ID: 430072
Sample Name: soft.dll
Cookbook: default.jbs
Time: 10:11:59
Date: 06/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

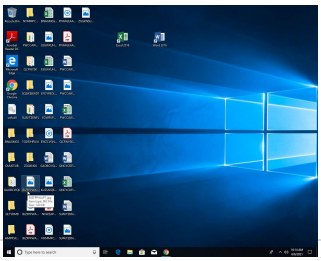
Analysis Report soft.dll

Overview

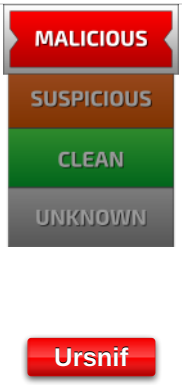
General Information

Sample Name:	soft.dll
Analysis ID:	430072
MD5:	627c8a536ed728..
SHA1:	03f6ab6dd415ca9.
SHA256:	10ab600004b40a..
Infos:	

Most interesting Screenshot:



Detection

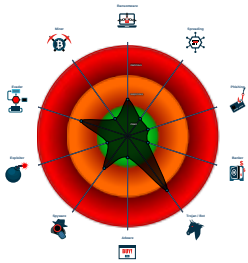


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- Contains functionality to call native f…
- Contains functionality to check if a d…
- Contains functionality to dynamically…
- Contains functionality to query CPU …
- Contains functionality to query locale…
- Contains functionality to read the PEB
- Contains functionality which may be…
- Creates a process in suspended mo…
- Detected potential crypto function
- Found large amount of non-executed…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 4760 cmdline: loaddll32.exe 'C:\Users\user\Desktop\soft.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 2292 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\soft.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5348 cmdline: rundll32.exe 'C:\Users\user\Desktop\soft.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5328 cmdline: rundll32.exe C:\Users\user\Desktop\soft.dll,Bottomget MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5908 cmdline: rundll32.exe C:\Users\user\Desktop\soft.dll,Groupshop MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 5912 cmdline: rundll32.exe C:\Users\user\Desktop\soft.dll,Stoodbroad MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

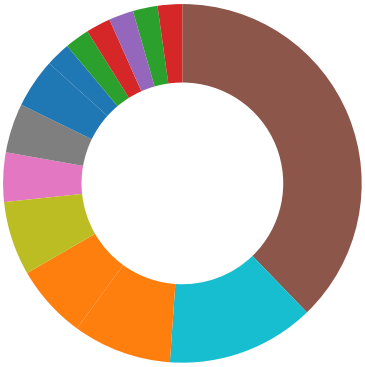
Yara Overview

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Compliance
- Spreading



- 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
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

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:

