ID: 545442
Sample Name: G7ABVJxc3Z
Cookbook: default.jbs
Time: 17:16:09
Date: 26/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

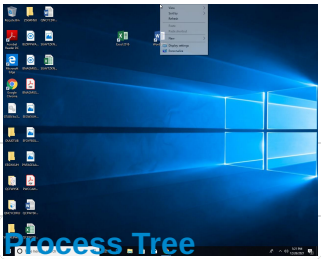
Windows Analysis Report G7ABVJxc3Z

Overview

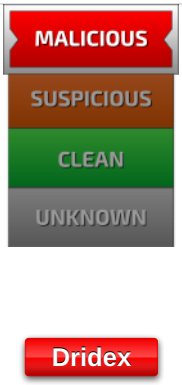
General Information

Sample Name:	G7ABVJxc3Z (renamed file extension from none to dll)
Analysis ID:	545442
MD5:	47c59530065e8e..
SHA1:	8fba3ea2428f92e..
SHA256:	e4db910a4147ac..
Tags:	32 dll Dridex exe trojan
Infos:	

Most interesting Screenshot:



Detection

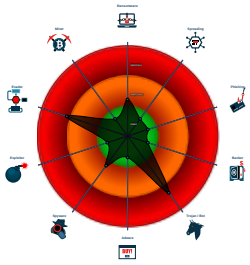


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- Machine Learning detection for samp…
- 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

Classification



- **System is w10x64**
- loaddll32.exe (PID: 7060 cmdline: loaddll32.exe "C:\Users\user\Desktop\G7ABVJxc3Z.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 7072 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\G7ABVJxc3Z.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 7096 cmdline: rundll32.exe "C:\Users\user\Desktop\G7ABVJxc3Z.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 6496 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7096 -s 728 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7084 cmdline: rundll32.exe C:\Users\user\Desktop\G7ABVJxc3Z.dll,Wgpomsdeeomtunmdrt MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 6944 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7084 -s 904 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Dridex


```
{
  "Version": 22201,
  "C2 list": [
    "104.36.167.47:443",
    "188.40.48.93:4664",
    "162.241.33.132:9217",
    "217.160.5.104:593"
  ],
  "RC4 keys": [
    "MVvOFIilF0NXOL2BGlf3SZonbBup17KA",
    "6UfDOLUgX3hJ3XaposUIUiva9uclhs6fenw01keZT6Cxe8VImuG9Uw6F4mFEkE0ddDT1py8ABw"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
00000003.00000000.360282236.000000006E981000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000004.00000002.377382797.000000006E981000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000003.00000000.358113522.000000006E981000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000004.00000000.352674863.000000006E981000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000001.00000002.806396499.000000006E981000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
Click to see the 1 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.0.rundll32.exe.6e980000.5.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
1.2.loaddll32.exe.6e980000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
3.0.rundll32.exe.6e980000.5.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
4.2.rundll32.exe.6e980000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
3.0.rundll32.exe.6e980000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
Click to see the 1 entries				

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

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Dridex unpacked file

System Summary:

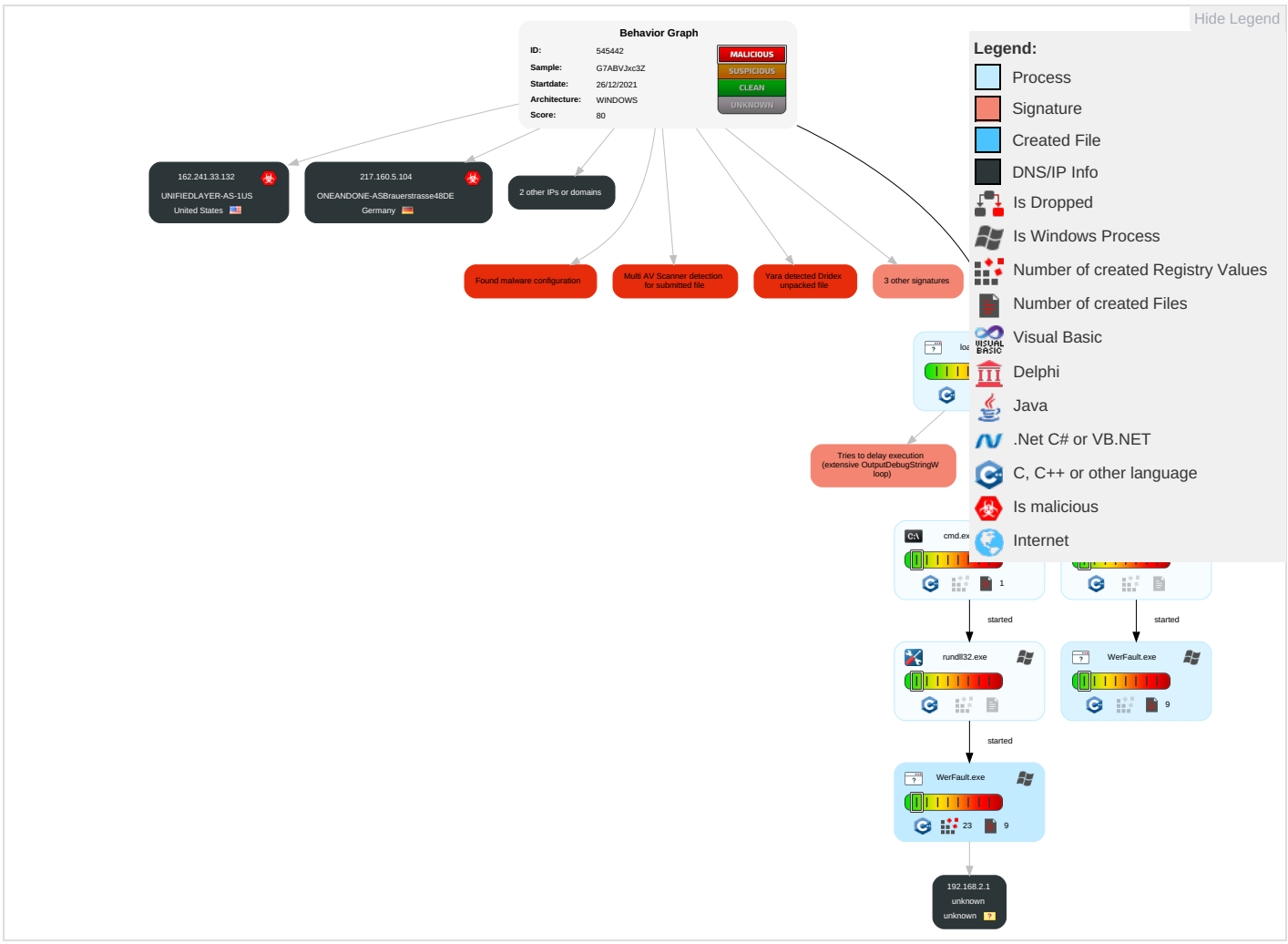
Malware Analysis System Evasion:

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	DLL Side-Loading 1	Process Injection 1 2	Virtualization/Sandbox Evasion 1	OS Credential Dumping	Security Software Discovery 2 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	DLL Side-Loading 1	Process Injection 1 2	LSASS Memory	Virtualization/Sandbox Evasion 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	DLL Side-Loading 1	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
G7ABVJxc3Z.dll	65%	Virustotal		Browse
G7ABVJxc3Z.dll	67%	ReversingLabs	Win32.Infostealer.Dridex	
G7ABVJxc3Z.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.rundll32.exe.6e980000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
4.0.rundll32.exe.6e980000.5.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
4.2.rundll32.exe.940000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.loaddll32.exe.6e980000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
4.0.rundll32.exe.6e980000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
4.0.rundll32.exe.940000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.0.rundll32.exe.940000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.rundll32.exe.1060000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.rundll32.exe.6e980000.5.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
1.2.loaddll32.exe.be0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
4.2.rundll32.exe.6e980000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
3.0.rundll32.exe.1060000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.rundll32.exe.1060000.3.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

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.241.33.132	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
104.36.167.47	unknown	United States		27640	GIGASNET-ASUS	true
217.160.5.104	unknown	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
188.40.48.93	unknown	Germany		24940	HETZNER-ASDE	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	545442
Start date:	26.12.2021
Start time:	17:16:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	G7ABVJxc3Z (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:	33
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:	mal80.troj.evad.winDLL@9/10@0/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 95.6% (good quality ratio 91.7%) • Quality average: 78.2% • Quality standard deviation: 27.4%
HCA Information:	• Successful, ratio: 53% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
17:17:45	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_4d42c1f24c11b6c9a2fc199d7a28c798fe9e5a_82810a17_186b5001\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):	0.9662020773051797

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_4d42c1f24c11b6c9a2fc199d7a28c798fe9e5a_82810a17_186b5001\Report.wer	
Encrypted:	false
SSDEEP:	192:9oim0oXMCHBUZMX4jed+RU/u7s+S274ItWc:+iAXrBUZMX4jeH/u7s+X4ItWc
MD5:	401120BD53CCBD27FA259A5A52A3B527
SHA1:	4596D5B1A4E845A3F197CC484016933EE39F053B
SHA-256:	9ACF262A25F29DC412E7EF650FB5129BF8A83BA25346941AB4576C27CC5E841B
SHA-512:	B07494F79D06CF8D3B17EEE66612C9259CD5770EEDA4BA74F3F18F994EC9420D875339F647609F01637693608848F6546F37EDBB4E69478EA5D33C5636DEF526
Malicious:	false
Reputation:	low
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.=.1.3.2.8.5.0.4.1.4.5.9.3.9.9.9.0.9.0.....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.=.1.3.2.8.5.0.4.1.4.6.3.9.9.3.6.6.3.1.....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.=.7.f.0.7.e.5.6.0.-.0.8.0.6.-.4.6.5.6.-.a.c.1.2.-.f.0.1.d.b.d.f.7.d.3.b.3.....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.c.7.c.6.6.1.d.-.d.7.7.7.-.4.4.5.b.-.9.1.2.6.-.2.8.e.f.2.f.4.0.e.f.9.d.....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.b.b.8.-.0.0.0.1.-.0.0.1.c.-.b.c.b.9.-.8.d.7.3.b.f.f.a.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\ReportQueue\AppCrash_rundll32.exe_dd9d398ae70aa8478325646a49f7ebef948b8_82810a17_1a2b65ac\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):	1.0002759996639048
Encrypted:	false
SSDEEP:	192:7ZiR0oXAHVzOMjed+x8/u7s+S274It7c:FifXoVzOMje3/u7s+X4It7c
MD5:	813D9ED5160FDC9DC97A0733BD09DEFA
SHA1:	0EDACF88A19E42498585027B63F2EE406A5F4D6B
SHA-256:	90F83440A54B694266E424BCCC282115E2D58B65463B7AED5F957CF6DE063CF4
SHA-512:	DF977B921414DBE1E822CE65817AD0D258D4000E78CCAEAE12336BE21EFA3E4065B98D5A31D04963286CF14930A8B782BC6C15CAD779376E1E5C2D91B2D490A
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.5.0.4.1.4.6.3.4.0.1.4.1.3.5.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.8.2.1.c.d.5.9.a.-.2.6.f.1.-.4.5.8.0.-.9.c.3.2.-.e.2.9.7.5.9.f.f.e.8.9.3.....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.0.7.0.4.b.8.2.-.3.f.b.4.-.4.6.2.5.-.b.4.c.8.-.8.c.d.b.5.5.7.f.e.7.0.5.....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.b.a.c.-.0.0.0.1.-.0.0.1.c.-.f.9.4.c.-.8.a.7.3.b.f.f.a.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.b.5.f.!.r.u.n.d.l.l.3.2...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.1.9.8.6././.0.1././.3.0.:.1.1.:.4.2.:.4.4.!.1.0.3.d.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3834.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Dec 27 01:17:40 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	45630
Entropy (8bit):	2.1458835196760435
Encrypted:	false
SSDEEP:	192:zaaTjqmBijUMxKAQO5SkbXhVlvVF0UsbyLh4ynL8HQFmHn2q:FPq5jPJn5Lbzx8Xb6h4ynL8Hf
MD5:	8D957DFDA180AE260476B920731DF1E8
SHA1:	4063564332B2114FEF43A3513EF5EB14C2A4C0E2
SHA-256:	DB82A80D9E633482F1CEB4F6C59E9D82E602F57B3EB1A09365ADB2824E82085D
SHA-512:	4C4AE531E9621D69AE58E285AD03021B054C540C5836D6D1BD22476D8B5D185818BC637CDED42AA866DB8C9091CD787D002CE7BB039A00522F558E96F18A57
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....4..a.....`.....1.....T.....8.....T.....F.....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\WER3FD6.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):	8270
Entropy (8bit):	3.697694350006487
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiVq6jL6YpL6eVgmfTwDS0RCprF89bPaHjsffFm:RrlsNio6v6Yl6eVgmfTUS07PaHIfQ

C:\ProgramData\Microsoft\Windows\WER\Temp\WER3FD6.tmp.WERInternalMetadata.xml	
MD5:	B40D89CECBEA01237E460AD07AE18016
SHA1:	59A60AAD0409CC31DFAC7C9AD4E464EC27D06395
SHA-256:	E40741C64433C448AB90964E400B18CFD2B5A107343C5A427F3CF0BD56A679EE
SHA-512:	D513C8AD7FE7084E7B4BB013F986D37B5BF579A1B78C95D42B43BEB91342AB283349BE24D48CDA65155124A5036775B601144787A28F000B7E5A6496575953CA
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.>.7.0.9.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4296.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):	4.471169157708748
Encrypted:	false
SSDEEP:	48:cvIwSD8zs5/rJgtWI9XvWSC8Bu8fm8M4JCdsA9DFSEN9+q8/F5nM34SrSZd:uITfDY+SNJJyiEN9C63DWZd
MD5:	C5CF0B967CC9D989DA37F35B67E7992F
SHA1:	39A7ADFBD15634540DFEFB05289FB2D46C146592
SHA-256:	8DE1787CE5CE6B747CA105A50B4B8B2DDD3F4B267BDBB4D8B6E206818DA1742C
SHA-512:	C7160DB450365C555168E9BD86D9670CFE2A0F2A81BAEE215747805AF4E261533F73FEDC9D2C093CB4C7734D8F4BEE6B7110F4D3D44F35954FA5425B8C89CED
Malicious:	false
Reputation:	low
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="1315348" />.. <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:\ProgramData\Microsoft\Windows\WER\Temp\WER47D4.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Mon Dec 27 01:17:45 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	48308
Entropy (8bit):	2.2004358665943657
Encrypted:	false
SSDEEP:	192:vVgIVKFbnDj4O5SkbDGFy3nLftXxxiHtQsoA9vZfvcuS:jVcn/5LbDBnztXxxiNEA3kR
MD5:	DD45119DAC9E4E0D06E04E22832EA9A6
SHA1:	077F7F9F6EAF38DD545DA6F65630AE8FA53500F0
SHA-256:	6EFE0206D8993F95D9C715AF46D45FD4184353942B2F9373092AAFC6B59227E1
SHA-512:	DC581F28DA85AFBA0ABB9D0BFCD10630A0AEE90CE67E8CA92230C3A645F35A8059FB9C92501D8941758E9D53341A8946251F891FA7ED938FA9C1043F74E0D34C
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....9..a.....|.....$...$ .....4.....`.....8.....T.....H"..l.....H .....4".....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\WER5293.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):	8350
Entropy (8bit):	3.6918698451750243
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiWH6H6YDI6X0gmf8ZS1RCpBg89bw6sfhQm:RrlsNi+6H6YM6kgmf8ZS1WwZfD
MD5:	BB8F1E2BEC9E477562A1A05CB781630C
SHA1:	BBD8B07D8B421A0579A0E24A43FB2D53BB0E5909
SHA-256:	84894CA197D9856A092B6DED52985951FB5DA8CBA16AC6250705567245DDAC4B

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5293.tmp.WERInternalMetadata.xml	
SHA-512:	833C061115C23F4B56B871BB44B0FCD3A36F51828615B8739381710B5B034BC7E33DE29013C3C117F1A1012EDD2F149FA4706E29A27BA90EA026006BE9F9C348
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.>.7.0.8.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5582.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4731
Entropy (8bit):	4.455987331590969
Encrypted:	false
SSDEEP:	48:cvIwSD8zs5/rJgtWI9XvWSC8BW8fm8M4JCdsA97Fu4+q8vjsA9l34SrS8d:ulTfDY+SNhJyO4KzTDW8d
MD5:	6D0C30D7278211F13828F8D66F139E16
SHA1:	5DDC9DA28F30D98DFF13C1EF52155DA35D362903
SHA-256:	4F4B967F276F89EAF29D855F46F44E69368D0A98E93673AABFA1FA8DCF08C2B2
SHA-512:	D7E16A33262E443758F9A4ECF80FE817E3A2DB7B0DF0232946FDD352599AB349CFBA7B51872E159B1A5669093629608FBC7229ED909DFF291E7FC66ADCD3746
Malicious:	false
Reputation:	low
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="1315348" />.. <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):	4.277988733245352
Encrypted:	false
SSDEEP:	12288:qrTfkC4ipVBB8+Fh/QHYym4nuMdBDd9LMHtXSIM68tjzKXw17SzzeT:KTfkC4ipVBB8+F2M
MD5:	F514F98C70C438A62868CAF90AB1F6C6
SHA1:	2D897951CA34A68FB2621F0E7288B41F18E97A0D
SHA-256:	F3BDE70C72EB661626133028E0E36BB7C4114017E3DF4DB5A5AC227FD884224B
SHA-512:	75E964D427A2931E24542FB5666060E0A535E2422E3AE3EA06E2CB78ACB3024281E413352E89728040ADD3E21D469C8D76B68B30D395DA26415E12A33586FB84
Malicious:	false
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.o3..... ....U&7..... .....

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):	4.03249306135428
Encrypted:	false
SSDEEP:	384:J29b5Rftx18PJ4XrsFcnE7kHPBqXmSeq5QMVyi6+/Xl4Lk4HZd1DoXzn7Xvwvm:89lRftx1CJ4XIFcE7ABqXNeq5QMVyi6Z
MD5:	81F3B3B999E7D2106B3C662761629020
SHA1:	2713968EA0F3C7D447121D0575504D5EF3D6B1A1
SHA-256:	38A46989C5B5E7FB9E5D01A2DB5276E6EA048D314F4EA81D05EA380AD5258F52
SHA-512:	58704682D66E7CC61FA38BB827FCE2222A5CB077D38B8981E24A2848575872ADD09812084820D36F9524144D3F2A7B434939A799F4587E86330D661A02FF2A71
Malicious:	false

C:\Windows\appcompat\Programs\Amcache.hve.LOG1	
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.o3..... ....S&7.HvLE.^.....Y.....Y~,..|c.H..:.fx.....0..... ..hbin.....p.\.,.....nk,.W48..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk .W48..... ....Z.....Root.....lf.....Root....nk .W48.....}..... .....*.....DeviceCensus.. .....vk.....WritePermissionsCheck...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.269426930570889
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:	G7ABVJxc3Z.dll
File size:	536576
MD5:	47c59530065e8e7e05a855879bf8a922
SHA1:	8fba3ea2428f92e8dc8497514d0817b54edc5be0
SHA256:	e4db910a4147ac44bef76f71e6b0d6bd193b89a6268dda3 5f3b1c210cc111fe4
SHA512:	c99e35f6313aa75f24b7bdb1cc9e91eb7246dd7cd79de9c 18f50d1f6ee27984ff075c108d1025e16dbd6d03087d11b cb6f927c5773e8a03d7bdd02c204782a42
SSDEEP:	6144:4KMlmhktm7mnmvetmzK/kxwv4Zm7mREqZzdaz dULd54f3X0kdVtL8faGAPlX:49hXAg5aX0CL8fI
File Content Preview:	MZ.....@.....P.....E;...;...;... .XI.....2.4.^....uh.{...6.F.....XI.....F.z.....u... .....z.....@...8.{.G...;.....Rich;..... .....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10005a10
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61B705D1 [Mon Dec 13 08:35:29 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:	e9192d34e4c9dcdf739aaa1d74025eb2

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x74d8	0x8000	False	0.360290527344	data	4.61113521989	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x9000	0x6fff8	0x70000	False	0.311179024833	data	7.3778786518	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x79000	0x80f4	0x7000	False	0.295828683036	data	6.02916609898	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x82000	0xec8	0x1000	False	0.090087890625	data	0.784979301457	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x83000	0x1214	0x2000	False	0.287475585938	data	4.27724948186	IMAGE_SCN_TYPE_COPY, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

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: 7060 Parent PID: 4636

General

Start time:	17:17:00
Start date:	26/12/2021
Path:	C:\Windows\System32\loaddll32.exe

Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\G7ABVJxc3Z.dll"
Imagebase:	0xbb0000
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: 00000001.00000002.806396499.000000006E981000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 7072 Parent PID: 7060

General

Start time:	17:17:01
Start date:	26/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\G7ABVJxc3Z.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: 7084 Parent PID: 7060

General

Start time:	17:17:01
Start date:	26/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\G7ABVJxc3Z.dll,Wgpomsdeeomtunmdrt
Imagebase:	0x1100000
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: 00000003.00000000.360282236.000000006E981000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000003.00000000.358113522.000000006E981000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 7096 Parent PID: 7072

General

Start time:	17:17:01
Start date:	26/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\G7ABVJxc3Z.dll",#1
Imagebase:	0x1100000
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: 00000004.00000002.377382797.000000006E981000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000004.00000000.352674863.000000006E981000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000004.00000000.351482277.000000006E981000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 6496 Parent PID: 7096

General

Start time:	17:17:36
Start date:	26/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7096 -s 728
Imagebase:	0x8b0000
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

Analysis Process: WerFault.exe PID: 6944 Parent PID: 7084

General

Start time:	17:17:40
Start date:	26/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7084 -s 904
Imagebase:	0x8b0000
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 Modified

Disassembly

Code Analysis