ID: 333659
Sample Name: ox9.dll
Cookbook: default.jbs
Time: 14:47:47
Date: 23/12/2020
Version: 31.0.0 Red Diamond

Table of Contents

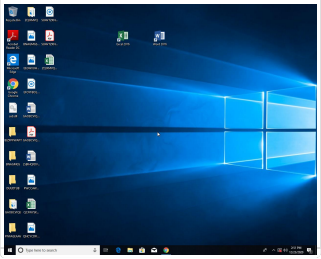
Analysis Report ox9.dll

Overview

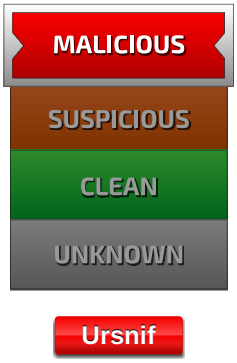
General Information

Sample Name:	ox9.dll
Analysis ID:	333659
MD5:	68cf96f4bc91628..
SHA1:	a1e1063ec8c366..
SHA256:	790191b7055085..
Tags:	dll gozi ISFB ursnif

Most interesting Screenshot:



Detection

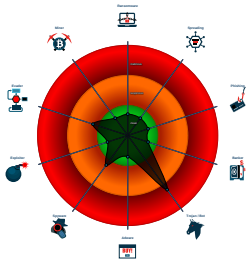


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- Writes or reads registry keys via WMI
- Writes registry values via WMI
- AV process strings found (often use…
- Antivirus or Machine Learning detec…
- Checks if Antivirus/Antispyware/Fire…
- Creates a DirectInput object (often fo…
- Monitors certain registry keys / valu…

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 6720 cmdline: loaddll32.exe 'C:\Users\user\Desktop\ox9.dll' MD5: 2D39D4DFDE8F7151723794029AB8A034)
  - rundll32.exe (PID: 7060 cmdline: rundll32.exe C:\Users\user\Desktop\ox9.dll,TestM MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 5388 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 4808 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5388 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.250008178.0000000003FF0000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.250275558.0000000003FF0000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.250091296.0000000003FF0000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000000.00000003.250163773.0000000003FF0000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000002.00000003.296233107.0000000007A50000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	

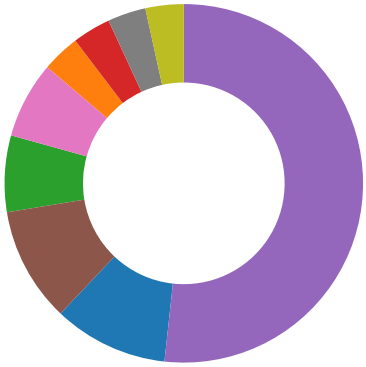
Click to see the 63 entries

Sigma Overview

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Hooking and other Techniques for Hiding and Protection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected Ursnif

E-Banking Fraud:

Yara detected Ursnif

System Summary:

Writes or reads registry keys via WMI

Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection:

Yara detected Ursnif

Stealing of Sensitive Information:

Yara detected Ursnif

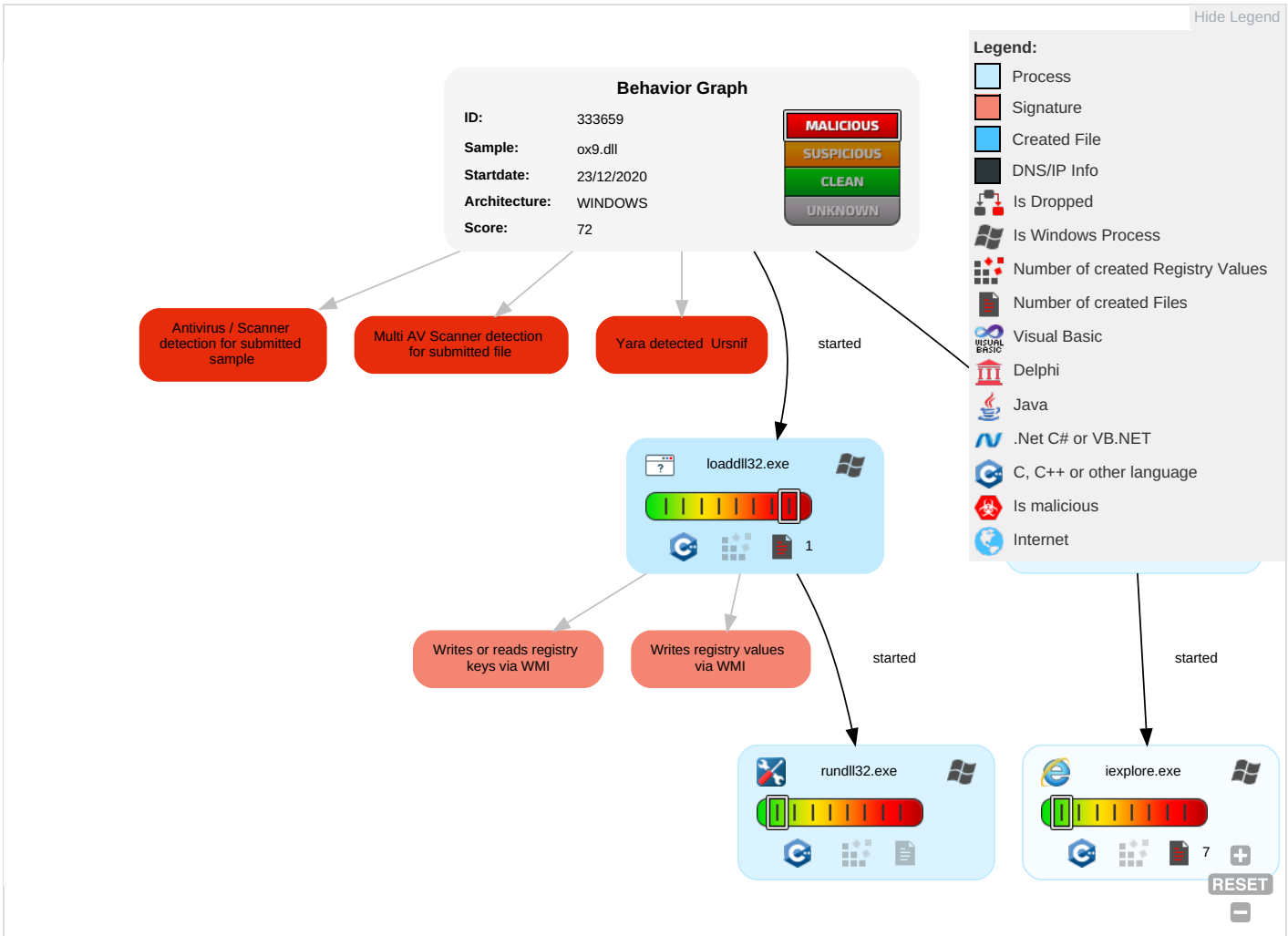
Remote Access Functionality:

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	Remot Servic Effect
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1	Masquerading 1	Input Capture 1	Query Registry 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remot Track Withou Author
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rundll32 1	LSASS Memory	Security Software Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remot Wipe D Withou Author
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Software Packing 1	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backup
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	System Information Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

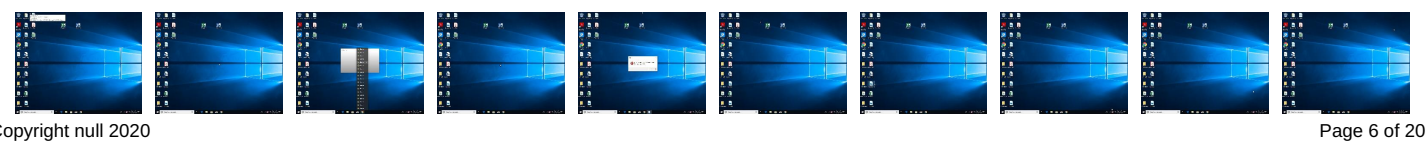
Behavior Graph



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
ox9.dll	16%	Virustotal		Browse
ox9.dll	8%	ReversingLabs	Win32.Malware.Generic	
ox9.dll	100%	Avira	HEUR/AGEN.1138179	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.d80000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.2.rundll32.exe.2e50000.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://hospader.xyz	0%	Avira URL Cloud	safe	
http://%s=%s&file://&os=%u.%u_%u_%u_x%uindex.html;	0%	Avira URL Cloud	safe	
http://https://hospader.xyz/index.htmn	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://hospader.xyz	loaddll32.exe, rundll32.exe	false	• Avira URL Cloud: safe	unknown
http://%s=%s&file://&os=%u.%u_%u_%u_x%uindex.html;	loaddll32.exe, 00000000.00000003.250008178.0000000003FF0000.00000004.00000040.sdmp, rundll32.exe, 00000002.00000003.296233107.0000000007A50000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	low
http://https://hospader.xyz/index.htmn	loaddll32.exe, 00000000.00000002.280880622.0000000003FF0000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	333659
Start date:	23.12.2020
Start time:	14:47:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ox9.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:	35
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:	mal72.troj.winDLL@6/4@0/0

EGA Information:	Failed
HDC Information:	Failed
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, ielowutil.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.147.198.201, 104.43.193.48, 52.255.188.83, 88.221.62.148, 23.210.248.85, 51.132.208.181, 92.122.213.247, 92.122.213.194, 93.184.221.240, 2.20.142.210, 2.20.142.209, 20.54.26.129, 152.199.19.161, 51.104.144.132, 52.155.217.156 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, e11290.dspg.akamaiedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, go.microsoft.com, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, ie9comview.vo.msecnd.net, wu.ec.azureedge.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, go.microsoft.com.edgekey.net, cs9.wpc.v0cdn.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:48:59	API Interceptor	1x 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

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{0B794028-4571-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	21592
Entropy (8bit):	1.7599225440225128
Encrypted:	false
SSDEEP:	48:Iw8GcprZGwpL+mG/ap8QxrGIpcb0xGvnZpvbqGoHqp9bAGo4FpmbHGWRnR:rgZTZl209WbNtbhfbDFMb1
MD5:	2A0DD7871BB42820035988B18A9746EB
SHA1:	A27BDD7AF385F225DC26AE672DE0C6807ADC956F
SHA-256:	8D8B11543070386A63861F19D134F973B1B0C926330BFC90525C073AA00F9E85
SHA-512:	EB59E25359CB7E7645D57B1C0F263689C21242E6A970705AB113C8A235278CF1434A5B8A83682507FC5D3A178EC6076C93EA79A678009BFD8E4281831DAE68ED
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0B79402A-4571-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	16984
Entropy (8bit):	1.5759540394149265
Encrypted:	false
SSDEEP:	48:Iwz7GcprSGwpaOG4pQ+GrapbS9rGQpBqGHHpcIsTGUpG:rFZaQu6wBS9Fjx2lkA
MD5:	FBF54B8D1BE04D815A000E0E53F76ECB
SHA1:	1524412DCA1FE5D930912F8AB3C60787BCD5D3EA
SHA-256:	018F241A5702721194AA944C6DECAEC034F851BF3EC78417CD536E87C87CCA9F
SHA-512:	C7447BF50292953ECBA2F2EEEB43255990C470AC40C0C07D81E8F655CADECAF223C81BD07C5873EC41546FFC9B1EE2BEF6CFE31A529C62DCADF81148694B0 6C
Malicious:	false
Reputation:	low
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Temp\~DF83D848A706E9044C.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	25657
Entropy (8bit):	0.3142129947050807
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9lRg9lRA9lTS9lTy9lSSd9lSSd9lwkz9lwkz9l2k6:kBqoxKAuvScS+353
MD5:	55205CEA1064B1A0ABEEE835CFEE2F3A

C:\Users\user\AppData\Local\Temp\~DF83D848A706E9044C.TMP	
SHA1:	A24DAE35B3EC49C0907C627040E7CC9B1E3CEB6E
SHA-256:	3F2D6ADC31770539E845423A25A75ABCD8B8DAF4EBEF83352F9961C3EE728795
SHA-512:	910A3803F2A38AFF9040B808BD5C1DE5F460AB70D31CB84130F3513D9653D05D07B21153DBD7419129B2ADE6F93FEA01BA48FD9E70D6A8D8B48A7C7CADFE82E
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

C:\Users\user\AppData\Local\Temp\~DFA1B9382F0B9E6393.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	12917
Entropy (8bit):	0.39473386569507696
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loJsF9loJM9lWJ9f4:kBqoIhn7f4
MD5:	71FA89E311D483041B776A22F23F9726
SHA1:	68227F7A9129F03AC885FEA490192AD749EBAECC
SHA-256:	7F638079099B85B4EADDCAFE8FA2EC6246E4CD150110F2D83C22D312D66AF84C
SHA-512:	56A19C804250696E7C5297DFA0CB01F7C10903B4CE0FBAFFDBD8B7D09E1BAAC754B8CF2132F910D4F4BB8D7D24137F28504DB2595F6E74CF2D275C6D8F94217
Malicious:	false
Reputation:	low
Preview:	.....*%..H..M..{y..+.0...(..... .....*%..H..M..{y..+.0...(..... ....

Static File Info

General

File type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Entropy (8bit):	6.175489362185205
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:	ox9.dll
File size:	238592
MD5:	68cf96f4bc91628e22e1526d9728990b
SHA1:	a1e1063ec8c3667e86e1afab81cb6bbea84485b3
SHA256:	790191b70550856b3e8ec108fdb82cd8d852822d6716ec865f21cfb5ad160b7c
SHA512:	ca6bb734df8bf35a2f3346ff5ad954ecc058a719b0eabf90d8c323b80ed6b8659cef5b5f51f65b149c48435bc396920549a72471b0cde1d70a02bf59dbf37b24
SSDEEP:	6144:bzLqexzY3mXAJ3WhC6aBpF7lZUPp0lts1BPz+A/OKwVdJ:bzLqmzDAEhCpTdS0Ls/UndJ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....D...%...%...%...:...%..n9...%...:...%...]X..%.....%...%...%...]O..%...]Y..%...w_..%...]Z..%..Rich.%.....

File Icon

Icon Hash:	0000000000000000

Static PE Info

General

Entrypoint:	0x10001e90
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x5BF54C59 [Wed Nov 21 12:15:21 2018 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	57e63e634cbe810da02084f9aa20228c

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
push FFFFFFFFh
push 1001DE58h
push 100136E0h
mov eax, dword ptr fs:[00000000h]
push eax
mov dword ptr fs:[00000000h], esp
add esp, FFFFFF6Ch
push ebx
push esi
push edi
mov dword ptr [ebp-18h], esp
mov dword ptr [1003A6ACh], esi
mov dword ptr [1003A6B0h], ebx
mov dword ptr [1003A6A0h], edi
mov dword ptr [1003A6A4h], ebp
push 00000000h
push 00000000h
push 00000000h
call 00007F982C78DE0Dh
cmp eax, 80100004h
jne 00007F982C77C924h
mov dword ptr [ebp-24h], 00000000h
jmp 00007F982C77C69Bh
mov eax, dword ptr [ebp-24h]
add eax, 01h
mov dword ptr [ebp-24h], eax
cmp dword ptr [ebp-24h], 00030D40h
jnl 00007F982C77C88Ah
mov dword ptr [ebp-4Ch], 00000016h
mov dword ptr [ebp-44h], 0000EA55h
mov ecx, dword ptr [ebp-4Ch]
and ecx, dword ptr [ebp-44h]
add ecx, dword ptr [ebp-44h]
mov dword ptr [ebp-54h], ecx
lea edx, dword ptr [ebp-44h]
mov dword ptr [ebp-6Ch], edx
mov eax, dword ptr [ebp-54h]
and eax, dword ptr [ebp-4Ch]
mov ecx, dword ptr [ebp-6Ch]

Instruction
add eax, dword ptr [ecx]
add eax, dword ptr [ebp-54h]
mov dword ptr [ebp-54h], eax
mov ecx, dword ptr [ebp-54h]
add ecx, 01h
mov eax, dword ptr [ebp-44h]
cdq
idiv ecx
mov edx, dword ptr [ebp-44h]
sub edx, eax
mov dword ptr [ebp-44h], edx
mov dword ptr [ebp-5Ch], 00003AE3h
lea eax, dword ptr [ebp-5Ch]
mov dword ptr [ebp-48h], eax

Rich Headers

Programming Language:	• [IMP] VS2005 build 50727 • [RES] VS2008 build 21022 • [LNK] VS2008 SP1 build 30729 • [C++] VS2008 SP1 build 30729 • [EXP] VS2008 SP1 build 30729 • [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x1e610	0x4b	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1de64	0x64	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3e000	0x960	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x3f000	0xc48	.reloc
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	0x1d000	0x158	.rdata
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
.text	0x1000	0x1b424	0x1b600	False	0.542380136986	data	6.20849155349	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x1d000	0x165b	0x1800	False	0.432454427083	data	5.17200747459	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x1f000	0x1eda0	0x1b800	False	0.616495028409	data	5.28349879083	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x3e000	0x960	0xa00	False	0.325	data	3.36470511525	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x3f000	0xe58	0x1000	False	0.655517578125	data	5.79968144285	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3e0a0	0x8a8	data	English	United States
RT_GROUP_ICON	0x3e948	0x14	data	English	United States

Imports

DLL	Import
SHLWAPI.dll	StrCmpIW, StrCmpNIW, StrStrW
WinSCard.dll	SCardListReaderGroupsA
SETUPAPI.dll	SetupGetFileCompressionInfoA
KERNEL32.dll	DeleteCriticalSection, CompareStringW, CompareStringA, GetLocaleInfoW, GetTimeZoneInformation, GetUserDefaultLCID, EnumSystemLocalesA, GetLocaleInfoA, VirtualAlloc, GetModuleHandleA, lstrcmpA, LoadLibraryA, GetCurrencyFormatW, FoldStringA, GetStringTypeExW, FormatMessageW, CreateMutexW, SetHandleCount, GetModuleHandleW, LCMapStringW, GetStdHandle, FindClose, GetCommandLineW, ExitProcess, CloseHandle, SetEvent, TerminateProcess, ResetEvent, GetCommandLineA, GetVersion, RtlUnwind, GetCurrentProcess, GetCurrentThreadId, TlsSetValue, TlsAlloc, TlsFree, SetLastError, TlsGetValue, GetLastError, GetCurrentThread, GetFileType, GetStartupInfoA, SetEnvironmentVariableA, GetModuleFileNameA, FreeEnvironmentStringsA, FreeEnvironmentStringsW, WideCharToMultiByte, GetEnvironmentStrings, GetEnvironmentStringsW, GetEnvironmentVariableA, GetVersionExA, HeapDestroy, HeapCreate, VirtualFree, HeapFree, WriteFile, InitializeCriticalSection, EnterCriticalSection, LeaveCriticalSection, FatalAppExitA, HeapAlloc, UnhandledExceptionFilter, GetCPInfo, GetACP, GetOEMCP, HeapReAlloc, IsBadWritePtr, GetProcAddress, MultiByteToWideChar, LCMapStringA, GetStringTypeA, GetStringTypeW, InterlockedDecrement, InterlockedIncrement, Sleep, IsValidLocale, IsValidCodePage

Exports

Name	Ordinal	Address
TestM	1	0x100021d0

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

UDP Packets

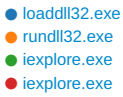
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 23, 2020 14:48:28.404864073 CET	53	65110	8.8.8.8	192.168.2.3
Dec 23, 2020 14:48:29.121452093 CET	58361	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:48:29.169548035 CET	53	58361	8.8.8.8	192.168.2.3
Dec 23, 2020 14:48:30.114955902 CET	63492	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:48:30.165930986 CET	53	63492	8.8.8.8	192.168.2.3
Dec 23, 2020 14:48:30.917431116 CET	60831	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:48:30.976716042 CET	53	60831	8.8.8.8	192.168.2.3
Dec 23, 2020 14:48:31.838191032 CET	60100	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:48:31.888993979 CET	53	60100	8.8.8.8	192.168.2.3
Dec 23, 2020 14:48:32.868786097 CET	53195	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:48:32.916671038 CET	53	53195	8.8.8.8	192.168.2.3
Dec 23, 2020 14:48:33.687350988 CET	50141	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:48:33.738328934 CET	53	50141	8.8.8.8	192.168.2.3
Dec 23, 2020 14:48:34.657922029 CET	53023	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:48:34.714694023 CET	53	53023	8.8.8.8	192.168.2.3
Dec 23, 2020 14:48:35.602807045 CET	49563	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:48:35.650652885 CET	53	49563	8.8.8.8	192.168.2.3
Dec 23, 2020 14:48:36.414601088 CET	51352	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:48:36.462564945 CET	53	51352	8.8.8.8	192.168.2.3
Dec 23, 2020 14:48:37.497421026 CET	59349	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:48:37.545444012 CET	53	59349	8.8.8.8	192.168.2.3
Dec 23, 2020 14:48:38.651247025 CET	57084	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:48:38.699233055 CET	53	57084	8.8.8.8	192.168.2.3
Dec 23, 2020 14:49:01.135190010 CET	58823	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:49:01.193116903 CET	53	58823	8.8.8.8	192.168.2.3
Dec 23, 2020 14:49:04.365133047 CET	57568	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:49:04.423106909 CET	53	57568	8.8.8.8	192.168.2.3
Dec 23, 2020 14:49:09.646558046 CET	50540	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:49:09.698144913 CET	53	50540	8.8.8.8	192.168.2.3
Dec 23, 2020 14:49:19.025155067 CET	54366	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Dec 23, 2020 14:49:19.084080935 CET	53	54366	8.8.8.8	192.168.2.3
Dec 23, 2020 14:49:19.549309015 CET	53034	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:49:19.597399950 CET	53	53034	8.8.8.8	192.168.2.3
Dec 23, 2020 14:49:20.749377012 CET	57762	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:49:20.807344913 CET	53	57762	8.8.8.8	192.168.2.3
Dec 23, 2020 14:49:29.838464022 CET	55435	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:49:29.906335115 CET	53	55435	8.8.8.8	192.168.2.3
Dec 23, 2020 14:49:31.084635973 CET	50713	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:49:31.144064903 CET	53	50713	8.8.8.8	192.168.2.3
Dec 23, 2020 14:49:32.016844988 CET	56132	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:49:32.075923920 CET	53	56132	8.8.8.8	192.168.2.3
Dec 23, 2020 14:49:32.082050085 CET	50713	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:49:32.132853031 CET	53	50713	8.8.8.8	192.168.2.3
Dec 23, 2020 14:49:33.004226923 CET	56132	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:49:33.063802958 CET	53	56132	8.8.8.8	192.168.2.3
Dec 23, 2020 14:49:33.084059954 CET	50713	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:49:33.134962082 CET	53	50713	8.8.8.8	192.168.2.3
Dec 23, 2020 14:49:34.019151926 CET	56132	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:49:34.078262091 CET	53	56132	8.8.8.8	192.168.2.3
Dec 23, 2020 14:49:35.097476006 CET	50713	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:49:35.148546934 CET	53	50713	8.8.8.8	192.168.2.3
Dec 23, 2020 14:49:36.020211935 CET	56132	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:49:36.079642057 CET	53	56132	8.8.8.8	192.168.2.3
Dec 23, 2020 14:49:39.114053965 CET	50713	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:49:39.173211098 CET	53	50713	8.8.8.8	192.168.2.3
Dec 23, 2020 14:49:40.035252094 CET	56132	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:49:40.094772100 CET	53	56132	8.8.8.8	192.168.2.3
Dec 23, 2020 14:49:43.792296886 CET	58987	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:49:43.840272903 CET	53	58987	8.8.8.8	192.168.2.3
Dec 23, 2020 14:49:47.061974049 CET	56579	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:49:47.120804071 CET	53	56579	8.8.8.8	192.168.2.3
Dec 23, 2020 14:50:18.945934057 CET	60633	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:50:18.994031906 CET	53	60633	8.8.8.8	192.168.2.3
Dec 23, 2020 14:50:20.128823996 CET	61292	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:50:20.193759918 CET	53	61292	8.8.8.8	192.168.2.3
Dec 23, 2020 14:51:21.278589010 CET	63619	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:51:21.379978895 CET	53	63619	8.8.8.8	192.168.2.3
Dec 23, 2020 14:51:22.089343071 CET	64938	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:51:22.147835970 CET	53	64938	8.8.8.8	192.168.2.3
Dec 23, 2020 14:51:23.039227009 CET	61946	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:51:23.098453045 CET	53	61946	8.8.8.8	192.168.2.3
Dec 23, 2020 14:51:23.565007925 CET	64910	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:51:23.621637106 CET	53	64910	8.8.8.8	192.168.2.3
Dec 23, 2020 14:51:24.299309969 CET	52123	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:51:24.358383894 CET	53	52123	8.8.8.8	192.168.2.3
Dec 23, 2020 14:51:25.118931055 CET	56130	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:51:25.178277016 CET	53	56130	8.8.8.8	192.168.2.3
Dec 23, 2020 14:51:25.979372025 CET	56338	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:51:26.035844088 CET	53	56338	8.8.8.8	192.168.2.3
Dec 23, 2020 14:51:27.075659037 CET	59420	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:51:27.132230997 CET	53	59420	8.8.8.8	192.168.2.3
Dec 23, 2020 14:51:27.853101969 CET	58784	53	192.168.2.3	8.8.8.8
Dec 23, 2020 14:51:27.909490108 CET	53	58784	8.8.8.8	192.168.2.3

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6720 Parent PID: 5604

General

Start time:	14:48:33
Start date:	23/12/2020
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\ox9.dll'
Imagebase:	0xe40000
File size:	120832 bytes
MD5 hash:	2D39D4DFDE8F7151723794029AB8A034
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.250008178.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.250275558.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.250091296.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.250163773.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.250403224.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.250414469.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.250128659.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.249239279.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.249450946.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.250225592.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.249165583.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security

	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.249815212.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.250352691.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.249699894.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.250196127.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000002.280880622.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.249008055.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.249760942.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.249961877.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.249091122.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.249914112.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.250330837.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.249866308.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.249311910.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.250252374.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.250050973.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.250389471.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.249641923.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.249581332.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.249519808.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.250297414.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.250373001.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000000.00000003.249379729.0000000003FF0000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 7060 Parent PID: 6720

General

Start time:	14:48:55
Start date:	23/12/2020
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true

Commandline:	rundll32.exe C:\Users\user\Desktop\ox9.dll,TestM
Imagebase:	0x890000
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, Description: Yara detected Ursnif, Source: 00000002.00000003.296233107.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.295957836.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.297126618.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.296545097.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.296348413.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.296753573.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.296489989.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.295524758.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.297234143.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.296045389.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.296622384.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.297082506.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.295889279.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.296699564.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.296426386.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.297207378.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.297019075.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.296884566.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.295819437.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.295082373.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.295298623.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.296969698.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.297189469.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.295195825.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.297165923.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.294971951.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.297221124.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security

	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.295621288.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.296835384.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.296127430.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000002.325725775.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.295729131.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000002.00000003.295414283.0000000007A50000.00000004.00000040.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 5388 Parent PID: 792

General

Start time:	14:48:59
Start date:	23/12/2020
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff60e970000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
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

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 4808 Parent PID: 5388

General

Start time:	14:49:00
Start date:	23/12/2020
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:5388 CREDAT:17410 /prefetch:2
Imagebase:	0x13c0000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis