ID: 544850
Sample Name: Pv3ZsGsdfS.dll
Cookbook: default.jbs
Time: 09:22:41
Date: 24/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report Pv3ZsGsdfS.dll 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Dridex 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
System Summary: 5
Jbx Signature Overview 5
AV Detection: 5
Networking: 5
E-Banking Fraud: 5
System Summary: 5
Malware Analysis System Evasion: 5
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 9
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
Contacted IPs 9
Public 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
Static File Info 12
General 12
File Icon 13
Static PE Info 13
General 13
Entrypoint Preview 13
Rich Headers 13
Data Directories 13
Sections 13
Resources 13
Imports 13
Version Infos 13
Possible Origin 13
Network Behavior 14
Code Manipulations 14
Statistics 14
Behavior 14
System Behavior 14
Analysis Process: loaddll32.exe PID: 6836 Parent PID: 5528 14
General 14
File Activities 14
Analysis Process: cmd.exe PID: 6852 Parent PID: 6836 14
General 14
File Activities 15
Analysis Process: rundll32.exe PID: 6900 Parent PID: 6852 15
General 15
Analysis Process: WerFault.exe PID: 7008 Parent PID: 6900 15
General 15

File Activities 15
File Created 15
File Deleted 15
File Written 15
Registry Activities 16
Key Created 16
Key Value Created 16
Disassembly 16
Code Analysis 16

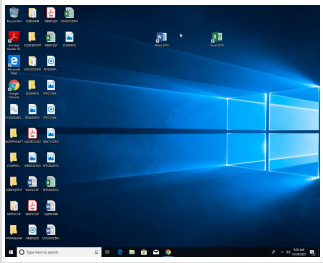
Windows Analysis Report Pv3ZsGsdfS.dll

Overview

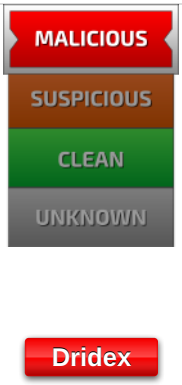
General Information

Sample Name:	Pv3ZsGsdfS.dll
Analysis ID:	544850
MD5:	63c22ce32346e0..
SHA1:	222cf86c3b59f46..
SHA256:	efbd76616dc1cd8..
Tags:	dll
Infos:	

Most interesting Screenshot:



Detection

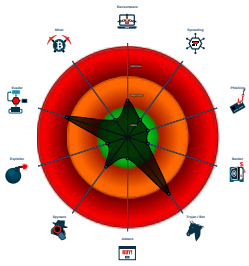


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected Dridex unpacked file
- Multi AV Scanner detection for subm…
- Sigma detected: Suspicious Call by …
- Tries to delay execution (extensive O…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- Found a high number of Window / Us…
- AV process strings found (often use…
- Sample file is different than original …
- One or more processes crash
- Contains functionality to query locale…
- Uses code obfuscation techniques (…
- Checks if the current process is bein…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6836 cmdline: loaddll32.exe "C:\Users\user\Desktop\Pv3ZsGsdfS.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 6852 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\Pv3ZsGsdfS.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6900 cmdline: rundll32.exe "C:\Users\user\Desktop\Pv3ZsGsdfS.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 7008 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6900 -s 684 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Dridex


```
{
  "Version": 22201,
  "C2 list": [
    "144.91.122.102:443",
    "85.10.248.28:593",
    "185.4.135.27:5228",
    "80.211.3.13:8116"
  ],
  "RC4 keys": [
    "3IC8sFlUX9XZuoBQY9u5LhcZnHsV7E5r",
    "hnk63OiMfIbUqQnY7gkPwplwC0Ue5ZkZBYMCTYTjntqX7zsy9OvtNUlthJZXRtFF6P52Zbz6R5"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
00000000.00000002.749937166.000000006F4B1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000003.00000000.360348773.000000006F4B1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000003.00000000.358630922.000000006F4B1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000003.00000002.401542049.000000006F4B1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
3.0.rundll32.exe.6f4b0000.5.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
3.2.rundll32.exe.6f4b0000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
0.2.loaddll32.exe.6f4b0000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
3.0.rundll32.exe.6f4b0000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Suspicious Call by Ordinal

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Dridex unpacked file

System Summary:

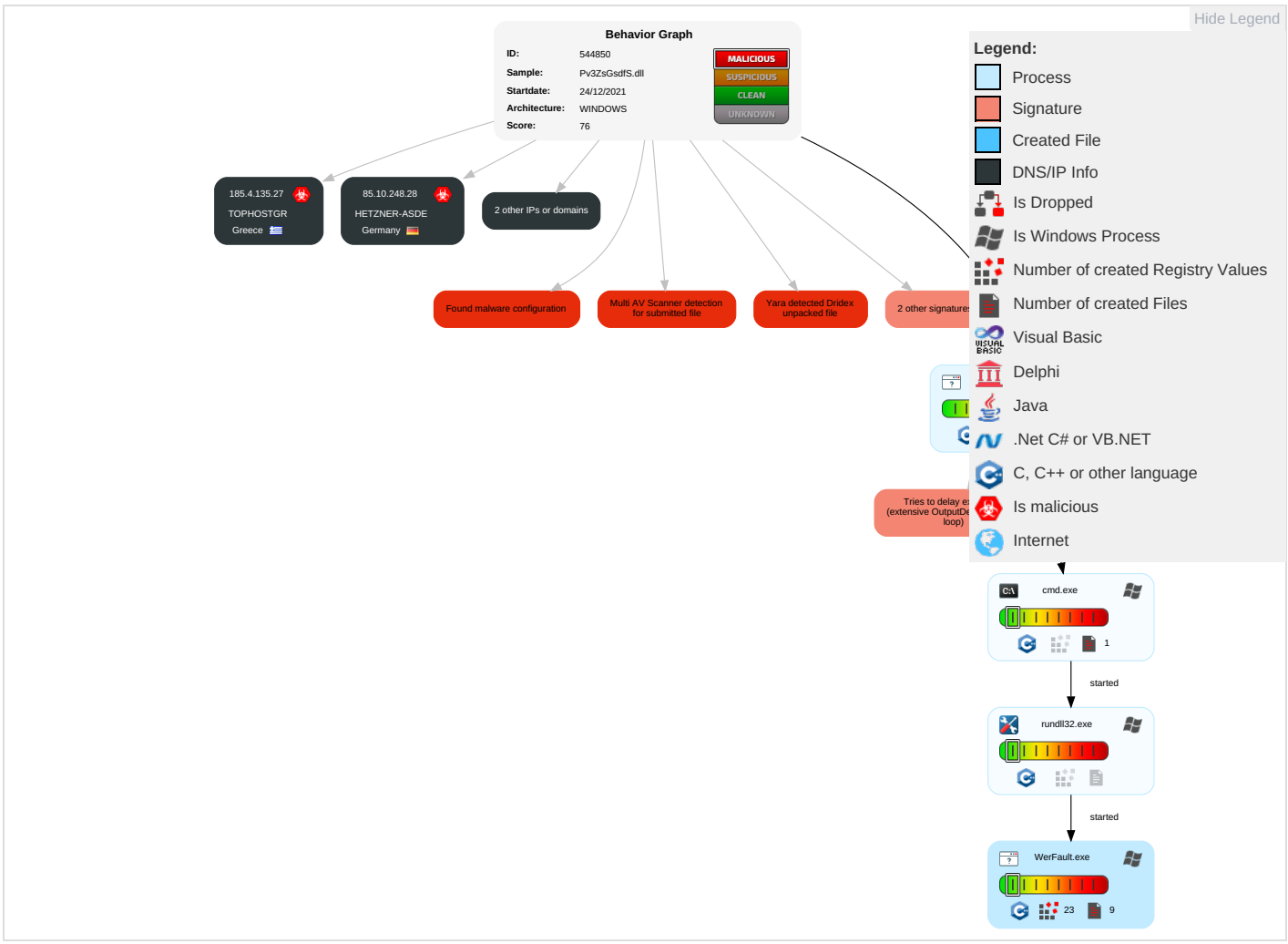
Malware Analysis System Evasion:

Tries to delay execution (extensive OutputDebugStringW loop)

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 1 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	Security Software Discovery 3 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Virtualization/Sandbox Evasion 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rundll32 1	NTDS	Process 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	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Account Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming o Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Owner/User Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poi
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Information Discovery 1 3	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cell Base Statio

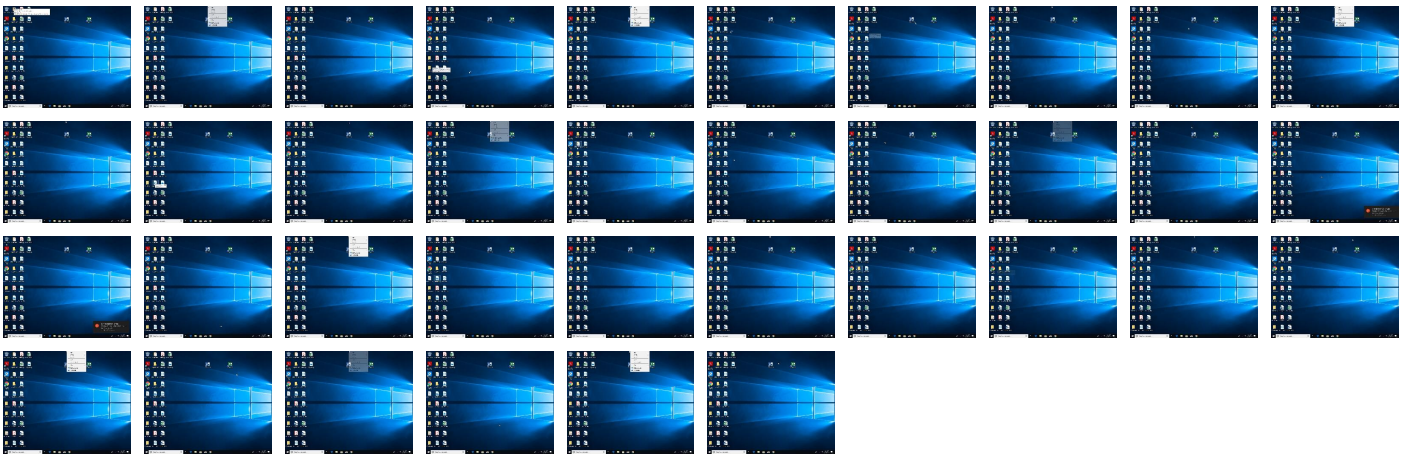
Behavior Graph



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
Pv3ZsGsdfS.dll	35%	ReversingLabs	Win32.Trojan.BotX	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.930000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.rundll32.exe.6f4b0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
3.0.rundll32.exe.6f4b0000.5.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
0.2.loaddll32.exe.1030000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.loaddll32.exe.6f4b0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
3.2.rundll32.exe.6f4b0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
3.0.rundll32.exe.930000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.rundll32.exe.930000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.baxleystamps.comDVarFileInfo$	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.4.135.27	unknown	Greece		199246	TOPHOSTGR	true
85.10.248.28	unknown	Germany		24940	HETZNER-ASDE	true
80.211.3.13	unknown	Italy		31034	ARUBA-ASNIT	true
144.91.122.102	unknown	Germany		51167	CONTABODE	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	544850
Start date:	24.12.2021
Start time:	09:22:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Pv3ZsGsdfS.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
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	25
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:	mal76.troj.evad.winDLL@6/6@0/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 52.3% (good quality ratio 50.4%) • Quality average: 79.2% • Quality standard deviation: 27%
HCA Information:	Failed

Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .dll
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_20f54535b4fc1ad4777e2f126bb0718bcd6544b5_82810a17_1a7fdfcd\Report.wer

Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	0.9131746768123783
Encrypted:	false
SSDEEP:	192:64siW0oXG/HBUZMX4jed+O/u7svS274ItWc:DsiQXG/BUZMX4jeL/u7svX4ItWc
MD5:	29579360B22432DFC0550492B810C2AD
SHA1:	8F3695C341FABAE6CB0488C2E19838F3D67CBD61
SHA-256:	448388426C2B1369CC525FC7649B835A8AC698E0612F88C1CDCA61984EDBE6B3
SHA-512:	4292836993B8AA7E138E24E3C1AE025FCA31C0D31BB21A6F8E303ABFB4606FBDDA9AB619F53E47A0C883F2C98FFFD5EC97680E8400CF275A65322D89FCF9DD4
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_20f54535b4fc1ad4777e2f126bb0718bcd6544b5_82810a17_1a7fdfcd\Report.wer	
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.4.8.4.0.2.2.9.7.6.4.5.6.6.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.8.4.8.4.0.2.4.1.8.5.8.2.5.9.1.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.f.c.4.9.9.2.b.-.c.1.4.b.-.4.9.b.5.-.8.f.c.9.-.8.5.c.1.f.2.d.f.e.9.6.7.....I.n.t.e.g.r.a.t.o.r.R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.e.f.8.7.0.c.a.a.-.5.1.c.6.-.4.d.8.0.-.9.8.0.e.-.e.2.3.c.6.c.8.5.3.6.d.8.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....N.s.A.p.p.N.a.m.e.=.r.u.n.d.l.l.3.2...e.x.e.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.R.U.N.D.L.L.3.2...E.X.E.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.a.f.4.-.0.0.0.1.-.0.0.1.7.-.d.9.3.e.-.5.a.0.0.e.b.f.8.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\Temp\WERA8BF.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Dec 24 17:23:51 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	45808
Entropy (8bit):	2.063465092606408
Encrypted:	false
SSDEEP:	192:lga6E0btUK302icO5SkbfC+O679tHT1Q3achcgGg7nET:GXXtUKJiT5LbBj79tHS3ach1
MD5:	6BA962499491EF50D34753FC43E70E78
SHA1:	FCDD29E7C70650CDEF5AAF15D6D1F65A6FB6D2AA
SHA-256:	2BE1C84338A24B862508C72D428D18E0FBE77006CD10C163FF81F8DB9633FFD0
SHA-512:	E810D101F784AE1FE327F359F7ABFBD756E4DE4EF7E842A6103EA4ADE6A9D60088660A46F1A516E304924D731847E6C8B311B62A393C85D89AAB51226FBE1BE9
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....'..a.....n-.....T.....8.....T.....@.....U.....B..... .....GenuineIntelW.....T.....a.....0..=.....P.a.c.i.f.i.c. .S.t.a.n.d.a.r.d. .T.i.m.e.....P.a.c.i.f.i.c. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB1E8.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8258
Entropy (8bit):	3.694780832129531
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi6jd67z/6Yau62gmfT6mSkCpr6q89bOGsfC6m:RrlsNic6X6YT62gmfT6mSCOlfW
MD5:	C2C685B0F4C57BF14EC69949014FC9E7
SHA1:	58ED607D8DEC974687FDB441B0957783BF57B567
SHA-256:	DEDB1C1CC0FEE5C433A3F484A0568AA349701325FCB48CB71348FF473B16DE7B
SHA-512:	A72C828DC593DE6CB08DE4E2BCB43FCD43441CCD4B7ADDFD21C75222B43CF28CDCE01178936630BA1FAF29CF1D31C45A1E7EA195FDFE01B34671C00AB2E2D29
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.9.0.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB515.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4630
Entropy (8bit):	4.459592349014678
Encrypted:	false
SSDEEP:	48:cvIwSD8zsaJgtWl9u4WSC8Bg8fm8M4JCdsfi2hFD+q8/08KBLc4SrS8d:uITfotxSNDJpiM58scDW8d
MD5:	A06DCD0393D3DE548D82518693742FB5
SHA1:	5BC6EE3EBF65DDFED1D0FFF8EB7BFE783D3805C3
SHA-256:	E7F298466D4C663D368F7DB05BF9F8FF076694B9BED76FFE750D46D37284BB31
SHA-512:	CB76A09686246456CD8CA5CF98CB2906E0D1ABB663474A7A2E4F9B428AB926998F063C68C07D1A5C51381C84FBE914F3A02F188F3BBF7D21F49D35665D1D3FB
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WERB515.tmp.xml	
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1311994" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Windows\appcompat\Programs\Amcache.hve	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.21783413807694
Encrypted:	false
SSDEEP:	12288:8Ci1aMWKiXr/IW87DN0bvHJsjDUhRzu3dKkzF7ZNq9kS+gab7KV+Ss:Vi1aMWKiXrgW87G+37XX
MD5:	D72F427F707F671A84F3C7CC3E4E3041
SHA1:	87173A87D9B1CDE0B1A53029D30AA52223C94363
SHA-256:	191CEA16D005286BDA625C0F12DDCC07C9DF3F7025F9236F11B2858604A1B167
SHA-512:	83FD8E1167696E4EC59C36F3A744AB15D50A8A70245490D8CC7D8494F9E662F906F427416114B5A0055896659FDD638A5C5848868547D2E4A86C5047E6A1F762
Malicious:	false
Reputation:	low
Preview:	regfV...V...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm..... .....1.._..... .....

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	3.5165609308437173
Encrypted:	false
SSDEEP:	384:JSb5VnIrnc82TVgG9K0XOmnQMR9ovOgl5:wlpAc8UVgGs0XVnQMEvP
MD5:	4A5692F77C142A5C921951F412C73996
SHA1:	118246C8365CADD57FCF448B9D491BAD688E70E8
SHA-256:	84058CF94519C692DCBC143DCB31998D33CFC649A143071E5373984EA6CD7468
SHA-512:	BC4DD6F71ABDA3C55F285B47B9264228A15098507D827C38880ABF840EB265A63220C1F99C021019C85034D1B2B5B85AEFAD2A8B1F80264B5CE754BD750B421
Malicious:	false
Reputation:	low
Preview:	regfU...U...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm..... .....7.._HvLE.N.....U.....N.....`... ..hbin.....p.\.,.....nk,..L.....@..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ..L..... ....Z.....Root.....lf.....Root....nk ..L.....}..... .....*.....DeviceCensus.....vk.....WritePermissionsCheck.....p...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.341894166997632
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:	Pv3ZsGsdfS.dll
File size:	565248
MD5:	63c22ce32346e029fa5a1ec1ae619d0f
SHA1:	222cf86c3b59f466292bb734be308cda77c3ddff
SHA256:	efbd76616dc1cd8210a8c54611f4ffa88e635f0f6ded2f8ff48311737635edda

General

SHA512:	413efdf48b13d8cd6cb9f799215a7c34588995ba5f48c4db855ad332c3b4b6b7c753ff361d0cd850a728ec68c76b47e96aaac604f3bdb069920d930c422bd0f4
SSDEEP:	12288:jGBK1zWlDqhPUVpqF9q9FAfPWvF+r3qTFCX1za7EV8RgfQOOvDC93:jNkIu2KAGIOwZ+v
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....R...<...<...<..k....<...=.S.<.=.....<.....<.....<.t.?...<.t.=.4.<.L.9...<.t...0.<..k....<..0..x.<.....<..1....<..k....<

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10005a80
Entrypoint Section:	.rdata
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61C43E40 [Thu Dec 23 09:15:44 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:	7119acbff3b38a52756367cf5bfb78f2

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x1000	0x699e	0x7000	False	0.390206473214	data	4.46675995806	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x79ed0	0x7a000	False	0.303953076972	data	7.45734301056	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x82000	0x6178	0x5000	False	0.246435546875	data	5.05789801748	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x89000	0x2f0	0x1000	False	0.090087890625	data	0.791740378228	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8a000	0x1138	0x2000	False	0.242065429688	data	4.12259394173	IMAGE_SCN_TYPE_COPY, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

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

Click to jump to process

System Behavior

Analysis Process: loaddll32.exe PID: 6836 Parent PID: 5528

General

Start time:	09:23:42
Start date:	24/12/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\Pv3ZsGsdfS.dll"
Imagebase:	0xb90000
File size:	116736 bytes
MD5 hash:	7DEB5DB86C0AC789123DEC286286B938
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: 00000000.00000002.749937166.000000006F4B1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6852 Parent PID: 6836

General

Start time:	09:23:43
Start date:	24/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\Pv3ZsGsdfS.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 Show Windows behavior

Analysis Process: rundll32.exe PID: 6900 Parent PID: 6852

General

Start time:	09:23:43
Start date:	24/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\Pv3ZsGsdfS.dll",#1
Imagebase:	0xe70000
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: 00000003.00000000.360348773.000000006F4B1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000003.00000000.358630922.000000006F4B1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000003.00000002.401542049.000000006F4B1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 7008 Parent PID: 6900

General

Start time:	09:23:47
Start date:	24/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6900 -s 684
Imagebase:	0xa20000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

Registry Activities Show Windows behavior

Key Created

Key Value Created

Disassembly

Code Analysis