ID: 356525
Sample Name: uxtheme.bin
Cookbook: default.jbs
Time: 09:30:33
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

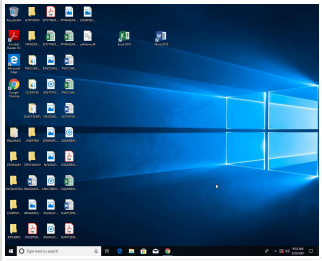
Analysis Report uxtheme.bin

Overview

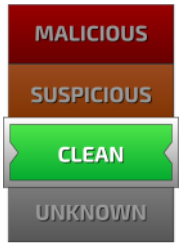
General Information

Sample Name:	uxtheme.bin (renamed file extension from bin to dll)
Analysis ID:	356525
MD5:	ceb5fbc654f39a7..
SHA1:	e1f19599ea001f2..
SHA256:	c6cfb034a82e6e4..
Tags:	OOOFobos

Most interesting Screenshot:



Detection

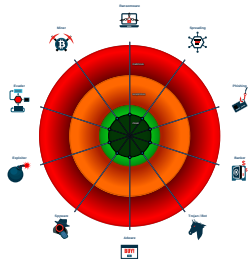


Score:	2
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- PE file contains an invalid checksum
- PE file contains more sections than …
- PE file contains sections with non-s…
- Program does not show much activi…

Classification



Startup

- **System is w10x64**
- loaddll64.exe (PID: 3040 cmdline: loaddll64.exe 'C:\Users\user\Desktop\uxtheme.dll' MD5: 40E30D559A47CDA935973FA18C34ABA6)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

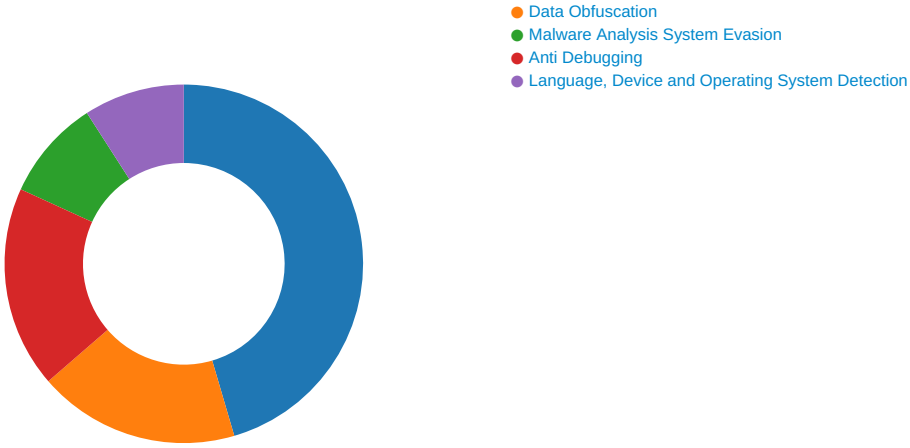
No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview

- System Summary



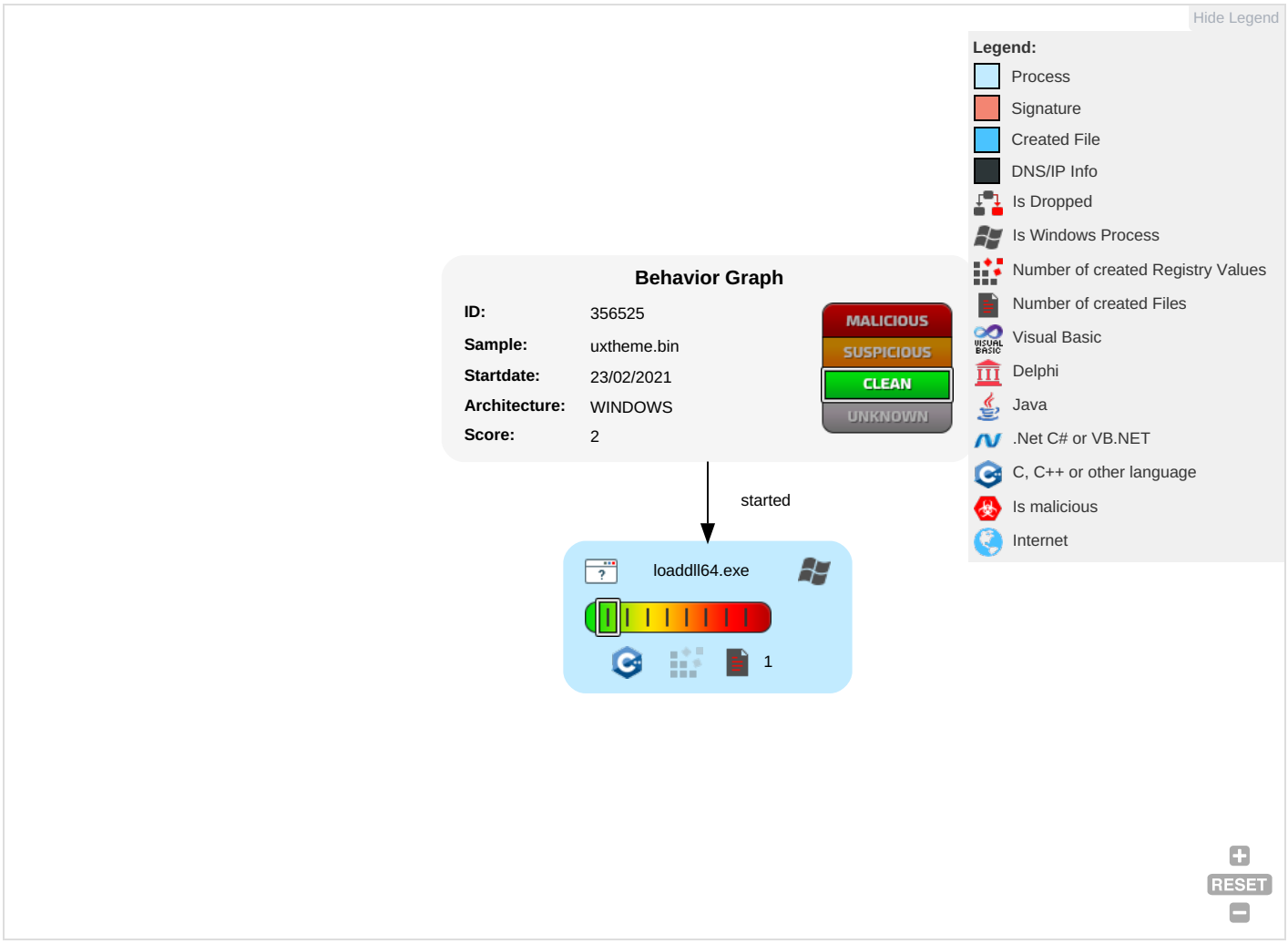
Click to jump to signature section

There are no malicious signatures, click here to show all signatures.

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Direct Volume Access	OS Credential Dumping	System Time Discovery 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	System Information Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

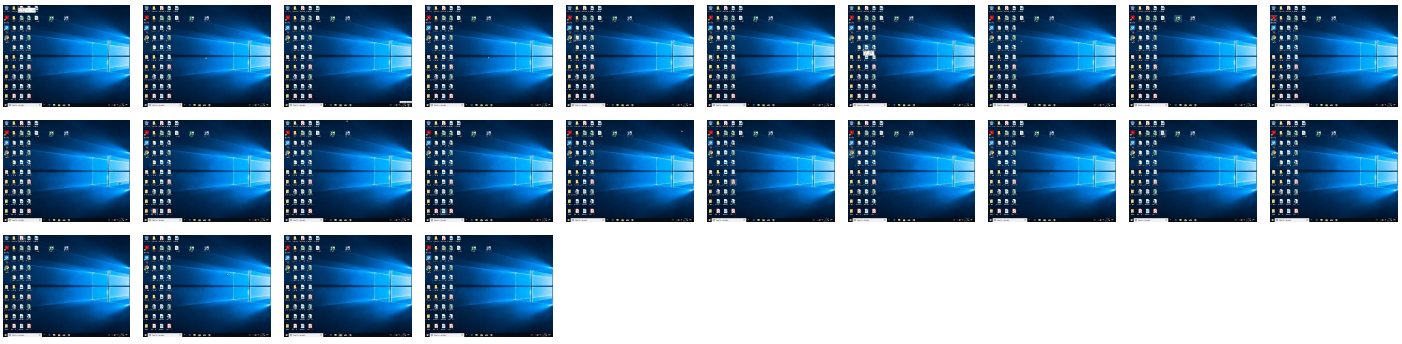
Behavior Graph



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
uxtheme.dll	1%	Virustotal		Browse
uxtheme.dll	2%	ReversingLabs		

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:	31.0.0 Emerald
Analysis ID:	356525
Start date:	23.02.2021
Start time:	09:30:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	uxtheme.bin (renamed file extension from bin to 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:	25
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:	CLEAN
Classification:	clean2.winDLL@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 88.9% (good quality ratio 64.4%) • Quality average: 61.3% • Quality standard deviation: 41.5%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe

Simulations

Behavior and APIs

No simulations

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) x86-64, for MS Windows
Entropy (8bit):	4.76233421620799
TrID:	• Win64 Dynamic Link Library (generic) (102004/3) 86.41% • Win64 Executable (generic) (12005/4) 10.17% • Generic Win/DOS Executable (2004/3) 1.70% • DOS Executable Generic (2002/1) 1.70% • VXD Driver (31/22) 0.03%
File name:	uxtheme.dll
File size:	47980
MD5:	ceb5fbc654f39a7b9ea9c62eeecdfa19
SHA1:	e1f19599ea001f2f7ee8d336edb7b114e0ef437e
SHA256:	c6cfb034a82e6e4fa018dd063e7e91e47f4034248b6ad90b62219e3c367a3673
SHA512:	2c8753cb76cb8b359f4f8f3bfc9c1c181270c65335b77b00a5b31753493bed5db446290ea88f1bad46ffb70f6f6ca8b5302a49364142c0f33155489625998962
SSDEEP:	384:9wbmN5sAYR04+ePkZz3oKxpfEqTIY5Fv4iBKflxMrdFPV7PxbTEcAAPrFMQlYjL:9gAs/cZz3DfEqTIYv4gKNwFPxPe5
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...&..].h.....& .....6.....0.....d.....@..... ....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General	
Entrypoint:	0x64881330
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x64880000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE, LINE_NUMS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5DECAA26 [Sun Dec 8 07:45:42 2019 UTC]
TLS Callbacks:	0x648816f0
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:	a55cf28123aec4893f9cb49d5e6312dd

Entrypoint Preview

Instruction
dec eax
sub esp, 48h
dec eax
mov eax, dword ptr [00002F55h]
mov dword ptr [eax], 00000000h
cmp edx, 01h
je 00007FE8B0B2905Ch
dec eax
add esp, 48h
jmp 00007FE8B0B28F06h
nop
dec esp
mov dword ptr [esp+38h], eax
mov dword ptr [esp+34h], edx
dec eax
mov dword ptr [esp+28h], ecx
call 00007FE8B0B291D2h
call 00007FE8B0B29ABDh
dec esp
mov eax, dword ptr [esp+38h]
mov edx, dword ptr [esp+34h]
dec eax
mov ecx, dword ptr [esp+28h]
dec eax
add esp, 48h
jmp 00007FE8B0B28ED6h
nop
dec eax
mov edx, ecx
dec eax
lea ecx, dword ptr [00005C76h]
jmp 00007FE8B0B2A4A6h
nop
dec eax
lea ecx, dword ptr [00000009h]
jmp 00007FE8B0B29039h
nop dword ptr [eax+00h]
ret
nop
nop
nop
nop
nop

Instruction
nop
nop
nop
nop
nop
nop
nop
nop
nop
nop
push ebp
dec eax
mov ebp, esp
dec eax
sub esp, 20h
mov edx, 00000001h
dec eax
lea ecx, dword ptr [00002C3Ch]
dec eax
mov eax, dword ptr [00007E69h]
call eax
mov ecx, 00000000h
dec eax
mov eax, dword ptr [00007DB3h]
call eax
nop
push ebp
dec eax
mov ebp, esp
dec eax
sub esp, 20h
dec eax
mov dword ptr [ebp+10h], ecx
mov dword ptr [ebp+18h], edx
dec esp
mov dword ptr [ebp+20h], eax
cmp dword ptr [ebp+18h], 01h
jne 00007FE8B0B29057h
call 00007FE8B0B3900Bh

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x8000	0x52	.edata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x9000	0x5f0	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x5000	0x228	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc000	0x64	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x4060	0x28	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x917c	0x140	.idata
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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1ac8	0x1c00	False	0.570033482143	data	5.86144287266	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_CNT_CODE, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
.data	0x3000	0x80	0x200	False	0.115234375	data	0.749836229165	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
.rdata	0x4000	0x2e0	0x400	False	0.337890625	data	3.0125063975	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
.pdata	0x5000	0x228	0x400	False	0.318359375	data	2.38404815471	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
.xdata	0x6000	0x1ac	0x200	False	0.36328125	data	3.42645904001	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.bss	0x7000	0x920	0x0	False	0	empty	0.0	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
.edata	0x8000	0x52	0x200	False	0.1484375	data	0.888027638897	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
.idata	0x9000	0x5f0	0x600	False	0.384765625	data	4.0283471072	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
.CRT	0xa000	0x58	0x200	False	0.056640625	data	0.201539378135	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
.tls	0xb000	0x10	0x200	False	0.02734375	data	0.0	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
.reloc	0xc000	0x64	0x200	False	0.19921875	data	1.06801655505	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_2BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_512BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
/4	0xd000	0x50	0x200	False	0.072265625	data	0.23653878451	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
/19	0xe000	0x1f08	0x2000	False	0.459350585938	data	5.82440214057	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
/31	0x10000	0x149	0x200	False	0.375	data	3.28729179067	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
/45	0x11000	0x222	0x400	False	0.2900390625	data	3.2353162452	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
/57	0x12000	0x48	0x200	False	0.12109375	data	0.707951245148	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_2048BYTES, IMAGE_SCN_ALIGN_32BYTES, IMAGE_SCN_ALIGN_8BYTES, IMAGE_SCN_ALIGN_8192BYTES, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ
/70	0x13000	0x9b	0x200	False	0.259765625	data	2.32078044454	IMAGE_SCN_ALIGN_MASK, IMAGE_SCN_ALIGN_256BYTES, IMAGE_SCN_ALIGN_16BYTES, IMAGE_SCN_ALIGN_64BYTES, IMAGE_SCN_ALIGN_1BYTES, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_ALIGN_1024BYTES, IMAGE_SCN_ALIGN_4BYTES, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_ALIGN_4096BYTES, IMAGE_SCN_MEM_READ

Imports

DLL	Import
KERNEL32.dll	DeleteCriticalSection, EnterCriticalSection, ExitProcess, GetCurrentProcess, GetCurrentProcessId, GetCurrentThreadId, GetLastError, GetSystemTimeAsFileTime, GetTickCount, InitializeCriticalSection, LeaveCriticalSection, QueryPerformanceCounter, RtlAddFunctionTable, RtlCaptureContext, RtlLookupFunctionEntry, RtlVirtualUnwind, SetUnhandledExceptionFilter, Sleep, TerminateProcess, TlsGetValue, UnhandledExceptionFilter, VirtualProtect, VirtualQuery, WinExec

DLL	Import
msvcrt.dll	__iob_func, _amsg_exit, _initterm, _lock, _unlock, abort, calloc, free, fwrite, realloc, signal, strlen, strncmp, vfprintf

Exports

Name	Ordinal	Address
GetCurrentThemeName	1	0x648813b0

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: loaddll64.exe PID: 3040 Parent PID: 5692

General

Start time:	09:31:24
Start date:	23/02/2021
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe 'C:\Users\user\Desktop\uxtheme.dll'
Imagebase:	0x7ff73f1f0000
File size:	147456 bytes
MD5 hash:	40E30D559A47CDA935973FA18C34ABA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis