

Security Analysis Report

Generated on: 2025-05-14 00:09:15

Basic Information

Verdict: no specific threat

Sample Name: Release.exe

File Type: PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive

SHA256: 18aab0e981eee9e4ef8e15d4b003b14b3a1b0bfb7233fade8ee4b6a22a5abbb9

Size: 2932642

Environment: Windows 7 64 bit

Threat Score: None

Detected Signatures

Name: Drops files marked as clean

Severity: Unknown

Description: Antivirus vendors marked dropped file "SharpSteam.dll" as clean (type is "PE32 executable")

Name: Overview of unique CLSIDs touched in registry

Severity: Unknown

Description: "Release.exe" touched "Computer" (Path: "HKCU\WOW6432NODE\CLSID\{20D04FE0-3AEA-1069-A2D0-08002B30309D}")

"Release.exe" touched "Memory Mapped Cache Mgr" (Path: "HKCU\WOW6432NODE\CLSID\{1F486A52-4C4A-4A49-A068-6495E640C64A}")

"Release.exe" touched "Microsoft Multiple AutoComplete List Container" (Path: "HKCU\WOW6432NODE\CLSID\{00000000-0000-0000-0000-000000000000}")

"Release.exe" touched "Microsoft Shell Folder AutoComplete List" (Path: "HKCU\WOW6432NODE\CLSID\{00000000-0000-0000-0000-000000000000}")

"Release.exe" touched "Microsoft AutoComplete" (Path: "HKCU\WOW6432NODE\CLSID\{00BB2763-6A81-4460-895A-49C4EEC7A3E2}")

"Release.exe" touched "Microsoft TipAutoCompleteClient Control" (Path: "HKCU\WOW6432NODE\CLSID\{00000000-0000-0000-0000-000000000000}")

Name: Loads rich edit control libraries

Severity: Unknown

Description: "Release.exe" loaded module "%WINDIR%\SysWOW64\riched20.dll" at 73900000

Name: Scanning for window names

Severity: Unknown

Description: "Release.exe" searching for class "#32770"

Name: Connects to LPC ports

Severity: Unknown

Description: "Release.exe" connecting to "\\ThemeApiPort"

• -----

Name: Dropped files

Severity: Unknown

Description: "SharpSteam.dll" has type "PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly for MS Windows"
"Microsoft.Management.Infrastructure.dll" has type "PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly for MS Windows"
"System.Management.Automation.dll" has type "PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly for MS Windows"
"MaterialDesignColors.dll" has type "PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly for MS Windows"
"MaterialDesignThemes.Wpf.dll" has type "PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly for MS Windows"
"UWPHook.exe" has type "PE32 executable (GUI) Intel 80386 Mono/.Net assembly for MS Windows"
"VDFParser.dll" has type "PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly for MS Windows"
"MaterialDesignThemes.Wpf.xml" has type "XML 1.0 document ASCII text with very long lines with CRLF line terminators"
"System.Management.Automation.xml" has type "XML 1.0 document ASCII text with CRLF line terminators"
"UWPHook.exe.config" has type "XML 1.0 document ASCII text with CRLF line terminators"

• -----

Name: Touches files in the Windows directory

Severity: Unknown

Description: "Release.exe" touched file "%WINDIR%\SysWOW64\oleaccrc.dll"
"Release.exe" touched file "%LOCALAPPDATA%\Microsoft\Windows\Caches"
"Release.exe" touched file "%LOCALAPPDATA%\Microsoft\Windows\Caches\cversions.1.db"
"Release.exe" touched file "%LOCALAPPDATA%\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-8597FCF2D404}\Cache.dat"
"Release.exe" touched file "%WINDIR%\SysWOW64\en-US\user32.dll.mui"
"Release.exe" touched file "%WINDIR%\Fonts\StaticCache.dat"
"Release.exe" touched file "%WINDIR%\Globalization\Sorting\SortDefault.nls"
"Release.exe" touched file "%WINDIR%\SysWOW64\en-US\msctf.dll.mui"
"Release.exe" touched file "%LOCALAPPDATA%\Microsoft\Windows\Caches"
"Release.exe" touched file "%LOCALAPPDATA%\Microsoft\Windows\Caches\cversions.1.db"
"Release.exe" touched file "%LOCALAPPDATA%\Microsoft\Windows\Caches\{AFBF9F1A-8EE8-4C77-AF34-8597FCF2D404}\Cache.dat"

• -----

Name: Found potential URL in binary/memory

Severity: Unknown

Description: Pattern match: "http://nsis.sf.net/NSIS_Error"

Heuristic match: "<param name=force>"

If true the change to the options will happen even if the existing options are read-only.

</param>

</member>

<member name=M: System.Management.Automation.CmdletInfo.Ge"

Heuristic match: "f some parameter is specified more than once.

</summary>

<param name=seen></param>

<param name=parameter></param>

<param name=parameterName></param>

</member>

<member name=M: Syste"

Heuristic match: "returns>

</member>

<member name=P: System.Management.Automation.Help.UpdatableHelpInfo.UnresolvedUri>

<summary>

Unresolved URI

</summary>

</member>

<member name=P: System.Managemen"

Pattern match: "http://localhost/"

Pattern match: "https://docs.microsoft.com/en-us/dotnet/framework/wpf/controls/adorners-overview"

Pattern match: "https://materialdesignicons.com/"

Pattern match: "https://github.com/Templarian/MaterialDesign/blob/master/LICENSE"

Pattern match: "http://blogs.msdn.com/greg_schechter/archive/2007/10/26/enter-the-planerator-dead-simple"

Pattern match: "http://referencesource.microsoft.com/#System.Windows.Forms/winforms/Managed/System/

Pattern match: "https://material.google.com/components/snackbars-toasts.html"

Pattern match: "https://github.com/MaterialDesignInXAML/MaterialDesignInXamlToolkit/issues/1812"

• -----

Name: Opens the Kernel Security Device Driver (KsecDD) of Windows

Severity: Unknown

Description: "Release.exe" opened "\\Device\\KsecDD"

• -----

Name: Reads configuration files

Severity: Unknown

Description: "Release.exe" read file "%USERPROFILE%\\Desktop\\desktop.ini"

• -----

Name: Reads information about supported languages

Severity: Unknown

Description: "Release.exe" (Path: "HKLM\\SYSTEM\\CONTROLSET001\\CONTROL\\NLS\\LOCALE"; Key: "00000000000000000000000000000000")

• -----

Name: Installs hooks/patches the running process

Severity: Unknown

Description: "Release.exe" wrote bytes "d055917564739a750000000051c1fa749498fa74ee9cfa7475dcfc742"

"Release.exe" wrote bytes "7111f9007a3bf800ab8b02007f950200fc8c0200729602006cc805001ecdf5007d26"

• -----

Name: Drops executable files

Severity: Unknown

Description: "SharpSteam.dll" has type "PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly for x86"

"Microsoft.Management.Infrastructure.dll" has type "PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly for x86"

"System.Management.Automation.dll" has type "PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly for x86"

"MaterialDesignColors.dll" has type "PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly for x86"

"MaterialDesignThemes.Wpf.dll" has type "PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly"
"UWPHook.exe" has type "PE32 executable (GUI) Intel 80386 Mono/.Net assembly for MS Windows"
"VDFParser.dll" has type "PE32 executable (DLL) (console) Intel 80386 Mono/.Net assembly for MS Windows"

• -----

Name: Reads the active computer name

Severity: Unknown

Description: "Release.exe" (Path: "HKLM\SYSTEM\CONTROLSET001\CONTROL\COMPUTERNAME\ACT

• -----

Name: Found an instant messenger related domain

Severity: Unknown

Description: details too long to display

• -----

Name: Detected increased number of ARP broadcast requests (network device lookup)

Severity: Unknown

Description: Attempt to find devices in networks: "192.168.242.7/32, 192.168.242.8/29, 192.168.242.16/29, 1

• -----

Name: Opens file with deletion access rights

Severity: Unknown

Description: "Release.exe" opened "%TEMP%\nsy74AA.tmp" with delete access

• -----

Name: Marks file for deletion

Severity: Unknown

Description: "C:\Release.exe" marked "%TEMP%\nsy74AA.tmp" for deletion

• -----

Name: The analysis extracted a file that was identified as malicious

Severity: Unknown

Description: 1/93 Antivirus vendors marked dropped file "UWPHook.exe" as malicious (classified as "

• -----

Name: Detected a large number of ARP broadcast requests (network device lookup)

Severity: Unknown

Description: Attempt to find devices in networks: "169.254.13.158/32, 169.254.19.64/32, 169.254.29.138/32,

• -----

Name: Sample was identified as malicious by at least one Antivirus engine

Severity: Unknown

Description: 2/38 Antivirus vendors marked sample as malicious (5% detection rate)

3/71 Antivirus vendors marked sample as malicious (4% detection rate)

• -----

=====

Processes

=====

Process: Unknown