_SZ, Length: 48, Data: RpcSs, EventSystem, ...
16:38:... services.exe  684  RegQueryValue  HKLM\System\CurrentControlSet\Servi...    NAME NOT FOUND   Length: 268
```

Process Hacker

Process Hacker is an open-source task manager and system monitoring tool for Windows, offering advanced process management and resource tracking capabilities.



Process Hacker [DESKTOP-VK5J749\BlackPerl]+ (Administrator)

Hacker View Tools Users Help

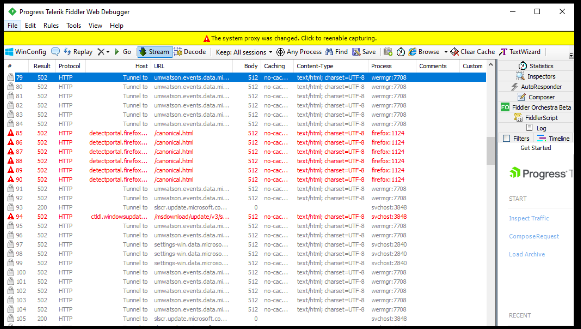
Refresh Options Find handles or DLLs System information Search Processes (Ctrl+K)

Processes Services Network Disk

```
Name                     PID   CPU    I/O total ...  Private b...  User name              Description
System Idle Process      0     55.95                 60 kB         NT AUTHORITY\SYSTEM
  System                 4     3.12                  200 kB        NT AUTHORITY\SYSTEM    NT Kernel & System
    smss.exe             364                         1.04 MB       NT AUTHORITY\SYSTEM    Windows Session Manager
    Memory Compression   1776                        900 kB        NT AUTHORITY\SYSTEM
  Interrupts                   36.30                 0                                    Interrupts and DPCs
Registry                 100                         3.54 MB       NT AUTHORITY\SYSTEM
csrss.exe                460                         1.82 MB       NT AUTHORITY\SYSTEM    Client Server Runtime Process
csrss.exe                536   0.80   384 B/s        1.89 MB       NT AUTHORITY\SYSTEM    Client Server Runtime Process
wininit.exe              568                         1.32 MB       NT AUTHORITY\SYSTEM    Windows Start-Up Application
  services.exe           684                         5.43 MB       NT AUTHORITY\SYSTEM    Services and Controller app
    svchost.exe          816                         11.4 MB       NT AUTHORITY\SYSTEM    Host Process for Windows Services
      dllhost.exe        3236                        3.77 MB       NT AUTHORITY\SYSTEM    COM Surrogate
      RuntimeBroker.exe  6136                        6.66 MB       DESKTOP-V...\BlackPerl Runtime Broker
      RuntimeBroker.exe  5088                        14.34 MB      DESKTOP-V...\BlackPerl Runtime Broker
      ApplicationFrame...6940                        13.21 MB      DESKTOP-V...\BlackPerl Application Frame Host
      UserOOBEBroker.... 5440                        1.88 MB       DESKTOP-V...\BlackPerl User OOBE Broker
```

Fiddler

Fiddler is a web debugging proxy tool that captures and analyzes web traffic to assist in troubleshooting and testing.



Progress Telerik Fiddler Web Debugger

File Edit Rules Tools View Help

The system proxy was changed. Click to reenable capturing.

WinConfig Replay Go Stream Decode Keep: All sessions Any Process Find Save Browse Clear Cache TextWizard

```
#    Result  Protocol  Host                    URL                              Body  Caching     Content-Type               Process        Comments  Custom
79   502     HTTP      Tunnel to               umwatson.events.data.mi...       512   no-cac...   text/html; charset=UTF-8   wermgr:7708
80   502     HTTP      Tunnel to               umwatson.events.data.mi...       512   no-cac...   text/html; charset=UTF-8   wermgr:7708
81   502     HTTP      Tunnel to               umwatson.events.data.mi...       512   no-cac...   text/html; charset=UTF-8   wermgr:7708
82   502     HTTP      Tunnel to               umwatson.events.data.mi...       512   no-cac...   text/html; charset=UTF-8   wermgr:7708
83   502     HTTP      Tunnel to               umwatson.events.data.mi...       512   no-cac...   text/html; charset=UTF-8   wermgr:7708
84   502     HTTP      Tunnel to               umwatson.events.data.mi...       512   no-cac...   text/html; charset=UTF-8   wermgr:7708
85   502     HTTP      detectportal.firefox...  /canonical.html                 512   no-cac...   text/html; charset=UTF-8   firefox:1124
86   502     HTTP      detectportal.firefox...  /canonical.html                 512   no-cac...   text/html; charset=UTF-8   firefox:1124
87   502     HTTP      detectportal.firefox...  /canonical.html                 512   no-cac...   text/html; charset=UTF-8   firefox:1124
88   502     HTTP      detectportal.firefox...  /canonical.html                 512   no-cac...   text/html; charset=UTF-8   firefox:1124
89   502     HTTP      detectportal.firefox...  /canonical.html                 512   no-cac...   text/html; charset=UTF-8   firefox:1124
90   502     HTTP      detectportal.firefox...  /canonical.html                 512   no-cac...   text/html; charset=UTF-8   firefox:1124
91   502     HTTP      Tunnel to               umwatson.events.data.mi...       512   no-cac...   text/html; charset=UTF-8   wermgr:7708
92   502     HTTP      Tunnel to               umwatson.events.data.mi...       512   no-cac...   text/html; charset=UTF-8   wermgr:7708
93   200     HTTP      Tunnel to               slscr.update.microsoft.co...     0                                          svchost:3848
94   502     HTTP      ctldl.windowsupdat...   /msdownload/update/v3/s...       512   no-cac...   text/html; charset=UTF-8   svchost:3848
95   502     HTTP      Tunnel to               umwatson.events.data.mi...       512   no-cac...   text/html; charset=UTF-8   wermgr:7708
96   502     HTTP      Tunnel to               umwatson.events.data.mi...       512   no-cac...   text/html; charset=UTF-8   wermgr:7708
97   502     HTTP      Tunnel to               settings-win.data.microso...     512   no-cac...   text/html; charset=UTF-8   svchost:2840
98   502     HTTP      Tunnel to               settings-win.data.microso...     512   no-cac...   text/html; charset=UTF-8   svchost:2840
99   502     HTTP      Tunnel to               settings-win.data.microso...     512   no-cac...   text/html; charset=UTF-8   svchost:2840
100  502     HTTP      Tunnel to               umwatson.events.data.mi...       512   no-cac...   text/html; charset=UTF-8   wermgr:7708
101  502     HTTP      Tunnel to               umwatson.events.data.mi...       512   no-cac...   text/html; charset=UTF-8   wermgr:7708
102  502     HTTP      Tunnel to               umwatson.events.data.mi...       512   no-cac...   text/html; charset=UTF-8   wermgr:7708
103  502     HTTP      Tunnel to               umwatson.events.data.mi...       512   no-cac...   text/html; charset=UTF-8   wermgr:7708
104  502     HTTP      Tunnel to               umwatson.events.data.mi...       512   no-cac...   text/html; charset=UTF-8   wermgr:7708
105  200     HTTP      Tunnel to               slscr.update.microsoft.co...     0                                          svchost:3848
```

Why You Should Consider Using a Malware Analysis Tool?

- Dynamic Malware Analysis Can Detect Previously Unknown Malware
- Assessing and Understanding Malware Behaviour
- Malware Mitigation
- Provide Rapid Incident Response
- Test Security Solution Effectiveness
- Enhancing Threat Intelligence

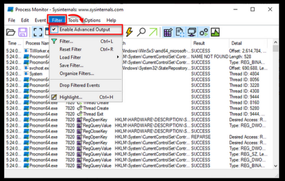
Online Sandboxes:

- Any.run
- Hybrid Analysis (Falcon Sandbox)
- Intezer Analyze
- Cuckoo Sandbox
- Joe Sandbox
- IRIS -H
- Triage
- Cape

PROCDOT

"Procdot is a platform for collaborative process documentation and optimization."

To parse the output file from ProcMon to ProcDot you need to enable few settings which list below

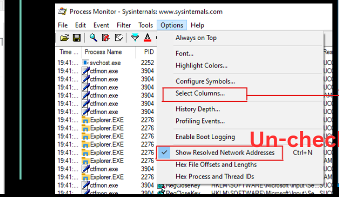


Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

☑ Enable Advanced Output

```
Time ...  Process Nam...     PID   Operation      Path                                     Result          Detail
5:24:0... TiWorker.e...                            ...Windows\WinSxS\amd64_microsoft-...   SUCCESS         Offset: 2,614,784, ...
5:24:0... Procmon64...                             ...M\System\CurrentControlSet\Contr...  NAME NOT FOUND  Length: 528
5:24:0... Procmon64...                             ...M\System\CurrentControlSet\Contr...  SUCCESS         Type: REG_BINA...
5:24:0... svchost.ex...                            ...Windows\System32\StateRepository...  SUCCESS         Offset: 690,688, Le...
5:24:0... System                                                                           SUCCESS         Thread ID: 4804
5:24:0... Procmon64...                                                                     SUCCESS         Thread ID: 8056
5:24:0... Procmon64...                                                                     SUCCESS         Thread ID: 3228
5:24:0... Procmon64...                                                                     SUCCESS         Thread ID: 4308
5:24:0... Procmon64...                                                                     SUCCESS         Thread ID: 9444
5:24:0... Procmon64.exe      7820  Thread Create                                           SUCCESS         Thread ID: 8160
5:24:0... Procmon64.exe      7820  Thread Create                                           SUCCESS         Thread ID: 5280
5:24:0... Procmon64.exe      7820  Thread Exit                                             SUCCESS         Thread ID: 9444, ...
5:24:0... Procmon64.exe      7820  RegOpenKey     HKLM\HARDWARE\DESCRIPTION\S...           SUCCESS         Desired Access: R...
5:24:0... Procmon64.exe      7820  RegQueryValue  HKLM\HARDWARE\DESCRIPTION\S...           SUCCESS         Type: REG_DWO...
5:24:0... Procmon64.exe      7820  RegCloseKey    HKLM\HARDWARE\DESCRIPTION\S...           SUCCESS
5:24:0... Procmon64.exe      7820  RegOpenKey     HKLM\System\CurrentControlSet\Contr...   REPARSE         Desired Access: R...
5:24:0... Procmon64.exe      7820  RegOpenKey     HKLM\System\CurrentControlSet\Contr...   SUCCESS         Desired Access: R...
5:24:0... Procmon64.exe      7820  RegQueryValue  HKLM\System\CurrentControlSet\Contr...   SUCCESS         Type: REG_DWO...
5:24:0... Procmon64.exe      7820  RegQueryValue  HKLM\System\CurrentControlSet\Contr...   SUCCESS         Type: REG_SZ, Le...
5:24:0... Procmon64.exe      7820  RegQueryValue  HKLM\System\CurrentControlSet\Contr...   SUCCESS         Type: REG_DWO...
5:24:0... Procmon64.exe      7820  RegQueryValue  HKLM\System\CurrentControlSet\Contr...   SUCCESS         Type: REG_BINA...
```



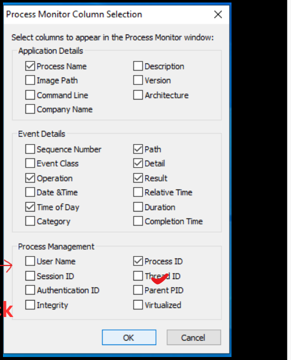
Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

☑ Show Resolved Network Addresses Ctrl+N

Un-check

```
Time ...  Process Name   PID
19:41:... svchost.exe    2252
19:41:... ctfmon.exe     3904
19:41:... ctfmon.exe     3904
19:41:... ctfmon.exe     3904
19:41:... ctfmon.exe     3904
19:41:... ctfmon.exe     3904
19:41:... ctfmon.exe     3904
19:41:... Explorer.EXE   2276
19:41:... Explorer.EXE   2276
19:41:... Explorer.EXE   2276
19:41:... Explorer.EXE   2276
19:41:... Explorer.EXE   2276
19:41:... Explorer.EXE   2276
19:41:... ctfmon.exe     3904
19:41:... Explorer.EXE   2276
19:41:... ctfmon.exe     3904
```



Process Monitor Column Selection

Select columns to appear in the Process Monitor window:

Application Details

☑ Process Name ☐ Description
☐ Image Path ☐ Version
☐ Command Line ☐ Architecture
☐ Company Name

Event Details

☐ Sequence Number ☑ Path
☐ Event Class ☑ Detail
☑ Operation ☑ Result
☐ Date &Time ☐ Relative Time
☑ Time of Day ☐ Duration
☐ Category ☐ Completion Time

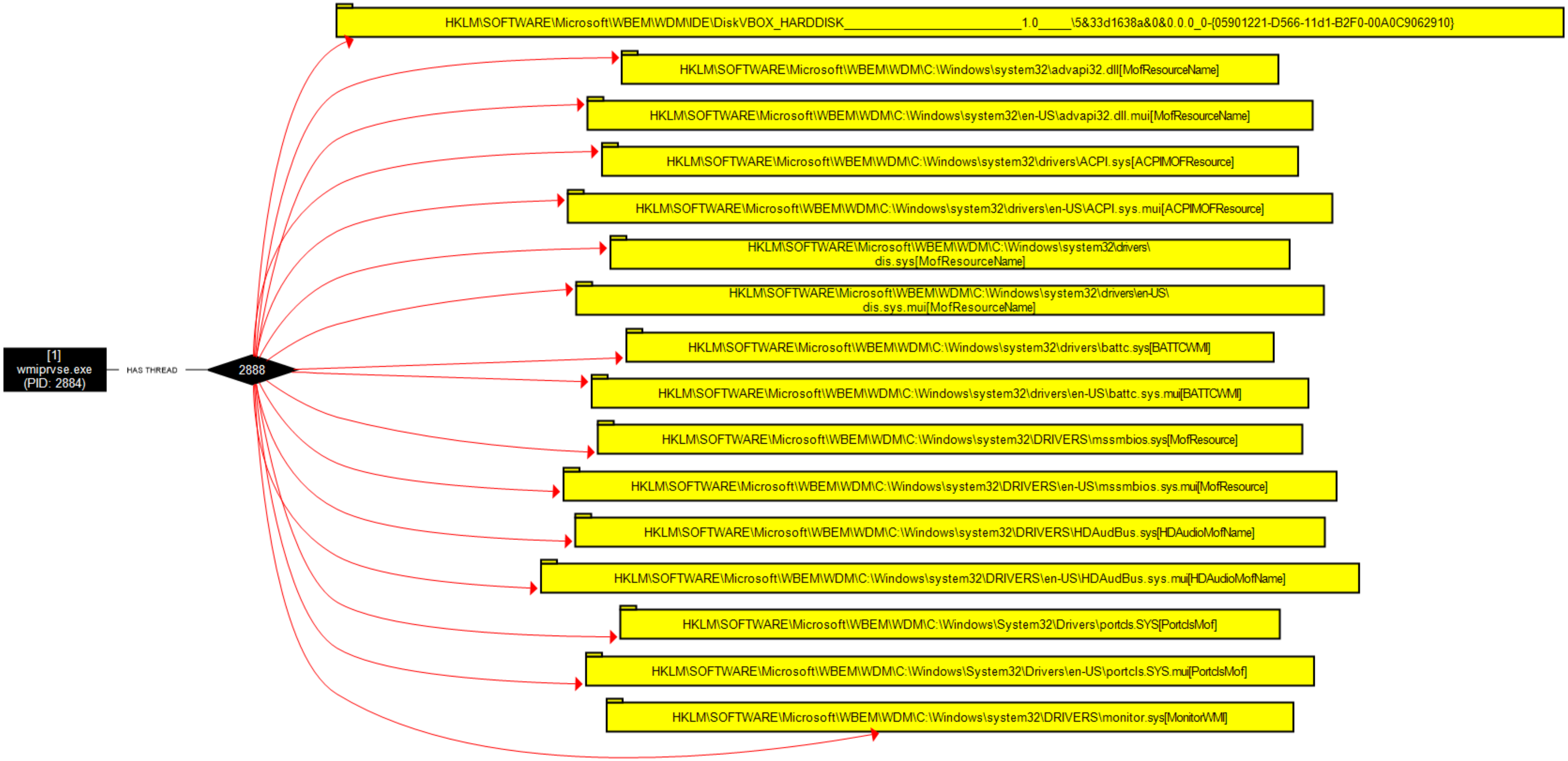
Process Management

☐ User Name ☑ Process ID
☐ Session ID ☐ Thread ID ✓
☐ Authentication ID ☐ Parent PID
☐ Integrity ☐ Virtualized

OK Cancel

blackperldfir.com

PROC-DOT output



[1]
wmiprvse.exe
(PID: 2884)

HAS THREAD

2888

HKLM\SOFTWARE\Microsoft\WBEM\WDM\IDE\DiskVBOX_HARDDISK___________________________1.0_____\5&33d1638a&0&0.0.0_0-{05901221-D566-11d1-B2F0-00A0C9062910}

HKLM\SOFTWARE\Microsoft\WBEM\WDM\C:\Windows\system32\advapi32.dll[MofResourceName]

HKLM\SOFTWARE\Microsoft\WBEM\WDM\C:\Windows\system32\en-US\advapi32.dll.mui[MofResourceName]

HKLM\SOFTWARE\Microsoft\WBEM\WDM\C:\Windows\system32\drivers\ACPI.sys[ACPIMOFResource]

HKLM\SOFTWARE\Microsoft\WBEM\WDM\C:\Windows\system32\drivers\en-US\ACPI.sys.mui[ACPIMOFResource]

HKLM\SOFTWARE\Microsoft\WBEM\WDM\C:\Windows\system32\drivers\dis.sys[MofResourceName]

HKLM\SOFTWARE\Microsoft\WBEM\WDM\C:\Windows\system32\drivers\en-US\dis.sys.mui[MofResourceName]

HKLM\SOFTWARE\Microsoft\WBEM\WDM\C:\Windows\system32\drivers\battc.sys[BATTCWMI]

HKLM\SOFTWARE\Microsoft\WBEM\WDM\C:\Windows\system32\drivers\en-US\battc.sys.mui[BATTCWMI]

HKLM\SOFTWARE\Microsoft\WBEM\WDM\C:\Windows\system32\DRIVERS\mssmbios.sys[MofResource]

HKLM\SOFTWARE\Microsoft\WBEM\WDM\C:\Windows\system32\DRIVERS\en-US\mssmbios.sys.mui[MofResource]

HKLM\SOFTWARE\Microsoft\WBEM\WDM\C:\Windows\system32\DRIVERS\HDAudBus.sys[HDAudioMofName]

HKLM\SOFTWARE\Microsoft\WBEM\WDM\C:\Windows\system32\DRIVERS\en-US\HDAudBus.sys.mui[HDAudioMofName]

HKLM\SOFTWARE\Microsoft\WBEM\WDM\C:\Windows\System32\Drivers\portcls.SYS[PortclsMof]

HKLM\SOFTWARE\Microsoft\WBEM\WDM\C:\Windows\System32\Drivers\en-US\portcls.SYS.mui[PortclsMof]

HKLM\SOFTWARE\Microsoft\WBEM\WDM\C:\Windows\system32\DRIVERS\monitor.sys[MonitorWMI]