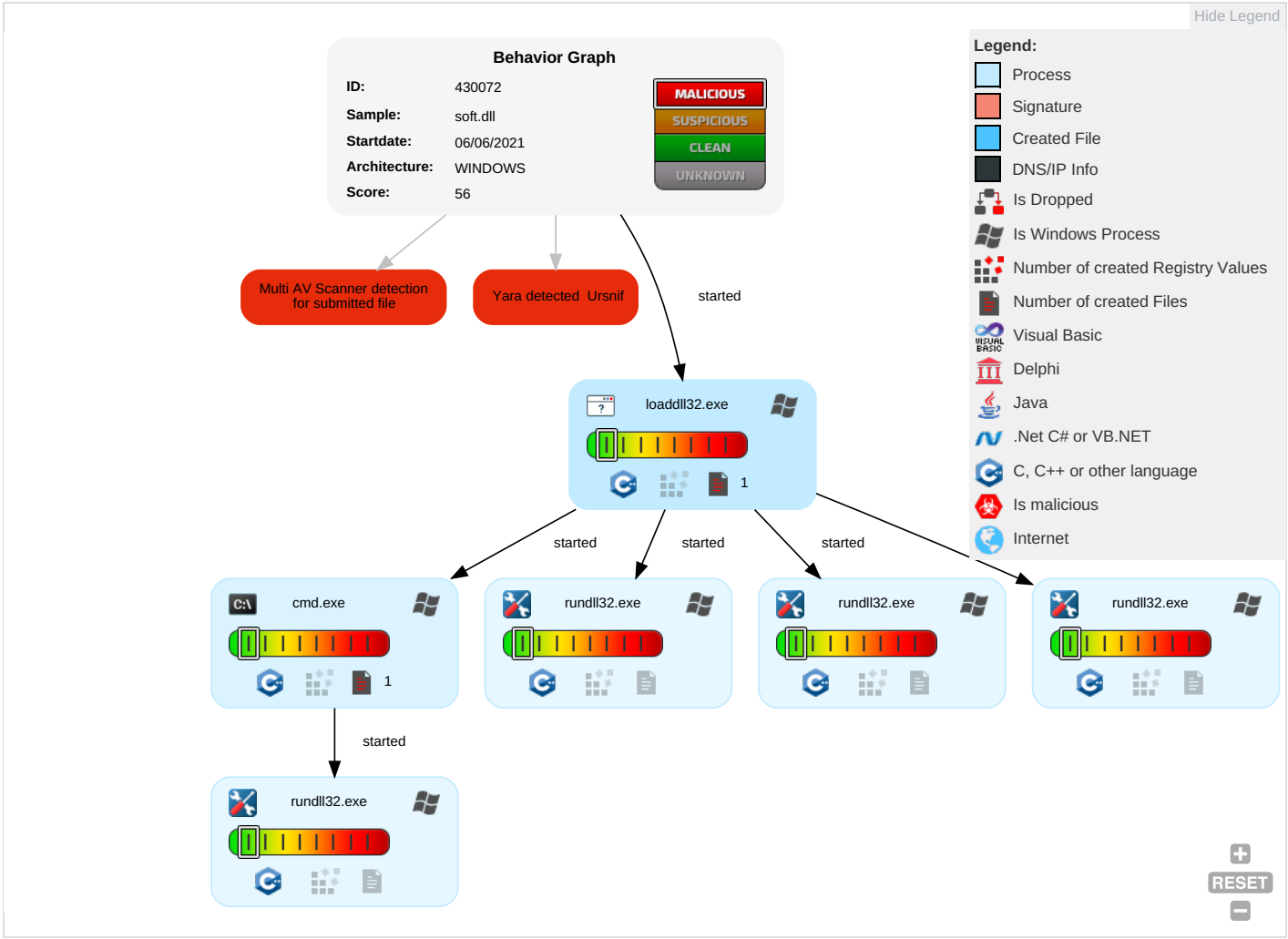
Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Valid Accounts	Native API 1	Path Interception	Process Injection 1 2	Rundll32 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Devic Without Authorizatic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	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	Remotely Wipe Data Without Authorizatic
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Information Discovery 2 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

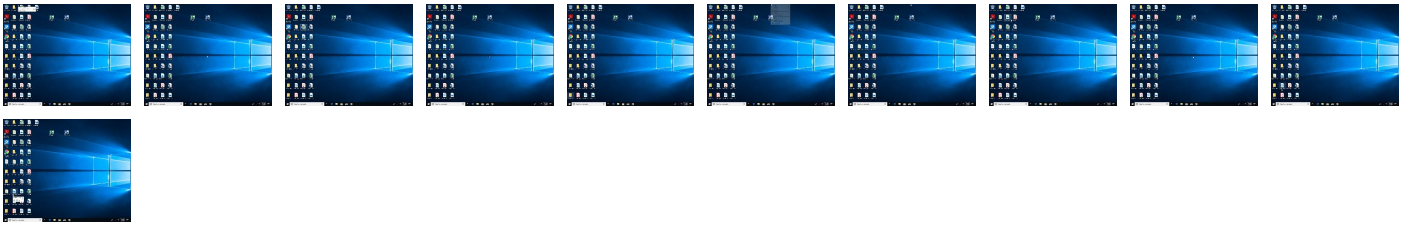
Behavior Graph



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
soft.dll	13%	Virustotal		Browse
soft.dll	14%	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:	32.0.0 Black Diamond
Analysis ID:	430072
Start date:	06.06.2021
Start time:	10:11:59
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	soft.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:	15
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:	mal56.troj.winDLL@11/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 45.3% (good quality ratio 43.5%) • Quality average: 84.6% • Quality standard deviation: 25.8%
HCA Information:	• Successful, ratio: 64% • 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): backgroundTaskHost.exe, SgrmBroker.exe, svchost.exe, UsoClient.exe • Not all processes where analyzed, report is missing behavior information

