ID: 544850
Sample Name: Pv3ZsGsdfS.dll
Cookbook: default.jbs
Time: 09:13:23
Date: 24/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

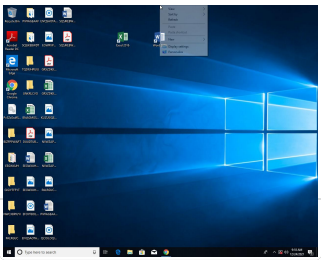
Windows Analysis Report Pv3ZsGsdfS.dll

Overview

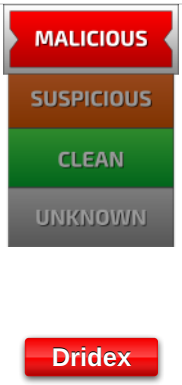
General Information

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

Most interesting Screenshot:



Detection

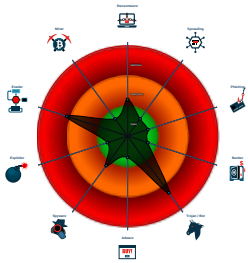


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6484 cmdline: loaddll32.exe "C:\Users\user\Desktop\Pv3ZsGsdfS.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 1964 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\Pv3ZsGsdfS.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 4492 cmdline: rundll32.exe "C:\Users\user\Desktop\Pv3ZsGsdfS.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 4716 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4492 -s 676 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
00000003.00000000.297484396.000000006EC61000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000000.299069466.000000006EC61000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000000.00000002.817398169.000000006EC61000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000003.00000002.335772232.000000006EC61000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.rundll32.exe.6ec60000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
3.0.rundll32.exe.6ec60000.5.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
3.0.rundll32.exe.6ec60000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
0.2.loaddll32.exe.6ec60000.2.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:

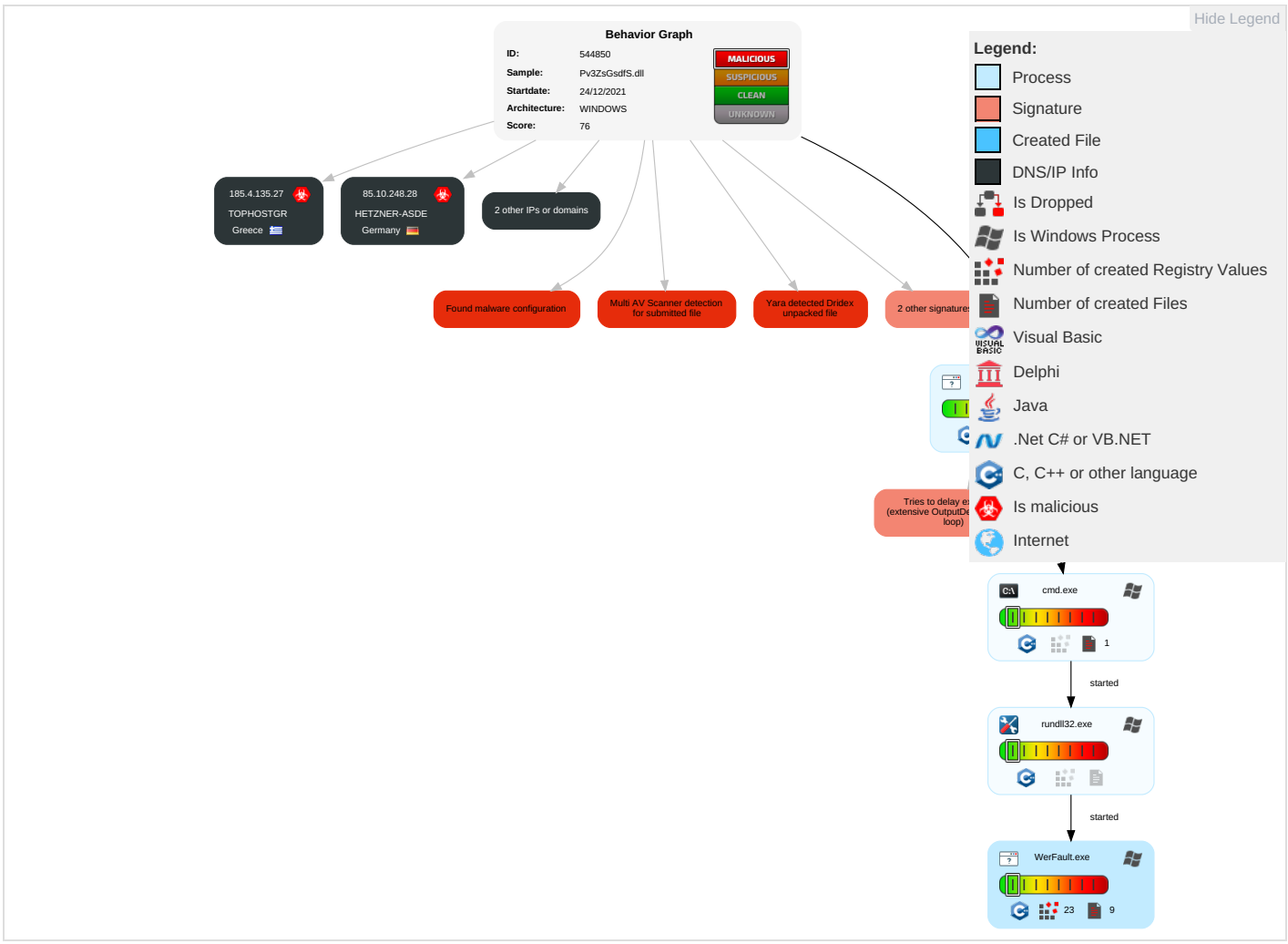
Malware Analysis System Evasion:

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	Security Software Discovery 3 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	Virtualization/Sandbox Evasion 1 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	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 Track Devic 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 Communica
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	Remote System 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	System Information Discovery 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

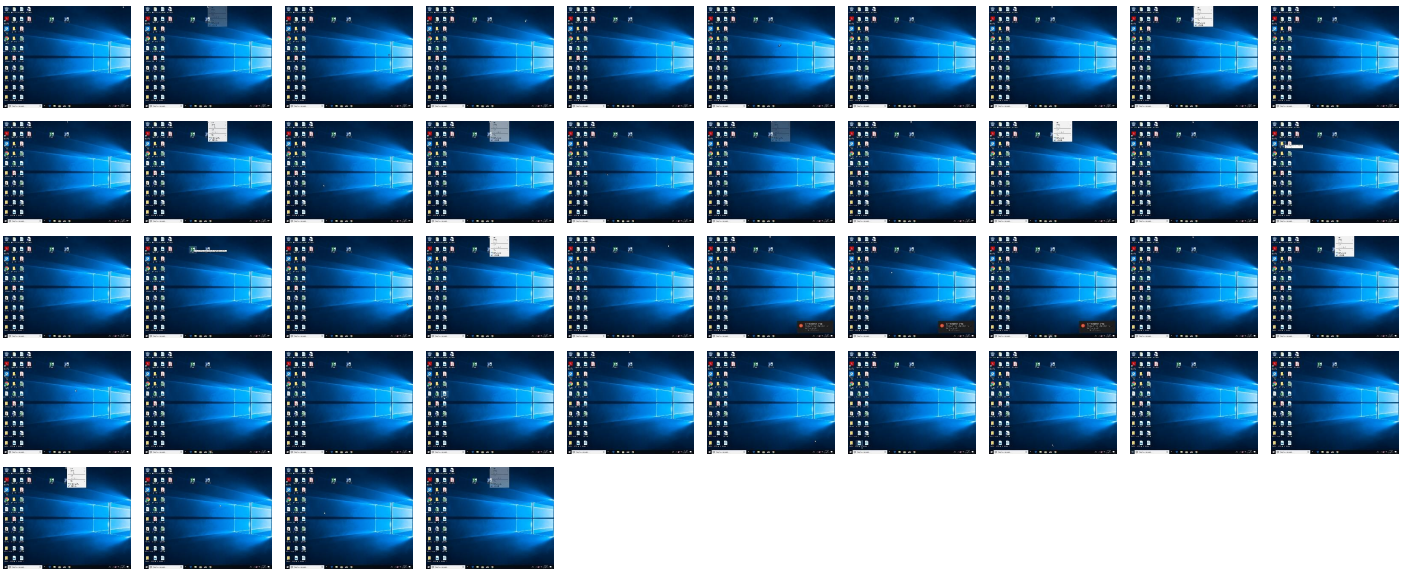
Behavior Graph



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	30%	Virustotal		Browse
Pv3ZsGsdfS.dll	35%	ReversingLabs	Win32.Trojan.BotX	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.rundll32.exe.6ec60000.5.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
3.0.rundll32.exe.6ec60000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
3.0.rundll32.exe.780000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.rundll32.exe.780000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.loaddll32.exe.6ec60000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
0.2.loaddll32.exe.630000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.rundll32.exe.6ec60000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
3.2.rundll32.exe.780000.0.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:	09:13:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 18s
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
Number of analysed new started processes analysed:	21
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: 100% (good quality ratio 96.1%) • Quality average: 78.4% • Quality standard deviation: 27.1%
HCA Information:	Failed

Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
09:14:36	API Interceptor	1x Sleep call for process: WerFault.exe modified

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_13ded830\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):	0.9111718068746235
Encrypted:	false
SSDEEP:	192:sBpxip0oXp/HBUZMX4jed+y/u7snS274ItWc:sJiHXp/BUZMX4jef/u7snX4ItWc
MD5:	98DB725A67C1B8A5B6180CEE5CAE23C5
SHA1:	13EDF737166203F780F919FD7504AF39C248C91C
SHA-256:	0B8587EBDE8B9CDF286B2424F2491CCBF835F66F6B9389F2702176969AE970DB
SHA-512:	ED0DD5F37DB7B47CB5F273394DFBFC1449D9A599C3CC810FECEFF5199D6FED2502166ABCB986D788282F53B7F3A810F522C98C940DF0AADB060F6440BBFE31E5
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_20f54535b4fc1ad4777e2f126bb0718bcd6544b5_82810a17_13ded830\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.=.1.3.2.8.4.8.3.9.6.6.8.3.0.9.5.0.5.8.....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.=.1.3.2.8.4.8.3.9.6.7.3.7.6.2.6.1.5.7.....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.=.e.c.3.c.1.7.d.5.-.b.9.b.8.-.4.4.7.6.-.8.b.2.8.-.d.7.d.d.3.e.0.0.5.e.a.5.....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.=.9.d.a.1.9.7.1.8.-.5.9.e.a.-.4.b.4.2.-.a.b.1.a.-.a.7.f.9.5.7.9.f.6.d.3.1.....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.=.0.0.0.0.1.1.8.c.-.0.0.0.1.-.0.0.1.c.-.6.3.b.f.-.b.7.b.0.e.9.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\WER420B.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Dec 24 17:14:30 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	39588
Entropy (8bit):	2.203119864197164
Encrypted:	false
SSDEEP:	192:8ni3B0pH4WvIO5Skbh+D2kJ9Cv1jyPnM:eeNy5Lbg2kJ9g1j+M
MD5:	79CC52BA1F0EDD26262D136E990D6984
SHA1:	E46079188D61F35B4E3D3ADFF6732DA30DB98E52
SHA-256:	DC0508215AACCF947F0B30DCEDF4E964DDF68C4E875EC363791270DCC51349F0
SHA-512:	ECEE6A6521EF416E8DF4A4FD436D0C0CC050CC9EF1C34E16BB400A111451880DB1C7F20CFCC8B2548067651F983C160E4542997B7F96A69B1C6DC1A69B5F0E8
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....a.....d.....l.....r*.....T.....8.....T.....l.....X.....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\WER4C9B.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):	8262
Entropy (8bit):	3.691032691100008
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi2j06G6Y5DJ6qgmfT6mS1CprY89bvzsfTFm:RrlsNiY06G6YtJ6qgmfT6mSYvYf8
MD5:	C87774744C9A5569A446F9BF33806F1E
SHA1:	3A66302FCC41E42BA718CCC8758A62A18163BC33
SHA-256:	511D0E9184E6E0C5BF06F83A2F9357D9C459A09CF7495F307FB657BFB6082BDA
SHA-512:	0381662D0F431B2547FDD12323994EDB80B58A91EE78362A1D4488CDA073CA4274B7E3B05144F0BAFEB51812DA6DC8877BF302C17B82BDB6BDC91834EAED84AB
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.>.4.4.9.2.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4EEE.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):	4.462909015903191
Encrypted:	false
SSDEEP:	48:cvIwSD8zsmtJgtWI9WAq6WSC8BYIa8fm8M4JCdsfi2hFfkHx+q8/08KBh4SrSRd:uITfK0aSNK0JpiZR58ODWRd
MD5:	31E7146B51BA7ED555179C77D3D1E3E7
SHA1:	FEED34F987DE4DC45B91EF062770E97122CCDE9B
SHA-256:	54F8D3359514FC8938C97263E2F3541F2B53B73A7BF329CFA4B7ACA811CAECC5
SHA-512:	347D73C81E080CF89EB5A34CF3F6F41791B3DEC515DB77E0298081A44180D729284519D0279904FD6CC8024A3900DFB85F2E20AB3FA01766C8F03817D6D9D859
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4EEE.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="1311985" />.. <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):	4.27745692143549
Encrypted:	false
SSDEEP:	12288:WTL1SAyOjLbq2EXipqU8s7DfJtHpKx9pYJwD4kAmtKPABK8JizStKX:uL1SAyOjLbq2EX8O
MD5:	B92BBD7D35F32F74D0898172B4E83114
SHA1:	30DADB66C00264F0D67F842D94E81403083A27F9
SHA-256:	97E33CBE253502A16CACAF286E2D77C2CFD250C50BB718BE5D95D8048CB52B81
SHA-512:	29C3F3BD7DBA05BFB647D749E3929C01C66F4AA7E3411F3163A98BB3F4461DFCE217D9551DE1EA3091060A4E6E63BB3A52503536407C4789E762C3C6180CF4E
Malicious:	false
Reputation:	low
Preview:	regfZ...Z...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.bX..... .....)\..... .....

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):	24576
Entropy (8bit):	4.0345755638050464
Encrypted:	false
SSDEEP:	384:e1Ez5Rftx1nPJ4X8sFcnE7koPBqXtSeq5QMVyi6+/8l4Lk4xZd1DoXzneXvwvI:WENRftx1PJ4X5FcE7VBqXseq5QMVyi6j
MD5:	50450D0949002809FB441A3343BD4957
SHA1:	9CBBBAA5EEA9963EC22F69B7578FAD5D8981179A
SHA-256:	69A6AE8B8F0D55BFAE3ED5C2483B501CF4A85B628528681601CE63FE3D35ADF3
SHA-512:	EE1B15A3B492B46F2657E4918D2F9DE6720C072C5E7A952A19A5DDCC6BC305F674BE5B4BFFF0963FB571C9C034AAB8FEE38AB6C79C6A6752CFCA976060076B87
Malicious:	false
Reputation:	low
Preview:	regfY...Y...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.bX..... .....)\.HvLE.^.....Y.....{...Kb..+..p[.....0..... ..hbin.....p.\..,.....nk,..<p..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ..<p..... ....Z.....Root.....lf.....Root....nk ..<p.....}..... .....*.....DeviceCensus..... ..vk.....WritePermissionsCheck...

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

General

SHA256:	efbd76616dc1cd8210a8c54611f4ffa88e635f0f6ded2f8ff48311737635edda
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: 6484 Parent PID: 3416

General

Start time:	09:14:19
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:	0x1220000
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: 00000000.00000002.817398169.000000006EC61000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 1964 Parent PID: 6484

General

Start time:	09:14:20

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:	0xd80000
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: 4492 Parent PID: 1964

General

Start time:	09:14:20
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:	0x1270000
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: 00000003.00000000.297484396.000000006EC61000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000003.00000000.299069466.000000006EC61000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000003.00000002.335772232.000000006EC61000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 4716 Parent PID: 4492

General

Start time:	09:14:23
Start date:	24/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4492 -s 676
Imagebase:	0xba0000
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