ID: 606301
Sample Name:
WOTZc2nssO.exe
Cookbook: default.jbs
Time: 20:19:08
Date: 09/04/2022
Version: 34.0.0 Boulder Opal

Table of Contents

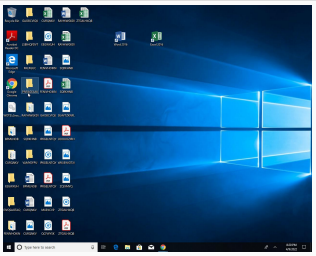
Windows Analysis Report

WOTZc2nssO.exe

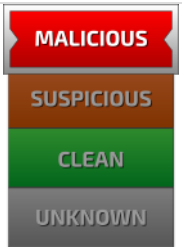
Overview

General Information

Sample Name:	WOTZc2nssO.exe (renamed file extension from exe to dll)
Analysis ID:	606301
MD5:	ba33bff302fdecf…
SHA1:	f422c218c50549…
SHA256:	55f53b1d9dac90..
Tags:	dll Dridex
Infos:	YARA SIGMA



Detection



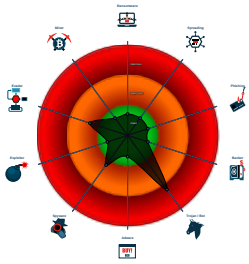
Dridex

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Yara detected Dridex unpacked file
- Multi AV Scanner detection for subm…
- Sigma detected: Suspicious Call by…
- Creates a DirectInput object (often f…
- Uses 32bit PE files
- Sample file is different than original …
- PE file contains strange resources
- Program does not show much activi…
- Creates a process in suspended mo…
- Checks if the current process is bei…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 3260 cmdline: loaddll32.exe "C:\Users\user\Desktop\WOTZc2nssO.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 5784 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\WOTZc2nssO.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 1356 cmdline: rundll32.exe "C:\Users\user\Desktop\WOTZc2nssO.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
WOTZc2nssO.dll	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Sigma Signatures

System Summary

Sigma detected: Suspicious Call by Ordinal

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

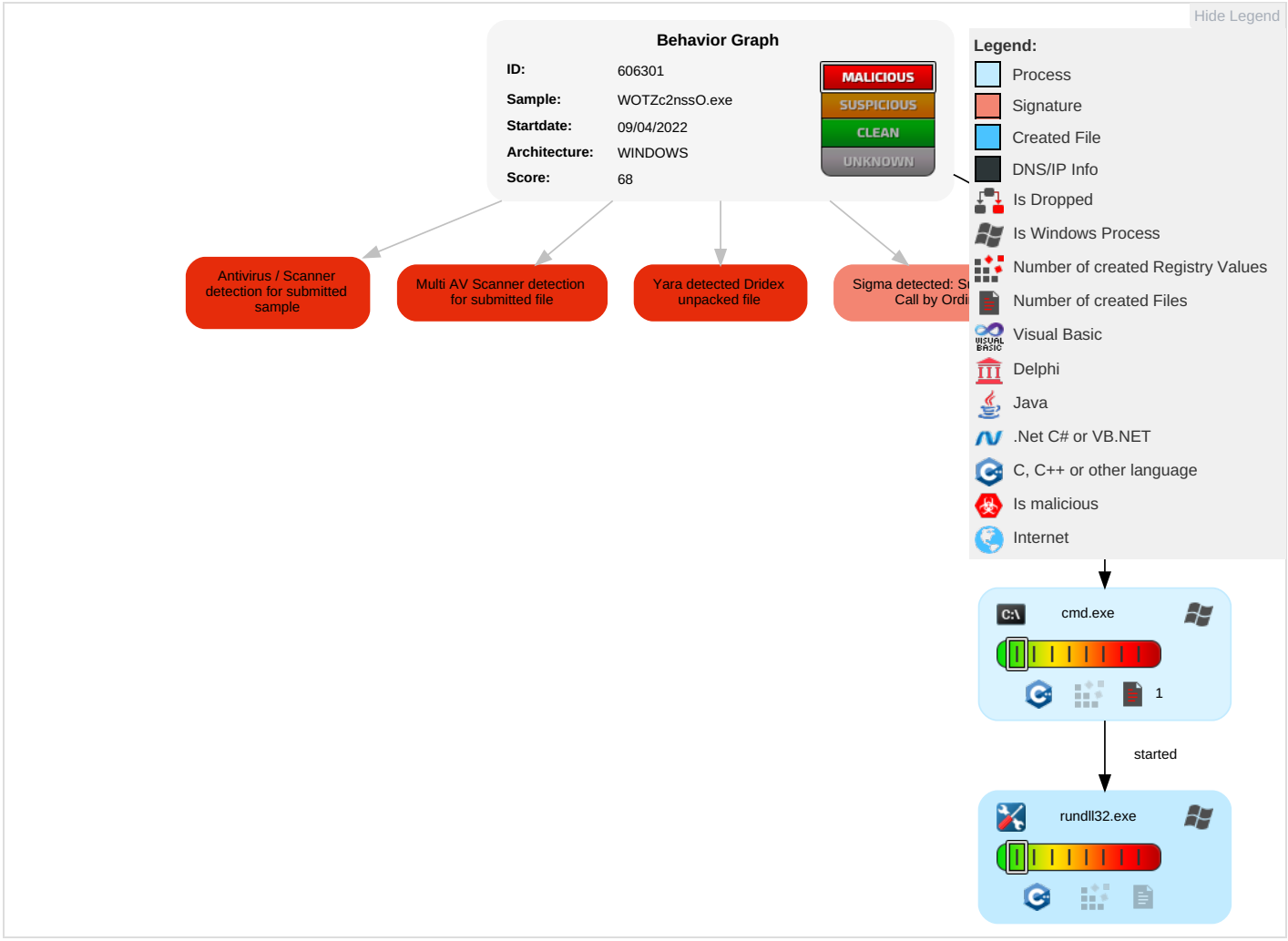
E-Banking Fraud

Yara detected Dridex unpacked file

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	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 1 Process Injection	1 Virtualization/Sandbox Evasion	1 Input Capture	1 Security Software Discovery	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Rundll32	LSASS Memory	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 Process Injection	Security Account Manager	1 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

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
WOTZc2nssO.dll	41%	Virustotal		Browse
WOTZc2nssO.dll	71%	ReversingLabs	Win32.Infostealer.Dridex	
WOTZc2nssO.dll	100%	Avira	HEUR/AGEN.1214843	

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

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	606301
Start date and time: 09/04/202220:19:08	2022-04-09 20:19:08 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	WOTZc2nssO.exe (renamed file extension from exe 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:	3
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:	mal68.troj.winDLL@5/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Stop behavior analysis, all processes terminated

Warnings

- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

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):	6.038106926488256
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:	WOTZc2nssO.dll
File size:	135168
MD5:	ba33bff302fdecf939ed96296d93593f
SHA1:	f422c218c50549a380234e6c57231e95a5774371
SHA256:	55f53b1d9dac903d695b48f52894117a87acd81c1c10fc6eafb6dad5d6bc28b4
SHA512:	3ca1e38a95818811f15aedd86bd202e4e698600e3a9143c338b4908ca8b5890f9f7a81f75df7f4337b1331de4e49428dd17d996bd21691e600385f67afcaabbf
SSDEEP:	3072:W3sOOO1kCH3gxtJC8UDqYfGbKDkvKjxCy:W3sOl1kqOC8U/6Ikyjx
TLSH:	E4D38D02F68382F6ED93A9B0091E667FE7715D0A45749399C3E57E66E433230E73A342
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..R.o..B..R.j..B...B...B..R.q..B..*+...B...B..*+...B..*+^..B..*+...B..Rich.B.....PE..L....R.a.....

File Icon

Icon Hash:	f9e0f484c2d0fc0e

Static PE Info

General	
Entrypoint:	0x5c0000
Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x5c0000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61AA52E1 [Fri Dec 3 17:24:49 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:	68b66fd5fe2322f1f5fcb9cf4ede12bd

Entrypoint Preview
Instruction
dec ebp
pop edx
nop
add byte ptr [ebx], al
add byte ptr [eax], al
add byte ptr [eax+eax], al
add byte ptr [eax], al

Data Directories			
Name	**Virtual Address**	**Virtual Size**	**Is in Section**
IMAGE_DIRECTORY_ENTRY_EXPORT	0x1c9a0	0x178	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1cc38	0x50	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1f000	0x9b0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1c980	0x1c	.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	0x1a000	0x60	.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	0x19000	0x19000	False	0.5660546875	data	6.34871846727	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x1a000	0x3000	0x3000	False	0.873779296875	Dyalog APL component file 64-bit non-journaled checksummed version 199.119	7.49659019864	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x1d000	0x1000	0x1000	False	0.151123046875	DOS executable (block device driver)	1.60850107338	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.CRT	0x1e000	0x1000	0x1000	False	0.0078125	ASCII text, with no line terminators	0.00984533685143	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x1f000	0x1000	0x1000	False	0.24951171875	data	2.91667869163	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x20000	0x1000	0x1000	False	0.161376953125	GLS_BINARY_LSB_FIRST	1.48069807529	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1f0e8	0x568	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x1f650	0x14	data		
RT_VERSION	0x1f668	0x344	data		

Imports

DLL	Import
KERNEL32.dll	LCMapStringA, IsBadReadPtr, HeapValidate, GetStringTypeA, GetStartupInfoA, GetLocaleInfoA, LoadLibraryA, GetConsoleOutputCP, FreeEnvironmentStringsA, FlushFileBuffers, DebugBreak, CreateFileA, GetLastError, GetEnvironmentStrings, OutputDebugStringA
USER32.dll	MessageBoxW
ADVAPI32.dll	GetUserNameW

Exports

Name	Ordinal	Address
CreateExecutivePlatform	2	0x5d78dc
DllCanUnloadNow	3	0x5d93d4
DllGetClassObject	4	0x5cdce5
DllRegisterServer	5	0x5c21c8
DllUnregisterServer	6	0x5cbdd1

Version Infos

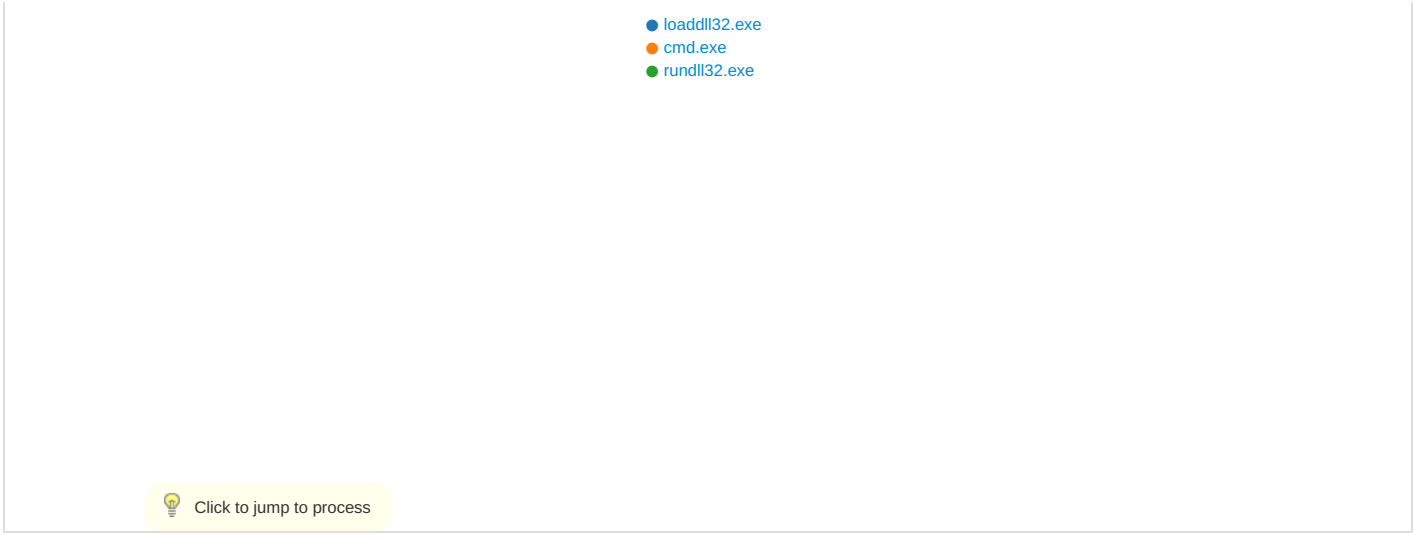
Description	Data
LegalCopyright	Copyright 2016-2021
InternalName	Target Corporation
FileVersion	2.1.66
CompanyName	Paramount Pictures
LegalTrademarks	Paramount Pictures
Comments	3.1.100
ProductName	Staples
ProductVersion	6.0.20
FileDescription	5.6.46
OriginalFilename	TESTAPP.EXE
Translation	0x0409 0x04e4

Network Behavior

No network behavior found

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: **3260**, Parent PID: **1724**

General	
Target ID:	0
Start time:	20:20:09
Start date:	09/04/2022
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\WOTZc2nssO.dll"
Imagebase:	0xd70000
File size:	116736 bytes
MD5 hash:	7DEB5DB86C0AC789123DEC286286B938
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: **5784**, Parent PID: **3260**

General	
Target ID:	1
Start time:	20:20:10
Start date:	09/04/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\WOTZc2nssO.dll",#1
Imagebase:	0x1190000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **1356**, Parent PID: **5784**

General

Target ID:	2
Start time:	20:20:10
Start date:	09/04/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\WOTZc2nssO.dll",#1
Imagebase:	0x70000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly