ID: 337718
Sample Name:
15790_Invoice_confirmation.exe
Cookbook: default.jbs
Time: 18:25:13
Date: 09/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

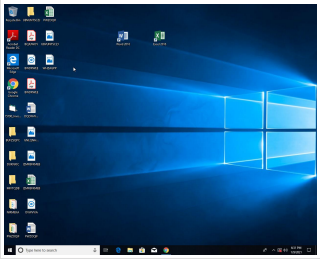
Analysis Report 15790_Invoice_confirmation.exe

Overview

General Information

Sample Name:	15790_Invoice_confirmation.exe
Analysis ID:	337718
MD5:	9090a8a7764697..
SHA1:	bfd3e70ce4230d0.
SHA256:	c4e0e2bc76880e..
Tags:	exe GuLoader

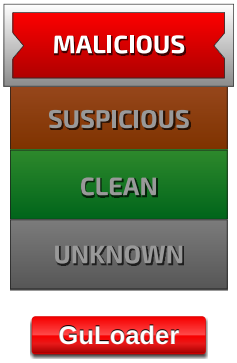
Most interesting Screenshot:



Errors

Sigma syntax error: Has an empty selector, Rule: Abusing Azure Browser SSO

Detection

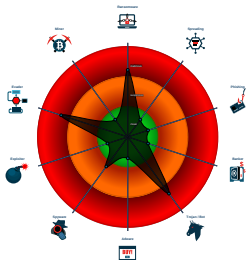


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Potential malicious icon found
- Yara detected GuLoader
- Detected RDTSC dummy instruction…
- Executable has a suspicious name (…
- Initial sample is a PE file and has a …
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Yara detected VB6 Downloader Gen…
- Abnormal high CPU Usage
- Contains functionality for execution …
- Contains functionality to read the PEB
- Creates a DirectInput object (often fo…
- Detected potential crypto function
- PE file contains strange resources
- Sample file is different than original …

Classification



Startup

- **System is w10x64**
- 15790_Invoice_confirmation.exe (PID: 5668 cmdline: 'C:\Users\user\Desktop\15790_Invoice_confirmation.exe' MD5: 9090A8A77646971374CEA3112AA3BEED)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

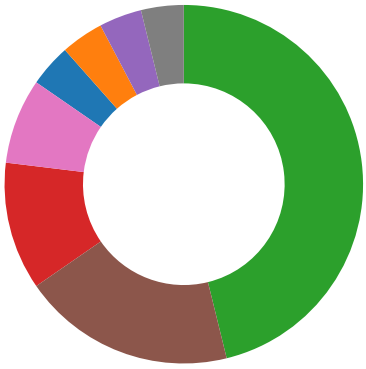
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: 15790_Invoice_confirmation.exe PID: 5668	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: 15790_Invoice_confirmation.exe PID: 5668	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- Compliance
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion

Click to jump to signature section

System Summary:

Potential malicious icon found

Executable has a suspicious name (potential lure to open the executable)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

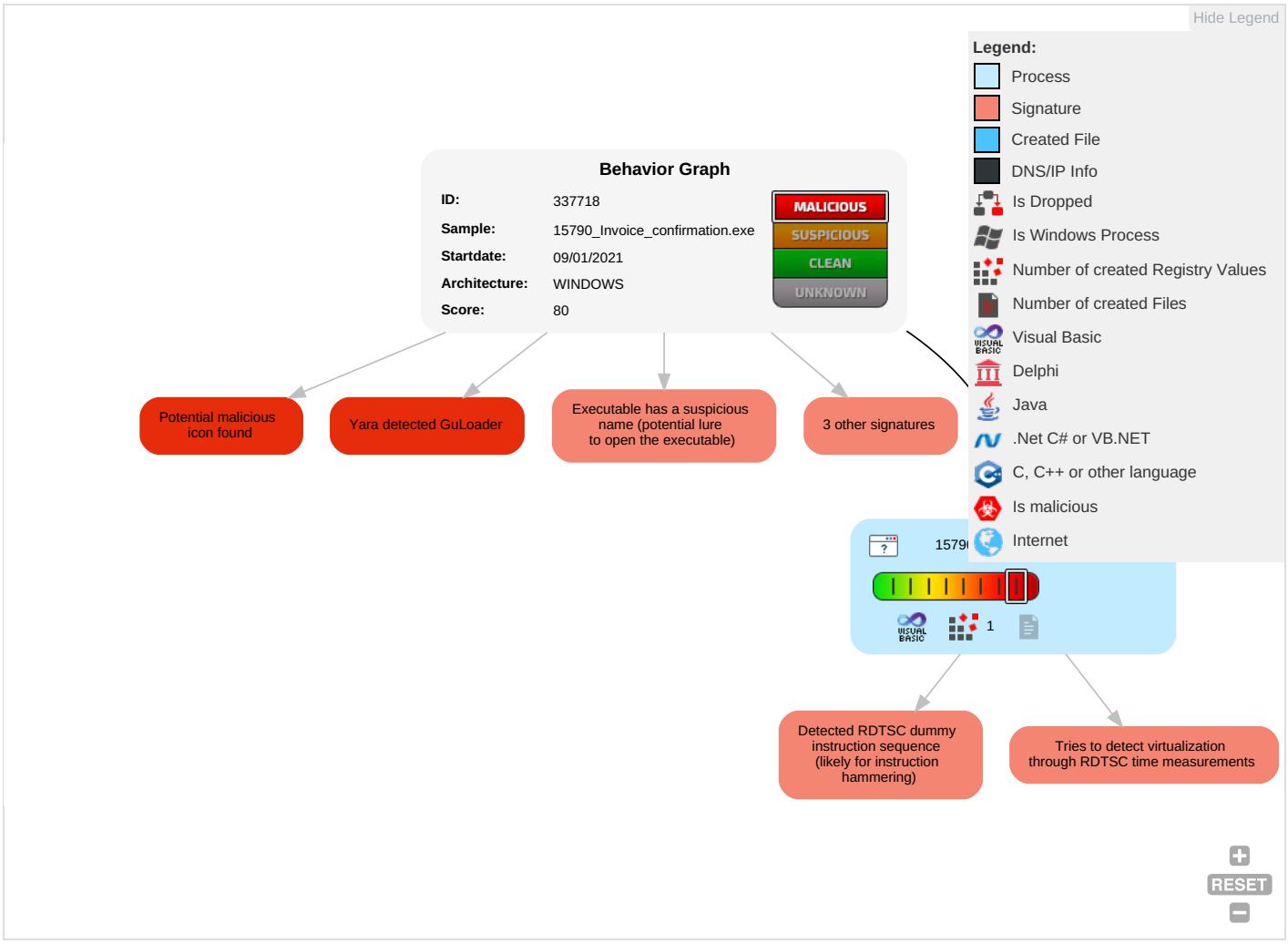
Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

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
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Process Injection 1	Input Capture 1	Security Software Discovery 3 1 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Obfuscated Files or Information 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	System Information Discovery 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups

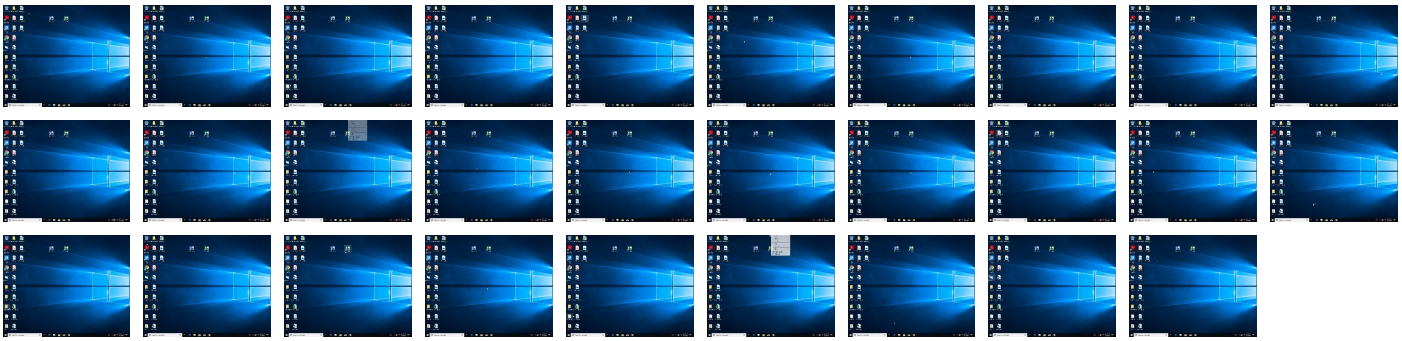
Behavior Graph



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

No Antivirus matches

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 Red Diamond
Analysis ID:	337718
Start date:	09.01.2021
Start time:	18:25:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	15790_Invoice_confirmation.exe
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:	21
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:	mal80.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 33.7% (good quality ratio 20%) • Quality average: 29.4% • Quality standard deviation: 29.9%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, MusNotifyIcon.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
Errors:	• Sigma syntax error: Has an empty selector, Rule: Abusing Azure Browser SSO

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 (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.6192694969709684
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	15790_Invoice_confirmation.exe
File size:	94208
MD5:	9090a8a77646971374cea3112aa3beed
SHA1:	bfd3e70ce4230d04e97a9ed394bfabf287a5bfe7
SHA256:	c4e0e2bc76880e6144bbc96ad64e55bd10f6f66805ccfd5a86c36182201372eb
SHA512:	297232d4bb6e1fb1f1b31b1ce499e7d25d4eb400e7a694 1d279f48736ebba8b57a53dbde9248f21dd8f75af3f004a6 2969cc1ed3d4f6e41956aebba15820917
SSDEEP:	1536:Z2euZu4vhLo8gE961bsy+wHVVQ5C6eUwoJXxLC:7nKo8+bnYwoJI
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....6...W...W...W...K...W...u...W...q...W..Rich.W.....PE..L...C._.....@...0.....P....@

File Icon

	
Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401600
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x5FF99543 [Sat Jan 9 11:36:35 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:	690ed9eee3aab240a93936dee17050b4

Entrypoint Preview

Instruction
push 00401C6Ch
call 00007F9CE891F715h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
cmp byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
mov ebp, 2B6E7B28h
or byte ptr [edi+574CAF4Dh], FFFFFFE4h
shr ecx, cl
add al, dh
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
insd
outsd
jnc 00007F9CE891F78Eh
insd
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
dec esp
xor dword ptr [eax], eax
sbb dword ptr [ebp+ebp*4+558C22ABh], esp
arpl word ptr [ecx+eax*4+2Ch], cx
cwde
add dword ptr [ecx+2898F8DDh], esp
jnl 00007F9CE891F6F1h
daa
imul ebx, dword ptr [ebp-7Ah], 4Ah
mov dword ptr [ebx+60067F19h], edx
xchg eax, ebx

Instruction
push 33AD4F3Ah
cdq
iretw
adc dword ptr [edi+00AA000Ch], esi
pushad
rcl dword ptr [ebx+00000000h], cl
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
cld
add eax, dword ptr [eax]
add byte ptr [edx+00h], al
add byte ptr [eax], al
add byte ptr [esi], al
add byte ptr [ebx+6Ch], cl
popad
jo 00007F9CE891F794h
xor eax, dword ptr [eax]
or eax, 4D000701h
imul esp, dword ptr [edi+72h], 0032656Eh
sbb dword ptr [ecx], eax
add byte ptr [edx+00h], al
and al, byte ptr [00000724h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x13cd4	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x17000	0x894	.rsrc
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	0x238	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x184	.text
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	0x132b8	0x14000	False	0.400012207031	data	6.06818823886	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x15000	0x14b0	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x17000	0x894	0x1000	False	0.16015625	data	1.85318303523	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x17764	0x130	data		
RT_ICON	0x1747c	0x2e8	data		
RT_ICON	0x17354	0x128	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x17324	0x30	data		
RT_VERSION	0x17150	0x1d4	data	Chinese	Taiwan

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaHresultCheck, __vbaVarMove, __vbaFreeVar, __vbaLenBstr, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaStrCat, __vbaHresultCheckObj, __vbaLenBstrB, _adj_fdiv_m32, __vbaAryDestruct, __vbaLateMemSt, __vbaExitProc, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, __vbaVarTstEq, __vbaAryConstruct2, __vbaR4Str, __vbaObjVar, DllFunctionCall, _adj_fpatan, __vbaLateIdCallLd, __vbaRedim, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, __vbaStrVarVal, __vbaDateVar, _CIlog, __vbaFileOpen, __vbaNew2, __vbaInStr, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaI4Var, __vbaVarDup, __vbaLateMemCallLd, _CIatan, __vbaStrMove, __vbaUI1Str, _allmul, _CItan, __vbaFPInt, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0404 0x04b0
ProductVersion	1.00
InternalName	klist
FileVersion	1.00
OriginalFilename	klist.exe
ProductName	Logaritm

Possible Origin

Language of compilation system	Country where language is spoken	Map
Chinese	Taiwan	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: 15790_Invoice_confirmation.exe PID: 5668 Parent PID: 5892

General

Start time:	18:26:00
Start date:	09/01/2021
Path:	C:\Users\user\Desktop\15790_Invoice_confirmation.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\15790_Invoice_confirmation.exe'
Imagebase:	0x400000
File size:	94208 bytes
MD5 hash:	9090A8A77646971374CEA3112AA3BEED
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\VB and VBA Program Settings	success or wait	1	660E2872	RegCreateKeyW
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\unwall	success or wait	1	660E2872	RegCreateKeyW
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\unwall\Oculus	success or wait	1	660E2872	RegCreateKeyW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\unwall\Oculus	Karseklippet	unicode	prenominate	success or wait	1	660E2183	RegSetValueExW

Disassembly

Code Analysis