ID: 404151
Sample Name: H78gXhk1NY.dll
Cookbook: default.jbs
Time: 18:53:35
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

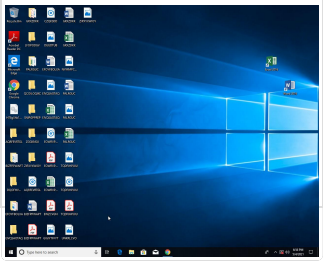
Analysis Report H78gXhk1NY.dll

Overview

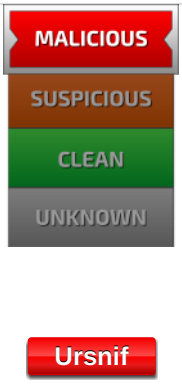
General Information

Sample Name:	H78gXhk1NY.dll
Analysis ID:	404151
MD5:	759e055bf47a9ce.
SHA1:	d6de742f6caf13d..
SHA256:	d8bcf8beebb5ab6.
Tags:	dll Gozi
Infos:	

Most interesting Screenshot:



Detection

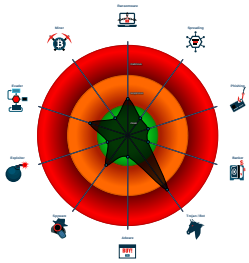


Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- Machine Learning detection for samp…
- Contains functionality to read the PEB
- Creates a DirectInput object (often fo…
- Creates a process in suspended mo…
- Detected potential crypto function
- PE file contains sections with non-s…
- Program does not show much activi…
- Uses 32bit PE files
- Uses code obfuscation techniques (…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 6272 cmdline: loaddll32.exe 'C:\Users\user\Desktop\H78gXhk1NY.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 6284 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\H78gXhk1NY.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6304 cmdline: rundll32.exe 'C:\Users\user\Desktop\H78gXhk1NY.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6292 cmdline: rundll32.exe C:\Users\user\Desktop\H78gXhk1NY.dll,DllServer MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

Threatname: Ursnif


```
{
  "RSA Public Key":
"bUd4GFcFHo0e+ZYUbkHaTKXmZ1xEyxvy7Ha6j1WAZbQ7YvMdkqTfD1vHD2y2CmFTRrLK1w5iQroYI0mUpJ4xNknlY+BmJf4xpeJRxxK0RRNeRbW5unSB2vXqxvlTgz6vNZY+9zeztuP2jXKpIm0/s+YxWnsT7eWUtQtD38NlsAPtJdp+
3rBxjzAWNKQj7wMA",
  "c2_domain": [
    "bing.com",
    "update4.microsoft.com",
    "under17.com",
    "urs-world.com"
  ],
  "botnet": "5566",
  "server": "12",
  "serpent_key": "10301029JSJUYDWG",
  "sleep_time": "10",
  "SetWaitableTimer_value": "0",
  "DGA_count": "10"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.279071628.0000000000F00000.00000004.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000003.00000002.254943759.0000000003100000.00000004.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000000.00000002.276028882.00000000008A0000.00000004.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.loaddll32.exe.8a0000.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
3.2.rundll32.exe.3100000.2.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
2.2.rundll32.exe.f00000.2.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

- AV Detection
- Compliance
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Stealing of Sensitive Information
- Remote Access Functionality

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

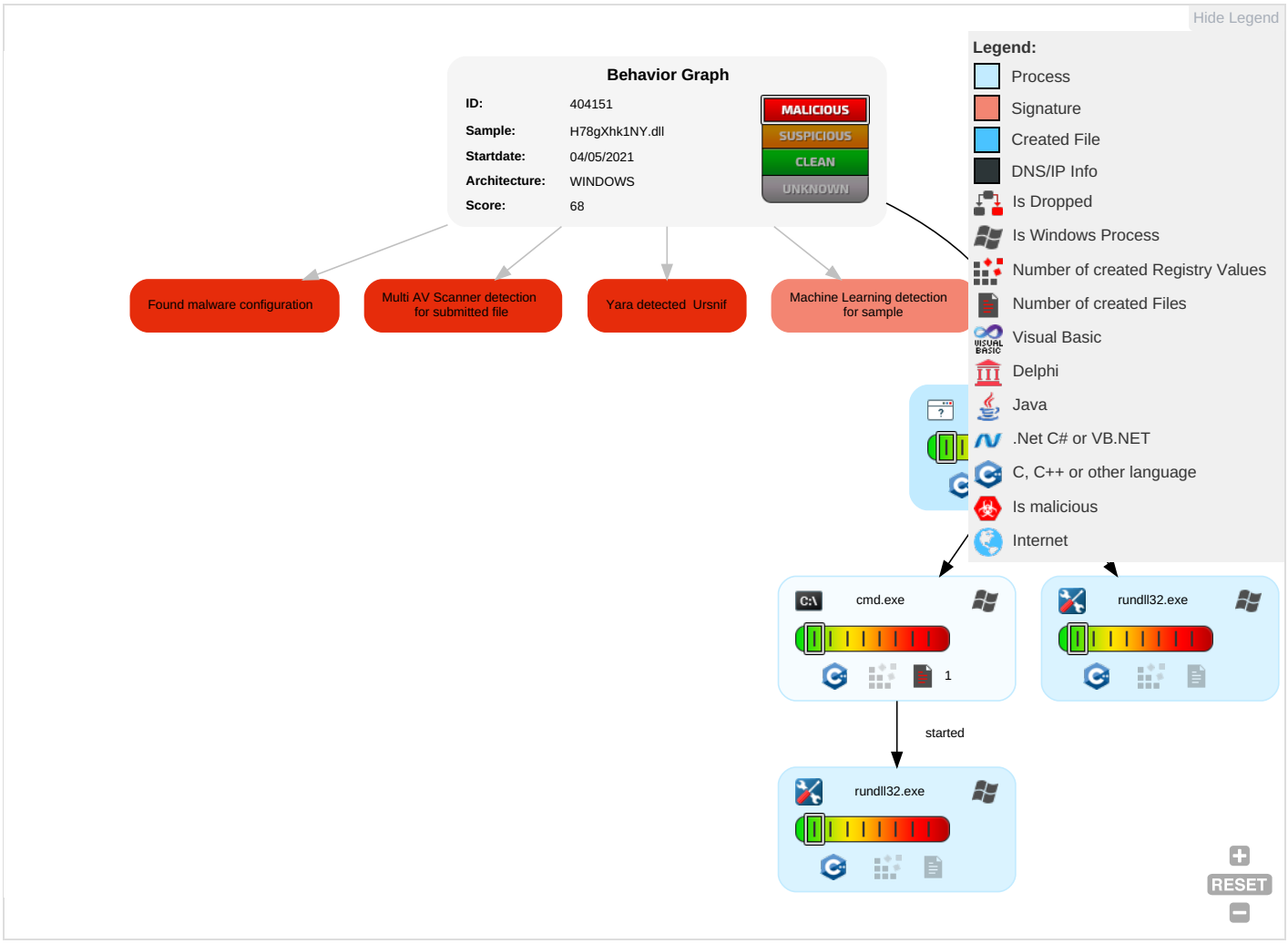
Remote Access Functionality:

Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 1	Rundll32 1	Input Capture 1	Virtualization/Sandbox Evasion 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1	LSASS Memory	System Information Discovery 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap

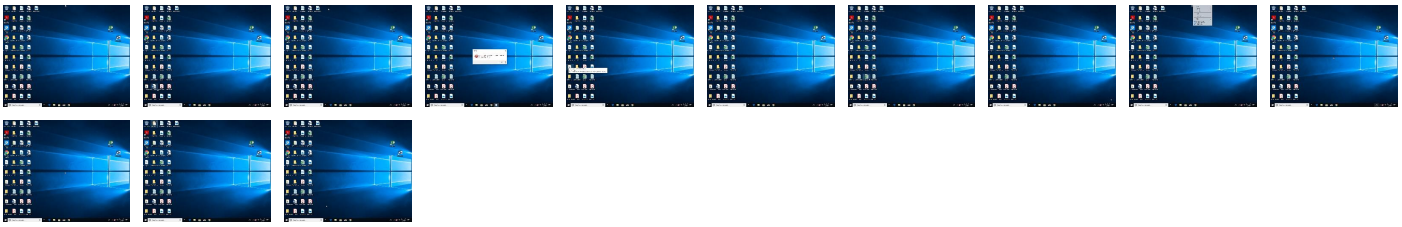
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
H78gXhk1NY.dll	74%	ReversingLabs	Win32.Trojan.Phonzy	
H78gXhk1NY.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404151
Start date:	04.05.2021
Start time:	18:53:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	H78gXhk1NY.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal68.troj.winDLL@7/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 98.4% (good quality ratio 85.8%) • Quality average: 64.1% • Quality standard deviation: 33.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • VT rate limit hit for: /opt/package/joesandbox/database/analysis/404151/sample/H78gXhk1NY.dll

Simulations

Behavior and APIs

Time	Type	Description
18:54:48	API Interceptor	2x Sleep call for process: loaddll32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.631417538663652
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	H78gXhk1NY.dll
File size:	133529
MD5:	759e055bf47a9ce1a7fce3e3276120f3
