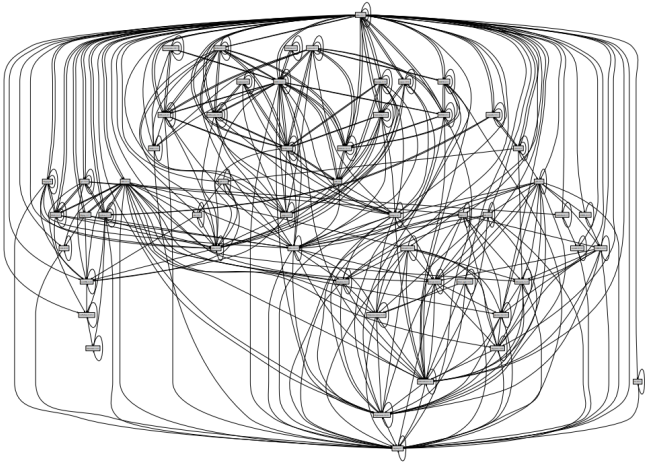
DLL Shell Game and other misdirections

SSTIC 2019



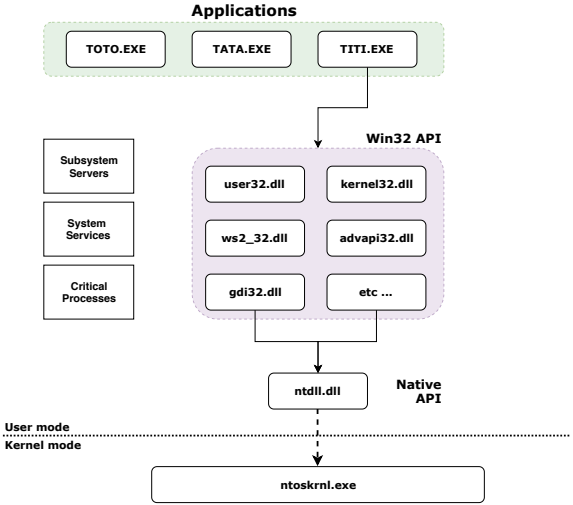
06/06/2019
Synacktiv
Lucas GEORGES

Table des matières

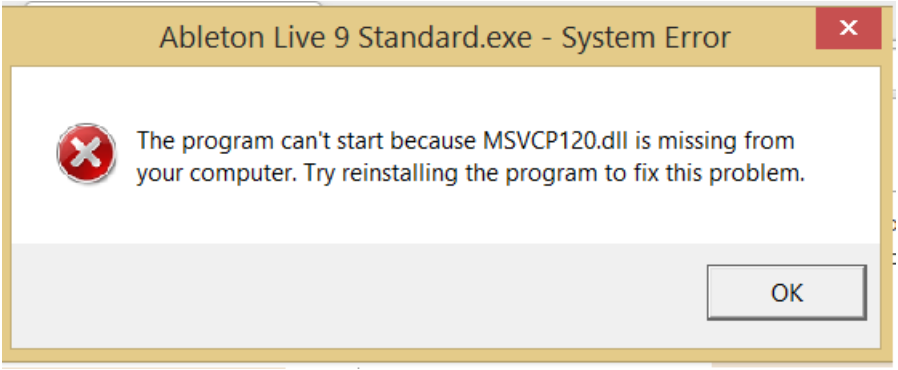
Whoami

- Twitter : @_lucas_georges_
- Reverser @ Synacktiv
- Located in Rennes ;p

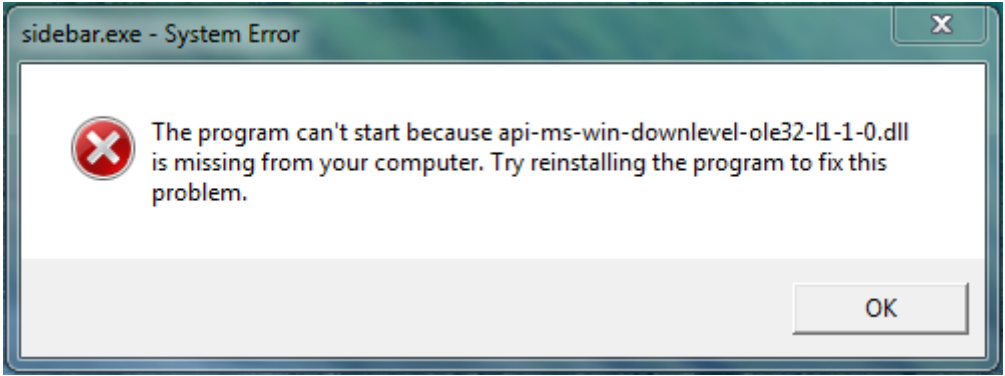
Dynamic Link Library (DLL) Dependencies



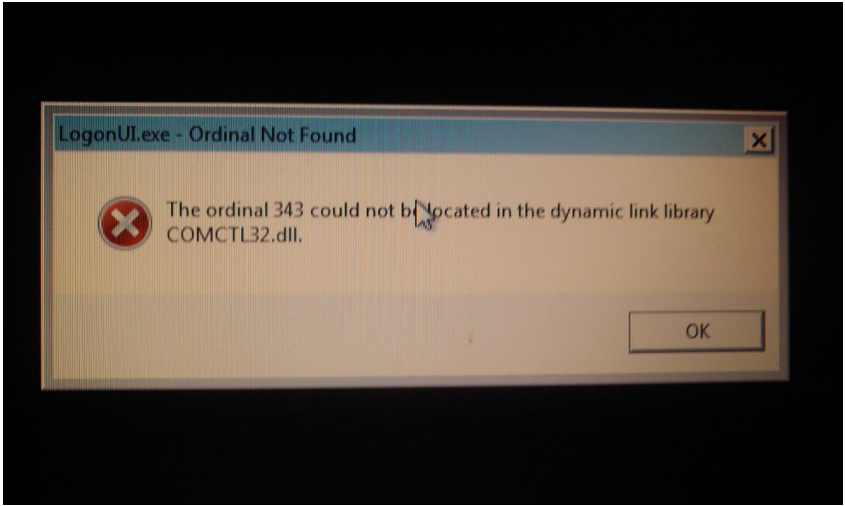
Missing DLL


Ableton Live 9 Standard.exe - System Error
The program can't start because MSVCP120.dll is missing from your computer. Try reinstalling the program to fix this problem.
OK

Missing DLL ?


sidebar.exe - System Error
The program can't start because api-ms-win-downlevel-ole32-l1-1-0.dll is missing from your computer. Try reinstalling the program to fix this problem.
OK

Missing Export



Missing ????

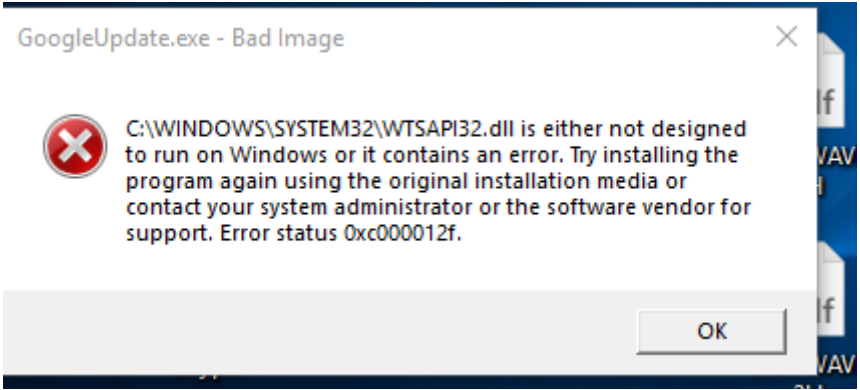
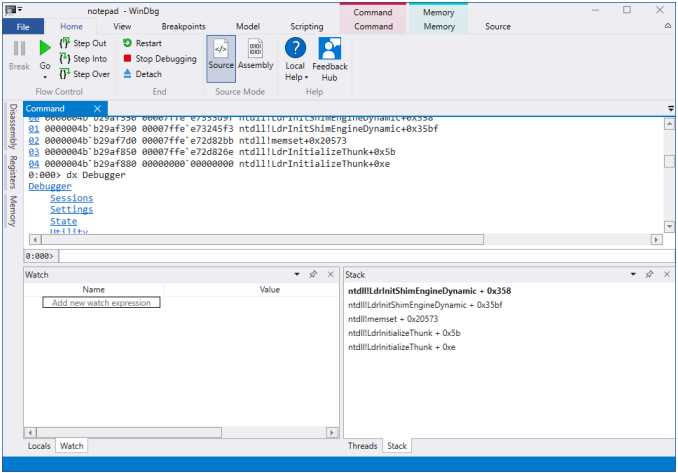
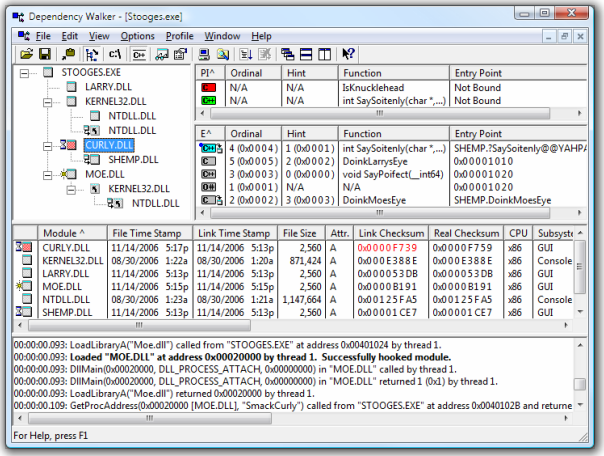

GoogleUpdate.exe - Bad Image
C:\WINDOWS\SYSTEM32\WTSAPI32.dll is either not designed to run on Windows or it contains an error. Try installing the program again using the original installation media or contact your system administrator or the software vendor for support. Error status 0xc000012f.
OK

Table des matières

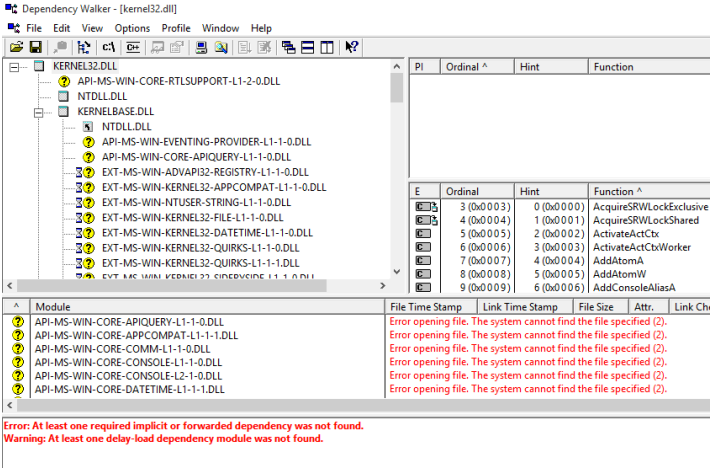
Windbg


notepad - WinDbg
File
Home
View
Breakpoints
Model
Scripting
Command
Memory
Source
Break
Go
Step Out
Step Into
Step Over
Restart
Stop Debugging
Detach
Source
Assembly
Local Help
Feedback Hub
Flow Control
End
Source Mode
Help
Disassembly
Registers
Memory
Command
01 0000004b`b29af390 00007ffe`e73245f3 ntdll!LdrInitShimEngineDynamic+0x35bf
02 0000004b`b29af7d0 00007ffe`e72d82bb ntdll!memset+0x20573
03 0000004b`b29af850 00007ffe`e72d826e ntdll!LdrInitializeThunk+0x5b
04 0000004b`b29af880 00000000`00000000 ntdll!LdrInitializeThunk+0xe
0:000> dx Debugger
Debugger
Sessions
Settings
State
0:000>
Watch
Name
Value
Add new watch expression
Stack
ntdll!LdrInitShimEngineDynamic + 0x358
ntdll!LdrInitShimEngineDynamic + 0x35bf
ntdll!memset + 0x20573
ntdll!LdrInitializeThunk + 0x5b
ntdll!LdrInitializeThunk + 0xe
Locals
Watch
Threads
Stack

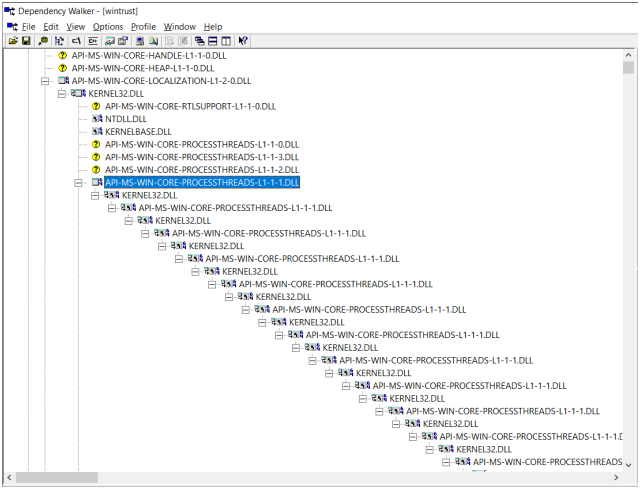
Dependency Walker



Dependency Walker on a modern binary

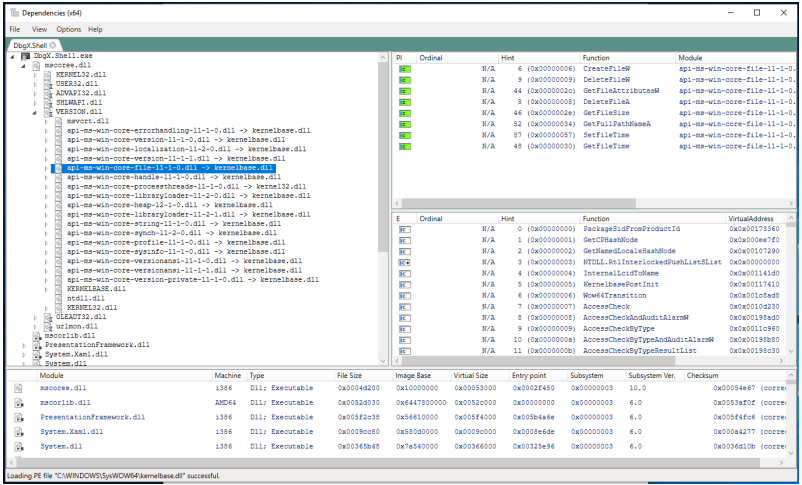


Dependency Walker on a modern binary



API-MS-WIN-CORE-HANDLE-L1-1-0.DLL
API-MS-WIN-CORE-HEAP-L1-1-0.DLL
API-MS-WIN-CORE-LOCALIZATION-L1-2-0.DLL
KERNEL32.DLL
API-MS-WIN-CORE-RTLSUPPORT-L1-1-0.DLL
NTDLL.DLL
KERNELBASE.DLL
API-MS-WIN-CORE-PROCESSTHREADS-L1-1-0.DLL
API-MS-WIN-CORE-PROCESSTHREADS-L1-1-3.DLL
API-MS-WIN-CORE-PROCESSTHREADS-L1-1-2.DLL
API-MS-WIN-CORE-PROCESSTHREADS-L1-1-1.DLL
KERNEL32.DLL
API-MS-WIN-CORE-PROCESSTHREADS-L1-1-1.DLL
KERNEL32.DLL
API-MS-WIN-CORE-PROCESSTHREADS-L1-1-1.DLL
KERNEL32.DLL
API-MS-WIN-CORE-PROCESSTHREADS-L1-1-1.DLL
KERNEL32.DLL
API-MS-WIN-CORE-PROCESSTHREADS-L1-1-1.DLL
KERNEL32.DLL
API-MS-WIN-CORE-PROCESSTHREADS-L1-1-1.DLL
KERNEL32.DLL
API-MS-WIN-CORE-PROCESSTHREADS-L1-1-1.DLL
KERNEL32.DLL
API-MS-WIN-CORE-PROCESSTHREADS-L1-1-1.DLL
KERNEL32.DLL
API-MS-WIN-CORE-PROCESSTHREADS-L1-1-1.DLL
KERNEL32.DLL
API-MS-WIN-CORE-PROCESSTHREADS-L1-1-1.DLL
KERNEL32.DLL
API-MS-WIN-CORE-PROCESSTHREADS-L1-1-1.D
KERNEL32.DLL
API-MS-WIN-CORE-PROCESSTHREADS

Dependencies

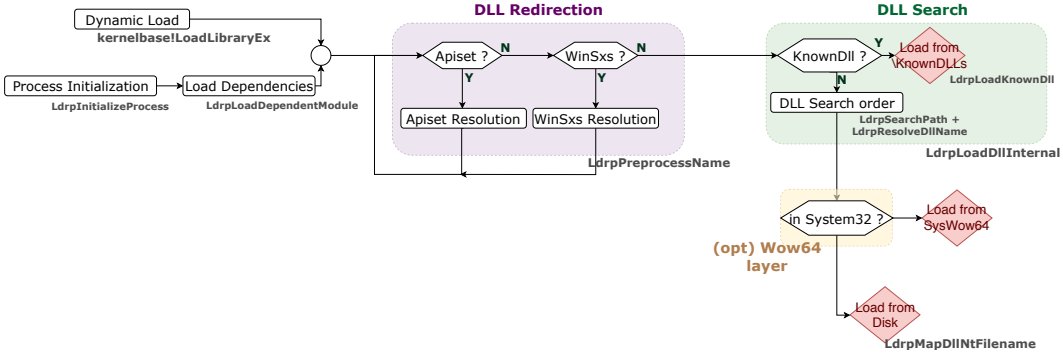


DEMO

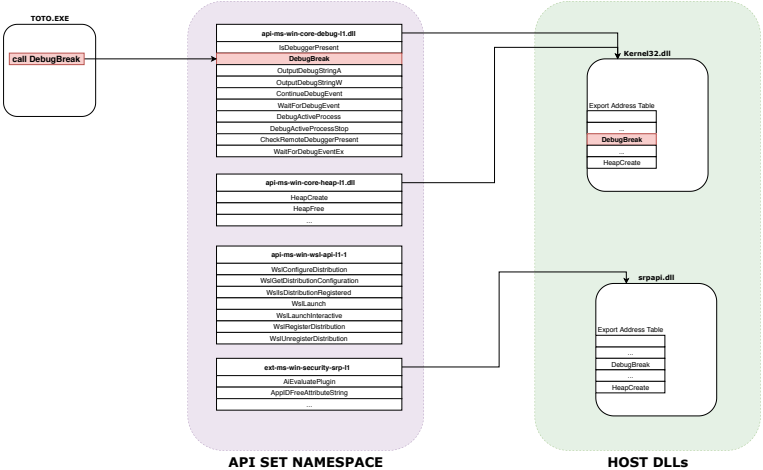
DEMO TIME!

Table des matières

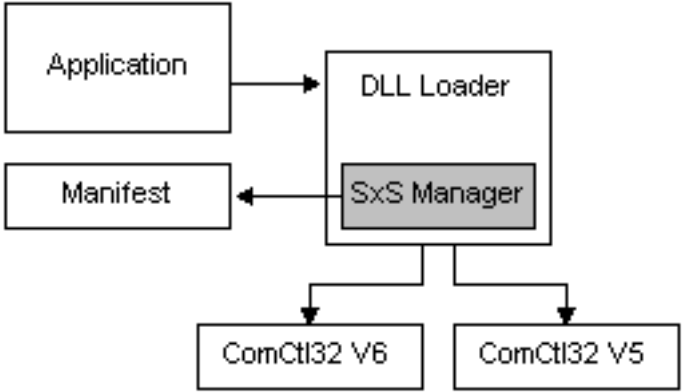
Diagram


Dynamic Load
kernelbase!LoadLibraryEx
Process Initialization
LdrpInitializeProcess
Load Dependencies
LdrpLoadDependentModule
DLL Redirection
Apiset ?
N
Y
WinSxs ?
N
Y
Apiset Resolution
WinSxs Resolution
LdrpPreprocessName
DLL Search
KnownDll ?
Y
N
Load from KnownDLLs
LdrpLoadKnownDll
DLL Search order
LdrpSearchPath +
LdrpResolveDllName
LdrpLoadDllInternal
in System32 ?
Load from SysWow64
(opt) Wow64 layer
Load from Disk
LdrpMapDllNtFilename

Apisets


TOTO.EXE
call DebugBreak
api-ms-win-core-debug-l1.dll
IsDebuggerPresent
DebugBreak
OutputDebugStringA
OutputDebugStringW
ContinueDebugEvent
WaitForDebugEvent
DebugActiveProcess
DebugActiveProcessStop
CheckRemoteDebuggerPresent
WaitForDebugEventEx
api-ms-win-core-heap-l1.dll
HeapCreate
HeapFree
...
api-ms-win-wsl-api-l1-1
WslConfigureDistribution
WslGetDistributionConfiguration
WslIsDistributionRegistered
WslLaunch
WslLaunchInteractive
WslRegisterDistribution
WslUnregisterDistribution
ext-ms-win-security-srp-l1
AlEvaluatePlugin
AppIDFreeAttributeString
...
Kernel32.dll
Export Address Table
...
DebugBreak
...
HeapCreate
srpapi.dll
Export Address Table
...
DebugBreak
...
HeapCreate
API SET NAMESPACE
HOST DLLs

WinSxS


Application
DLL Loader
Manifest
SxS Manager
ComCtl32 V6
ComCtl32 V5

PE manifest

Embedded PE manifest for Opera's installer

```
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
  <dependency>
    <dependentAssembly>
      <assemblyIdentity
        type="win32" name="Microsoft.Windows.Common-Controls"
        version="6.0.0.0" processorArchitecture="*"
        publicKeyToken="6595b64144ccf1df" language="*">
      </assemblyIdentity>
    </dependentAssembly>
  </dependency>
  <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
    <security>
      <requestedPrivileges>
        <requestedExecutionLevel level="asInvoker" uiAccess="false"></requestedExecutionLevel>
      </requestedPrivileges>
    </security>
  </trustInfo>
</assembly>
```

PE manifest

Embedded PE manifest for Chrome executable

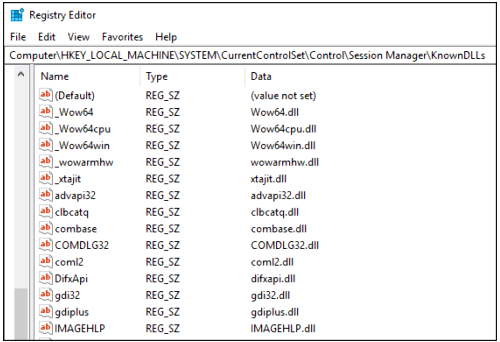
```
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
  <dependency> <!-- "Microsoft.Windows.Common-Controls" dependency --!></dependency>
  <dependency>
    <dependentAssembly>
      <assemblyIdentity type="win32" name="74.0.3729.169" version="74.0.3729.169" language="*"></
          assemblyIdentity>
    </dependentAssembly>
  </dependency>
  <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3"> <!-- runAsInvoker --!></trustInfo>
  <compatibility xmlns="urn:schemas-microsoft-com:compatibility.v1">
    <application>
      <supportedOS Id="{e2011457-1546-43c5-a5fe-008deee3d3f0}"></supportedOS>
      <supportedOS Id="{35138b9a-5d96-4fbd-8e2d-a2440225f93a}"></supportedOS>
      <supportedOS Id="{4a2f28e3-53b9-4441-ba9c-d69d4a4a6e38}"></supportedOS>
      <supportedOS Id="{1f676c76-80e1-4239-95bb-83d0f6d0da78}"></supportedOS>
      <supportedOS Id="{8e0f7a12-bfb3-4fe8-b9a5-48fd50a15a9a}"></supportedOS>
    </application>
  </compatibility>
</assembly>
```

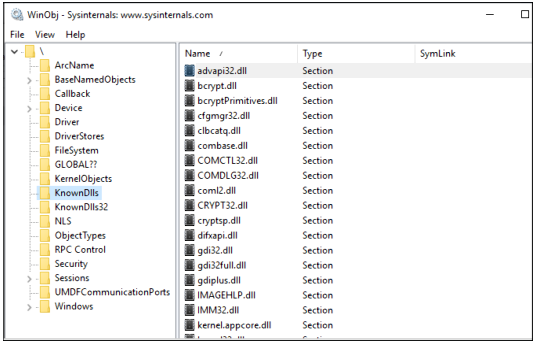
PE manifest

C :\Program Files (x86)\Google\Chrome\Application\74.0.3729.169\74.0.3729.169.manifest

```
<assembly
  xmlns='urn:schemas-microsoft-com:asm.v1' manifestVersion='1.0'>
  <assemblyIdentity
     name='74.0.3729.169'
     version='74.0.3729.169'
     type='win32'/>
  <file name='chrome_elf.dll'/>
</assembly>
```

KnownDlls


Registry Editor
File Edit View Favorites Help
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\KnownDLLs
Name Type Data
(Default) REG_SZ (value not set)
_Wow64 REG_SZ Wow64.dll
_Wow64cpu REG_SZ Wow64cpu.dll
_Wow64win REG_SZ Wow64win.dll
_wowarmhw REG_SZ wowarmhw.dll
_xtajit REG_SZ xtajit.dll
advapi32 REG_SZ advapi32.dll
clbcatq REG_SZ clbcatq.dll
combase REG_SZ combase.dll
COMDLG32 REG_SZ COMDLG32.dll
coml2 REG_SZ coml2.dll
DifxApi REG_SZ difxapi.dll
gdi32 REG_SZ gdi32.dll
gdiplus REG_SZ gdiplus.dll
IMAGEHLP REG_SZ IMAGEHLP.dll


WinObj - Sysinternals: www.sysinternals.com
File View Help
\
ArcName
BaseNamedObjects
Callback
Device
Driver
DriverStores
FileSystem
GLOBAL??
KernelObjects
KnownDlls
KnownDlls32
NLS
ObjectTypes
RPC Control
Security
Sessions
UMDFCommunicationPorts
Windows
Name Type SymLink
advapi32.dll Section
bcrypt.dll Section
bcryptPrimitives.dll Section
cfgmgr32.dll Section
clbcatq.dll Section
combase.dll Section
COMCTL32.dll Section
COMDLG32.dll Section
coml2.dll Section
CRYPT32.dll Section
cryptsp.dll Section
difxapi.dll Section
gdi32.dll Section
gdi32full.dll Section
gdiplus.dll Section
IMAGEHLP.dll Section
IMM32.dll Section
kernel.appcore.dll Section

KnownDlls

```
NTSTATUS NTAPI SmpInitializeKnownDllsInternal(...)
{
    PLDR_VERIFY_IMAGE_INFO VerifyImageInfo = {
        .CallbackInfo.ImportCallbackRoutine = SmpProcessModuleImports
    };

    for (auto DllPath : SmpRandomizeDllList(&SmpKnownDllsList))
    {
        OBJECT_ATTRIBUTES KnownDllOa = {
            .ObjectName = DllPath
        };
        // [...]

        if (!NT_SUCCESS(NtOpenFile(&DllHandle, 1179680i64, &KnownDllOa, &Isb, FILE_SHARE_READ | FILE_SHARE_DELETE, 96)))
            continue;

        NTSTATUS VerificationStatus = LdrVerifyImageMatchesChecksumEx(KnownDllHandle, &VerifyImageInfo);
        if (!NT_SUCCESS(VerificationStatus))
        {
            if (/* condition */)
            {
                RtlInitUnicodeString(&LogString, L"Non-DLL file included in KnownDLL list.");
                SmpTerminate(&LogString, 5i64, 3i64);
                __debugbreak();
            }

            RtlInitUnicodeString(&LogString, L"Verification of a KnownDLL failed.");
            goto ON_ERROR;
        }
        NtClose(DllHandle);
    }
}
```

KnownDlls

```
  // Retrieve IMPORT_DATA_DIRECTORY
  status_1 = RtlpImageDirectoryEntryToDataEx(
             (unsigned __int64)_image_base_address,
             v17,
             IMAGE_DIRECTORY_ENTRY_IMPORT,
             &_LastRvaSection,
             &ImportEntry);
  Import = ImportEntry;
  if ( status_1 < 0 )
    Import = 0i64;


  ImportEntry = Import;
  CurrentImport = Import;
  if ( Import )
  {


    // Iterate over IMAGE_IMPORT_DESCRIPTOR entries
    _LastRvaSection = 0i64;
    while ( 1 )
    {
      ImportName = Import->Name;
      if ( !(_DWORD)ImportName )
        break;
      if ( v10 )
        ImportNameAscii = (__int64)&_image_base_address[(unsigned int)ImportName];
      else
        ImportNameAscii = RtlImageRvaToVa(NtHeaders, _image_base_address, ImportName, &_LastRvaSection);



      // call SmpProcessModuleImports(HANDLE SmpContext, char *ImportName) in order to add imports dependencies to the KnownDlls list
      Context->CallbackInfo.Callback((void *)Context->CallbackInfo.CallbackParameter, (void *)ImportNameAscii);
      ++Import;
      CurrentImport = Import;
    }
  }
}
```

ntdll.dll!LdrVerifyImageMatchesChecksumEx

DLL Search Order

If **SafeDllSearchMode** is enabled, the search order is as follows:

1. The directory from which the application loaded.
2. The system directory. Use the **GetSystemDirectory** function to get the path of this directory.
3. The 16-bit system directory. There is no function that obtains the path of this directory, but it is searched.
4. The Windows directory. Use the **GetWindowsDirectory** function to get the path of this directory.
5. The current directory.
6. The directories that are listed in the PATH environment variable. Note that this does not include the per-application path specified by the **App Paths** registry key. The **App Paths** key is not used when computing the DLL search path.

Source : https ://docs.microsoft.com/en-us/windows/desktop/dlls/dynamic-link-library-search-order

System32 folder redirection

Implemented in wow64 binaries (`wow64cpu.dll`, `wow64win.dll` and `wow64.dll`)

Original Path	Redirected Path
`"C:\Windows\SysWow64\ntdll.dll"`	`"C:\Windows\SysWow64\ntdll.dll"`
`"C:\Windows\System32\ntdll.dll"`	`"C:\Windows\SysWow64\ntdll.dll"`
`"C:\Windows\Sysnative\ntdll.dll"`	`"C:\Windows\System32\ntdll.dll"`

Exemptions

- `"C:\Windows\System32\catroot"`
- `"C:\Windows\System32\catroot2"`
- `"C:\Windows\System32\driverstore"`
- `"C:\Windows\System32\drivers\etc"`
- `"C:\Windows\System32\hostdriverstore"`
- `"C:\Windows\System32\logfiles"`
- `"C:\Windows\System32\spool"`

Diagram

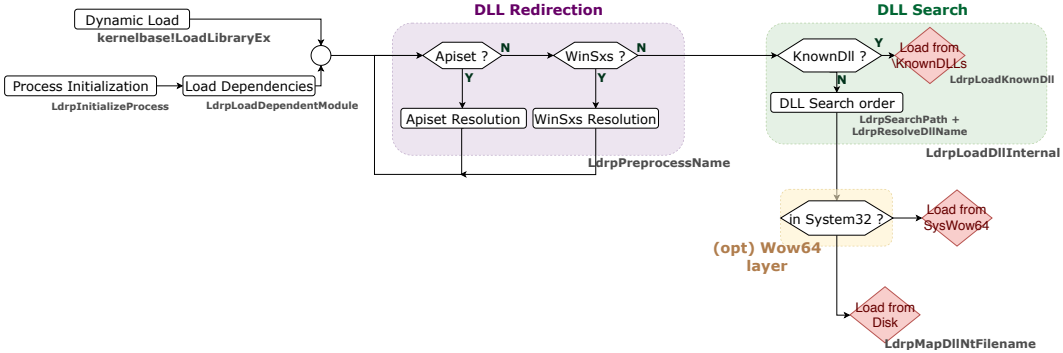
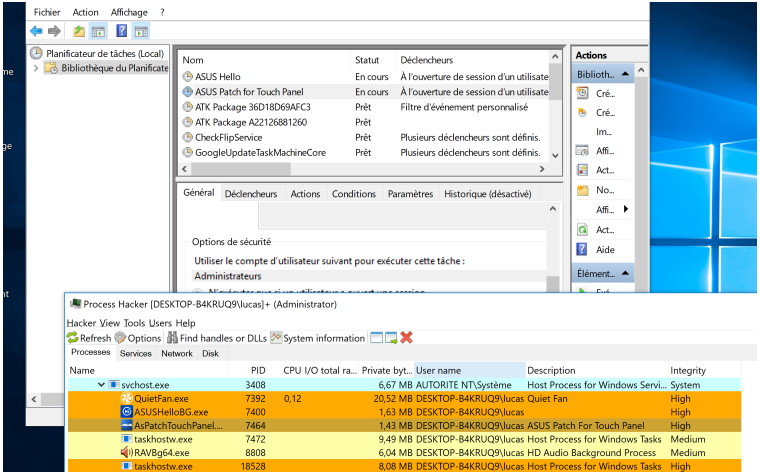
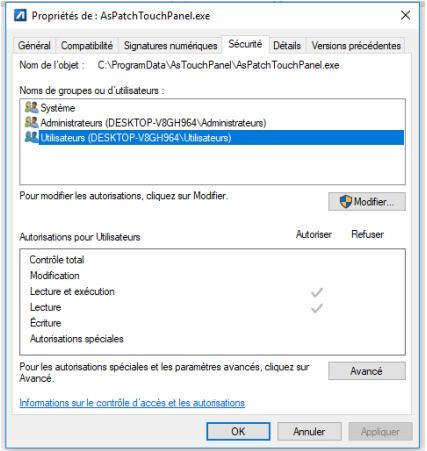

Dynamic Load
kernelbase!LoadLibraryEx
Process Initialization
LdrpInitializeProcess
Load Dependencies
LdrpLoadDependentModule
DLL Redirection
Apiset ?
N
Y
WinSxs ?
N
Y
Apiset Resolution
WinSxs Resolution
LdrpPreprocessName
DLL Search
KnownDll ?
Y
N
Load from KnownDLLs
LdrpLoadKnownDll
DLL Search order
LdrpSearchPath + LdrpResolveDllName
LdrpLoadDllInternal
in System32 ?
Load from SysWow64
(opt) Wow64 layer
Load from Disk
LdrpMapDllNtFilename

Table des matières

Asus Delayload plant

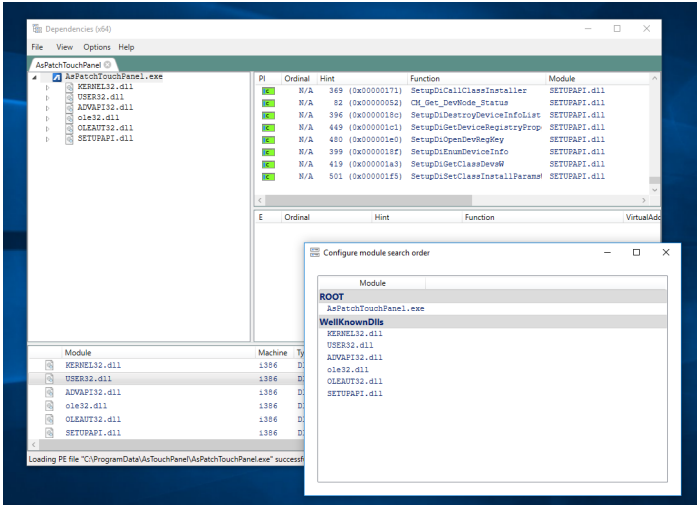


Asus Delayload plant



- The binary can't be rewritten
- But any user can write a file or a folder in the same folder
- Let's find a DLL to plant!

Asus Delayload plant



Asus Delayload plant

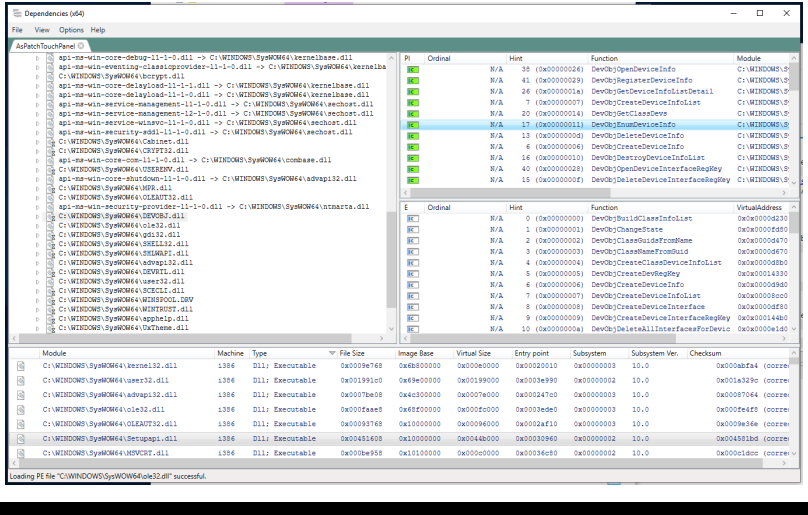
Process Monitor - Sysinternals: www.sysinternals.com

File Edit Event Filter Tools Options Help

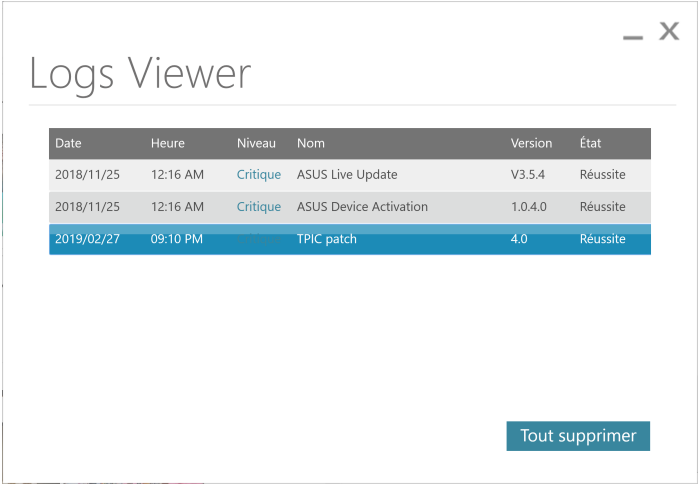
Time of...	Process Name	Operation	Path	Result	Detail
16:31:2...	AsPatchTouchPanel.exe	CreateFile	C:\Windows\SysWOW64\uxtheme.dll	SUCCESS	Desired Access: Read Data/List Di
16:31:2...	AsPatchTouchPanel.exe	CreateFileMap...	C:\Windows\SysWOW64\uxtheme.dll	FILE LOCKED WITH ONLY REA...	SyncType: SyncTypeCreateSectio
16:31:2...	AsPatchTouchPanel.exe	CreateFileMap...	C:\Windows\SysWOW64\uxtheme.dll	SUCCESS	SyncType: SyncTypeOther
16:31:2...	AsPatchTouchPanel.exe	Load Image	C:\Windows\SysWOW64\uxtheme.dll	SUCCESS	Image Base: 0x70580000, Image S
16:31:2...	AsPatchTouchPanel.exe	CloseFile	C:\Windows\SysWOW64\uxtheme.dll	SUCCESS	
16:31:2...	AsPatchTouchPanel.exe	Load Image	C:\Windows\SysWOW64\msctf.dll	SUCCESS	Image Base: 0x76680000, Image S
16:31:2...	AsPatchTouchPanel.exe	CreateFile	C:\Windows\SysWOW64\dwmapi.dll	SUCCESS	Desired Access: Read Attributes, D
16:31:2...	AsPatchTouchPanel.exe	QueryBasicInfo...	C:\Windows\SysWOW64\dwmapi.dll	SUCCESS	CreationTime: 12/04/2018 00:34:5
16:31:2...	AsPatchTouchPanel.exe	CloseFile	C:\Windows\SysWOW64\dwmapi.dll	SUCCESS	
16:31:2...	AsPatchTouchPanel.exe	CreateFile	C:\Windows\SysWOW64\dwmapi.dll	SUCCESS	Desired Access: Read Data/List Di
16:31:2...	AsPatchTouchPanel.exe	CreateFileMap...	C:\Windows\SysWOW64\dwmapi.dll	FILE LOCKED WITH ONLY REA...	SyncType: SyncTypeCreateSectio
16:31:2...	AsPatchTouchPanel.exe	CreateFileMap...	C:\Windows\SysWOW64\dwmapi.dll	SUCCESS	SyncType: SyncTypeOther
16:31:2...	AsPatchTouchPanel.exe	Load Image	C:\Windows\SysWOW64\dwmapi.dll	SUCCESS	Image Base: 0x6f070000, Image S
16:31:2...	AsPatchTouchPanel.exe	CloseFile	C:\Windows\SysWOW64\dwmapi.dll	SUCCESS	
16:31:2...	AsPatchTouchPanel.exe	CreateFile	C:\Windows\Fonts\StaticCache.dat	SUCCESS	Desired Access: Generic Read, Di
16:31:2...	AsPatchTouchPanel.exe	QueryStandardI...	C:\Windows\Fonts\StaticCache.dat	SUCCESS	AllocationSize: 19 202 048, EndOf
16:31:2...	AsPatchTouchPanel.exe	ReadFile	C:\Windows\Fonts\StaticCache.dat	SUCCESS	Offset: 0, Length: 60, Priority: Low
16:31:2...	AsPatchTouchPanel.exe	CreateFileMap...	C:\Windows\Fonts\StaticCache.dat	FILE LOCKED WITH ONLY REA...	SyncType: SyncTypeCreateSectio
16:31:2...	AsPatchTouchPanel.exe	QueryStandardI...	C:\Windows\Fonts\StaticCache.dat	SUCCESS	AllocationSize: 19 202 048, EndOf
16:31:2...	AsPatchTouchPanel.exe	CreateFileMap...	C:\Windows\Fonts\StaticCache.dat	SUCCESS	SyncType: SyncTypeOther
16:31:2...	AsPatchTouchPanel.exe	Load Image	C:\Windows\SysWOW64\powrprof.dll	SUCCESS	Image Base: 0x74840000, Image S
16:31:2...	AsPatchTouchPanel.exe	Thread Create		SUCCESS	Thread ID: 9824
16:31:2...	AsPatchTouchPanel.exe	Thread Create		SUCCESS	Thread ID: 20692
16:31:2...	AsPatchTouchPanel.exe	CreateFile	C:\ProgramData\AsTouchPanel\DEVOBJ.dll	NAME NOT FOUND	Desired Access: Read Attributes, D
16:31:2...	AsPatchTouchPanel.exe	CreateFile	C:\Windows\SysWOW64\devobj.dll	SUCCESS	Desired Access: Read Attributes, D
16:31:2...	AsPatchTouchPanel.exe	QueryBasicInfo...	C:\Windows\SysWOW64\devobj.dll	SUCCESS	CreationTime: 12/04/2018 00:34:5
16:31:2...	AsPatchTouchPanel.exe	CloseFile	C:\Windows\SysWOW64\devobj.dll	SUCCESS	
16:31:2...	AsPatchTouchPanel.exe	CreateFile	C:\Windows\SysWOW64\devobj.dll	SUCCESS	Desired Access: Read Data/List Di
16:31:2...	AsPatchTouchPanel.exe	CreateFileMap...	C:\Windows\SysWOW64\devobj.dll	FILE LOCKED WITH ONLY REA...	SyncType: SyncTypeCreateSectio
16:31:2...	AsPatchTouchPanel.exe	CreateFileMap...	C:\Windows\SysWOW64\devobj.dll	SUCCESS	SyncType: SyncTypeOther
16:31:2...	AsPatchTouchPanel.exe	Load Image	C:\Windows\SysWOW64\devobj.dll	SUCCESS	Image Base: 0x73e10000, Image S
16:31:2...	AsPatchTouchPanel.exe	CloseFile	C:\Windows\SysWOW64\devobj.dll	SUCCESS	
16:31:2...	AsPatchTouchPanel.exe	Load Image	C:\Windows\SysWOW64\wintrust.dll	SUCCESS	Image Base: 0x76510000, Image S
16:31:2...	AsPatchTouchPanel.exe	Load Image	C:\Windows\SysWOW64\msasn1.dll	SUCCESS	Image Base: 0x76a80000, Image S

Showing 125 of 427 770 events (0.0%) Backed by virtual memory

Asus Delayload plant



Asus Delayload plant



WinSxS redirection

svchost.exe (1116)	Host Process for Windows Services	C:\Windows\system32\svchost.exe	Microsoft Corporat...	NT AUTHORITY\LOCAL SERVICE	C:\Wir
svchost.exe (1144)	Host Process for Windows Services	C:\Windows\system32\svchost.exe	Microsoft Corporat...	NT AUTHORITY\SYSTEM	C:\Wir
taskhostw.exe (4080)	Host Process for Windows Tasks	C:\Windows\system32\taskhostw.exe	Microsoft Corporat...	WINDEV1810EVAL\user	taskho
launcher.exe (3296)	Opera Internet Browser	C:\Program Files\Opera\launcher.exe	Opera Software	NT AUTHORITY\SYSTEM	"C:\Pro
installer.exe (1908)	Opera Installer	C:\Windows\TEMP\opera autoupdate\installer.exe	Opera Software	NT AUTHORITY\SYSTEM	"C:\W
opera_autoupdate.exe (3004)	Opera auto-updater	C:\Program Files\Opera\57.0.3098.106\opera_auto...	Opera Software	NT AUTHORITY\SYSTEM	"C:\Pro
opera_autoupdate.exe (984)	Opera auto-updater	C:\Program Files\Opera\57.0.3098.106\opera_auto...	Opera Software	NT AUTHORITY\SYSTEM	"C:\Pro
svchost.exe (1256)	Host Process for Windows Services	C:\Windows\system32\svchost.exe	Microsoft Corporat...	NT AUTHORITY\SYSTEM	C:\Wir
svchost.exe (1284)	Host Process for Windows Services	C:\Windows\System32\svchost.exe	Microsoft Corporat...	NT AUTHORITY\SYSTEM	C:\Wir
svchost.exe (1316)	Host Process for Windows Services	C:\Windows\System32\svchost.exe	Microsoft Corporat...	NT AUTHORITY\LOCAL SERVICE	C:\Wir
svchost.exe (1336)	Host Process for Windows Services	C:\Windows\system32\svchost.exe	Microsoft Corporat...	NT AUTHORITY\SYSTEM	C:\Wir
sihost.exe (3948)	Shell Infrastructure Host	C:\Windows\system32\sihost.exe	Microsoft Corporat...	WINDEV1810EVAL\user	sihost.e
svchost.exe (1448)	Host Process for Windows Services	C:\Windows\system32\svchost.exe	Microsoft Corporat...	NT AUTHORITY\LOCAL SERVICE	C:\Wir

- `launcher.exe` copy `installer.exe` from `C:\Program Files\Opera\${version}\installer.exe` into a temporary directory, `C:\Windows\Temp\opera autoupdate\`
- `launcher.exe` calls `CreateProcess` on the temporary executable
- `installer.exe` is executed and **also** drops a temporary DLL `C:\Windows\Temp\Opera_installer_${timestamp}.dll` which is then loaded in the `installer.exe`'s proces.
- `C:\Windows\Temp\opera autoupdate\installer.exe` is automatically deleted when the process exits.

WinSxS redirection

Embedded PE manifest for Opera's installer

```
<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">
  <dependency>
    <dependentAssembly>
      <assemblyIdentity
        type="win32" name="Microsoft.Windows.Common-Controls"
        version="6.0.0.0" processorArchitecture="*"
        publicKeyToken="6595b64144ccf1df" language="*">
      </assemblyIdentity>
    </dependentAssembly>
  </dependency>
  <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
    <security>
      <requestedPrivileges>
        <requestedExecutionLevel level="asInvoker" uiAccess="false"></requestedExecutionLevel>
      </requestedPrivileges>
    </security>
  </trustInfo>
</assembly>
```

WinSxS redirection

installer.exe	1908	RegOpenKey	HKLM\Software\Microsoft\Windows\CurrentVersion\SideBySide\AssemblyStorageRoots	NAM
installer.exe	1908	QueryOpen	C:\Windows\Temp\opera autoupdate\installer.exe.Local	NAM
installer.exe	1908	CreateFile	C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.17763.195_none_05b436ac07203599	SUC
installer.exe	1908	QueryOpen	C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.17763.195_none_05b436ac07203599\comctl32.dll	SUC
installer.exe	1908	CreateFile	C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.17763.195_none_05b436ac07203599\comctl32.dll	SUC

WinSxS redirection

installer.exe	3744	QueryOpen	C:\Windows\Temp\opera autoupdate\installer.exe.Local	SUCCESS
installer.exe	3744	CreateFile	C:\Windows\Temp\opera autoupdate\installer.exe.Local\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.17763.195_none_05b436ac07203599	SUCCESS
installer.exe	3744	QueryOpen	C:\Windows\Temp\opera autoupdate\installer.exe.Local\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.17763.195_none_05b436ac07203599\comctl32.dll	SUCCESS
installer.exe	3744	CreateFile	C:\Windows\Temp\opera autoupdate\installer.exe.Local\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.17763.195_none_05b436ac07203599\comctl32.dll	SUCCESS
installer.exe	3744	CreateFileMapping	C:\Windows\Temp\opera autoupdate\installer.exe.Local\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.17763.195_none_05b436ac07203599\comctl32.dll	FILE LOCKED
installer.exe	3744	CreateFileMapping	C:\Windows\Temp\opera autoupdate\installer.exe.Local\comctl32.dll	SUCCESS
installer.exe	3744	Load Image	C:\Windows\Temp\opera autoupdate\installer.exe.Local\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.17763.195_none_05b436ac07203599\comctl32.dll	SUCCESS
installer.exe	3744	CloseFile	C:\Windows\Temp\opera autoupdate\installer.exe.Local\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.17763.195_none_05b436ac07203599\comctl32.dll	SUCCESS

WinSxS redirection

Demo

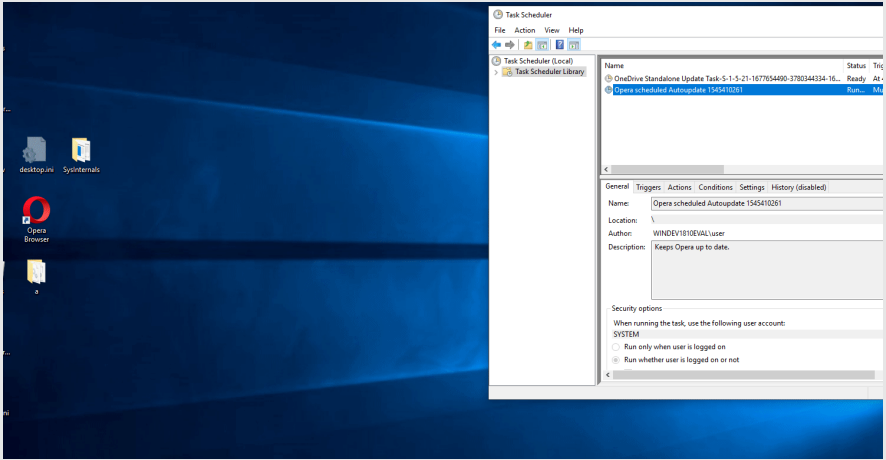


Table des matières

Conclusion

Lien vers le projet : https ://www.github.com/lucasg/Dependencies.git

AVEZ-VOUS
DES QUESTIONS ?

MERCI DE VOTRE ATTENTION

SYNACKTIV
DIGITAL SECURITY