ID: 392876
Sample Name: 0WzJdqE4Rw
Cookbook: default.jbs
Time: 23:31:57
Date: 19/04/2021
Version: 31.0.0 Emerald

Table of Contents

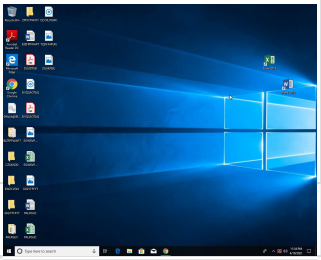
Analysis Report 0WzJdqE4Rw

Overview

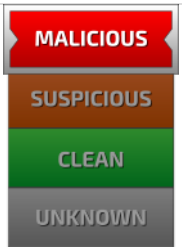
General Information

Sample Name:	0WzJdqE4Rw (renamed file extension from none to dll)
Analysis ID:	392876
MD5:	d596fd09b8431db.
SHA1:	9e436235e8e0e6..
SHA256:	a6bd76295d3032..
Tags:	40112 Dridex
Infos:	

Most interesting Screenshot:



Detection



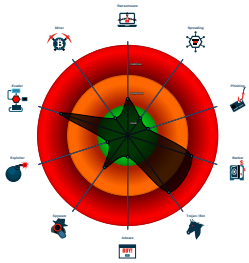
Dridex Dropper

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**
- loaddll32.exe (PID: 5684 cmdline: loaddll32.exe 'C:\Users\user\Desktop\0WzJdqE4Rw.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 5940 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\0WzJdqE4Rw.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5744 cmdline: rundll32.exe 'C:\Users\user\Desktop\0WzJdqE4Rw.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": [
    "AhGDjKatq8OVBsCNBxsJHbQSf84QZXMd170Lw0kGCrK",
    "ZZ9zhvNgYZKh5HVVVEDNPVdpdSY2d6pJ4ZBqsvPVEDjyOFNIkXQwmhTyNKiurfq"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.503419518.000000006DE81000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

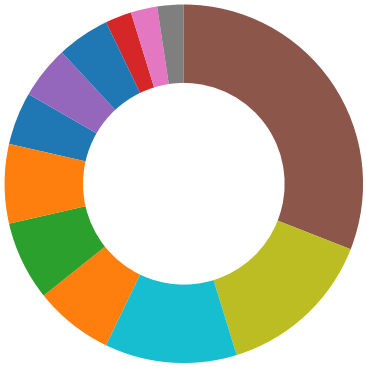
Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.rundll32.exe.6de80000.3.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- 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

Click to jump to signature section

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)

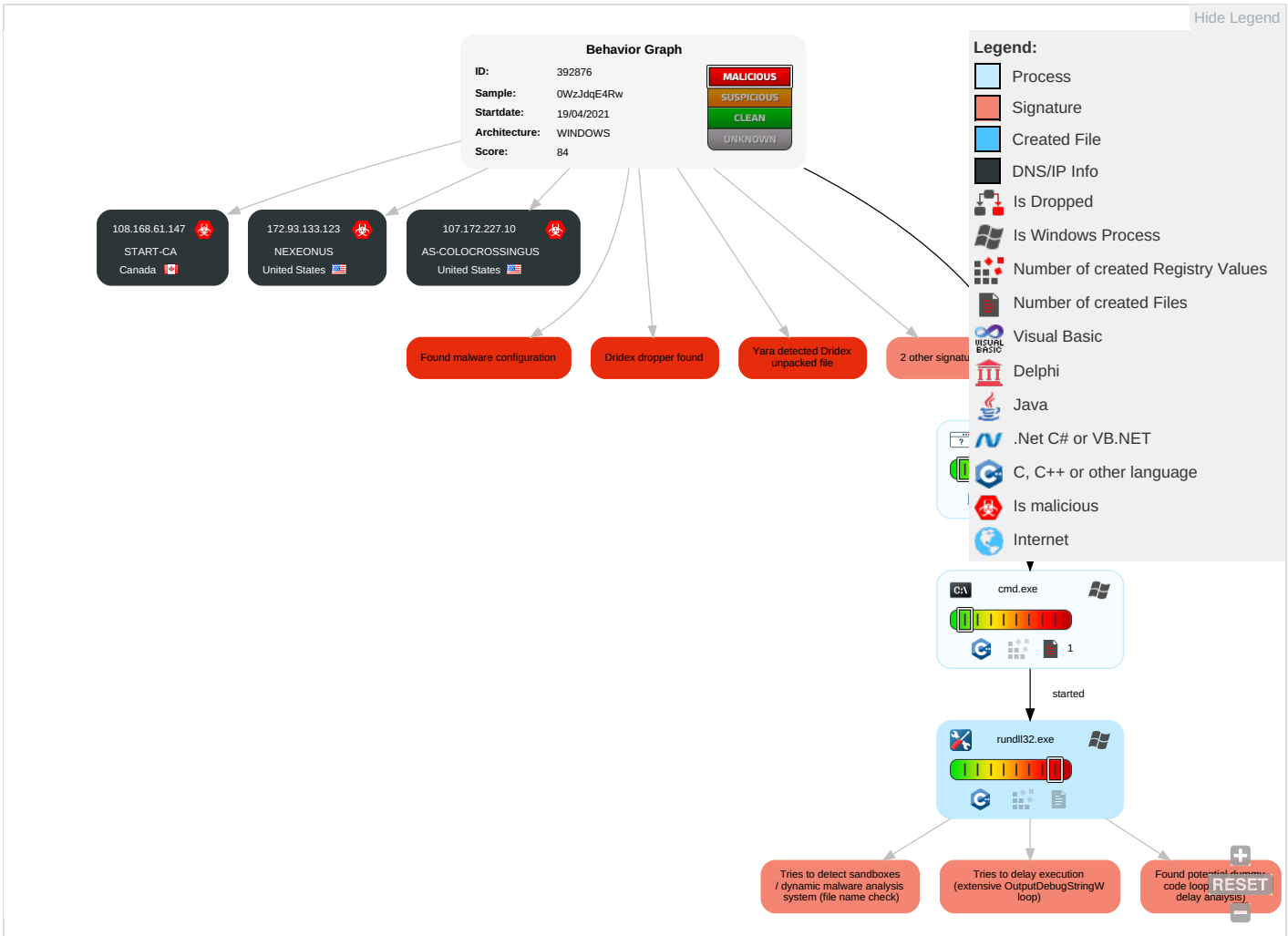
Anti Debugging:

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	Input Capture 1	Security Software Discovery 2 2	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop or Insecure Network Communicati
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	Archive Collected Data 1	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 t Redirect Phor 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 t 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 Communicati
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

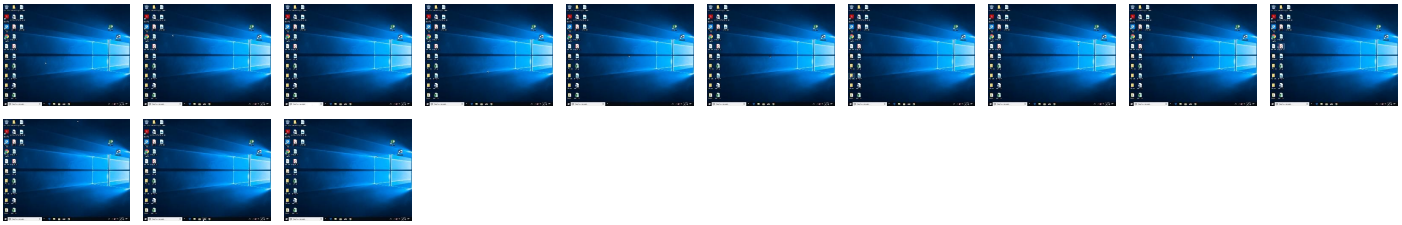
Behavior Graph



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
0WzJdqE4Rw.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.2c30000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

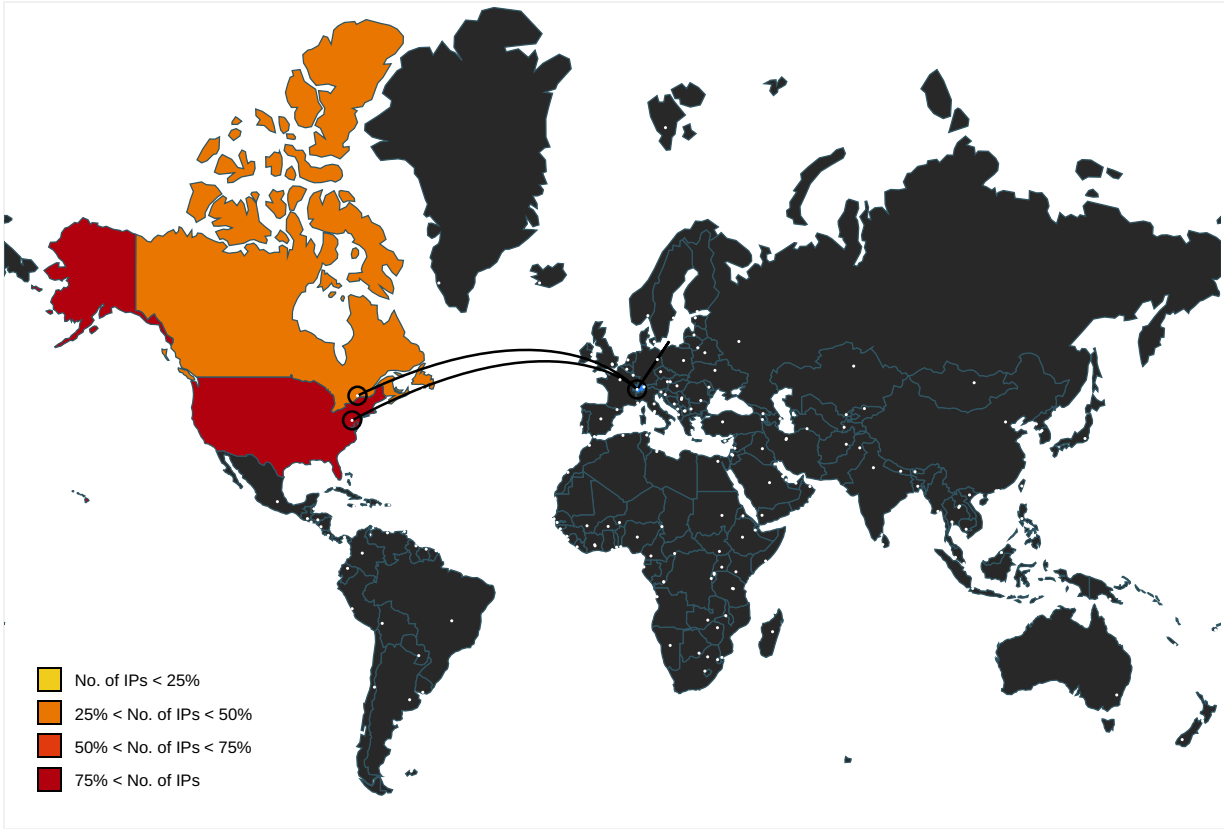
No Antivirus matches

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:	31.0.0 Emerald
Analysis ID:	392876
Start date:	19.04.2021

Start time:	23:31:57
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	0WzJdqE4Rw (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:	24
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:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe

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	3cneNhQXLA.dll	Get hash	malicious	Browse	
	O3Hv20MLTO.dll	Get hash	malicious	Browse	
	3C3QlrM2vJ.dll	Get hash	malicious	Browse	
	JVDmOtlXaN.dll	Get hash	malicious	Browse	
	EyHBhihBLX.dll	Get hash	malicious	Browse	
	9ID7hh46jC.dll	Get hash	malicious	Browse	
	EY5QMIrtiV.dll	Get hash	malicious	Browse	
	3o1SlAow2W.dll	Get hash	malicious	Browse	
	1RQzW0mVpe.dll	Get hash	malicious	Browse	
	n7o1W05MC8.dll	Get hash	malicious	Browse	
	fzs2RFsIyX.dll	Get hash	malicious	Browse	
	rpq7FU7REX.dll	Get hash	malicious	Browse	
	MQaT6y2WR1.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	2AkfHL53PG.dll	Get hash	malicious	Browse	
	yHofZqHUpA.dll	Get hash	malicious	Browse	
	t8gXIfeO1k.dll	Get hash	malicious	Browse	
	bJZDQZ7Yup.dll	Get hash	malicious	Browse	
	4d4QR5t7LQ.dll	Get hash	malicious	Browse	
	KGY6KoZer1.dll	Get hash	malicious	Browse	
	u8UYedd5N8.dll	Get hash	malicious	Browse	
107.172.227.10	3cneNhQXLA.dll	Get hash	malicious	Browse	
	O3Hv20MLTO.dll	Get hash	malicious	Browse	
	3C3QlrM2vJ.dll	Get hash	malicious	Browse	
	JVDmOtlXaN.dll	Get hash	malicious	Browse	
	EyHBhihBLX.dll	Get hash	malicious	Browse	
	9ID7hh46jC.dll	Get hash	malicious	Browse	
	EY5QMIrtiV.dll	Get hash	malicious	Browse	
	3o1SlAow2W.dll	Get hash	malicious	Browse	
	1RQzW0mVpe.dll	Get hash	malicious	Browse	
	n7o1W05MC8.dll	Get hash	malicious	Browse	
	fzs2RFslyX.dll	Get hash	malicious	Browse	
	rpq7FU7REX.dll	Get hash	malicious	Browse	
	MQaT6y2WR1.dll	Get hash	malicious	Browse	
	2AkfHL53PG.dll	Get hash	malicious	Browse	
	yHofZqHUpA.dll	Get hash	malicious	Browse	
	t8gXIfeO1k.dll	Get hash	malicious	Browse	
	bJZDQZ7Yup.dll	Get hash	malicious	Browse	
	4d4QR5t7LQ.dll	Get hash	malicious	Browse	
	KGY6KoZer1.dll	Get hash	malicious	Browse	
	u8UYedd5N8.dll	Get hash	malicious	Browse	
108.168.61.147	3cneNhQXLA.dll	Get hash	malicious	Browse	
	O3Hv20MLTO.dll	Get hash	malicious	Browse	
	3C3QlrM2vJ.dll	Get hash	malicious	Browse	
	JVDmOtlXaN.dll	Get hash	malicious	Browse	
	EyHBhihBLX.dll	Get hash	malicious	Browse	
	9ID7hh46jC.dll	Get hash	malicious	Browse	
	EY5QMIrtiV.dll	Get hash	malicious	Browse	
	3o1SlAow2W.dll	Get hash	malicious	Browse	
	1RQzW0mVpe.dll	Get hash	malicious	Browse	
	n7o1W05MC8.dll	Get hash	malicious	Browse	
	fzs2RFslyX.dll	Get hash	malicious	Browse	
	rpq7FU7REX.dll	Get hash	malicious	Browse	
	MQaT6y2WR1.dll	Get hash	malicious	Browse	
	2AkfHL53PG.dll	Get hash	malicious	Browse	
	yHofZqHUpA.dll	Get hash	malicious	Browse	
	t8gXIfeO1k.dll	Get hash	malicious	Browse	
	bJZDQZ7Yup.dll	Get hash	malicious	Browse	
	4d4QR5t7LQ.dll	Get hash	malicious	Browse	
	KGY6KoZer1.dll	Get hash	malicious	Browse	
	u8UYedd5N8.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-COLOCROSSINGUS	3cneNhQXLA.dll	Get hash	malicious	Browse	• 107.172.227.10
	O3Hv20MLTO.dll	Get hash	malicious	Browse	• 107.172.227.10
	3C3QlrM2vJ.dll	Get hash	malicious	Browse	• 107.172.227.10
	JVDmOtlXaN.dll	Get hash	malicious	Browse	• 107.172.227.10
	EyHBhihBLX.dll	Get hash	malicious	Browse	• 107.172.227.10
	9ID7hh46jC.dll	Get hash	malicious	Browse	• 107.172.227.10
	EY5QMIrtiV.dll	Get hash	malicious	Browse	• 107.172.227.10
	3o1SlAow2W.dll	Get hash	malicious	Browse	• 107.172.227.10
	1RQzW0mVpe.dll	Get hash	malicious	Browse	• 107.172.227.10

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	n7o1W05MC8.dll	Get hash	malicious	Browse	• 107.172.227.10
	fzs2RFsIyX.dll	Get hash	malicious	Browse	• 107.172.227.10
	rpq7FU7REX.dll	Get hash	malicious	Browse	• 107.172.227.10
	MQaT6y2WR1.dll	Get hash	malicious	Browse	• 107.172.227.10
	2AkfHL53PG.dll	Get hash	malicious	Browse	• 107.172.227.10
	yHofZqHUpA.dll	Get hash	malicious	Browse	• 107.172.227.10
	t8gXIfeO1k.dll	Get hash	malicious	Browse	• 107.172.227.10
	bJZDQZ7Yup.dll	Get hash	malicious	Browse	• 107.172.227.10
	4d4QR5t7LQ.dll	Get hash	malicious	Browse	• 107.172.227.10
	KGY6KoZer1.dll	Get hash	malicious	Browse	• 107.172.227.10
	u8UYedd5N8.dll	Get hash	malicious	Browse	• 107.172.227.10
NEXEONUS	3cneNhQXLA.dll	Get hash	malicious	Browse	• 172.93.133.123
	O3Hv20MLTO.dll	Get hash	malicious	Browse	• 172.93.133.123
	3C3QlrM2vJ.dll	Get hash	malicious	Browse	• 172.93.133.123
	JVDmOtlXaN.dll	Get hash	malicious	Browse	• 172.93.133.123
	EyHBhihBLX.dll	Get hash	malicious	Browse	• 172.93.133.123
	9ID7hh46jC.dll	Get hash	malicious	Browse	• 172.93.133.123
	EY5QMIrtiV.dll	Get hash	malicious	Browse	• 172.93.133.123
	3o1SlAow2W.dll	Get hash	malicious	Browse	• 172.93.133.123
	1RQzW0mVpe.dll	Get hash	malicious	Browse	• 172.93.133.123
	n7o1W05MC8.dll	Get hash	malicious	Browse	• 172.93.133.123
	fzs2RFsIyX.dll	Get hash	malicious	Browse	• 172.93.133.123
	rpq7FU7REX.dll	Get hash	malicious	Browse	• 172.93.133.123
	MQaT6y2WR1.dll	Get hash	malicious	Browse	• 172.93.133.123
	2AkfHL53PG.dll	Get hash	malicious	Browse	• 172.93.133.123
	yHofZqHUpA.dll	Get hash	malicious	Browse	• 172.93.133.123
	t8gXIfeO1k.dll	Get hash	malicious	Browse	• 172.93.133.123
	bJZDQZ7Yup.dll	Get hash	malicious	Browse	• 172.93.133.123
	4d4QR5t7LQ.dll	Get hash	malicious	Browse	• 172.93.133.123
	KGY6KoZer1.dll	Get hash	malicious	Browse	• 172.93.133.123
	u8UYedd5N8.dll	Get hash	malicious	Browse	• 172.93.133.123
START-CA	3cneNhQXLA.dll	Get hash	malicious	Browse	• 108.168.61.147
	O3Hv20MLTO.dll	Get hash	malicious	Browse	• 108.168.61.147
	3C3QlrM2vJ.dll	Get hash	malicious	Browse	• 108.168.61.147
	JVDmOtlXaN.dll	Get hash	malicious	Browse	• 108.168.61.147
	EyHBhihBLX.dll	Get hash	malicious	Browse	• 108.168.61.147
	9ID7hh46jC.dll	Get hash	malicious	Browse	• 108.168.61.147
	EY5QMIrtiV.dll	Get hash	malicious	Browse	• 108.168.61.147
	3o1SlAow2W.dll	Get hash	malicious	Browse	• 108.168.61.147
	1RQzW0mVpe.dll	Get hash	malicious	Browse	• 108.168.61.147
	n7o1W05MC8.dll	Get hash	malicious	Browse	• 108.168.61.147
	fzs2RFsIyX.dll	Get hash	malicious	Browse	• 108.168.61.147
	rpq7FU7REX.dll	Get hash	malicious	Browse	• 108.168.61.147
	MQaT6y2WR1.dll	Get hash	malicious	Browse	• 108.168.61.147
	2AkfHL53PG.dll	Get hash	malicious	Browse	• 108.168.61.147
	yHofZqHUpA.dll	Get hash	malicious	Browse	• 108.168.61.147
	t8gXIfeO1k.dll	Get hash	malicious	Browse	• 108.168.61.147
	bJZDQZ7Yup.dll	Get hash	malicious	Browse	• 108.168.61.147
	4d4QR5t7LQ.dll	Get hash	malicious	Browse	• 108.168.61.147
	KGY6KoZer1.dll	Get hash	malicious	Browse	• 108.168.61.147
	u8UYedd5N8.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):	7.534911371173021
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:	0WzJdqE4Rw.dll
File size:	165888
MD5:	d596fd09b8431db69ac77ffdfd138f3f
SHA1:	9e436235e8e0e6f0c0a87ebd4b0d53688a7b994c
SHA256:	a6bd76295d3032edba531572417b1349bb4ba8d167fa593d954fd7dcc63cb2ca
SHA512:	8a7fedd4751d2f03c353b061ddbdbe046e7d6ba20e453fe490cda0389e689b286738e181c62fe2f66da800ddfc6928c2c787df5c643648070f092520b113bbf7
SSDEEP:	3072:KmNFcsGvTmf9vOmoM0IZ5kPjBxYvdIL2KyOQaOP8+cMTH1PxsMYQnF1b1l:bLc7UtOpM1Z5k1xYO2LXjTH1pH5nF1p
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:	0x607DE63B [Mon Apr 19 20:21:15 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

Instruction
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
mov edx, 00000000h
cmpss xmm1, xmm2, 03h
cmp edx, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
je 00007FB218E01DB3h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h
mov eax, 00000000h

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	0x958	0xa00	False	0.535546875	data	4.25539889565	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.pdata	0xb000	0x20a39	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
.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: loaddll32.exe PID: 5684 Parent PID: 5572

General

Start time:	23:32:51
Start date:	19/04/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\0WzJdqE4Rw.dll'
Imagebase:	0xb50000
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: 5940 Parent PID: 5684

General

Start time:	23:32:52
Start date:	19/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\0WzJdqE4Rw.dll',#1
Imagebase:	0x150000
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: 5744 Parent PID: 5940

General

Start time:	23:32:52
Start date:	19/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\0WzJdqE4Rw.dll',#1
Imagebase:	0xe0000
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: 00000003.00000002.503419518.000000006DE81000.00000020.00020000.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	6DE95E36	ReadFile

Disassembly

Code Analysis