

JOeSandbox Cloud BASIC



ID: 413058

Sample Name:

5a866993_by_Libranalysis

Cookbook: default.jbs

Time: 07:13:37

Date: 13/05/2021

Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents	2
Analysis Report 5a866993_by_Libranalysis	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Malware Configuration	4
Threatname: Dridex	4
Yara Overview	4
Memory Dumps	4
Unpacked PEs	4
Sigma Overview	5
Signature Overview	5
AV Detection:	5
Networking:	5
E-Banking Fraud:	5
Malware Analysis System Evasion:	5
Anti Debugging:	5
Mitre Att&ck Matrix	5
Behavior Graph	6
Screenshots	7
Thumbnails	7
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	11
Dropped Files	11
Created / dropped Files	11
Static File Info	12
General	12
File Icon	12
Static PE Info	12
General	12
Entrypoint Preview	12
Data Directories	13
Sections	13
Resources	14
Imports	14
Version Infos	14
Network Behavior	14

Code Manipulations	14
Statistics	14
Behavior	14
System Behavior	15
Analysis Process: loadll32.exe PID: 6032 Parent PID: 5804	15
General	15
File Activities	15
Analysis Process: cmd.exe PID: 6040 Parent PID: 6032	15
General	15
File Activities	16
Analysis Process: rundll32.exe PID: 6012 Parent PID: 6040	16
General	16
File Activities	16
File Read	16
Disassembly	16
Code Analysis	16

Analysis Report 5a866993_by_Libranalysis

Overview

General Information

Sample Name:

5a866993_by_Libranalysis
(renamed file extension from none to dll)

Analysis ID:

413058

MD5:

5a8669939cc5c7...

SHA1:

4c3c6bbbcc0ce1...

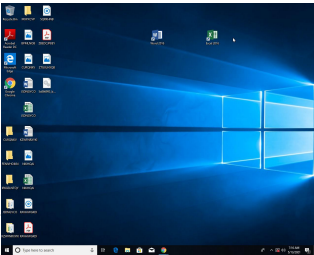
SHA256:

439d76a549397a...

Infos:

Most interesting Screenshot:



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Dridex Dropper

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

Signatures

Dridex dropper found

Found malware configuration

Yara detected Dridex unpacked file

C2 URLs / IPs found in malware con...

Found potential dummy code loops (...)

Machine Learning detection for samp...

Tries to delay execution (extensive O...

Tries to detect sandboxes / dynamic...

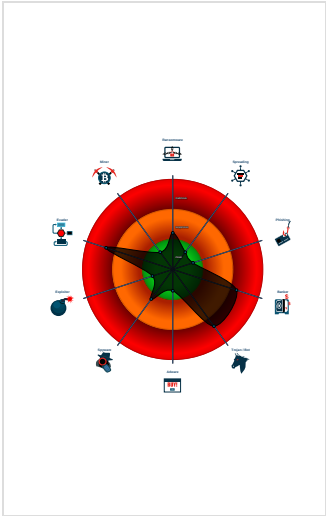
Abnormal high CPU Usage

Checks if the current process is bein...

Contains functionality to call native f...

Contains functionality to check if a d...

Classification



Startup

System is w10x64

 loadaddll32.exe (PID: 6032 cmdline: loadaddll32.exe 'C:\Users\user\Desktop\5a866993_by_Libranalysis.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)

 cmd.exe (PID: 6040 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\5a866993_by_Libranalysis.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)

 rundll32.exe (PID: 6012 cmdline: rundll32.exe 'C:\Users\user\Desktop\5a866993_by_Libranalysis.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)

cleanup

Malware Configuration

Threatname: Dridex

```
{
  "Version": 40112,
  "C2 list": [
    "107.172.227.10:443",
    "172.93.133.123:2303",
    "108.168.61.147:8172"
  ],
  "RC4 keys": [
    "AhGDjKatq80VBsCNBxsJHbQSf84QZXmd170Lw0kGCrK",
    "ZZ9zhvNgYZKhSHVVEDNPVdpdSY2d6pJ4ZBqsvPVEDjy0FNikXQwmhTyNKiurfq"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.593188580.0000000073621000.00000 020.00020000.sdmf	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Unpacked PEs

Copyright Joe Security LLC 2021

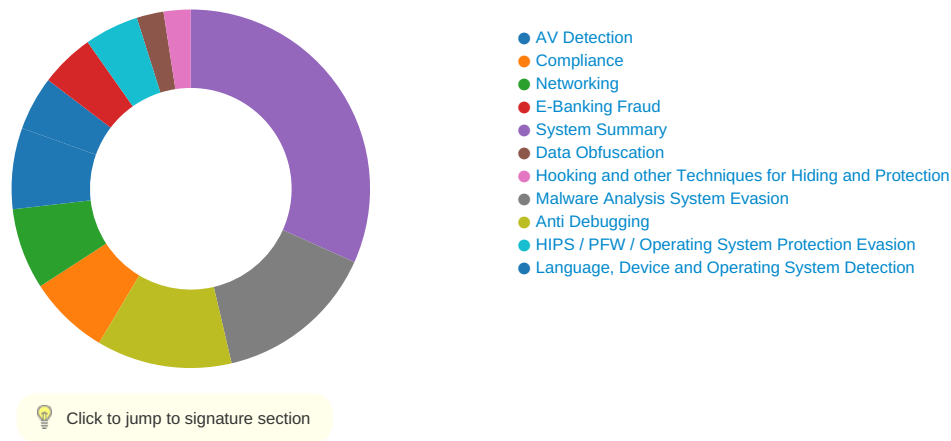
Page 4 of 16

Source	Rule	Description	Author	Strings
2.2.rundll32.exe.73620000.3.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



AV Detection:



Found malware configuration

Machine Learning detection for sample

Networking:



C2 URLs / IPs found in malware configuration

E-Banking Fraud:



Dridex dropper found

Yara detected Dridex unpacked file

Malware Analysis System Evasion:



Tries to delay execution (extensive OutputDebugStringW loop)

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

Anti Debugging:

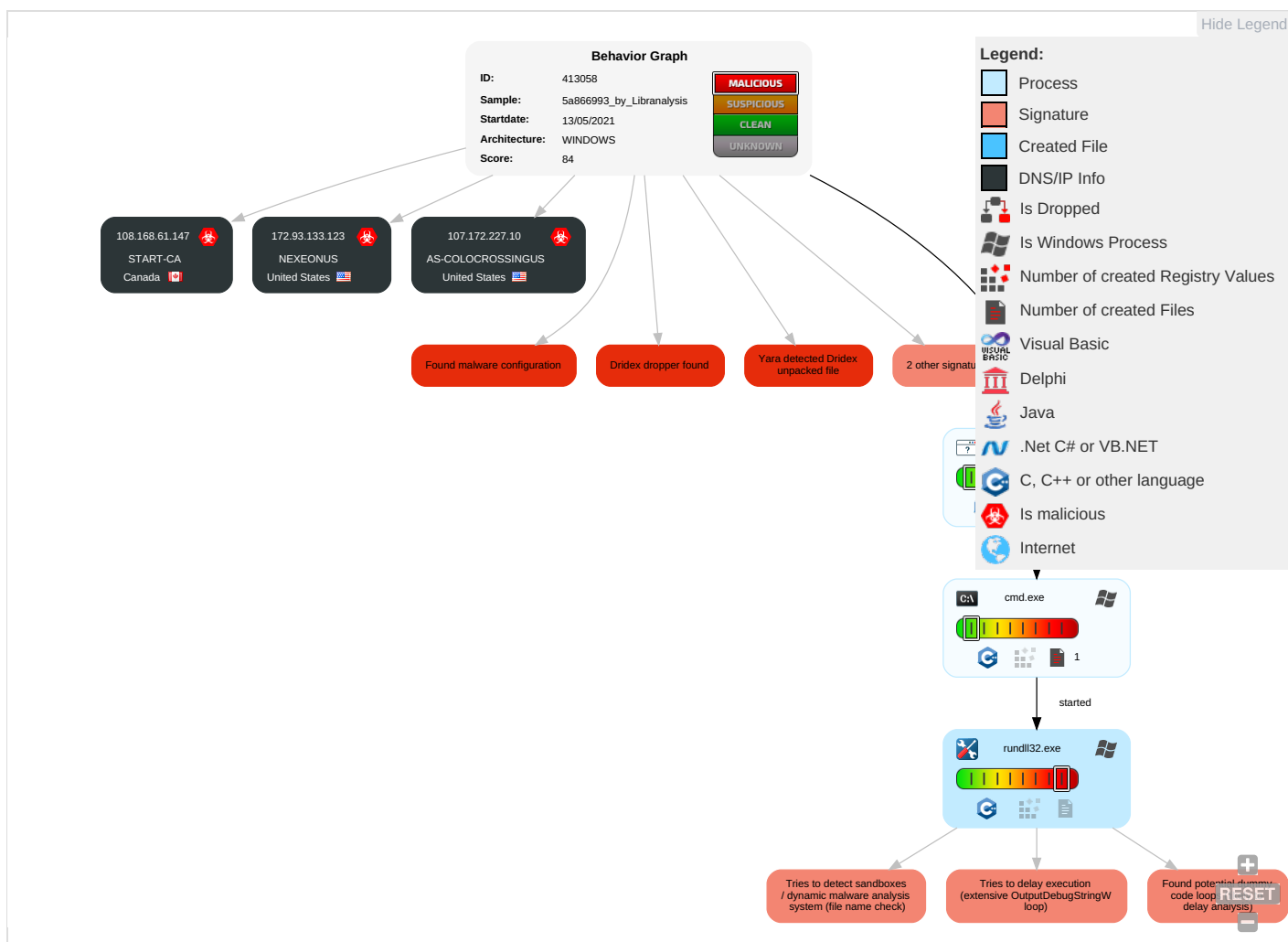


Found potential dummy code loops (likely to delay analysis)

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 1 2	Virtualization/Sandbox Evasion 3 1 1	OS Credential Dumping	Security Software Discovery 2 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	Virtualization/Sandbox Evasion 3 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated 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
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rundll32 1	NTDS	Application Window 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	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Point

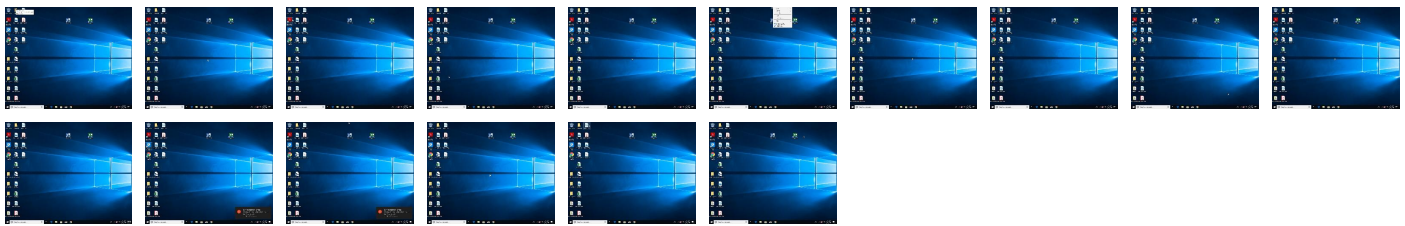
Behavior Graph



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
5a866993_by_Libranalysis.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.rundll32.exe.33a0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		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
172.93.133.123	unknown	United States		20278	NEXEONUS	true
107.172.227.10	unknown	United States		36352	AS-COLOCROSSINGUS	true
108.168.61.147	unknown	Canada		40788	START-CA	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	413058
Start date:	13.05.2021

Start time:	07:13:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	5a866993_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:	8
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.bank.troj.evad.winDLL@5/0@0/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 99.1% (good quality ratio 92.9%) • Quality average: 76.4% • 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

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
172.93.133.123	923fc959_by_Libranalysis.dll	Get hash	malicious	Browse	
	4387387b_by_Libranalysis.dll	Get hash	malicious	Browse	
	88ae0574_by_Libranalysis.dll	Get hash	malicious	Browse	
	6c489f0f_by_Libranalysis.dll	Get hash	malicious	Browse	
	11560b5f_by_Libranalysis.dll	Get hash	malicious	Browse	
	d3caf501_by_Libranalysis.dll	Get hash	malicious	Browse	
	0446dbd6_by_Libranalysis.dll	Get hash	malicious	Browse	
	d604307c_by_Libranalysis.dll	Get hash	malicious	Browse	
	801ae348_by_Libranalysis.dll	Get hash	malicious	Browse	
	465a4420_by_Libranalysis.dll	Get hash	malicious	Browse	
	e04d2479_by_Libranalysis.dll	Get hash	malicious	Browse	
	07060522_by_Libranalysis.dll	Get hash	malicious	Browse	
	651c2dd4_by_Libranalysis.dll	Get hash	malicious	Browse	
	18e87211_by_Libranalysis.dll	Get hash	malicious	Browse	
	c74a9dac_by_Libranalysis.dll	Get hash	malicious	Browse	
	f3f12cfd_by_Libranalysis.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
107.172.227.10	fc70cbd_by_Libranalysis.dll	Get hash	malicious	Browse	
	d67ecd2_by_Libranalysis.dll	Get hash	malicious	Browse	
	6f0c2867_by_Libranalysis.dll	Get hash	malicious	Browse	
	6bf25c84_by_Libranalysis.dll	Get hash	malicious	Browse	
	3d006cd2_by_Libranalysis.dll	Get hash	malicious	Browse	
	923fc959_by_Libranalysis.dll	Get hash	malicious	Browse	
	4387387b_by_Libranalysis.dll	Get hash	malicious	Browse	
	88ae0574_by_Libranalysis.dll	Get hash	malicious	Browse	
	6c489f0f_by_Libranalysis.dll	Get hash	malicious	Browse	
	11560b5f_by_Libranalysis.dll	Get hash	malicious	Browse	
	d3caf501_by_Libranalysis.dll	Get hash	malicious	Browse	
	0446dbd6_by_Libranalysis.dll	Get hash	malicious	Browse	
	d604307c_by_Libranalysis.dll	Get hash	malicious	Browse	
	801ae348_by_Libranalysis.dll	Get hash	malicious	Browse	
	465a4420_by_Libranalysis.dll	Get hash	malicious	Browse	
	e04d2479_by_Libranalysis.dll	Get hash	malicious	Browse	
	07060522_by_Libranalysis.dll	Get hash	malicious	Browse	
	651c2dd4_by_Libranalysis.dll	Get hash	malicious	Browse	
	18e87211_by_Libranalysis.dll	Get hash	malicious	Browse	
	c74a9dac_by_Libranalysis.dll	Get hash	malicious	Browse	
108.168.61.147	f3f12cfd_by_Libranalysis.dll	Get hash	malicious	Browse	
	fc70cbd_by_Libranalysis.dll	Get hash	malicious	Browse	
	d67ecd2_by_Libranalysis.dll	Get hash	malicious	Browse	
	6f0c2867_by_Libranalysis.dll	Get hash	malicious	Browse	
	3d006cd2_by_Libranalysis.dll	Get hash	malicious	Browse	
	923fc959_by_Libranalysis.dll	Get hash	malicious	Browse	
	4387387b_by_Libranalysis.dll	Get hash	malicious	Browse	
	88ae0574_by_Libranalysis.dll	Get hash	malicious	Browse	
	6c489f0f_by_Libranalysis.dll	Get hash	malicious	Browse	
	11560b5f_by_Libranalysis.dll	Get hash	malicious	Browse	
	d3caf501_by_Libranalysis.dll	Get hash	malicious	Browse	
	0446dbd6_by_Libranalysis.dll	Get hash	malicious	Browse	
	d604307c_by_Libranalysis.dll	Get hash	malicious	Browse	
	801ae348_by_Libranalysis.dll	Get hash	malicious	Browse	
	465a4420_by_Libranalysis.dll	Get hash	malicious	Browse	
	e04d2479_by_Libranalysis.dll	Get hash	malicious	Browse	
	07060522_by_Libranalysis.dll	Get hash	malicious	Browse	
	651c2dd4_by_Libranalysis.dll	Get hash	malicious	Browse	
	18e87211_by_Libranalysis.dll	Get hash	malicious	Browse	
	c74a9dac_by_Libranalysis.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-COLOCROSSINGUS	3d006cd2_by_Libranalysis.dll	Get hash	malicious	Browse	107.172.227.10
	923fc959_by_Libranalysis.dll	Get hash	malicious	Browse	107.172.227.10
	4387387b_by_Libranalysis.dll	Get hash	malicious	Browse	107.172.227.10
	88ae0574_by_Libranalysis.dll	Get hash	malicious	Browse	107.172.227.10
	6c489f0f_by_Libranalysis.dll	Get hash	malicious	Browse	107.172.227.10
	11560b5f_by_Libranalysis.dll	Get hash	malicious	Browse	107.172.227.10
	d3caf501_by_Libranalysis.dll	Get hash	malicious	Browse	107.172.227.10
	0446dbd6_by_Libranalysis.dll	Get hash	malicious	Browse	107.172.227.10
	d604307c_by_Libranalysis.dll	Get hash	malicious	Browse	107.172.227.10
	801ae348_by_Libranalysis.dll	Get hash	malicious	Browse	107.172.227.10
	465a4420_by_Libranalysis.dll	Get hash	malicious	Browse	107.172.227.10
	e04d2479_by_Libranalysis.dll	Get hash	malicious	Browse	107.172.227.10

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	07060522_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	651c2dd4_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	18e87211_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	c74a9dac_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	f3f12cfd_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	fc70cbd_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	d67ecdc2_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
	6f0c2867_by_Libranalysis.dll	Get hash	malicious	Browse	• 107.172.227.10
NEXEONUS	3d006cd2_by_Libranalysis.dll	Get hash	malicious	Browse	• 172.93.133.123
	923fc959_by_Libranalysis.dll	Get hash	malicious	Browse	• 172.93.133.123
	4387387b_by_Libranalysis.dll	Get hash	malicious	Browse	• 172.93.133.123
	88ae0574_by_Libranalysis.dll	Get hash	malicious	Browse	• 172.93.133.123
	6c489f0f_by_Libranalysis.dll	Get hash	malicious	Browse	• 172.93.133.123
	11560b5f_by_Libranalysis.dll	Get hash	malicious	Browse	• 172.93.133.123
	d3caf501_by_Libranalysis.dll	Get hash	malicious	Browse	• 172.93.133.123
	0446dbd6_by_Libranalysis.dll	Get hash	malicious	Browse	• 172.93.133.123
	d604307c_by_Libranalysis.dll	Get hash	malicious	Browse	• 172.93.133.123
	801ae348_by_Libranalysis.dll	Get hash	malicious	Browse	• 172.93.133.123
	465a4420_by_Libranalysis.dll	Get hash	malicious	Browse	• 172.93.133.123
	e04d2479_by_Libranalysis.dll	Get hash	malicious	Browse	• 172.93.133.123
	07060522_by_Libranalysis.dll	Get hash	malicious	Browse	• 172.93.133.123
	651c2dd4_by_Libranalysis.dll	Get hash	malicious	Browse	• 172.93.133.123
	18e87211_by_Libranalysis.dll	Get hash	malicious	Browse	• 172.93.133.123
	c74a9dac_by_Libranalysis.dll	Get hash	malicious	Browse	• 172.93.133.123
	f3f12cfd_by_Libranalysis.dll	Get hash	malicious	Browse	• 172.93.133.123
	fc70cbd_by_Libranalysis.dll	Get hash	malicious	Browse	• 172.93.133.123
	d67ecdc2_by_Libranalysis.dll	Get hash	malicious	Browse	• 172.93.133.123
	6f0c2867_by_Libranalysis.dll	Get hash	malicious	Browse	• 172.93.133.123
START-CA	3d006cd2_by_Libranalysis.dll	Get hash	malicious	Browse	• 108.168.61.147
	923fc959_by_Libranalysis.dll	Get hash	malicious	Browse	• 108.168.61.147
	4387387b_by_Libranalysis.dll	Get hash	malicious	Browse	• 108.168.61.147
	88ae0574_by_Libranalysis.dll	Get hash	malicious	Browse	• 108.168.61.147
	6c489f0f_by_Libranalysis.dll	Get hash	malicious	Browse	• 108.168.61.147
	11560b5f_by_Libranalysis.dll	Get hash	malicious	Browse	• 108.168.61.147
	d3caf501_by_Libranalysis.dll	Get hash	malicious	Browse	• 108.168.61.147
	0446dbd6_by_Libranalysis.dll	Get hash	malicious	Browse	• 108.168.61.147
	d604307c_by_Libranalysis.dll	Get hash	malicious	Browse	• 108.168.61.147
	801ae348_by_Libranalysis.dll	Get hash	malicious	Browse	• 108.168.61.147
	465a4420_by_Libranalysis.dll	Get hash	malicious	Browse	• 108.168.61.147
	e04d2479_by_Libranalysis.dll	Get hash	malicious	Browse	• 108.168.61.147
	07060522_by_Libranalysis.dll	Get hash	malicious	Browse	• 108.168.61.147
	651c2dd4_by_Libranalysis.dll	Get hash	malicious	Browse	• 108.168.61.147
	18e87211_by_Libranalysis.dll	Get hash	malicious	Browse	• 108.168.61.147
	c74a9dac_by_Libranalysis.dll	Get hash	malicious	Browse	• 108.168.61.147
	f3f12cfd_by_Libranalysis.dll	Get hash	malicious	Browse	• 108.168.61.147
	fc70cbd_by_Libranalysis.dll	Get hash	malicious	Browse	• 108.168.61.147
	d67ecdc2_by_Libranalysis.dll	Get hash	malicious	Browse	• 108.168.61.147
	6f0c2867_by_Libranalysis.dll	Get hash	malicious	Browse	• 108.168.61.147

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):	7.534900025338564
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:	5a866993_by_Libranalysis.dll
File size:	165888
MD5:	5a8669939cc5c7dc13f95d308fb509a9
SHA1:	4c3c6bbbcc0ce1e5a04a7fb65db30f255f2a9bf5
SHA256:	439d76a549397ad0e6814cec88e82fb5275ade77fd4e40c1834411138f0e3006
SHA512:	3834f56bd01472b5acec05ec4cb5ab8468396e993ec3a7848d8c09a94fa2bd22208e36f45064c50812b6330fe78d8140066f9c6296580ebfe1c4920bc8a150f1
SSDEEP:	3072:DmNFcsGvTmf9vOmoM0IZ5kPjBxYvdIL2KyOQaOP8+cMTH1PxsMYQnF1b1!yLc7UtOpM1Z5k1xYO2LXjTH1pH5nF1p
File Content Preview:	MZ.....@.....b.?.&.Q.&.Q.&.Q.....v.Q.@k..0.Q.+.....Q.8...{.Q./..R.Q./...7.Q..C....Q./...k.Q.@k....Q.&.P...Q..C.,i.Q.H.U...Q.=....Q..i....Q..n....Q...S.,Q...U...Q.....Q.Rich&.Q.....

File Icon

	
Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x40974b
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x609CAFE5 [Thu May 13 04:49:41 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	987b9d7dc84d935c3675da82d40e06f2

Entrypoint Preview

Instruction

```
mov edx, 00000000h
mov edx, 00000000h
cmpss xmm1, xmm2, 03h
sub eax, 00002233h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
```

[illegible]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x1001	0x1001	.text
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa71c	0x59	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2c000	0x390	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x2d000	0x640	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xa04b	0x38	.rdata
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	0xa000	0x50	.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	0x88c2	0x8a00	False	0.426007699275	data	5.59277211248	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xa000	0xb3d	0xa00	False	0.535546875	data	4.25539889565	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pdata	0xb000	0x204a3	0x1e400	False	0.84991606405	data	7.87197522751	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2c000	0x390	0x400	False	0.41796875	data	3.02156416239	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x2d000	0x640	0x800	False	0.6357421875	data	5.25632437688	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x2c060	0x32c	data		

Imports

DLL	Import
USER32.dll	DragDetect, TranslateMessage, EnumDisplayDevicesW, GetMenuState
KERNEL32.dll	GetSystemDefaultUILanguage, GetPriorityClass, GetModuleHandleW, OutputDebugStringA, LoadLibraryA, CloseHandle, LoadLibraryExA
WINTRUST.dll	CryptCATAdminCalcHashFromFileHandle
GDI32.dll	OffsetClipRgn
ADVAPI32.dll	RegLoadAppKeyW, CloseEncryptedFileRaw

Version Infos

Description	Data
LegalCopyright	Copyright 2018
InternalName	ofl
FileVersion	1.3.6923.00
Full Version	1.3.6_000-b00
CompanyName	Oracle Corporation
ProductName	Ofll(EH) Watgevae KT 8
ProductVersion	1.3.6923.00
FileDescription	Java(TM) Platform SE binary
OriginalFilename	ofl.dll
Translation	0x0000 0x04b0

Network Behavior

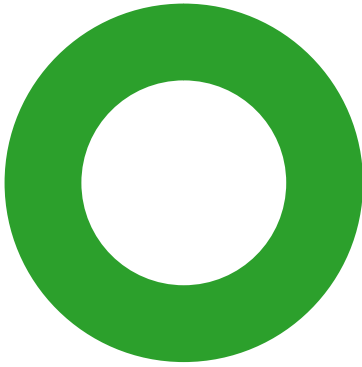
No network behavior found

Code Manipulations

Statistics

Behavior

- loaddll32.exe
- cmd.exe
- rundll32.exe



Click to jump to process

System Behavior

Analysis Process: loadll32.exe PID: 6032 Parent PID: 5804

General

Start time:	07:14:27
Start date:	13/05/2021
Path:	C:\Windows\System32\loadll32.exe
Wow64 process (32bit):	true
Commandline:	loadll32.exe 'C:\Users\user\Desktop\5a866993_by_Libranalysis.dll'
Imagebase:	0x1160000
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: 6040 Parent PID: 6032

General

Start time:	07:14:27
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\5a866993_by_Libranalysis.dll',#1
Imagebase:	0x2a0000
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: 6012 Parent PID: 6040

General

Start time:	07:14:27
Start date:	13/05/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\5a866993_by_Libranalysis.dll',#1
Imagebase:	0x12d0000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000002.00000002.593188580.000000073621000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	73635E36	ReadFile

Disassembly

Code Analysis