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) Intel 80386, for MS Windows
Entropy (8bit):	6.516081805018269
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:	soft.dll
File size:	472064
MD5:	627c8a536ed728b1b9e6d2dad958ac0c
SHA1:	03f6ab6dd415ca980cc0ab1f36f3d306e18c99bc
SHA256:	10ab600004b40a318004a19a90374c6430dcf5b2219dda9e6e017a424e3e0503
SHA512:	ec2073aae6c7a5e9ce936f1e97ada62cb8d793877048c45a0c4e5281844b058ccb82d5314e0b71da28998a6095fc9eb2ce61ff8276541d051c3cae0ed0aa216f
SSDEEP:	12288:e+Y4HM0hzA82rPr7XidWUrtiK+h6Ol5tz4ynpivaR+:rYvLHi4Ur7+h6OlrR+
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<.}.x..Nx..Nx..Nq..Nn..NC..Oz..NC..O|..NC..Oi..NC..Ou..N.I.Ns..Nx..N...NC..Oy..NC..OX..NC..Ny..NC..Oy..NRichx..N.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10028bd
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x1000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x59253A0D [Wed May 24 07:45:17 2017 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	fe31dd6739d0b573a8bd9bb5789aff6b

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
cmp dword ptr [ebp+0Ch], 01h
jne 00007F99C8F994D7h
call 00007F99C8F99C8Ah
push dword ptr [ebp+10h]
push dword ptr [ebp+0Ch]
push dword ptr [ebp+08h]
call 00007F99C8F9938Ah
add esp, 0Ch
pop ebp
retn 000Ch
push ebp
mov ebp, esp
push dword ptr [ebp+08h]
call 00007F99C8F99191h
pop ecx
pop ebp
ret
mov dword ptr [ecx], 01054AB0h
ret
push ebp
mov ebp, esp
test byte ptr [ebp+08h], 00000001h
push esi
mov esi, ecx
mov dword ptr [esi], 01054AB0h
je 00007F99C8F994DCh
push 0000000Ch
push esi
call 00007F99C8F994A6h
pop ecx
pop ecx
mov eax, esi
pop esi
pop ebp
retn 0004h

Instruction
push ebp
mov ebp, esp
push 00000000h
call dword ptr [0105415Ch]
push dword ptr [ebp+08h]
call dword ptr [01054160h]
push C0000409h
call dword ptr [01054158h]
push eax
call dword ptr [01054154h]
pop ebp
ret
push ebp
mov ebp, esp
sub esp, 00000324h
push 00000017h
call 00007F99C8FC8D0Bh
test eax, eax
je 00007F99C8F994D7h
push 00000002h
pop ecx
int 29h
mov dword ptr [01070C88h], eax
mov dword ptr [01070C84h], ecx
mov dword ptr [01070C80h], edx
mov dword ptr [01070C7Ch], ebx
mov dword ptr [01070C78h], esi
mov dword ptr [01070C74h], edi
mov word ptr [01070CA0h], ss
mov word ptr [eax], es

Rich Headers

Programming Language:	• [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x6f180	0x70	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x6f1f0	0x64	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xc3000	0x488	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc4000	0x2c58	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x6dc60	0x54	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x6dcb8	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x54000	0x47c	.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	0x52de6	0x52e00	False	0.593246252828	data	6.78851030835	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x54000	0x1bdec	0x1be00	False	0.523735285874	data	4.90694135639	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x70000	0x51e28	0xc00	False	0.2138671875	data	2.95477963021	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
.gfids	0xc2000	0x228	0x400	False	0.25390625	data	1.74574859447	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0xc3000	0x488	0x600	False	0.364583333333	data	3.05582166323	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc4000	0x2c58	0x2e00	False	0.771654211957	data	6.63160130152	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xc30a0	0x34c	data	English	United States
RT_MANIFEST	0xc33f0	0x91	XML 1.0 document text	English	United States

Imports

DLL	Import
KERNEL32.dll	GetModuleFileNameA, GetEnvironmentVariableA, GetVersion, GetTempPathA, OpenMutexA, GetSystemDirectoryA, LoadLibraryA, FileTimeToLocalFileTime, VirtualProtectEx, ExitProcess, GetCurrentProcessId, CreateEventA, OutputDebugStringW, WriteConsoleW, CreateFileW, ReadConsoleW, ReadFile, CloseHandle, HeapReAlloc, HeapSize, GetStringTypeW, SetFilePointerEx, GetFileSizeEx, SetStdHandle, GetConsoleMode, GetConsoleCP, WriteFile, FlushFileBuffers, SetConsoleCtrlHandler, GetProcessHeap, SetEnvironmentVariableW, FreeEnvironmentStringsW, GetEnvironmentStringsW, WideCharToMultiByte, MultiByteToWideChar, GetCommandLineW, GetCommandLineA, GetCPInfo, GetOEMCP, GetACP, IsValidCodePage, FindNextFileW, FindFirstFileExW, FindClose, GetCurrentThread, GetFileType, GetStdHandle, EnumSystemLocalesW, GetUserDefaultLCID, IsValidLocale, GetLocaleInfoW, LCMapStringW, CompareStringW, GetTimeFormatW, GetDateFormatW, HeapAlloc, HeapFree, GetModuleFileNameW, GetModuleHandleExW, LoadLibraryExW, GetProcAddress, FreeLibrary, TlsFree, TlsSetValue, TlsGetValue, TlsAlloc, InitializeCriticalSectionAndSpinCount, DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, RtlUnwind, SetLastError, GetLastError, InterlockedFlushSList, InterlockedPushEntrySList, RaiseException, EncodePointer, GetModuleHandleW, GetStartupInfoW, IsDebuggerPresent, InitializeSListHead, GetSystemTimeAsFileTime, GetCurrentThreadId, QueryPerformanceCounter, IsProcessorFeaturePresent, TerminateProcess, GetCurrentProcess, SetUnhandledExceptionFilter, UnhandledExceptionFilter, DecodePointer
ole32.dll	CoCreateInstance, CoUninitialize, CoInitialize, CLSIDFromString
comsvcs.dll	SafeRef
OLEAUT32.dll	VarRound, VarR8FromBool, SafeArrayCreateVectorEx, VariantChangeTypeEx, VarUI1FromBool, VarI8FromCy, DispCallFunc, VarAdd, OleCreatePropertyFrame, VarCyMulI8, VariantCopy, VarBstrFromI4, SysAllocString, VarNeg, VarUI8FromStr, VarMonthName, VarDateFromI2, VarUI4FromI8, VarTokenizeFormatString, SafeArrayDestroyData, VarUI1FromDate, VarNot, VarBoolFromCy, VarUI8FromCy, VarBstrFromR4, VariantTimeToDosDateTime, VarDateFromUI1, VarI2FromI4, VarUI4FromCy, VarBoolFromUI1, OaBuildVersion, VarUI1FromStr, VarDateFromDisp, VarBstrFromDisp, VarCyFromDisp, VarCyFromR4, VarI8FromDec, SysAllocStringByteLen, VarI8FromDate, VarI8FromUI8, VarI2FromCy, BSTR_UserUnmarshal, VarUI4FromUI8, VarI8FromR8, VarFormatFromTokens, VarUI4FromR8, SysStringByteLen, VarUI4FromDisp, VarI8FromDisp, RegisterTypeLib, OleCreateFontIndirect, BSTR_UserMarshal, VarUI4FromBool, VarFormat, VarUI4FromI2, VarI2FromUI1, CreateTypeLib2, SafeArrayAllocDescriptorEx, SysFreeString, VarUI4FromUI1, VarXor, SafeArrayCreateEx, OleLoadPicturePath, VariantCopyInd, VarUI1FromI4, VarUI1FromDisp, VarFix, VarUI8FromUI2, SafeArraySetRecordInfo, LoadTypeLib, CreateTypeLib, VarUI1FromI2, VarCyFromDate, VarDateFromR4, VarBoolFromI4, VariantInit, VarI2FromI8, VarDateFromUdateEx, LoadRegTypeLib, RegisterActiveObject, VarDecMul, VarBoolFromDate, SysReAllocString, VarUI8FromI2, VarCyFromStr, VarBstrFromR8, VarCyFromI2, VarUI8FromI1, GetRecordInfoFromTypeInfo, VarCat, VarUI4FromUI2, VarBoolFromR4, SafeArrayPtrOfIndex, VarI8FromBool, VarI8FromUI4, VarUI4FromI4, UnRegisterTypeLib, OleLoadPicture, LHashValOfNameSysA, VarInt, VarUI4FromDec, VarUI4FromI1, VarAnd, SystemTimeToVariantTime, DosDateTimeToVariantTime, VarUI8FromR8, VarDiv, SafeArrayRedim, VarUI8FromBool, VarUI8FromUI1, VarUI8FromR4, VarUI2FromUI4, VarCyFromI4, VarDecAdd, LHashValOfNameSys, VarUI4FromDate, VarCyFromUI1, OleLoadPictureFile, VarBoolFromDisp, VarI2FromR4, VarBstrFromBool, VarI8FromI2, VarBstrFromI2, CreateStdDispatch, OleCreatePictureIndirect, GetRecordInfoFromGuids, VarBstrFromCy, GetActiveObject, VarUI1FromR8, VarDecDiv, VarDateFromStr, SysReAllocStringLen, VarUI1FromR4, VarFormatNumber, VarI8FromR4, VarI2FromR8, VarI8FromStr, VarUI4FromR4, OleCreatePropertyFrameIndirect, VarFormatPercent, VarDateFromR8, VarUI8FromDisp, VarParseNumFromStr, VarI8FromUI1, RevokeActiveObject, VariantTimeToSystemTime, VarUI2FromDec, SysStringLen, ClearCustData, OleIconToCursor, SafeArrayGetRecordInfo, VarCyFromR8, VarDateFromCy, VarBoolFromStr, OleTranslateColor, VarBstrFromDate, VarI2FromUI8, VarDecAbs, SafeArrayCreate, BSTR_UserFree, VarUI8FromDate, SafeArrayDestroyDescriptor, OleSavePictureFile, SysAllocStringLen, VarNumFromParseNum, VarI8FromUI2, SafeArrayAllocData, LoadTypeLibEx, VarAbs, SafeArrayAllocDescriptor, VarFormatCurrency, VarWeekdayName, VarDateFromBool, VarDecSub, QueryPathOfRegTypeLib, VarDateFromI4, VariantChangeType, VarBoolFromR8, VarI8FromI1, VarCyFromBool, VarUI1FromCy, VariantClear, VarUI8FromI8, VarFormatDateTime, VarUI4FromStr, VarBstrFromUI1, BSTR_UserSize, VarBoolFromI2

