ID: 392875
Sample Name: P0DNoD3M7G
Cookbook: default.jbs
Time: 23:31:56
Date: 19/04/2021
Version: 31.0.0 Emerald

Table of Contents

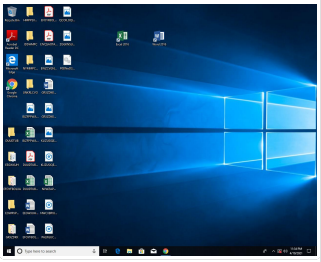
Analysis Report P0DNoD3M7G

Overview

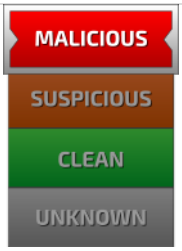
General Information

Sample Name:	P0DNoD3M7G (renamed file extension from none to dll)
Analysis ID:	392875
MD5:	6132233b774e37..
SHA1:	b32ab2153285df6.
SHA256:	34bfcb0fa8c5d49..
Tags:	40112 Dridex
Infos:	

Most interesting Screenshot:



Detection



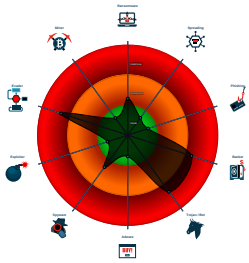
Dridex Dropper

Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Dridex dropper found
- Found malware configuration
- Multi AV Scanner detection for subm…
- 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
- Antivirus or Machine Learning detec…
- 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: 912 cmdline: loaddll32.exe 'C:\Users\user\Desktop\P0DNoD3M7G.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 2396 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\P0DNoD3M7G.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5596 cmdline: rundll32.exe 'C:\Users\user\Desktop\P0DNoD3M7G.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- **cleanup**

