ID: 412403
Sample Name:
c63f1121_by_Libranalysis
Cookbook: default.jbs
Time: 17:12:28
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

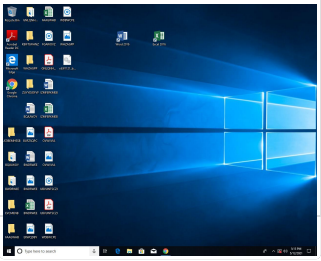
Analysis Report c63f1121_by_Libranalysis

Overview

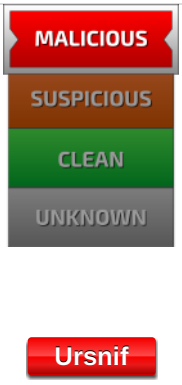
General Information

Sample Name:	c63f1121_by_Libranalysis (renamed file extension from none to dll)
Analysis ID:	412403
MD5:	c63f11211f899e3..
SHA1:	4d5baeaf852156d.
SHA256:	70f617d8686bdc7.
Infos:	

Most interesting Screenshot:



Detection

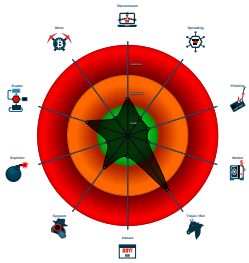


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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
- Creates a process in suspended mo…
- Detected potential crypto function
- Found potential string decryption / a…
- PE file contains an invalid checksum

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 6632 cmdline: loaddll32.exe 'C:\Users\user\Desktop\c63f1121_by_Libranalysis.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 6640 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\c63f1121_by_Libranalysis.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6664 cmdline: rundll32.exe 'C:\Users\user\Desktop\c63f1121_by_Libranalysis.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6652 cmdline: rundll32.exe C:\Users\user\Desktop\c63f1121_by_Libranalysis.dll,Dark@@4 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6708 cmdline: rundll32.exe C:\Users\user\Desktop\c63f1121_by_Libranalysis.dll,Schoolpress@@8 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 6724 cmdline: rundll32.exe C:\Users\user\Desktop\c63f1121_by_Libranalysis.dll,Triangleart@@8 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

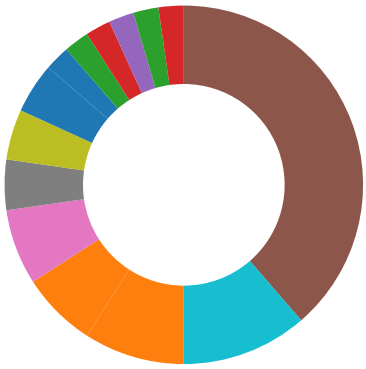
Yara Overview

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:

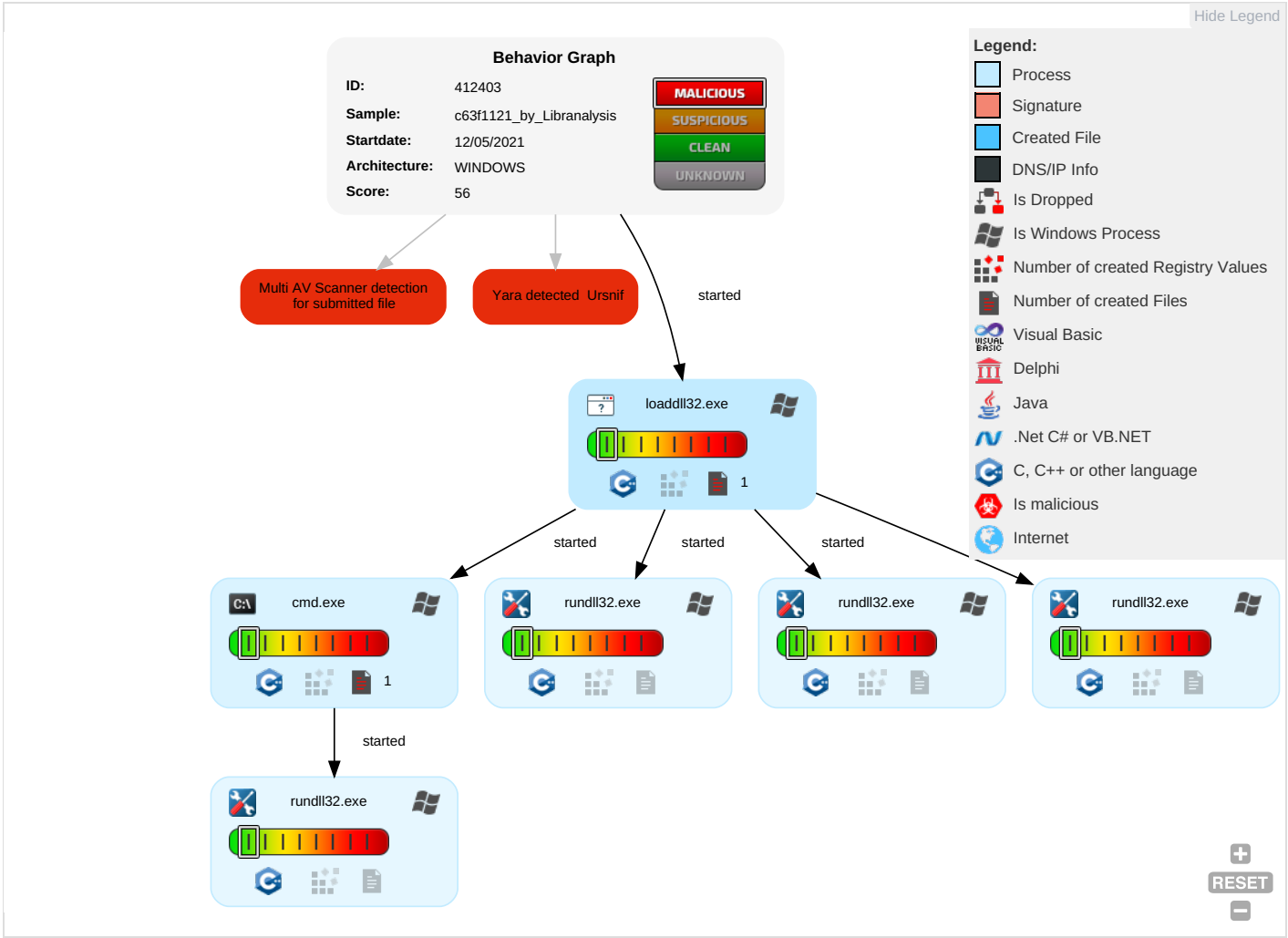
Yara detected Ursnif

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 1	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	

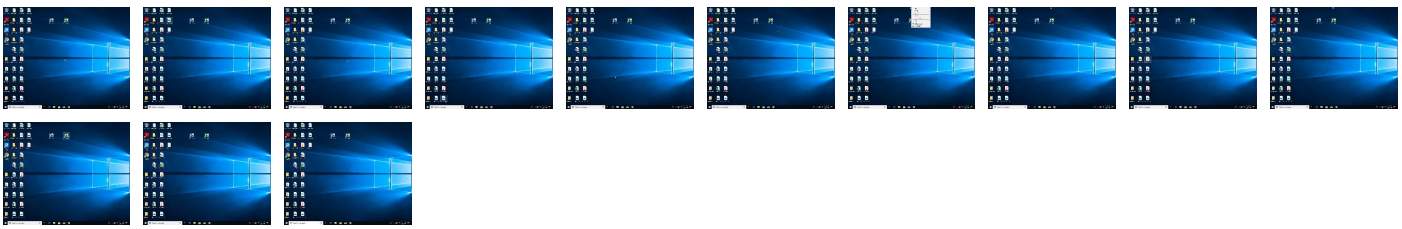
Behavior Graph



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
c63f1121_by_Libranalysis.dll	21%	Virustotal		Browse
c63f1121_by_Libranalysis.dll	11%	ReversingLabs	Win32.Trojan.Razy	

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:	412403
Start date:	12.05.2021
Start time:	17:12:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	c63f1121_by_Libranalysis (renamed file extension from none 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:	7
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:	Failed
HDC Information:	• Successful, ratio: 4.2% (good quality ratio 4%) • Quality average: 78.8% • Quality standard deviation: 29.2%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI

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):	6.694754169899549
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:	c63f1121_by_Libranalysis.dll
File size:	482816
MD5:	c63f11211f899e38c1c230594024950a
SHA1:	4d5baeaf852156dbe8053a1c600c7d96049f5967
SHA256:	70f617d8686bdc7d17d4f3b992a27f2532686815aaf5289841b87fd0c198ff3a
SHA512:	acb47d73ee0ae648188d90ba65584e4261ca8c174305e30e7249d7c8daeccb7b1ac71d8c85d269077b1397adbd29e3deba99ffb89f24c02e8dccbefab14f556b
SSDEEP:	12288:I5wfdldhr+GsAmRljPDeV1QlPqY5ExsETZCnMWxGuXPmEb8bVFaJ:I5adldhlDmfjPdglZCnR6jw
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....R...R...R...[.....7...P...7...@...R.....7...W...7...X...7...S...7...J...7.u.S...7...S...RichR.....PE..L..

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x102aa97
Entrypoint Section:	.text

General

Digitally signed:	false
Imagebase:	0x1000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6092A053 [Wed May 5 13:40:35 2021 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:	9c4dbee4f67fcf1f44b302fd37d240a5

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
cmp dword ptr [ebp+0Ch], 01h
jne 00007FE828F11C07h
call 00007FE828F12522h
push dword ptr [ebp+10h]
push dword ptr [ebp+0Ch]
push dword ptr [ebp+08h]
call 00007FE828F11AAAh
add esp, 0Ch
pop ebp
retn 000Ch
jmp 00007FE828F1F976h
push ebp
mov ebp, esp
and dword ptr [01088AA0h], 00000000h
sub esp, 24h
or dword ptr [010740ACh], 01h
push 0000000Ah
call 00007FE828F43CEBh
test eax, eax
je 00007FE828F11DAFh
and dword ptr [ebp-10h], 00000000h
xor eax, eax
push ebx
push esi
push edi
xor ecx, ecx
lea edi, dword ptr [ebp-24h]
push ebx
cpuid
mov esi, ebx
pop ebx
mov dword ptr [edi], eax
mov dword ptr [edi+04h], esi
mov dword ptr [edi+08h], ecx
xor ecx, ecx
mov dword ptr [edi+0Ch], edx
mov eax, dword ptr [ebp-24h]
mov edi, dword ptr [ebp-1Ch]
mov dword ptr [ebp-0Ch], eax
xor edi, 6C65746Eh
mov eax, dword ptr [ebp-18h]
xor eax, 49656E69h
mov dword ptr [ebp-08h], eax

Instruction
mov eax, dword ptr [ebp-20h]
xor eax, 756E6547h
mov dword ptr [ebp-04h], eax
xor eax, eax
inc eax
push ebx
cpuid
mov esi, ebx
pop ebx
lea ebx, dword ptr [ebp-24h]
mov dword ptr [ebx], eax
mov eax, dword ptr [ebp-04h]
mov dword ptr [ebx+04h], esi
or eax, edi
or eax, dword ptr [ebp-08h]
mov dword ptr [ebx+08h], ecx
mov dword ptr [ebx+0Ch], edx
jne 00007FE828F11C45h
mov eax, dword ptr [ebp-24h]
and eax, 0FFF3FF0h
cmp eax, 000106C0h
je 00007FE828F11C25h
cmp eax, 00020660h
je 00007FE828F11C1Eh

Rich Headers

Programming Language:	• [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x725e0	0x78	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x72658	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x8a000	0x4a8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x8b000	0x2984	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x70d0c	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	0x70d60	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x5e000	0x1b4	.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	0x5c9e8	0x5ca00	False	0.615445238698	data	6.76388282152	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x5e000	0x150ea	0x15200	False	0.523761094675	data	5.71930655491	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x74000	0x15d14	0xe00	False	0.208426339286	DOS executable (COM, 0x8C-variant)	2.91984916435	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x8a000	0x4a8	0x600	False	0.367838541667	data	3.03803804684	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8b000	0x2984	0x2a00	False	0.793712797619	data	6.70935013464	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x8a0a0	0x36c	data	English	United States
RT_MANIFEST	0x8a410	0x91	XML 1.0 document text	English	United States

Imports

DLL	Import
KERNEL32.dll	WriteConsoleW, FindFirstChangeNotificationW, GetEnvironmentVariableW, LoadLibraryW, CreateEventW, FileTimeToLocalFileTime, DeviceIoControl, WaitForSingleObject, VirtualProtectEx, VirtualProtect, GetVersion, CloseHandle, CreateFileW, OutputDebugStringW, ReadConsoleW, ReadFile, IsProcessorFeaturePresent, IsDebuggerPresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetStartupInfoW, GetModuleHandleW, GetCurrentProcess, TerminateProcess, QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, RaiseException, RtlUnwind, InterlockedPushEntrySList, InterlockedFlushSList, GetLastError, SetLastError, EncodePointer, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, FreeLibrary, GetProcAddress, LoadLibraryExW, ExitProcess, GetModuleHandleExW, GetModuleFileNameW, GetCurrentThread, HeapAlloc, GetCPInfo, HeapFree, FindClose, FindFirstFileExW, FindNextFileW, IsValidCodePage, GetACP, GetOEMCP, GetCommandLineA, GetCommandLineW, MultiByteToWideChar, WideCharToMultiByte, GetEnvironmentStringsW, FreeEnvironmentStringsW, SetEnvironmentVariableW, GetDateFormatW, GetTimeFormatW, CompareStringW, LCMapStringW, GetLocaleInfoW, IsValidLocale, GetUserDefaultLCID, EnumSystemLocalesW, GetProcessHeap, GetStdHandle, GetFileType, SetConsoleCtrlHandler, GetStringTypeW, HeapSize, HeapReAlloc, SetStdHandle, FlushFileBuffers, WriteFile, GetConsoleCP, GetConsoleMode, GetFileSizeEx, SetFilePointerEx, DecodePointer
CRYPT32.dll	CryptDecodeObject, CertVerifyCertificateChainPolicy, CertFreeCertificateChain, CertGetCertificateChain, CryptAcquireCertificatePrivateKey, CryptImportPublicKeyInfo, CertDeleteCertificateFromStore, CertAddCertificateContextToStore, CertFreeCertificateContext, CertCreateCertificateContext, CertCloseStore, CryptEncodeObject
Secur32.dll	ImpersonateSecurityContext, InitializeSecurityContextW, DeleteSecurityContext, FreeContextBuffer

Exports

Name	Ordinal	Address
Dark@@4	1	0x1029882
Schoolpress@@8	2	0x1029898
Triangleart@@8	3	0x10299a8

Version Infos

Description	Data
LegalCopyright	Settle equal Corporation. All rights reserved
InternalName	Property Womentogether
FileVersion	6.6.8.172
CompanyName	Settle equal Corporation
Money	90
ProductName	Settle equal Rope lie
ProductVersion	6.6.8.172
FileDescription	Settle equal Rope lie
OriginalFilename	Cell.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: 6632 Parent PID: 5856

General

Start time:	17:13:16
Start date:	12/05/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\c63f1121_by_Libranalysis.dll'
Imagebase:	0xcf0000
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: 6640 Parent PID: 6632

General

Start time:	17:13:16
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\c63f1121_by_Libranalysis.dll',#1
Imagebase:	0x11d0000

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: 6652 Parent PID: 6632

General

Start time:	17:13:16
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\c63f1121_by_Libranalysis.dll,Dark@@4
Imagebase:	0x1170000
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: 6664 Parent PID: 6640

General

Start time:	17:13:16
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\c63f1121_by_Libranalysis.dll',#1
Imagebase:	0x1170000
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: 6708 Parent PID: 6632

General

Start time:	17:13:20
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\c63f1121_by_Libranalysis.dll,Schoolpress@@8
Imagebase:	0x1170000
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: 6724 Parent PID: 6632

General

Start time:	17:13:23
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\c63f1121_by_Libranalysis.dll,Triangleart@@8
Imagebase:	0x1170000
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