

JOeSandbox Cloud BASIC



ID: 393200

Sample Name: Dridex.exe

Cookbook: default.jbs

Time: 10:00:37

Date: 20/04/2021

Version: 31.0.0 Emerald

Table of Contents

Table of Contents	2
Analysis Report Dridex.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Malware Configuration	4
Yara Overview	4
Sigma Overview	4
Signature Overview	4
AV Detection:	5
Data Obfuscation:	5
Malware Analysis System Evasion:	5
HIPS / PFW / Operating System Protection Evasion:	5
Mitre Att&ck Matrix	5
Behavior Graph	6
Screenshots	6
Thumbnails	6
Antivirus, Machine Learning and Genetic Malware Detection	7
Initial Sample	7
Dropped Files	7
Unpacked PE Files	7
Domains	8
URLs	8
Domains and IPs	8
Contacted Domains	8
Contacted IPs	8
Public	8
General Information	8
Simulations	9
Behavior and APIs	9
Joe Sandbox View / Context	9
IPs	9
Domains	10
ASN	10
JA3 Fingerprints	10
Dropped Files	10
Created / dropped Files	11
Static File Info	11
General	11
File Icon	11
Static PE Info	11
General	11
Entrypoint Preview	11
Rich Headers	12
Data Directories	12
Sections	13
Imports	13
Network Behavior	13
Snort IDS Alerts	13
Network Port Distribution	14
TCP Packets	14
Code Manipulations	15
Statistics	15

Behavior	15
System Behavior	16
Analysis Process: Dridex.exe PID: 2296 Parent PID: 5652	16
General	16
File Activities	16
File Read	16
Registry Activities	16
Analysis Process: Dridex.exe PID: 4116 Parent PID: 2296	16
General	16
File Activities	17
File Created	17
Disassembly	18
Code Analysis	18

Analysis Report Dridex.exe

Overview

General Information

Sample Name:	Dridex.exe
Analysis ID:	393200
MD5:	6e5654da58c03d..
SHA1:	594f33ad9d7f856..
SHA256:	e30b76f9454a5fd..
Tags:	Dridex ProcessHollowing RunPE
Infos:	
Most interesting Screenshot:	

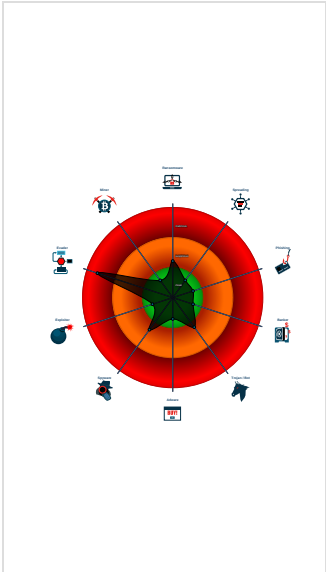
Detection

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Antivirus / Scanner detection for sub...
Detected unpacking (changes PE se...
Multi AV Scanner detection for subm...
Contain functionality to detect virtua...
Contains functionality to inject code ...
Injects a PE file into a foreign proce...
Machine Learning detection for samp...
Tries to detect sandboxes / dynamic...
Antivirus or Machine Learning detec...
Contains functionality to call native f...
Contains functionality to check if a w...
Contains functionality to enumerate ...
Contains functionality to query locale ...
Contains functionality to read the PEB

Classification



Startup

- System is w10x64
- Dridex.exe (PID: 2296 cmdline: 'C:\Users\user\Desktop\Dridex.exe' MD5: 6E5654DA58C03DF6808466F0197207ED)
 - Dridex.exe (PID: 4116 cmdline: C:\Users\user\Desktop\Dridex.exe MD5: 6E5654DA58C03DF6808466F0197207ED)
- cleanup

Malware Configuration

No configs have been found

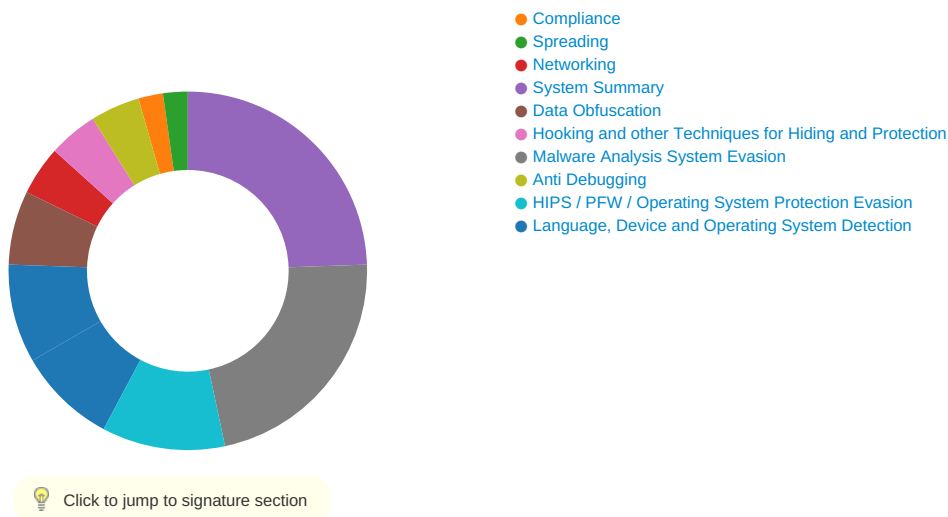
Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Signature Overview



AV Detection:



Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Data Obfuscation:



Detected unpacking (changes PE section rights)

Malware Analysis System Evasion:



Contain functionality to detect virtual machines

Tries to detect sandboxes / dynamic malware analysis system (file name check)

HIPS / PFW / Operating System Protection Evasion:



Contains functionality to inject code into remote processes

Injects a PE file into a foreign processes

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 2 2 2	Virtualization/Sandbox Evasion 2 2 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communi
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 2 2 2	LSASS Memory	Security Software Discovery 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS Redirect F Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Virtualization/Sandbox Evasion 2 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 1	NTDS	Process Discovery 3	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	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulat Device Communi



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Dridex.exe	89%	Virustotal		Browse
Dridex.exe	86%	Metadefender		Browse
Dridex.exe	100%	ReversingLabs	Win32.Backdoor.Draxed	
Dridex.exe	100%	Avira	TR/Taranis.403	
Dridex.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.Dridex.exe.400000.1.unpack	100%	Avira	TR/Taranis.403		Download File
1.0.Dridex.exe.400000.0.unpack	100%	Avira	TR/Taranis.403		Download File
3.1.Dridex.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.Dridex.exe.990000.4.unpack	100%	Avira	TR/Taranis.403		Download File
3.0.Dridex.exe.400000.0.unpack	100%	Avira	TR/Taranis.403		Download File
3.2.Dridex.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.1.Dridex.exe.400000.0.unpack	100%	Avira	TR/Taranis.403		Download File
1.2.Dridex.exe.9c0000.6.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
1.2.Dridex.exe.26f0000.7.unpack	100%	Avira	TR/Taranis.403		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.252.100.44	unknown	Indonesia		59147	IDNIC-DRUPADI-AS-IDPTDrupadiPrimalD	false
89.108.71.148	unknown	Russian Federation		43146	AGAVA3RU	false
221.132.35.56	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	false
94.73.155.12	unknown	Turkey		34619	CIZGITR	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	393200

Start date:	20.04.2021
Start time:	10:00:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Dridex.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
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	38
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:	mal84.evad.winEXE@3/0@0/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 51% (good quality ratio 48.6%) • Quality average: 76.7% • Quality standard deviation: 29%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:04:16	API Interceptor	15x Sleep call for process: Dridex.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
89.108.71.148	Dridex.exe	Get hash	malicious	Browse	
221.132.35.56	Dridex.exe	Get hash	malicious	Browse	
94.73.155.12	Dridex.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
IDNIC-DRUPADI-AS-IDPTDrupadiPrimaID	Dridex.exe	Get hash	malicious	Browse	103.252.100.44
VNPT-AS-VNVNPTCorpVN	Dridex.exe	Get hash	malicious	Browse	221.132.35.56
	PO45937008ADENGY.exe	Get hash	malicious	Browse	123.31.43.181
	8QGgIvUeYO.exe	Get hash	malicious	Browse	103.42.58.103
	networkmanager	Get hash	malicious	Browse	14.188.135.58
	WUHU95App3	Get hash	malicious	Browse	113.183.33.163
	G0ESHZsrvg.exe	Get hash	malicious	Browse	103.255.237.180
	6OUYcd3Gls.exe	Get hash	malicious	Browse	103.255.237.180
	http://singaedental.vn/wp-content/IQ/	Get hash	malicious	Browse	202.92.7.113
	http://covisa.com.br/paypal-closed-y2hir/ABqY1RAPJaNGnFw9flbsTw3mbHnBB1OUWRV6kbbvfAyr4bmEsDoeNMECXf3fg6io/	Get hash	malicious	Browse	202.92.7.113
	Adjunto_2021.doc	Get hash	malicious	Browse	202.92.7.113
	Dok 0501 012021 Q_93291.doc	Get hash	malicious	Browse	202.92.7.113
	11_extracted.exe	Get hash	malicious	Browse	103.207.39.131
	http://https://correolimpio.telefonica.es/atp/url-check.php?URL=https%3A%2F%2Fnhabeland.vn%2Fsecurirys%2FRbvPk%2F&D=53616c7465645f5f824c0b393b6f3e2d3c9a50d9826547979a4ceae42fdf4a21ec36a319de1437ef72976b2e7ef710bdb842a205880238cf08cf04b46eccce50114dbc4447f1aa62068b81b9d426da6b&V=1	Get hash	malicious	Browse	103.255.237.61
	SecuriteInfo.com.ArtemisC5924E341E9E.exe	Get hash	malicious	Browse	103.255.237.239
	INFO 2020 DWP_947297.doc	Get hash	malicious	Browse	14.177.232.31
	MESSAGIO 83-46447904.doc	Get hash	malicious	Browse	123.31.24.142
	Order List and Quantities.ppt	Get hash	malicious	Browse	103.207.39.131
	Purchase list.ppt	Get hash	malicious	Browse	103.207.39.131
	2020141248757837844.ppt	Get hash	malicious	Browse	103.207.39.131
	PurchaseOrder#Q7677.ppt	Get hash	malicious	Browse	103.207.39.131
AGAVA3RU	Dridex.exe	Get hash	malicious	Browse	89.108.71.148
	Zh2Gv0wJtk.exe	Get hash	malicious	Browse	80.78.246.22
	c3XD756MSN.exe	Get hash	malicious	Browse	89.108.88.140
	O6RQ377jNN.exe	Get hash	malicious	Browse	89.108.88.140
	SecuriteInfo.com.Trojan.Siggen12.58144.411.exe	Get hash	malicious	Browse	89.108.88.140
	7Q1bVVkIIL.exe	Get hash	malicious	Browse	89.108.88.140
	R2o3eEx5Zj.exe	Get hash	malicious	Browse	89.108.88.140
	5MZKivSsq7.exe	Get hash	malicious	Browse	80.78.245.80
	z9mXoeDPej.exe	Get hash	malicious	Browse	89.108.88.140
	SecuriteInfo.com.W32.AIDetect.malware1.20229.exe	Get hash	malicious	Browse	89.108.88.140
	SecuriteInfo.com.W32.AIDetect.malware1.15067.exe	Get hash	malicious	Browse	89.108.88.140
	SecuriteInfo.com.W32.AIDetect.malware1.13347.exe	Get hash	malicious	Browse	89.108.88.140
	SecuriteInfo.com.W32.AIDetect.malware1.8119.exe	Get hash	malicious	Browse	89.108.88.140
	seed.exe	Get hash	malicious	Browse	89.108.88.140
	SecuriteInfo.com.Heur.17834.xls	Get hash	malicious	Browse	89.108.122.188
	SecuriteInfo.com.Heur.9646.xls	Get hash	malicious	Browse	89.108.122.188
	SecuriteInfo.com.Heur.17834.xls	Get hash	malicious	Browse	89.108.122.188
	SecuriteInfo.com.Heur.9646.xls	Get hash	malicious	Browse	89.108.122.188
	Claim-2016732059-02092021.xls	Get hash	malicious	Browse	89.108.122.188
	Claim-2016732059-02092021.xls	Get hash	malicious	Browse	89.108.122.188

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):	7.640683635227719
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:	Dridex.exe
File size:	176128
MD5:	6e5654da58c03df6808466f0197207ed
SHA1:	594f33ad9d7f85625a88c24903243ba9788fba86
SHA256:	e30b76f9454a5fd3d11b5792ff93e56c52bf5dfba6ab375c3b96e17af562f5fc
SHA512:	6542a42528f11085376ba893615cd7b68b37e1c78427c678db658e6174ca8d0ac893b071aa55e8d3924a6a22356f7322eadf025f10e26c4a0c9858e3c12eb264
SSDEEP:	3072:qZkKstjomW1XBJqhhPQa77I79KQXF6yvf4FkbmB7VU2fMa+:zvUmgqkm9KQXF6yvwCbu7gT
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode....\$.B... B...B#..B...B)..Bj..B...Bj..B...B...BW..B9..B...B.. .B...BW..Bi..BRich..B.....PE..L..b.QV...