Malware Configuration

Threatname: Dridex


```
{
  "Version": 40112,
  "C2 list": [
    "8.210.53.215:443",
    "72.249.22.245:2303",
    "188.40.137.206:8172"
  ],
  "RC4 keys": [
    "RL2wu3FXHUGPGOtIL6lP6N0VZhCf8JeWK7yz9s",
    "hv0xsKjSe3xEYSnSvgjXlHRW9ricyO0t9ZWgJA8A1xjwSsIZgs78qb4LqGAl5z9P2rtE"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
00000003.00000002.488352077.0000000070A91000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

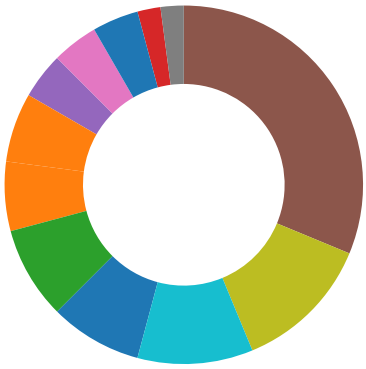
Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.rundll32.exe.70a90000.3.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

Multi AV Scanner detection for submitted file

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)

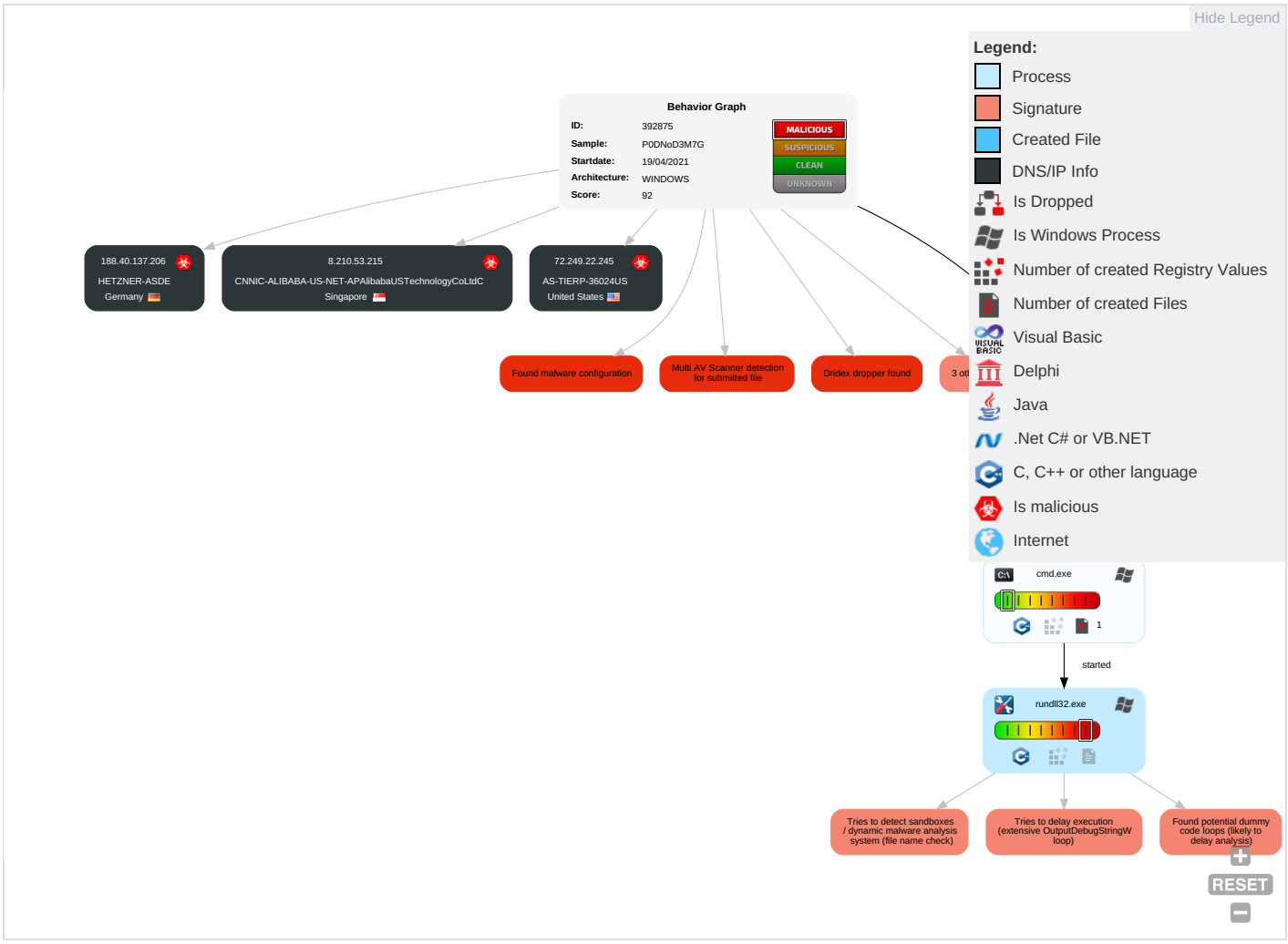
Anti Debugging:

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 Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	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 3	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

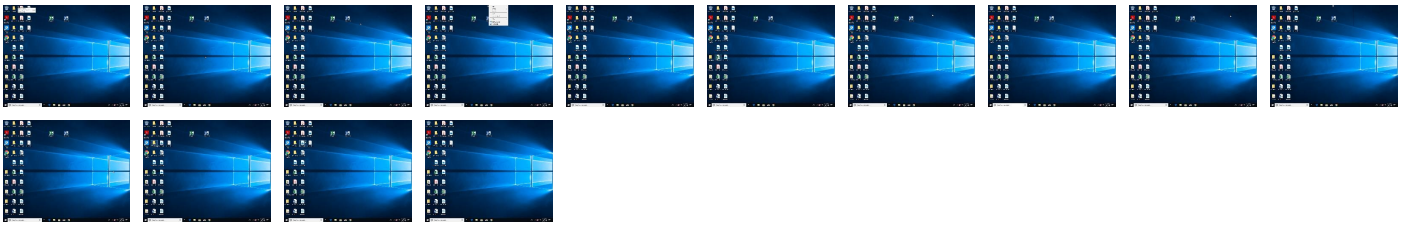
Behavior Graph



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
P0DNoD3M7G.dll	63%	Virustotal		Browse
P0DNoD3M7G.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.ea0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
3.2.rundll32.exe.e803d4.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://ansicon.adoxa.vze.com/6	loaddll32.exe, 00000000.00000002.218272982.0000000070ABB000.00000002.00020000.sdmp, P0DNoD3M7G.dll	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
72.249.22.245	unknown	United States		36024	AS-TIERP-36024US	true
188.40.137.206	unknown	Germany		24940	HETZNER-ASDE	true
8.210.53.215	unknown	Singapore		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	392875
Start date:	19.04.2021
Start time:	23:31:56
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 27s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	P0DNoD3M7G (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:	23
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:	mal92.bank.troj.evad.winDLL@5/0@0/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 51.7% (good quality ratio 48.5%) • Quality average: 78.6% • Quality standard deviation: 28.7%
HCA Information:	• Successful, ratio: 88% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
72.249.22.245	Em37gCCOY4.dll	Get hash	malicious	Browse	
	nNBe3YZPD1.dll	Get hash	malicious	Browse	
	rECHXI23ab.dll	Get hash	malicious	Browse	
	u3ZfUNqtTA.dll	Get hash	malicious	Browse	
	i2mWN0eEZi.dll	Get hash	malicious	Browse	
	mbhe8pot46.dll	Get hash	malicious	Browse	
	BVB6FskvT6.dll	Get hash	malicious	Browse	
	LqV2hePJuc.dll	Get hash	malicious	Browse	
	TmWrP3Q5GS.dll	Get hash	malicious	Browse	
	FsfUPJt3ju.dll	Get hash	malicious	Browse	
	rqNx5BpAOZ.dll	Get hash	malicious	Browse	
	F9yKzoQC8A.dll	Get hash	malicious	Browse	
	g4TMqcOd80.dll	Get hash	malicious	Browse	
	x2F4br2kxL.dll	Get hash	malicious	Browse	
	89qYKQ34j2.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	s9SjdUrdoD.dll	Get hash	malicious	Browse	
	341sWszBlb.dll	Get hash	malicious	Browse	
	7MY4BnDZbU.dll	Get hash	malicious	Browse	
	TfxSPxK2fz.dll	Get hash	malicious	Browse	
	ri9xYZlG5g.dll	Get hash	malicious	Browse	
188.40.137.206	Em37gCCOY4.dll	Get hash	malicious	Browse	
	nNBe3YZPD1.dll	Get hash	malicious	Browse	
	rECHXI23ab.dll	Get hash	malicious	Browse	
	u3ZfUNqtTA.dll	Get hash	malicious	Browse	
	i2mWN0eEZi.dll	Get hash	malicious	Browse	
	mbhe8pot46.dll	Get hash	malicious	Browse	
	BVB6FskvT6.dll	Get hash	malicious	Browse	
	LqV2hePJuc.dll	Get hash	malicious	Browse	
	TmWrP3Q5GS.dll	Get hash	malicious	Browse	
	FsfUPJt3ju.dll	Get hash	malicious	Browse	
	rqNx5BpAOZ.dll	Get hash	malicious	Browse	
	F9yKzoQC8A.dll	Get hash	malicious	Browse	
	g4TMqcOd80.dll	Get hash	malicious	Browse	
	x2F4br2kxL.dll	Get hash	malicious	Browse	
	89qYKQ34j2.dll	Get hash	malicious	Browse	
	s9SjdUrdoD.dll	Get hash	malicious	Browse	
	341sWszBlb.dll	Get hash	malicious	Browse	
	7MY4BnDZbU.dll	Get hash	malicious	Browse	
	TfxSPxK2fz.dll	Get hash	malicious	Browse	
	ri9xYZlG5g.dll	Get hash	malicious	Browse	
8.210.53.215	Em37gCCOY4.dll	Get hash	malicious	Browse	
	nNBe3YZPD1.dll	Get hash	malicious	Browse	
	rECHXI23ab.dll	Get hash	malicious	Browse	
	u3ZfUNqtTA.dll	Get hash	malicious	Browse	
	i2mWN0eEZi.dll	Get hash	malicious	Browse	
	mbhe8pot46.dll	Get hash	malicious	Browse	
	BVB6FskvT6.dll	Get hash	malicious	Browse	
	LqV2hePJuc.dll	Get hash	malicious	Browse	
	TmWrP3Q5GS.dll	Get hash	malicious	Browse	
	FsfUPJt3ju.dll	Get hash	malicious	Browse	
	rqNx5BpAOZ.dll	Get hash	malicious	Browse	
	F9yKzoQC8A.dll	Get hash	malicious	Browse	
	g4TMqcOd80.dll	Get hash	malicious	Browse	
	x2F4br2kxL.dll	Get hash	malicious	Browse	
	89qYKQ34j2.dll	Get hash	malicious	Browse	
	s9SjdUrdoD.dll	Get hash	malicious	Browse	
	341sWszBlb.dll	Get hash	malicious	Browse	
	7MY4BnDZbU.dll	Get hash	malicious	Browse	
	TfxSPxK2fz.dll	Get hash	malicious	Browse	
	ri9xYZlG5g.dll	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	Em37gCCOY4.dll	Get hash	malicious	Browse	• 8.210.53.215
	nNBe3YZPD1.dll	Get hash	malicious	Browse	• 8.210.53.215
	rECHXI23ab.dll	Get hash	malicious	Browse	• 8.210.53.215
	u3ZfUNqtTA.dll	Get hash	malicious	Browse	• 8.210.53.215
	i2mWN0eEZi.dll	Get hash	malicious	Browse	• 8.210.53.215
	mbhe8pot46.dll	Get hash	malicious	Browse	• 8.210.53.215
	BVB6FskvT6.dll	Get hash	malicious	Browse	• 8.210.53.215
	LqV2hePJuc.dll	Get hash	malicious	Browse	• 8.210.53.215
	TmWrP3Q5GS.dll	Get hash	malicious	Browse	• 8.210.53.215
	FsfUPJt3ju.dll	Get hash	malicious	Browse	• 8.210.53.215
	rqNx5BpAOZ.dll	Get hash	malicious	Browse	• 8.210.53.215

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	F9yKzoQC8A.dll	Get hash	malicious	Browse	• 8.210.53.215
	g4TMqcOd80.dll	Get hash	malicious	Browse	• 8.210.53.215
	x2F4br2kxL.dll	Get hash	malicious	Browse	• 8.210.53.215
	89qYKQ34j2.dll	Get hash	malicious	Browse	• 8.210.53.215
	s9SjdUrdoD.dll	Get hash	malicious	Browse	• 8.210.53.215
	341sWszBlb.dll	Get hash	malicious	Browse	• 8.210.53.215
	7MY4BnDZbU.dll	Get hash	malicious	Browse	• 8.210.53.215
	TfxSPxK2fz.dll	Get hash	malicious	Browse	• 8.210.53.215
	ri9xYZlG5g.dll	Get hash	malicious	Browse	• 8.210.53.215
AS-TIERP-36024US	Em37gCCOY4.dll	Get hash	malicious	Browse	• 72.249.22.245
	nNBe3YZPD1.dll	Get hash	malicious	Browse	• 72.249.22.245
	rECHXI23ab.dll	Get hash	malicious	Browse	• 72.249.22.245
	u3ZfUNqtTA.dll	Get hash	malicious	Browse	• 72.249.22.245
	i2mWN0eEZi.dll	Get hash	malicious	Browse	• 72.249.22.245
	mbhe8pot46.dll	Get hash	malicious	Browse	• 72.249.22.245
	BVB6FskvT6.dll	Get hash	malicious	Browse	• 72.249.22.245
	LqV2hePJuc.dll	Get hash	malicious	Browse	• 72.249.22.245
	TmWrP3Q5GS.dll	Get hash	malicious	Browse	• 72.249.22.245
	FsfUPJt3ju.dll	Get hash	malicious	Browse	• 72.249.22.245
	rqNx5BpAOZ.dll	Get hash	malicious	Browse	• 72.249.22.245
	F9yKzoQC8A.dll	Get hash	malicious	Browse	• 72.249.22.245
	g4TMqcOd80.dll	Get hash	malicious	Browse	• 72.249.22.245
	x2F4br2kxL.dll	Get hash	malicious	Browse	• 72.249.22.245
	89qYKQ34j2.dll	Get hash	malicious	Browse	• 72.249.22.245
	s9SjdUrdoD.dll	Get hash	malicious	Browse	• 72.249.22.245
	341sWszBlb.dll	Get hash	malicious	Browse	• 72.249.22.245
	7MY4BnDZbU.dll	Get hash	malicious	Browse	• 72.249.22.245
	TfxSPxK2fz.dll	Get hash	malicious	Browse	• 72.249.22.245
	ri9xYZlG5g.dll	Get hash	malicious	Browse	• 72.249.22.245
HETZNER-ASDE	Em37gCCOY4.dll	Get hash	malicious	Browse	• 188.40.137.206
	nNBe3YZPD1.dll	Get hash	malicious	Browse	• 188.40.137.206
	AnyDesk.exe	Get hash	malicious	Browse	• 116.202.17 2.152
	rECHXI23ab.dll	Get hash	malicious	Browse	• 188.40.137.206
	u3ZfUNqtTA.dll	Get hash	malicious	Browse	• 188.40.137.206
	i2mWN0eEZi.dll	Get hash	malicious	Browse	• 188.40.137.206
	mbhe8pot46.dll	Get hash	malicious	Browse	• 188.40.137.206
	BVB6FskvT6.dll	Get hash	malicious	Browse	• 188.40.137.206
	LqV2hePJuc.dll	Get hash	malicious	Browse	• 188.40.137.206
	TmWrP3Q5GS.dll	Get hash	malicious	Browse	• 188.40.137.206
	FsfUPJt3ju.dll	Get hash	malicious	Browse	• 188.40.137.206
	rqNx5BpAOZ.dll	Get hash	malicious	Browse	• 188.40.137.206
	F9yKzoQC8A.dll	Get hash	malicious	Browse	• 188.40.137.206
	shipping document.exe	Get hash	malicious	Browse	• 144.76.118.195
	g4TMqcOd80.dll	Get hash	malicious	Browse	• 188.40.137.206
	x2F4br2kxL.dll	Get hash	malicious	Browse	• 188.40.137.206
	89qYKQ34j2.dll	Get hash	malicious	Browse	• 188.40.137.206
	s9SjdUrdoD.dll	Get hash	malicious	Browse	• 188.40.137.206
	341sWszBlb.dll	Get hash	malicious	Browse	• 188.40.137.206
	7MY4BnDZbU.dll	Get hash	malicious	Browse	• 188.40.137.206

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):	7.546572177323037
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:	P0DNoD3M7G.dll
File size:	162304
MD5:	6132233b774e373cf727e90a84fbbd14
SHA1:	b32ab2153285df6a2e3bdd130f966426c538726e
SHA256:	34bfcb0fa8c5d49dd601ea9134bb77ed4d2be8bd6782f713183faed72ffcdfaa
SHA512:	6ebb234f0e41979de479ca4ee56501629988264c1b7acd794c149c89ec6cb718ddf1748e86f408d8fe781ae76ef05311b1496be18e5fc3705a8978ba6d9a57c5
SSDEEP:	3072:QA6cVUieJXfe5aL7FBMOJr7uC3IDaAunyw654/Q2uZAlDO:Q3J256FBMO93IuAiywi4Y2Z
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:	0x423d10
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:	0x607DE646 [Mon Apr 19 20:21:26 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:	835c0fbcc6459f6264f92edd519c6e5e

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

Instruction
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
mov eax, 00000000h
mov eax, 00000000h
je 00007FE53CEC66CBh
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	0x2668c	0x59	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2b000	0x340	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x2c000	0x144	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x24040	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	0x24000	0x3c	.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	0x22fae	0x23000	False	0.761558314732	data	7.55754035599	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x24000	0x283e	0x2a00	False	0.778180803571	data	7.45228827843	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pdata	0x27000	0x3862	0x1600	False	0.867897727273	MMDF mailbox	7.59898369456	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
.rsrc	0x2b000	0x340	0x400	False	0.3896484375	data	2.73261677544	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2c000	0x144	0x200	False	0.619140625	data	4.19021581125	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x2b060	0x2e0	data	English	United States

Imports

DLL	Import
KERNEL32.dll	OutputDebugStringA, LoadLibraryExA, CloseHandle, GetModuleHandleW, GetProfileSectionW, OpenSemaphoreW
ole32.dll	CreateStreamOnHGlobal
ADVAPI32.dll	RegLoadAppKeyW
USER32.dll	TranslateMessage
OPENGL32.dll	glVertex3f

Version Infos

Description	Data
LegalCopyright	Freeware
InternalName	ANSI32
FileVersion	1.66
CompanyName	Jason Hood
Comments	http://ansicon.adoxa.vze.com/
ProductName	ANSICON
ProductVersion	1.66
FileDescription	ANSI Console
OriginalFilename	ANSI32.dll
Translation	0x0409 0x04b0

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

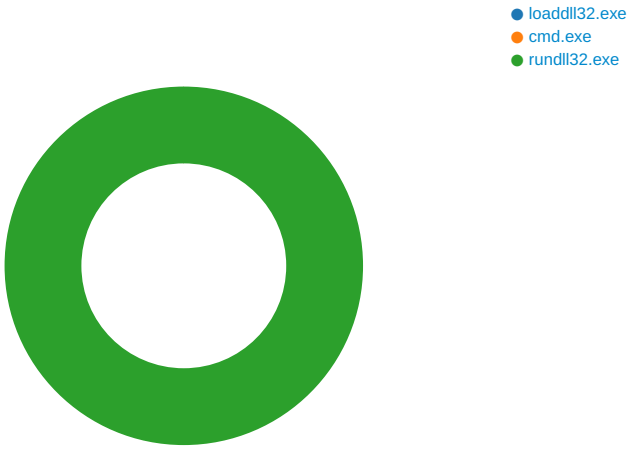
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loaddll32.exe PID: 912 Parent PID: 5616

General

Start time:	23:32:50
Start date:	19/04/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\P0DNoD3M7G.dll'
Imagebase:	0xcb0000
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: 2396 Parent PID: 912

General

Start time:	23:32:51
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\P0DNoD3M7G.dll',#1
Imagebase:	0xbd0000
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: 5596 Parent PID: 2396

General

Start time:	23:32:51
Start date:	19/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\P0DNoD3M7G.dll',#1
Imagebase:	0x7ff7488e0000
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: 00000003.00000002.488352077.0000000070A91000.00000020.00020000.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	70AA5E36	ReadFile

Disassembly

Code Analysis