Exports

Name	Ordinal	Address
Bottomget	1	0x1036380
Groupshop	2	0x1036200
Stoodbroad	3	0x1036cf0

Version Infos

Description	Data
LegalCopyright	Copyright (C) Microsoft Corp. 1981-1999
InternalName	come.dll
FileVersion	5.6.8.577

Description	Data
CompanyName	Microsoft Corporation
ProductName	Microsoft(R) Windows NT(R) Operating System
ProductVersion	5.6.8.577
FileDescription	Microsoft Wall Even Right
OriginalFilename	come.dll
Translation	0x0409 0x04b0

Possible Origin

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

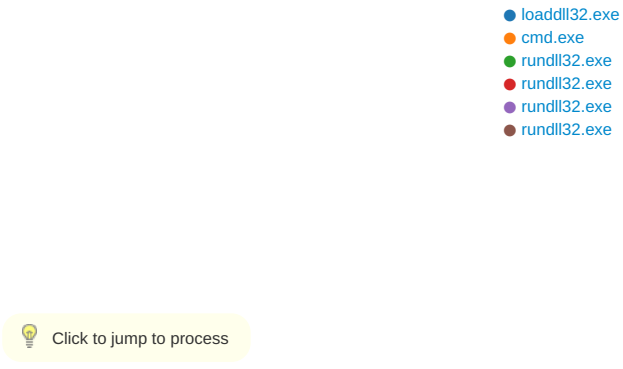
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 4760 Parent PID: 5648

General

Start time:	10:12:43
Start date:	06/06/2021
Path:	C:\Windows\System32\loaddll32.exe

Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\soft.dll'
Imagebase:	0xe30000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
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: cmd.exe PID: 2292 Parent PID: 4760

General

Start time:	10:12:44
Start date:	06/06/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\soft.dll',#1
Imagebase:	0xbd0000
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: 5328 Parent PID: 4760

General

Start time:	10:12:44
Start date:	06/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\soft.dll,Bottomget
Imagebase:	0x270000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 5348 Parent PID: 2292

General

Start time:	10:12:44
Start date:	06/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\soft.dll',#1
Imagebase:	0x270000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 5908 Parent PID: 4760

General

Start time:	10:12:48
Start date:	06/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\soft.dll,Groupshop
Imagebase:	0x270000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: rundll32.exe PID: 5912 Parent PID: 4760

General

Start time:	10:12:53
Start date:	06/06/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\soft.dll,Stoodbroad
Imagebase:	0x270000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis