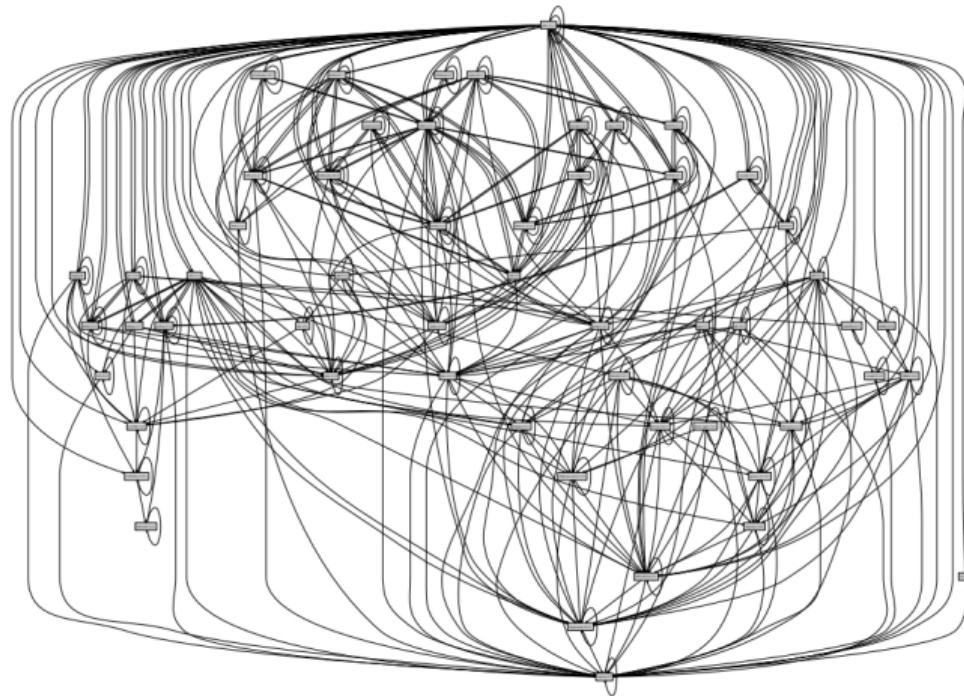




DLL Shell Game and other misdirections

SSTIC 2019



06/06/2019
Synacktiv
Lucas GEORGES



Table des matières

1 Introduction

2 Tools

3 DLL Redirections

4 Vulnerabilities

5 Conclusion

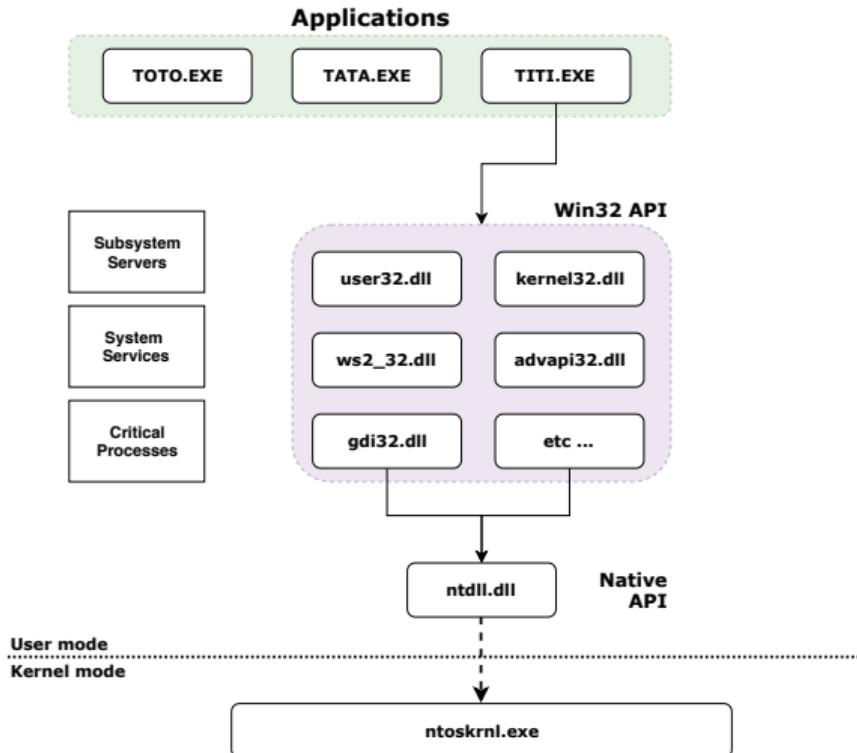


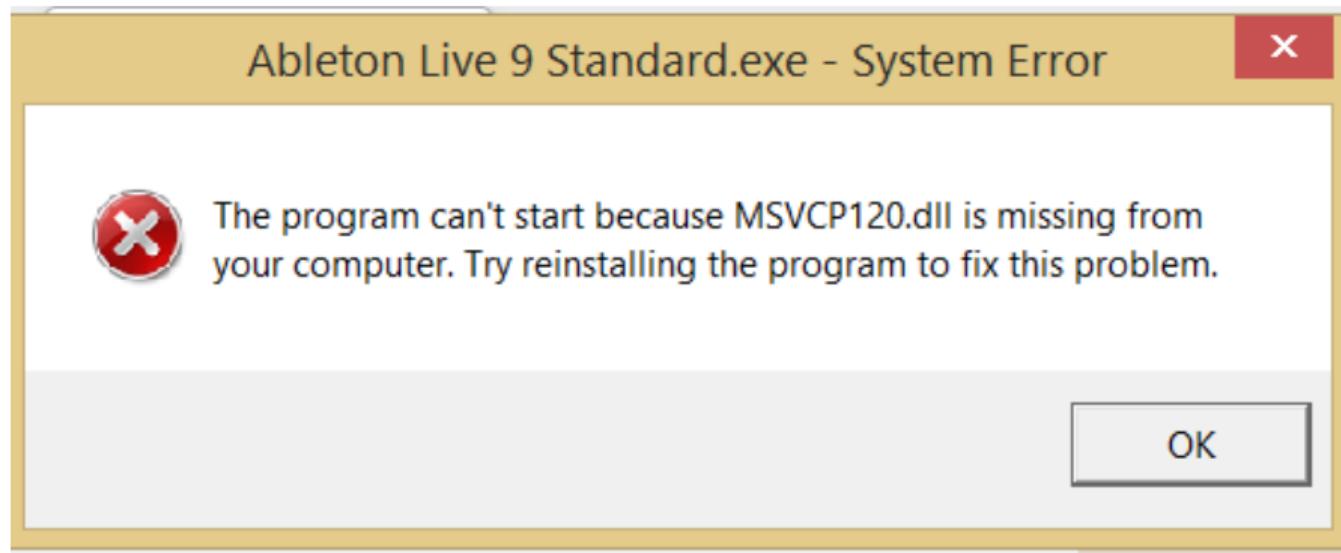
Whoami



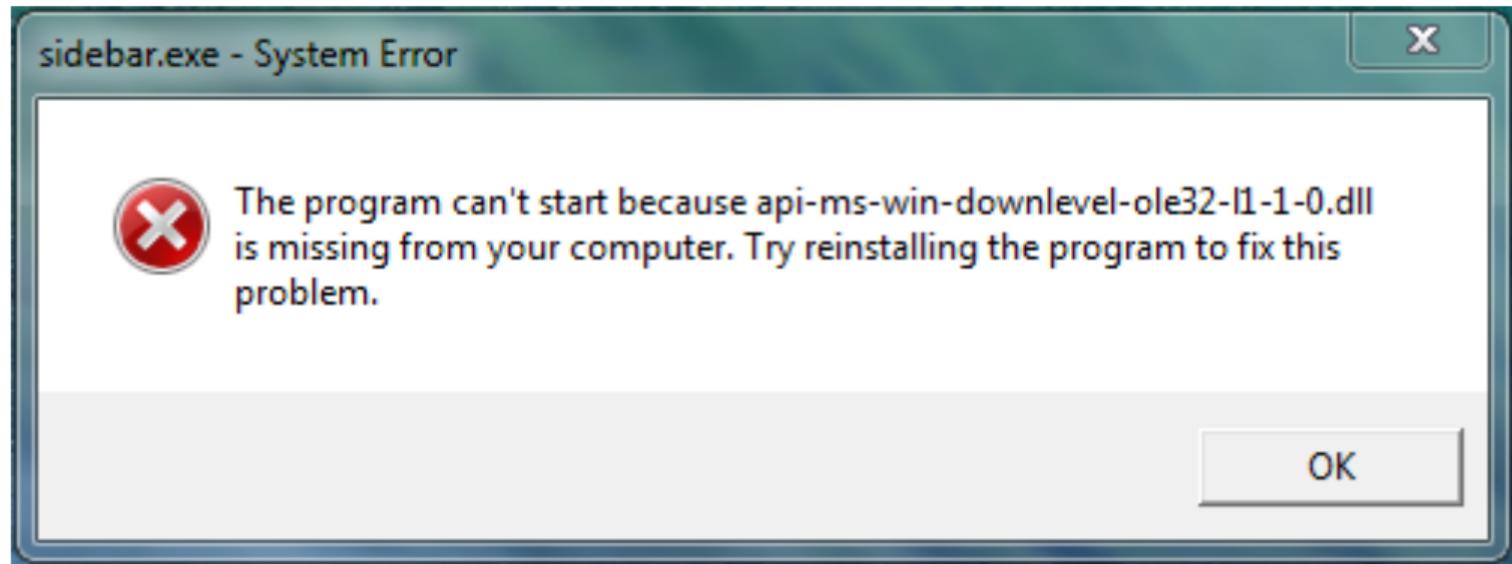
- Twitter : @_lucas_georges_
- Reverser @ Synacktiv
- Located in Rennes ;p

Dynamic Link Library (DLL) Dependencies



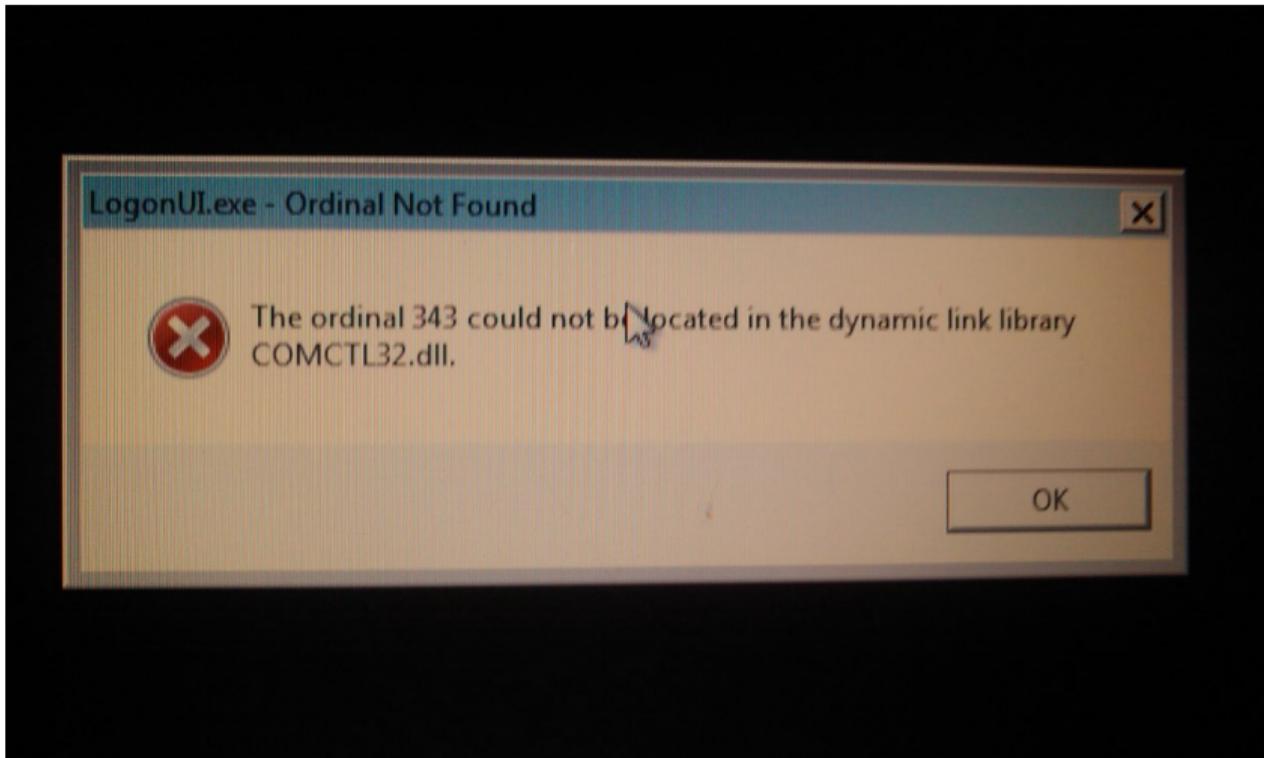


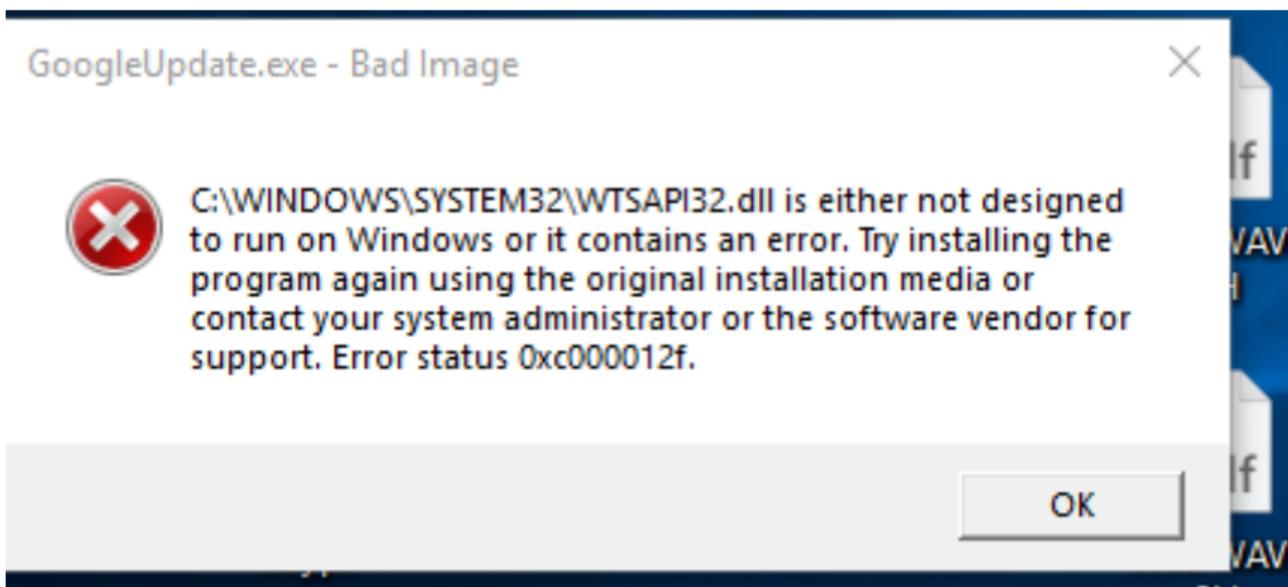
Missing DLL?





Missing Export





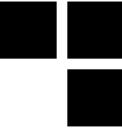


Table des matières

1 Introduction

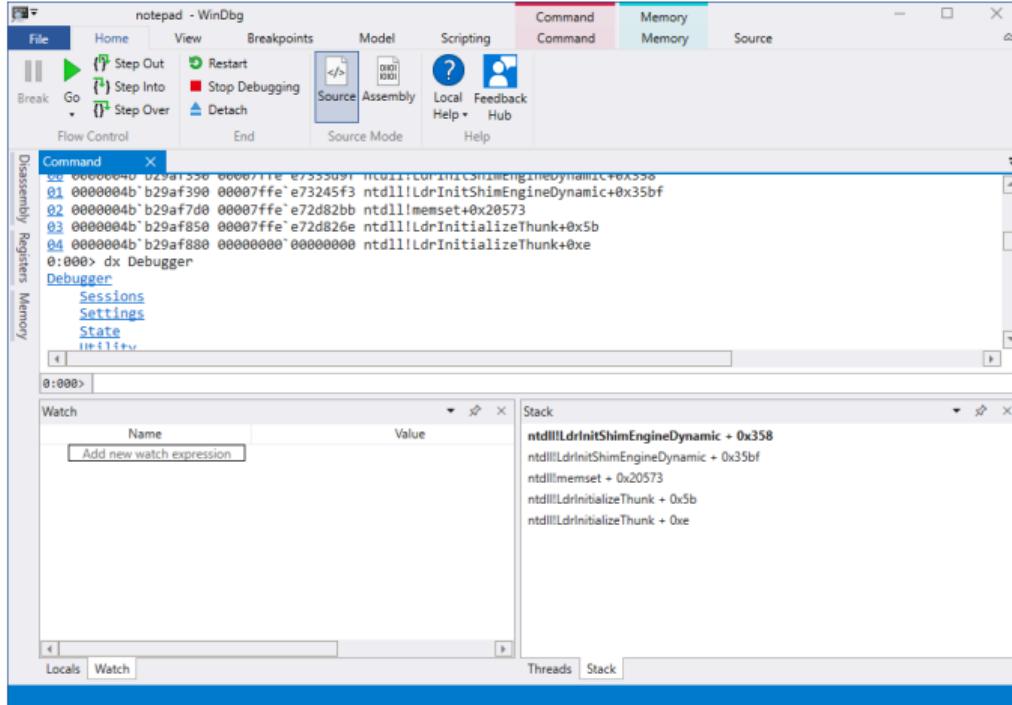
2 Tools

3 DLL Redirections

4 Vulnerabilities

5 Conclusion

Windbg



Dependency Walker



Dependency Walker - [Stooges.exe]

File Edit View Options Profile Window Help

Module Tree:

- STOOGES.EXE
 - LARRY.DLL
 - KERNEL32.DLL
 - NTDLL.DLL
 - CURLY.DLL
 - SHEMP.DLL
 - MOE.DLL
 - KERNEL32.DLL
 - NTDLL.DLL

Imports Table:

| Ordinal | Hint | Function | Entry Point |
|---------|------|-----------------------------|-------------|
| N/A | N/A | IsKnucklehead | Not Bound |
| N/A | N/A | int SaySoitenly(char *,...) | Not Bound |

Exports Table:

| Ordinal | Hint | Function | Entry Point |
|------------|------------|-----------------------------|----------------------------|
| 4 (0x0004) | 1 (0x0001) | int SaySoitenly(char *,...) | SHEMP.!SaySoitenly@@YAHPPA |
| 5 (0x0005) | 2 (0x0002) | DoinkLarrysEye | 0x00001010 |
| 3 (0x0003) | 0 (0x0000) | void SayPoifect(_int64) | 0x00001020 |
| 1 (0x0001) | N/A | N/A | 0x00001020 |
| 2 (0x0002) | 3 (0x0003) | DoinkMoesEye | SHEMP.DoinkMoesEye |

Modules Table:

| Module ^ | File Time Stamp | Link Time Stamp | File Size | Attr. | Link Checksum | Real Checksum | CPU | Subsystem |
|--------------|------------------|------------------|-----------|-------|---------------|---------------|-----|-----------|
| CURLY.DLL | 11/14/2006 5:17p | 11/14/2006 5:13p | 2,560 | A | 0x0000F739 | 0x0000F759 | x86 | GUI |
| KERNEL32.DLL | 08/30/2006 1:22a | 08/30/2006 1:20a | 871,424 | A | 0x000E388E | 0x000E388E | x86 | Console |
| LARRY.DLL | 11/14/2006 5:13p | 11/14/2006 5:13p | 2,560 | A | 0x000053DB | 0x000053DB | x86 | GUI |
| MOE.DLL | 11/14/2006 5:15p | 11/14/2006 5:15p | 2,560 | A | 0x0000B191 | 0x0000B191 | x86 | GUI |
| NTDLL.DLL | 08/30/2006 1:23a | 08/30/2006 1:21a | 1,147,664 | A | 0x00125FA5 | 0x00125FA5 | x86 | Console |
| SHEMP.DLL | 11/14/2006 5:13p | 11/14/2006 5:13p | 2,560 | A | 0x00001CE7 | 0x00001CE7 | x86 | GUI |

Log:

```
00:00:00:093: LoadLibraryA("Moe.dll") called from "STOOGES.EXE" at address 0x00401024 by thread 1.  
00:00:00:093: Loaded "MOE.DLL" at address 0x00020000 by thread 1. Successfully hooked module.  
00:00:00:093: DILMain(0x00020000, DLL_PROCESS_ATTACH, 0x00000000) in "MOE.DLL" called by thread 1.  
00:00:00:093: DILMain(0x00020000, DLL_PROCESS_ATTACH, 0x00000000) in "MOE.DLL" returned 1 (0x1) by thread 1.  
00:00:00:093: LoadLibraryA("Moe.dll") returned 0x00200000 by thread 1.  
00:00:00:109: GetProcAddress(0x00020000 [MOE.DLL], "SmackCurly") called from "STOOGES.EXE" at address 0x00401028 and returned 0x00001020.
```

For Help, press F1

Dependency Walker on a modern binary



Dependency Walker - [kernel32.dll]

File Edit View Options Profile Window Help

Kernel32.DLL

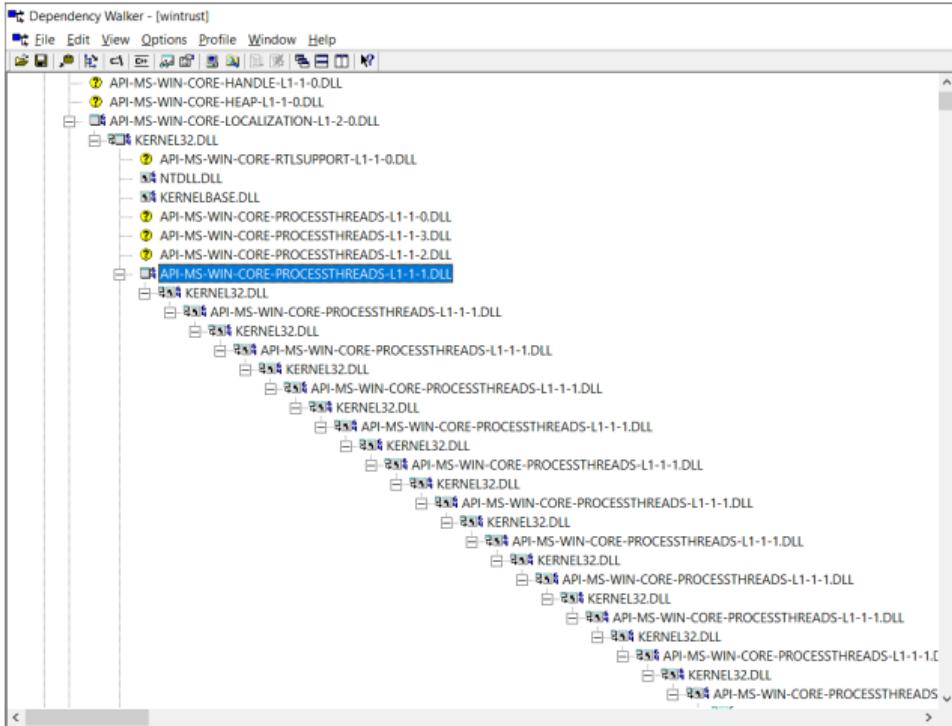
- API-MS-WIN-CORE-RTLSUPPORT-L1-2-0.DLL
- NTDLL.DLL
- KERNELBASE.DLL
 - NTDLL.DLL
 - API-MS-WIN-EVENTING-PROVIDER-L1-1-0.DLL
 - API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL
 - EXT-MS-WIN-ADVAPI32-REGISTRY-L1-1-0.DLL
 - EXT-MS-WIN-KERNEL32-APPCOMPAT-L1-1-0.DLL
 - EXT-MS-WIN-NTUSER-STRING-L1-1-0.DLL
 - EXT-MS-WIN-KERNEL32-FILE-L1-1-0.DLL
 - EXT-MS-WIN-KERNEL32-DATETIME-L1-1-0.DLL
 - EXT-MS-WIN-KERNEL32-QUIRKS-L1-1-0.DLL
 - EXT-MS-WIN-KERNEL32-QUIRKS-L1-1-1.DLL
 - EVT-MS-WIN-KERNEL32-SIDERSVINE-L1-1-1.DLL

| PI | Ordinal ^ | Hint | Function |
|----|------------|------------|-------------------------|
| | 3 (0x0 03) | 0 (0x0 00) | AcquireSRWLockExclusive |
| | 4 (0x0 04) | 1 (0x0 01) | AcquireSRWLockShared |
| | 5 (0x0 05) | 2 (0x0 02) | ActivateActCtx |
| | 6 (0x0 06) | 3 (0x0 03) | ActivateActCtxWorker |
| | 7 (0x0 07) | 4 (0x0 04) | AddAtomA |
| | 8 (0x0 08) | 5 (0x0 05) | AddAtomW |
| | 9 (0x0 09) | 6 (0x0 06) | AddConsoleAliasA |

| Module | File Time Stamp | Link Time Stamp | File Size | Attr. | Link Chi |
|--------------------------------------|-----------------|-----------------|-----------|-------|--|
| API-MS-WIN-CORE-APIQUERY-L1-1-0.DLL | | | | | Error opening file. The system cannot find the file specified (2). |
| API-MS-WIN-CORE-APPCOMPAT-L1-1-1.DLL | | | | | Error opening file. The system cannot find the file specified (2). |
| API-MS-WIN-CORE-COMM-L1-1-0.DLL | | | | | Error opening file. The system cannot find the file specified (2). |
| API-MS-WIN-CORE-CONSOLE-L1-1-0.DLL | | | | | Error opening file. The system cannot find the file specified (2). |
| API-MS-WIN-CORE-CONSOLE-L2-1-0.DLL | | | | | Error opening file. The system cannot find the file specified (2). |
| API-MS-WIN-CORE-DATETIME-L1-1-1.DLL | | | | | Error opening file. The system cannot find the file specified (2). |

Error: At least one required implicit or forwarded dependency was not found.
Warning: At least one delay-load dependency module was not found.

Dependency Walker on a modern binary



Dependencies

The screenshot shows the DbgXShell interface with the 'Dependencies (x64)' tab selected. The left pane displays the dependency tree for the application 'DbgX.Shell.exe'. The right pane contains two tables: one for imports and one for exports.

Imports Table:

| PI | Ordinal | Hint | Function | Module |
|----|---------|--------------|--------------------|---------------------------------|
| E | 6 | (0x00000006) | CreateFileW | api-ms-win-core-file-l1-1-0.dll |
| E | 9 | (0x00000009) | DeleteFileW | api-ms-win-core-file-l1-1-0.dll |
| E | 44 | (0x0000002c) | GetFileAttributesW | api-ms-win-core-file-l1-1-0.dll |
| E | 8 | (0x00000008) | DeleteFileA | api-ms-win-core-file-l1-1-0.dll |
| E | 46 | (0x0000002a) | GetFileSize | api-ms-win-core-file-l1-1-0.dll |
| E | 52 | (0x00000034) | GetFullPathNameA | api-ms-win-core-file-l1-1-0.dll |
| E | 87 | (0x00000057) | SetFileTime | api-ms-win-core-file-l1-1-0.dll |
| E | 48 | (0x00000030) | GetFileTime | api-ms-win-core-file-l1-1-0.dll |

Exports Table:

| E | Ordinal | Hint | Function | VirtualAddress |
|---|---------|--------------|-----------------------------------|----------------|
| E | 0 | (0x00000000) | PackageSidFromProductId | 0x000173360 |
| E | 1 | (0x00000001) | GetCPHashNode | 0x000ee7e0 |
| E | 2 | (0x00000002) | GetNameAndLocaleHashNode | 0x0001017290 |
| E | 3 | (0x00000003) | NTDLL.RtlInterlockedPushListSList | 0x0000000000 |
| E | 4 | (0x00000004) | InternalLcidToName | 0x0001141d0 |
| E | 5 | (0x00000005) | KernelbasePostInit | 0x0001117410 |
| E | 6 | (0x00000006) | Wcm64Transition | 0x0001c8ed8 |
| E | 7 | (0x00000007) | AccessCheck | 0x000101d230 |
| E | 8 | (0x00000008) | AccessCheckAndAuditAlarmW | 0x0001958d0 |
| E | 9 | (0x00000009) | AccessCheckByType | 0x000111960 |
| E | 10 | (0x0000000a) | AccessCheckByTypeAndAuditAlarmW | 0x000198b80 |
| E | 11 | (0x0000000b) | AccessCheckByTypeResultList | 0x000198c30 |

Module Table:

| Module | Machine | Type | File Size | Image Base | Virtual Size | Entry point | Subsystem | Subsystem Ver. | Checksum |
|---------------------------|---------|-----------------|------------|--------------|--------------|-------------|------------|----------------|----------------------|
| mscoree.dll | I386 | Dll; Executable | 0x0004d200 | 0x100000000 | 0x00053000 | 0x0002f450 | 0x00000003 | 10.0 | 0x00054e67 (correct) |
| mscorlib.dll | AMD64 | Dll; Executable | 0x0052d000 | 0x6447800000 | 0x0052c000 | 0x00000000 | 0x00000003 | 6.0 | 0x0053af0f (correct) |
| PresentationFramework.dll | I386 | Dll; Executable | 0x005f2c38 | 0x56610000 | 0x005f4000 | 0x005b4e4e | 0x00000003 | 6.0 | 0x0054fc6 (correct) |
| System.Kernel.dll | I386 | Dll; Executable | 0x0009cc80 | 0x58000000 | 0x0009c000 | 0x0008e6de | 0x00000003 | 6.0 | 0x000aa277 (correct) |
| System.dll | I386 | Dll; Executable | 0x00365b48 | 0x7a540000 | 0x00366000 | 0x00323e96 | 0x00000003 | 6.0 | 0x0036d10b (correct) |

Loading PE file "C:\WINDOWS\SysWOW64\kernelbase.dll" successful.



DEMO

DEMO TIME!



Table des matières

1 Introduction

2 Tools

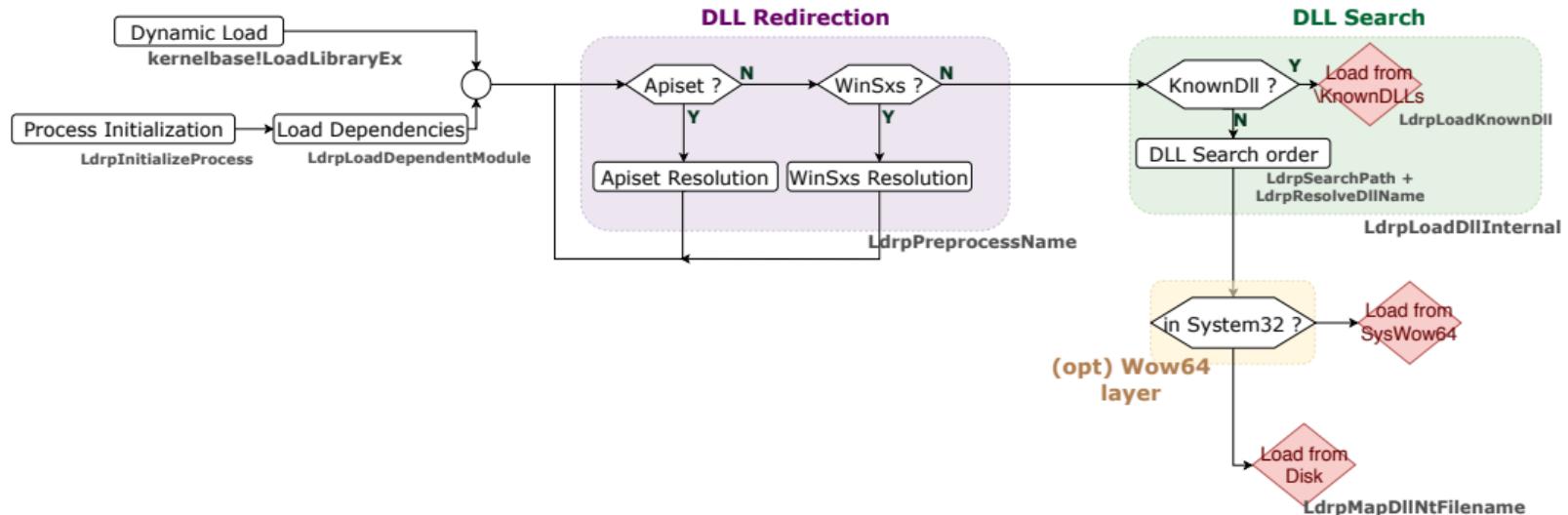
3 DLL Redirections

4 Vulnerabilities

5 Conclusion

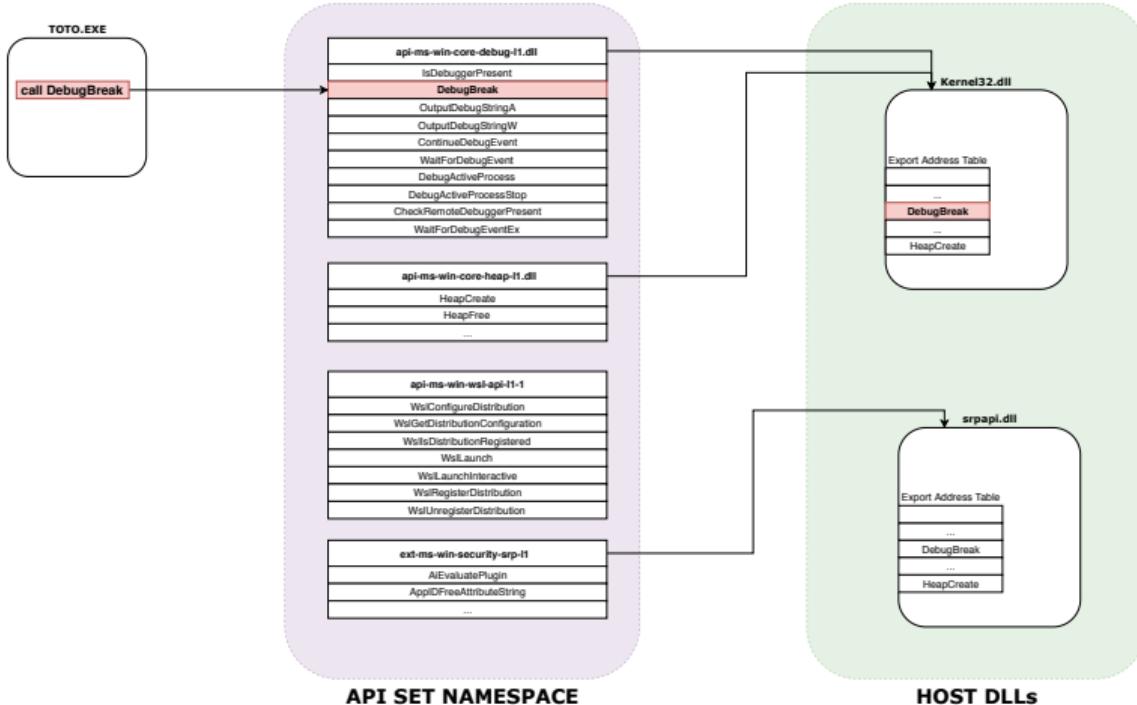


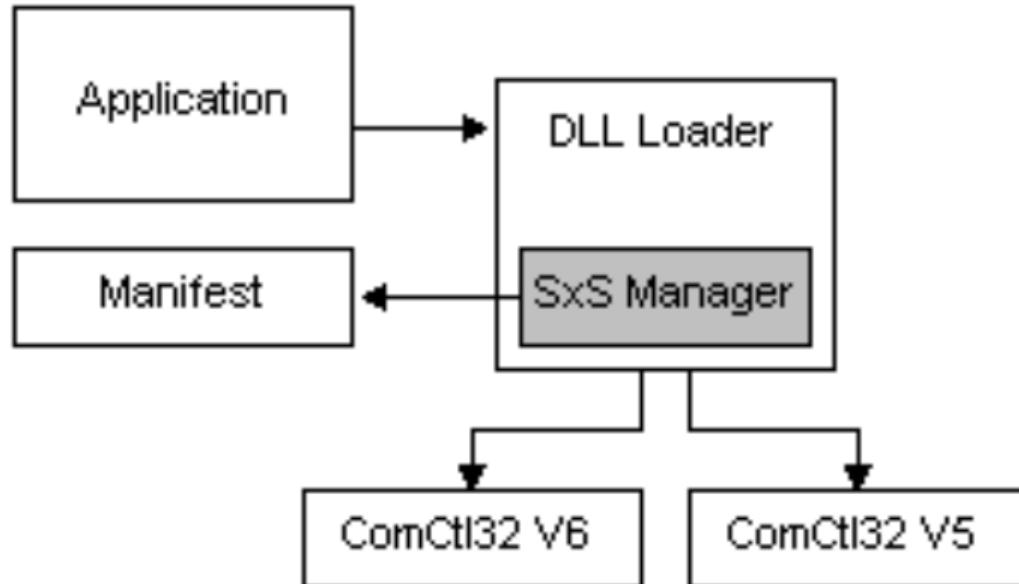
Diagram





Apisets







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>
  </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-5d96-4fdb-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 |
| DfxApi | REG_SZ | dfxapi.dll |
| gdi32 | REG_SZ | gdi32.dll |
| gdiplus | REG_SZ | gdiplus.dll |
| IMAGEHELP | REG_SZ | IMAGEHELP.dll |

WinObj - Sysinternals: www.sysinternals.com

File View Help

KnownDLLs

| 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 | |
| gdipplus.dll | Section | |
| IMAGEHELP.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->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

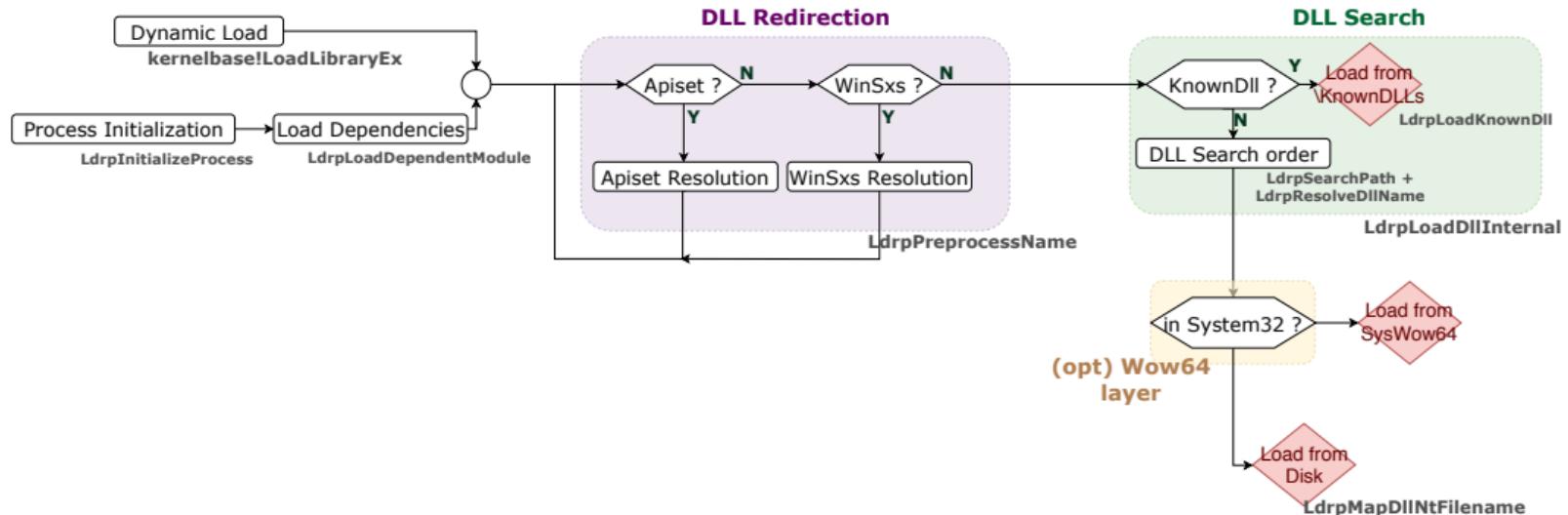




Table des matières

1 Introduction

2 Tools

3 DLL Redirections

4 Vulnerabilities

5 Conclusion

Asus Delayload plant



The screenshot shows two windows side-by-side. On the left is the Windows Task Scheduler interface. The main pane lists several scheduled tasks:

| Nom | Statut | Déclencheurs |
|-----------------------------|----------|---|
| ASUS Hello | En cours | À l'ouverture de session d'un utilisateur |
| ASUS Patch for Touch Panel | En cours | À l'ouverture de session d'un utilisateur |
| ATK Package 36D18D69AFC3 | Prêt | Filtre d'événement personnalisé |
| ATK Package A22126881260 | Prêt | |
| CheckFlipService | Prêt | Plusieurs déclencheurs sont définis. |
| GoogleUpdateTaskMachineCore | Prêt | Plusieurs déclencheurs sont définis. |

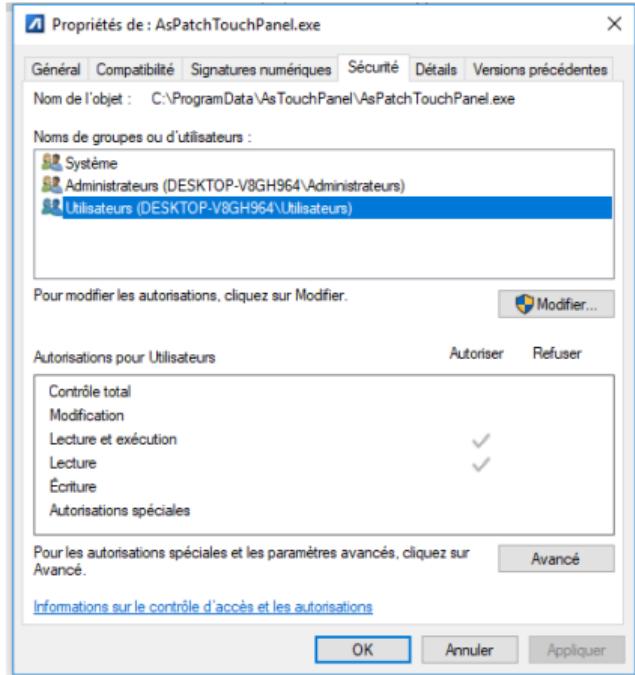
The right pane shows the 'Actions' menu with various options like Biblioth... (highlighted), Cré..., Cré..., Im..., Affi..., Act..., No..., Affi..., Act..., and Aide. Below the Task Scheduler is a message box asking to use the 'Administrateurs' account to run the task.

On the right, the Process Hacker application is open, showing a list of running processes:

| Name | PID | CPU I/O total ra... | Private byt... | User name | Description | Integrity |
|-----------------------|-------|---------------------|----------------|--------------------------------|-----------------------------------|-----------|
| svchost.exe | 3408 | | | 6,67 MB AUTORITE NT\Système | Host Process for Windows Servi... | System |
| QuietFan.exe | 7392 | 0,12 | | 20,52 MB DESKTOP-B4KRUQ9\lucas | Quiet Fan | High |
| ASUSHelloBG.exe | 7400 | | | 1,63 MB DESKTOP-B4KRUQ9\lucas | | High |
| AsPatchTouchPanel.... | 7464 | | | 1,43 MB DESKTOP-B4KRUQ9\lucas | ASUS Patch For Touch Panel | High |
| taskhostw.exe | 7472 | | | 9,49 MB DESKTOP-B4KRUQ9\lucas | Host Process for Windows Tasks | Medium |
| RAVBg64.exe | 8808 | | | 6,04 MB DESKTOP-B4KRUQ9\lucas | HD Audio Background Process | Medium |
| taskhostw.exe | 18528 | | | 8,08 MB DESKTOP-B4KRUQ9\lucas | Host Process for Windows Tasks | High |

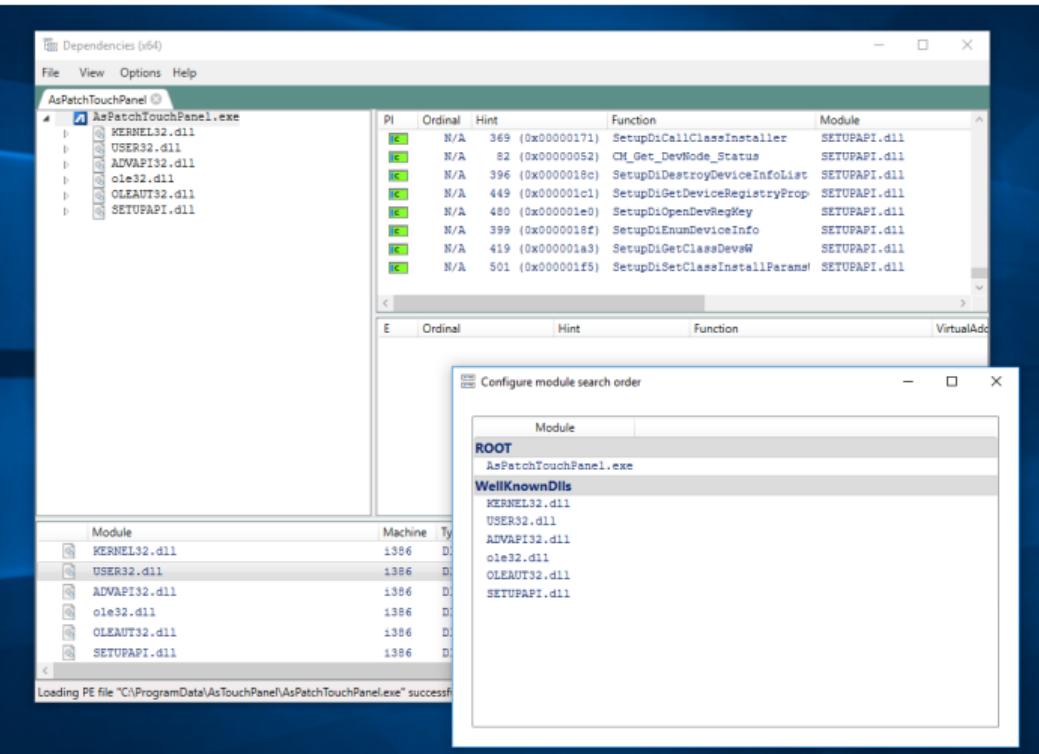


Asus Delayload plant



- 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



| 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: SyncTypeCreateSection |
| 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 | |
| 16:31:2... | AsPatchTouchPanel.exe | CreateFile | C:\Windows\SysWOW64\dwmapi.dll | SUCCESS | Image Base: 0x76680000, Image S... |
| 16:31:2... | AsPatchTouchPanel.exe | QueryBasicInfo... | C:\Windows\SysWOW64\dwmapi.dll | SUCCESS | Desired Access: Read Attributes, L... |
| 16:31:2... | AsPatchTouchPanel.exe | CloseFile | C:\Windows\SysWOW64\dwmapi.dll | SUCCESS | CreationTime: 12/04/2018 00:34:5... |
| 16:31:2... | AsPatchTouchPanel.exe | CreateFile | C:\Windows\SysWOW64\dwmapi.dll | SUCCESS | |
| 16:31:2... | AsPatchTouchPanel.exe | CreateFileMap... | C:\Windows\SysWOW64\dwmapi.dll | FILE LOCKED WITH ONLY REA... | SyncType: SyncTypeCreateSection |
| 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: SyncTypeCreateSection |
| 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\powprof.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 | |
| 16:31:2... | AsPatchTouchPanel.exe | CreateFileMap... | C:\Windows\SysWOW64\devobj.dll | FILE LOCKED WITH ONLY REA... | SyncType: SyncTypeCreateSection |
| 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 | |
| 16:31:2... | AsPatchTouchPanel.exe | Load Image | C:\Windows\SysWOW64\msasn1.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... |

Asus Delayload plant

Dependencies (x64)

File View Options Help

AsPatchTouchPanel

PI Ordinal Hint Function Module

E Ordinal Hint Function VirtualAddress

| Module | Machine | Type | File Size | Image Base | Virtual Size | Entry point | Subsystem | Subsystem Ver. | Checksum |
|---------------------------------|---------|-----------------|------------|------------|--------------|-------------|------------|----------------|--------------------|
| C:\WINDOWS\SysoW64\kernel32.dll | 1386 | Dll: Executable | 0x0009e768 | 0x68000000 | 0x000e0000 | 0x00020010 | 0x00000003 | 10.0 | 0x000abfa4 (corre) |
| C:\WINDOWS\SysoW64\user32.dll | 1386 | Dll: Executable | 0x001991c0 | 0x69e00000 | 0x01990000 | 0x0003e990 | 0x00000002 | 10.0 | 0x001a329c (corre) |
| C:\WINDOWS\SysoW64\advapi32.dll | 1386 | Dll: Executable | 0x0007be08 | 0x43000000 | 0x0007e000 | 0x000247e0 | 0x00000003 | 10.0 | 0x0008764 (corre) |
| C:\WINDOWS\SysoW64\ole32.dll | 1386 | Dll: Executable | 0x000fae8 | 0x6f000000 | 0x000fc000 | 0x0003ede0 | 0x00000003 | 10.0 | 0x000feff8 (corre) |
| C:\WINDOWS\SysoW64\oleaut32.dll | 1386 | Dll: Executable | 0x00093768 | 0x10000000 | 0x00096000 | 0x0002af10 | 0x00000003 | 10.0 | 0x0009e36e (corre) |
| C:\WINDOWS\SysoW64\Setupapi.dll | 1386 | Dll: Executable | 0x00451608 | 0x10000000 | 0x0044b000 | 0x00030960 | 0x00000002 | 10.0 | 0x004581bd (corre) |
| C:\WINDOWS\SysoW64\MSVCR7.dll | 1386 | Dll: Executable | 0x000be958 | 0x10100000 | 0x000e0000 | 0x0003e680 | 0x00000002 | 10.0 | 0x000c1d0c (corre) |

Loading PE file "C:\WINDOWS\SysoW64\ole32.dll" successful.



- X

Logs Viewer

| Date | Heure | Niveau | Nom | Version | État |
|------------|----------|----------|------------------------|---------|----------|
| 2018/11/25 | 12:16 AM | Critique | ASUS Live Update | V3.5.4 | Réussite |
| 2018/11/25 | 12:16 AM | Critique | ASUS Device Activation | 1.0.4.0 | Réussite |
| 2019/02/27 | 09:10 PM | Critique | TPIC patch | 4.0 | Réussite |

Tout supprimer



WinSxS redirection

| | | | | |
|-----------------------------|-----------------------------------|--|--|----------|
| svchost.exe (1116) | Host Process for Windows Services | C:\Windows\system32\svchost.exe | Microsoft Corporat... NT AUTHORITY\LOCAL SERVICE | C:\Win |
| svchost.exe (1144) | Host Process for Windows Services | C:\Windows\system32\svchost.exe | Microsoft Corporat... NT AUTHORITY\SYSTEM | C:\Win |
| 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:\Win |
| svchost.exe (1284) | Host Process for Windows Services | C:\Windows\System32\svchost.exe | Microsoft Corporat... NT AUTHORITY\SYSTEM | C:\Win |
| svchost.exe (1316) | Host Process for Windows Services | C:\Windows\System32\svchost.exe | Microsoft Corporat... NT AUTHORITY\LOCAL SERVICE | C:\Win |
| svchost.exe (1336) | Host Process for Windows Services | C:\Windows\system32\svchost.exe | Microsoft Corporat... NT AUTHORITY\SYSTEM | C:\Win |
| 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:\Win |

- 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 process.
- 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 | RenOpenKey | HKEY_LOCAL_MACHINE\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_6553604144ccf1df_6.0.17763.195_none_05b436ac07203599 | SUCI |
| Installer.exe | 1908 | QueryOpen | C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.17763.195_none_05b436ac07203599\comctl32.dll | SUCI |
| Installer.exe | 1908 | CreateFile | C:\Windows\WinSxS\amd64_microsoft.windows.common-controls_6595b64144ccf1df_6.0.17763.195_none_05b436ac07203599\comctl32.dll | SUCI |



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_6595b64144cc1df_6.0.17763.195_none_05b436ac07203599 | | | SUCCESS |
| installer.exe | 3744 | QueryOpen | C:\Windows\Temp\opera autoupdate\installer.exe | Local\amd64_microsoft.windows.common-controls_6595b64144cc1df_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_6595b64144cc1df_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_6595b64144cc1df_6.0.17763.195_none_05b436ac07203599\comctl32.dll | | | FILE LOCKED |
| installer.exe | 3744 | CreateFileMapping | C:\Windows\Temp\opera autoupdate\installer.exe | Local\msctf4.dll | | | SUCCESS |
| installer.exe | 3744 | Load Image | C:\Windows\Temp\opera autoupdate\installer.exe | Local\amd64_microsoft.windows.common-controls_6595b64144cc1df_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_6595b64144cc1df_6.0.17763.195_none_05b436ac07203599\comctl32.dll | | | SUCCESS |

WinSxS redirection



Demo

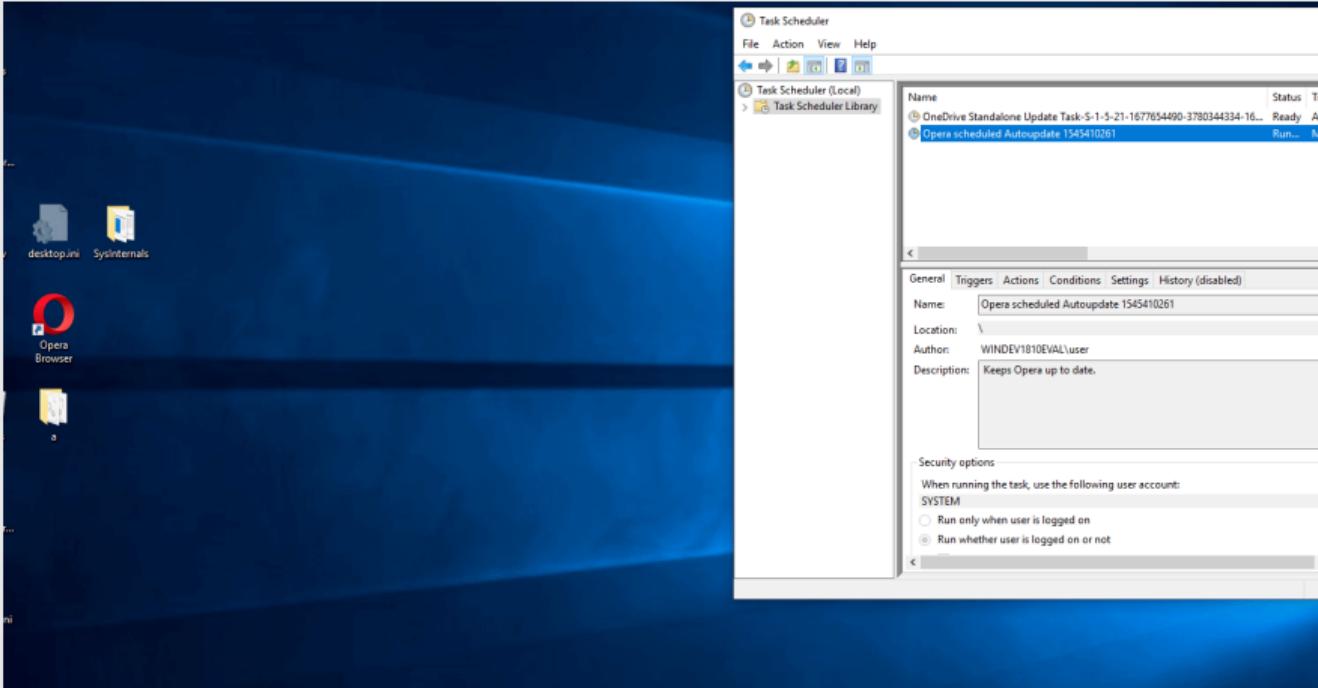




Table des matières

1 Introduction

2 Tools

3 DLL Redirections

4 Vulnerabilities

5 Conclusion



Conclusion

The screenshot shows a tweet from Lucas Georges (@_lucas_georges_). The tweet reads: "Nice, my tool made its way into @msdev's MSDN :)" and includes a link to a Microsoft document titled "Understanding the Dependencies of a Visual C++ Application" from docs.microsoft.com. The tweet was posted at 10:45 am - 21 Apr 2019. It has 14 retweets and 17 likes. The tweet card also shows icons for reply, retweet, and like.

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



AVEZ-VOUS
DES QUESTIONS?