File Icon

	
Icon Hash:	c08c6665996135a7

Static PE Info

General	
Entrypoint:	0x402410
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:	0x5651A962 [Sun Nov 22 11:39:14 2015 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:	3c0df6d8c78f9ce11bee326616d075a2

Entrypoint Preview

Instruction
push ebp
mov ebp, esp

Instruction
push FFFFFFFFh
push 00403770h
push 00402612h
mov eax, dword ptr fs:[00000000h]
push eax
mov dword ptr fs:[00000000h], esp
sub esp, 68h
push ebx
push esi
push edi
mov dword ptr [ebp-18h], esp
xor ebx, ebx
mov dword ptr [ebp-04h], ebx
push 00000002h
call dword ptr [00403260h]
pop ecx
or dword ptr [00407128h], FFFFFFFFh
or dword ptr [0040712Ch], FFFFFFFFh
call dword ptr [00403264h]
mov ecx, dword ptr [0040711Ch]
mov dword ptr [eax], ecx
call dword ptr [00403268h]
mov ecx, dword ptr [00407118h]
mov dword ptr [eax], ecx
mov eax, dword ptr [0040326Ch]
mov eax, dword ptr [eax]
mov dword ptr [00407124h], eax
call 00007FBD588A11F7h
cmp dword ptr [00406FD0h], ebx
jne 00007FBD588A106Eh
push 0040260Eh
call dword ptr [00403270h]
pop ecx
call 00007FBD588A11C9h
push 00405028h
push 00405024h
call 00007FBD588A11B4h
mov eax, dword ptr [00407114h]
mov dword ptr [ebp-6Ch], eax
lea eax, dword ptr [ebp-6Ch]
push eax
push dword ptr [00407110h]
lea eax, dword ptr [ebp-64h]
push eax
lea eax, dword ptr [ebp-70h]
push eax
lea eax, dword ptr [ebp-60h]
push eax
call dword ptr [00403278h]
push 00405020h
push 00405000h
call 00007FBD588A1181h

Rich Headers

Programming Language:	[C++] VS2002 (.NET) build 9466 [EXP] VC++ 6.0 SP5 build 8804 [ASM] VS2002 (.NET) build 9466
-----------------------	---

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x1000	0x10	.text
IMAGE_DIRECTORY_ENTRY_IMPORT	0x3980	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x8000	0x23e9c	.rsrc

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0xa000	0x22	.rsrc
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	0x3000	0x2f0	.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	0x1850	0x2000	False	0.381591796875	data	4.8857712628	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x3000	0x1148	0x2000	False	0.22705078125	data	3.18379463097	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x5000	0x2130	0x2000	False	0.441162109375	data	4.29630200062	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x8000	0x23e9c	0x24000	False	0.962103949653	data	7.93888068706	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Imports

DLL	Import
MFC42.DLL	
MSVCRT.dll	_controlfp, _onexit, __dllonexit, _except_handler3, __set_app_type, __p_fmode, __p_commode, _adjust_fdiv, __setusermatherr, _initterm, __getmainargs, _acmdln, _setmbcp, __CxxFrameHandler, strtol, _exit, _XcptFilter, exit
KERNEL32.dll	FindNextFileW, GetTimeZoneInformation, ExitProcess, GetModuleFileNameA, FlushFileBuffers, SetStdHandle, HeapDestroy, FindFirstFileA, HeapReAlloc, GetDateFormatA, GetEnvironmentStrings, GetACP, GetCommandLineA, GetModuleHandleA, GetStartupInfoA, GetLocaleInfoW, CreateFileW, MapViewOfFile, GetOEMCP, CreateFileA, GetModuleFileNameW
USER32.dll	IsIconic, GetCaretBlinkTime, ShowWindow, UpdateWindow, GetCursorPos, PeekMessageW, RegisterClipboardFormatW, GetSystemMetrics, HideCaret, GetSystemMenu, AppendMenuA, SendMessageA, LoadIconA, MessageBoxIndirectA, GetDesktopWindow, DrawIcon, EnableWindow, GetClientRect
GDI32.dll	GetCharABCWidthsFloatA, CreateCompatibleDC
ADVAPI32.dll	RegDeleteKeyW
OLEAUT32.dll	VariantClear

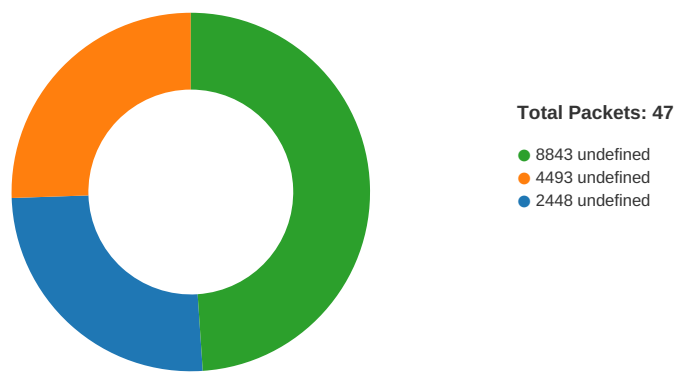
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/20/21-09:53:56.512323	ICMP	384	ICMP PING			192.168.2.6	205.185.216.42
04/20/21-09:53:56.548392	ICMP	449	ICMP Time-To-Live Exceeded in Transit			84.17.52.126	192.168.2.6
04/20/21-09:53:56.548789	ICMP	384	ICMP PING			192.168.2.6	205.185.216.42
04/20/21-09:53:56.585493	ICMP	449	ICMP Time-To-Live Exceeded in Transit			5.56.20.161	192.168.2.6
04/20/21-09:53:56.585894	ICMP	384	ICMP PING			192.168.2.6	205.185.216.42
04/20/21-09:53:56.632458	ICMP	449	ICMP Time-To-Live Exceeded in Transit			81.95.2.138	192.168.2.6
04/20/21-09:53:56.634351	ICMP	384	ICMP PING			192.168.2.6	205.185.216.42
04/20/21-09:53:56.684778	ICMP	449	ICMP Time-To-Live Exceeded in Transit			151.139.80.6	192.168.2.6

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/20/21-09:53:56.686368	ICMP	384	ICMP PING			192.168.2.6	205.185.216.42
04/20/21-09:53:56.736294	ICMP	449	ICMP Time-To-Live Exceeded in Transit			151.139.80.13	192.168.2.6
04/20/21-09:53:56.736727	ICMP	384	ICMP PING			192.168.2.6	205.185.216.42
04/20/21-09:53:56.786580	ICMP	408	ICMP Echo Reply			205.185.216.42	192.168.2.6

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 20, 2021 10:03:56.292613029 CEST	49713	2448	192.168.2.3	94.73.155.12
Apr 20, 2021 10:03:59.285557985 CEST	49713	2448	192.168.2.3	94.73.155.12
Apr 20, 2021 10:04:05.301655054 CEST	49713	2448	192.168.2.3	94.73.155.12
Apr 20, 2021 10:04:18.342212915 CEST	49723	4493	192.168.2.3	103.252.100.44
Apr 20, 2021 10:04:18.568540096 CEST	4493	49723	103.252.100.44	192.168.2.3
Apr 20, 2021 10:04:19.084112883 CEST	49723	4493	192.168.2.3	103.252.100.44
Apr 20, 2021 10:04:19.307770014 CEST	4493	49723	103.252.100.44	192.168.2.3
Apr 20, 2021 10:04:19.818506002 CEST	49723	4493	192.168.2.3	103.252.100.44
Apr 20, 2021 10:04:20.042088032 CEST	4493	49723	103.252.100.44	192.168.2.3
Apr 20, 2021 10:04:21.064090014 CEST	49726	8843	192.168.2.3	89.108.71.148
Apr 20, 2021 10:04:21.147289038 CEST	8843	49726	89.108.71.148	192.168.2.3
Apr 20, 2021 10:04:21.662472963 CEST	49726	8843	192.168.2.3	89.108.71.148
Apr 20, 2021 10:04:21.751689911 CEST	8843	49726	89.108.71.148	192.168.2.3
Apr 20, 2021 10:04:22.256321907 CEST	49726	8843	192.168.2.3	89.108.71.148
Apr 20, 2021 10:04:22.338612080 CEST	8843	49726	89.108.71.148	192.168.2.3
Apr 20, 2021 10:04:23.359273911 CEST	49729	8843	192.168.2.3	221.132.35.56
Apr 20, 2021 10:04:26.380806923 CEST	49729	8843	192.168.2.3	221.132.35.56
Apr 20, 2021 10:04:32.382071972 CEST	49729	8843	192.168.2.3	221.132.35.56
Apr 20, 2021 10:04:46.302922010 CEST	49732	2448	192.168.2.3	94.73.155.12
Apr 20, 2021 10:04:49.414755106 CEST	49732	2448	192.168.2.3	94.73.155.12
Apr 20, 2021 10:04:55.415363073 CEST	49732	2448	192.168.2.3	94.73.155.12
Apr 20, 2021 10:05:08.458399057 CEST	49742	4493	192.168.2.3	103.252.100.44
Apr 20, 2021 10:05:08.683224916 CEST	4493	49742	103.252.100.44	192.168.2.3
Apr 20, 2021 10:05:09.197618008 CEST	49742	4493	192.168.2.3	103.252.100.44
Apr 20, 2021 10:05:09.421516895 CEST	4493	49742	103.252.100.44	192.168.2.3
Apr 20, 2021 10:05:09.932132959 CEST	49742	4493	192.168.2.3	103.252.100.44
Apr 20, 2021 10:05:10.157634974 CEST	4493	49742	103.252.100.44	192.168.2.3
Apr 20, 2021 10:05:11.182188034 CEST	49743	8843	192.168.2.3	89.108.71.148
Apr 20, 2021 10:05:11.262833118 CEST	8843	49743	89.108.71.148	192.168.2.3
Apr 20, 2021 10:05:11.775959969 CEST	49743	8843	192.168.2.3	89.108.71.148
Apr 20, 2021 10:05:11.858793974 CEST	8843	49743	89.108.71.148	192.168.2.3
Apr 20, 2021 10:05:12.370151043 CEST	49743	8843	192.168.2.3	89.108.71.148
Apr 20, 2021 10:05:12.450613022 CEST	8843	49743	89.108.71.148	192.168.2.3

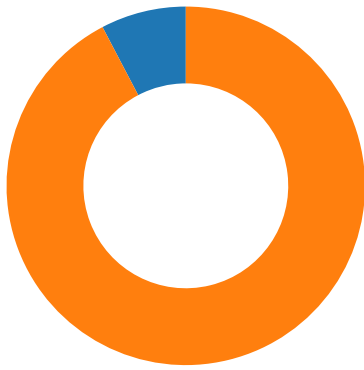
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 20, 2021 10:05:13.468441010 CEST	49744	8843	192.168.2.3	221.132.35.56
Apr 20, 2021 10:05:16.479630947 CEST	49744	8843	192.168.2.3	221.132.35.56
Apr 20, 2021 10:05:22.496309042 CEST	49744	8843	192.168.2.3	221.132.35.56
Apr 20, 2021 10:05:35.533082008 CEST	49745	2448	192.168.2.3	94.73.155.12
Apr 20, 2021 10:05:38.543840885 CEST	49745	2448	192.168.2.3	94.73.155.12
Apr 20, 2021 10:05:44.544382095 CEST	49745	2448	192.168.2.3	94.73.155.12
Apr 20, 2021 10:05:57.566203117 CEST	49749	4493	192.168.2.3	103.252.100.44
Apr 20, 2021 10:05:57.784306049 CEST	4493	49749	103.252.100.44	192.168.2.3
Apr 20, 2021 10:05:58.295567036 CEST	49749	4493	192.168.2.3	103.252.100.44
Apr 20, 2021 10:05:58.515402079 CEST	4493	49749	103.252.100.44	192.168.2.3
Apr 20, 2021 10:05:59.029887915 CEST	49749	4493	192.168.2.3	103.252.100.44
Apr 20, 2021 10:05:59.247181892 CEST	4493	49749	103.252.100.44	192.168.2.3
Apr 20, 2021 10:06:00.269778013 CEST	49750	8843	192.168.2.3	89.108.71.148
Apr 20, 2021 10:06:00.351015091 CEST	8843	49750	89.108.71.148	192.168.2.3
Apr 20, 2021 10:06:00.858256102 CEST	49750	8843	192.168.2.3	89.108.71.148
Apr 20, 2021 10:06:00.939048052 CEST	8843	49750	89.108.71.148	192.168.2.3
Apr 20, 2021 10:06:01.452007055 CEST	49750	8843	192.168.2.3	89.108.71.148
Apr 20, 2021 10:06:01.534965038 CEST	8843	49750	89.108.71.148	192.168.2.3
Apr 20, 2021 10:06:02.551201105 CEST	49751	8843	192.168.2.3	221.132.35.56
Apr 20, 2021 10:06:05.561764956 CEST	49751	8843	192.168.2.3	221.132.35.56
Apr 20, 2021 10:06:11.577871084 CEST	49751	8843	192.168.2.3	221.132.35.56
Apr 20, 2021 10:06:24.615189075 CEST	49752	2448	192.168.2.3	94.73.155.12
Apr 20, 2021 10:06:27.626169920 CEST	49752	2448	192.168.2.3	94.73.155.12
Apr 20, 2021 10:06:33.626544952 CEST	49752	2448	192.168.2.3	94.73.155.12
Apr 20, 2021 10:06:46.657027960 CEST	49763	4493	192.168.2.3	103.252.100.44
Apr 20, 2021 10:06:46.883133888 CEST	4493	49763	103.252.100.44	192.168.2.3
Apr 20, 2021 10:06:47.386786938 CEST	49763	4493	192.168.2.3	103.252.100.44
Apr 20, 2021 10:06:47.612837076 CEST	4493	49763	103.252.100.44	192.168.2.3
Apr 20, 2021 10:06:48.128803968 CEST	49763	4493	192.168.2.3	103.252.100.44
Apr 20, 2021 10:06:48.354705095 CEST	4493	49763	103.252.100.44	192.168.2.3
Apr 20, 2021 10:06:50.473021030 CEST	49764	8843	192.168.2.3	89.108.71.148
Apr 20, 2021 10:06:50.553571939 CEST	8843	49764	89.108.71.148	192.168.2.3
Apr 20, 2021 10:06:51.136691093 CEST	49764	8843	192.168.2.3	89.108.71.148
Apr 20, 2021 10:06:51.217472076 CEST	8843	49764	89.108.71.148	192.168.2.3
Apr 20, 2021 10:06:51.887130976 CEST	49764	8843	192.168.2.3	89.108.71.148
Apr 20, 2021 10:06:51.967732906 CEST	8843	49764	89.108.71.148	192.168.2.3
Apr 20, 2021 10:06:52.986123085 CEST	49765	8843	192.168.2.3	221.132.35.56
Apr 20, 2021 10:06:55.996977091 CEST	49765	8843	192.168.2.3	221.132.35.56

Code Manipulations

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: Dridex.exe PID: 2296 Parent PID: 5652

General

Start time:	10:03:51
Start date:	20/04/2021
Path:	C:\Users\user\Desktop\Dridex.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Dridex.exe'
Imagebase:	0x400000
File size:	176128 bytes
MD5 hash:	6E5654DA58C03DF6808466F0197207ED
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Dridex.exe	unknown	176128	success or wait	1	9834A6	ReadFile

Registry Activities

Key Path				Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: Dridex.exe PID: 4116 Parent PID: 2296

General

Start time:	10:03:52
Start date:	20/04/2021
Path:	C:\Users\user\Desktop\Dridex.exe

Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Dridex.exe
Imagebase:	0x400000
File size:	176128 bytes
MD5 hash:	6E5654DA58C03DF6808466F0197207ED
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	409948	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	409948	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\I\NetCache	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	409948	HttpSendRequestW
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	409948	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	409948	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\I\NetCookies	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	409948	HttpSendRequestW
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	409948	HttpSendRequestW
C:\Users\user\AppData\Local	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	409948	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\I\NetCookies	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	409948	HttpSendRequestW
C:\Users\user	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	409948	HttpSendRequestW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	409948	HttpSendRequestW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	object name collision	1	409948	HttpSendRequestW

Disassembly

Code Analysis