SHA1:	d6de742f6caf13d4a9aa75287d041596fbcea73a
SHA256:	d8bcf8beebb5ab690b52094df6317f023f62f044e8107508d84d06d4700fe81a
SHA512:	7bba491da19915bc7719063206b8718d061641d12d833979cc27136811b40ec1fa1ab913d3847c7068f90b2a90706bd288cb62342f62c294fc2d140f88fa1b7b
SSDEEP:	1536:tm15JsYYm3GCVS7ZicTJzRVd620ZmB9RMli0msUdqZEACW4jySTLW:eLsacThRVd6pmBPM07vYZEA4/W
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....._W...6e..6e..6e..)v..6e...w..6e.Rich.6e.....PE..L.....f`.....!.....ko.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10006f6b
Entrypoint Section:	.code
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x6066E9D0 [Fri Apr 2 09:54:24 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	3f728412058b62c418b1091768b74d7b

Entrypoint Preview

Instruction
push ebx
push esi
and dword ptr [esp], 00000000h
or dword ptr [esp], ebp
mov ebp, esp
add esp, FFFFFFF8h
push esp
mov dword ptr [esp], FFFF0000h
call 00007FCF9C8D5211h
push eax
add dword ptr [esp], 00000247h
sub dword ptr [esp], eax
push esi
mov dword ptr [esp], 00001567h
call 00007FCF9C8D4187h
push eax
or dword ptr [esp], eax
pop eax
jne 00007FCF9C8D948Bh
pushad
push 00000000h
mov dword ptr [esp], esi
xor esi, esi
xor esi, dword ptr [ebx+0041C627h]
mov eax, esi
pop esi
push ebx
add dword ptr [esp], 40h
sub dword ptr [esp], ebx
push ebp
add dword ptr [esp], 00001000h
sub dword ptr [esp], ebp
mov dword ptr [ebp-04h], 00000000h
push dword ptr [ebp-04h]
xor dword ptr [esp], eax
push 00000000h
call dword ptr [ebx+0041F05Ch]

Instruction
mov dword ptr [ebp-04h], ecx
xor ecx, dword ptr [ebp-04h]
or ecx, eax
and edi, 00000000h
xor edi, ecx
mov ecx, dword ptr [ebp-04h]
push edi
pop dword ptr [ebp-04h]
push dword ptr [ebp-04h]
pop dword ptr [ebx+0041CAEDh]
cmp ebx, 00000000h
jbe 00007FCF9C8D947Ch
push 00000000h
add dword ptr [esp], edx
push dword ptr [ebx+0041C166h]
pop edx
add edx, ebx
mov dword ptr [ebx+0041C166h], edx
pop edx
push 00000000h
add dword ptr [esp], edx
push dword ptr [ebx+0041CECAh]
pop edx
add edx, ebx
mov dword ptr [ebx+0041CECAh], edx
pop edx
push ebp
and ebp, 00000000h
or ebp, dword ptr [ebx+0041C166h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x1a000	0x64	.data
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1f0fc	0x118	.data
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1f000	0xfc	.data
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.code	0x1000	0x185f2	0x18600	False	0.670042067308	data	6.53345039933	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1a000	0x64	0x200	False	0.16796875	data	1.0662581269	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x1b000	0x1000	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0x1c000	0x20b3	0x2200	False	0.359834558824	data	2.96025706595	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.data	0x1f000	0x7b2	0x800	False	0.45703125	data	4.70767794561	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Imports

DLL	Import
user32.dll	GetActiveWindow, SetWindowsHookExA, GetLayeredWindowAttributes
kernel32.dll	GetProcAddress, LoadLibraryA, VirtualProtect, VirtualAlloc, lstrlenA, lstrcatA, lstrcmpA, GetEnvironmentVariableW
ole32.dll	OleInitialize, OleQueryCreateFromData, IIDFromString, CLIPFORMAT_UserUnmarshal, OleCreateEmbeddingHelper, HDC_UserSize
msimg32.dll	AlphaBlend, TransparentBlt
comdlg32.dll	PageSetupDlgA, PrintDlgA
oledlg.dll	OleUICanConvertOrActivateAs, OleUIChangeSourceW, OleUIConvertA
comctl32.dll	CreateStatusWindow, LBItemFromPt, DPA_Create, FlatSB_ShowScrollBar, ImageList_GetFlags
oleacc.dll	IID_IAccessible, LresultFromObject
version.dll	VerFindFileW, VerInstallFileA, VerQueryValueA, VerQueryValueW
gdiplus.dll	GdipEnumerateMetafileDestPointI, GdipCreateBitmapFromHBITMAP, GdipSetPenUnit, GdipGetImageEncoders, GdipGetPathPointsI
winspool.drv	FindNextPrinterChangeNotification, ConnectToPrinterDlg, SetPrinterDataW, GetPrinterW, DeletePrinterDataExW
shell32.dll	SHGetSpecialFolderPathA
advapi32.dll	GetKernelObjectSecurity, CryptEnumProviderTypesA, RegQueryValueExW, RegisterIdleTask

Exports

Name	Ordinal	Address
DllServer	1	0x1000447b

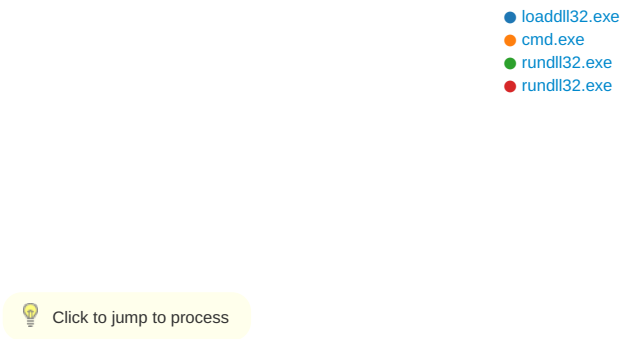
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6272 Parent PID: 5820

General

Start time:	18:54:27
Start date:	04/05/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\H78gXhk1NY.dll'
Imagebase:	0x290000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000000.00000002.276028882.00000000008A0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6284 Parent PID: 6272

General

Start time:	18:54:27
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\H78gXhk1NY.dll',#1
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6292 Parent PID: 6272

General

Start time:	18:54:28
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\H78gXhk1NY.dll,DllServer
Imagebase:	0xf40000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000002.00000002.279071628.0000000000F00000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6304 Parent PID: 6284

General

Start time:	18:54:28
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\H78gXhk1NY.dll',#1
Imagebase:	0xf40000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000003.00000002.254943759.0000000003100000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

Disassembly

Code Analysis