ID: 545442
Sample Name: G7ABVJxc3Z.dll
Cookbook: default.jbs
Time: 17:25:28
Date: 26/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

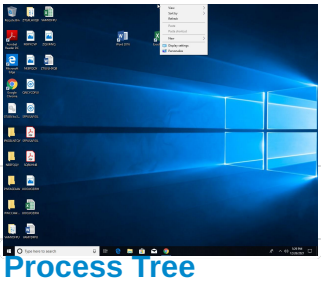
Windows Analysis Report G7ABVJxc3Z.dll

Overview

General Information

Sample Name:	G7ABVJxc3Z.dll
Analysis ID:	545442
MD5:	47c59530065e8e..
SHA1:	8fba3ea2428f92e..
SHA256:	e4db910a4147ac..
Tags:	32 dll Dridex exe trojan
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

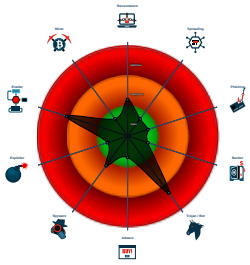
Dridex

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



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6380 cmdline: loaddll32.exe "C:\Users\user\Desktop\G7ABVJxc3Z.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 6376 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\G7ABVJxc3Z.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6484 cmdline: rundll32.exe "C:\Users\user\Desktop\G7ABVJxc3Z.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 5728 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6484 -s 740 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6496 cmdline: rundll32.exe C:\Users\user\Desktop\G7ABVJxc3Z.dll,Wgpomsdeeomtunmdrt MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 4864 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6496 -s 864 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
00000002.00000000.740603075.000000006E471000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000003.00000002.831692261.000000006E471000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000000.00000002.1054100443.000000006E471000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000002.00000000.742949248.000000006E471000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000003.00000000.733407707.000000006E471000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
Click to see the 1 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.0.rundll32.exe.6e470000.5.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
2.0.rundll32.exe.6e470000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
3.2.rundll32.exe.6e470000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
2.0.rundll32.exe.6e470000.5.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
0.2.loaddll32.exe.6e470000.2.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:

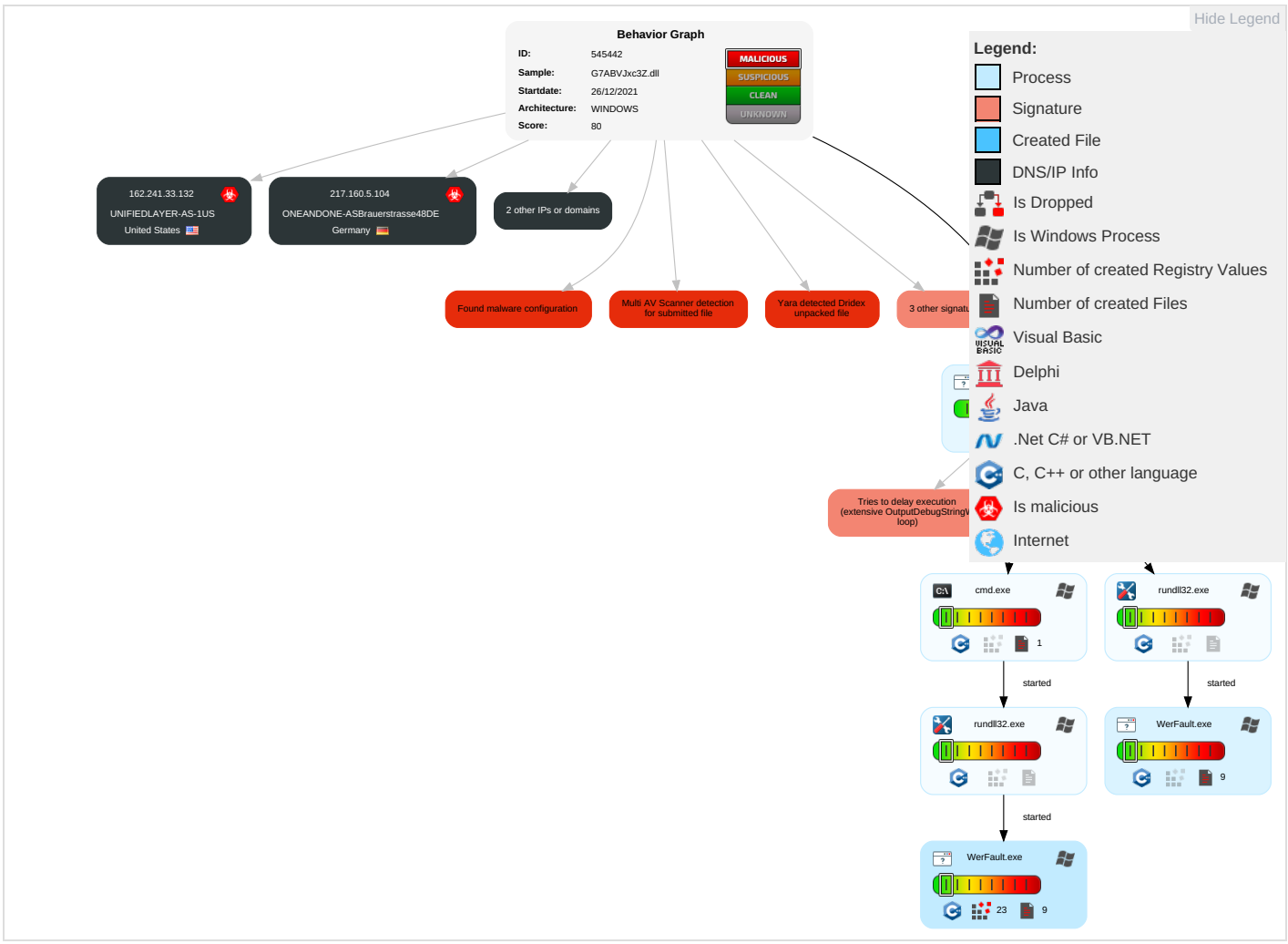
Malware Analysis System Evasion:

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	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	DLL Side-Loading 1	Process Injection 1 2	LSASS Memory	Security Software Discovery 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 Redirect PI Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Virtualization/Sandbox Evasion 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	DLL Side-Loading 1	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-I 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

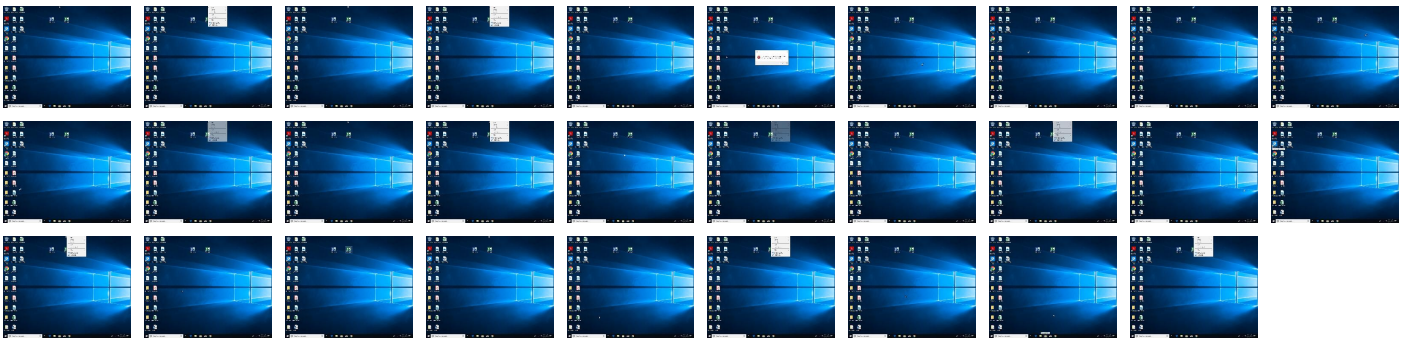
Behavior Graph



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
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
2.2.rundll32.exe.5b0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.rundll32.exe.3280000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.rundll32.exe.3280000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.rundll32.exe.3280000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.rundll32.exe.6e470000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
2.0.rundll32.exe.5b0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.rundll32.exe.6e470000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
3.0.rundll32.exe.6e470000.5.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
0.2.loaddll32.exe.1180000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.rundll32.exe.6e470000.5.unpack	100%	Avira	HEUR/AGEN.1144420		Download File

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.6e470000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
2.0.rundll32.exe.5b0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.rundll32.exe.6e470000.2.unpack	100%	Avira	HEUR/AGEN.1144420		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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	545442
Start date:	26.12.2021
Start time:	17:25:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	G7ABVJxc3Z.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:	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:	mal80.troj.evad.winDLL@9/10@0/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 56.1% (good quality ratio 52.2%) • Quality average: 77.2% • Quality standard deviation: 30.1%
HCA Information:	• Successful, ratio: 53% • Number of executed functions: 0 • Number of non-executed functions: 0
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_4d42c1f24c11b6c9a2fc199d7a28c798fe9e5a_82810a17_173d852c\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):	0.9654598579721348
Encrypted:	false
SSDEEP:	192:IniV0oX3CHBUZMX4jed+RU/u7sHS274ItWc:4i7XqBUZMX4jeH/u7sHX4ItWc
MD5:	93091EC43D665EC917DA2B6DEF3C1986
SHA1:	C2F1761C9D079582704C4E1EB9D7B6E071E2B8A0
SHA-256:	06910F058548C44A52ABA2D0F95F71C2F84B7CB608702A4D630DB06A5191D98E

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_4d42c1f24c11b6c9a2fc199d7a28c798fe9e5a_82810a17_173d852c\Report.wer	
SHA-512:	8A855DE218DAAEDF1479D6134A8513E7ED9836202A41B85AC90B3CF02F48B23EEE6E8DD8A4598D27732A394AB3F2EB08FEA7969B4ADC47B9ECFB513F4BADB153
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.=.1.3.2.8.5.0.0.9.6.1.9.8.8.7.7.1.8.8.....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.=.1.3.2.8.5.0.0.9.6.2.7.4.9.7.0.2.9.9.....R.e.p.o.r.t.S.t.a.t.u.s.=.9.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.6.2.f.2.8.9.9.8.-.b.6.2.1.-.4.3.c.8.-.a.9.4.d.-.0.b.d.9.d.1.e.3.a.5.3.8.....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.=.c.6.4.6.2.a.3.6.-.f.5.7.4.-.4.5.d.9.-.8.7.1.e.-.0.f.2.8.8.c.a.7.2.1.7.5.....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.=.0.0.0.0.1.9.5.4.-.0.0.0.1.-.0.0.1.b.-.c.6.5.4.-.d.2.5.1.7.5.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.!.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_dd9d398ae70aa8478325646a49f7ebef948b8_82810a17_125d0cc0\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):	1.0000448208544093
Encrypted:	false
SSDEEP:	192:sqifB0oXkHVzOMjed+x8/u7sOS274It7c:sqifvXsVzOMje3/u7sOX4It7c
MD5:	717352CD42907A1560CC3A9878394AF7
SHA1:	8219062D9152D35481EACA6E77AB659CCC92C01D
SHA-256:	3B77FF498A4AD8C84A4FCC826A420B93C27EB86B2FA2867D3F78A5502B96EFFC
SHA-512:	DDA2C9E5ED4D60F91CC0636184F3EEDD2F9ACE92C9C3A8C2BCEBB1C7386C0EB0DFE9E8CB966542A3E11A65152F6D18C7A8B7D2DBCF6356F4BBDC89293D22C047
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.=.1.3.2.8.5.0.0.9.6.2.4.1.2.5.1.7.1.3.....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.=.7.e.f.f.a.a.1.e.-.6.b.7.a.-.4.b.2.b.-.9.d.1.f.-.d.a.5.f.2.0.7.2.7.0.4.f.....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.=.7.5.a.6.5.c.b.8.-.4.3.a.4.-.4.2.f.a.-.9.c.0.6.-.4.2.5.a.0.3.7.e.4.1.f.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.=.0.0.0.0.1.9.6.0.-.0.0.0.1.-.0.0.1.b.-.f.3.d.6.-.c.e.5.1.7.5.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\WER427.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):	4.4479686247920664
Encrypted:	false
SSDEEP:	48:cvIwSD8zs5JgtWI9+i7WSC8BF8fm8M4JCdsA97Fej+q8vjsA9B4SrSOd:uITfLZiKSNYJyKKzzDWOd
MD5:	EEABF8D07101FD6411D2E76E3A546286
SHA1:	1D85E981286F68BBFBFEC81169E4766F082EE88F
SHA-256:	1A41F6023E303ED99DBA0945C98141C450E61F4D47C962479000937E7B5FE2B1
SHA-512:	4B090B15289481F7EFA4FBBA52A0A60B5CCF689EB8DCF1F9E8D0D28937BFBB4919431975D5558EAEE5E0ED329B27A333DFA34AA915BA0DF99165A5F3806E961E
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="1314817" />.. <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\WERE64C.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Sun Dec 26 16:27:01 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	46978
Entropy (8bit):	2.1386478701324085
Encrypted:	false
SSDEEP:	192:WmsgUOTajHiAM6SM4eO5Skb44ynjngyfxTIT/qw86om6nxTLzdeXYeq:bPabcBb5Lb44ynjgujqxTLz0l3
MD5:	206968ED73ECB16B39091E3625D9E8B0
SHA1:	2A98F0A379AAE0F97913FC801ECF159E09255E4E
SHA-256:	CFE4A48F936677001FD583B3956081ABCB47071C47667F57C36FDB7721078FBA

C:\ProgramData\Microsoft\Windows\WER\Temp\WERE64C.tmp.dmp	
SHA-512:	5DF3181BBE7CB38549AA965B8AA69EFD5984DB683C18834104A42009AA840947900261077FDEF7B92CB460F840891E129A6E74E43AD2636DDB6FB3350E151A1B
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....a.....`.....1.....T.....8.....T.....p.....U.....B..... .....GenuineIntelW.....T.....T.....a.....0..=.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .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\WEREE1D.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):	8272
Entropy (8bit):	3.6954724365915483
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiTa6ft16YnY66VgmfTwDSD+prV89bIZoSmsf7uZm:RrlsNiO6ft16YY66VgmfTUS1IZoSFf6U
MD5:	7DF9F40560D821B578853C8AC59820CF
SHA1:	AC4C351449BD25EA0C96154B639608C4DBDFC9E3
SHA-256:	72B22A8BBF5A8C54889D0C69E38A657A6E80ADD044B13984DF2FA06AE0E08D50
SHA-512:	1CEC619AA943A0811847BDE98A7E002BBF862C21C2D843B4A4F3F6E272F62BB08F404E17B5F3F2493D032B9D5932255612A558D75FDB60C51992872BD9686BCA
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.>.6.4.8.4.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF36D.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):	4.462773353078608
Encrypted:	false
SSDEEP:	48:cvIwSD8zs5JgtWI9+i7WSC8By8fm8M4JCdsA9DFoVk+q8/F5n/4SrSLd:uITfLZiKSN9JyVCVDWLd
MD5:	2B32C46F97FB98D0B8ED6299C04C3C60
SHA1:	ED6759009A19FA06FFB87EDBA2368A5C6A6018F9
SHA-256:	1A867D30844F3A066C98E1937B7F9BEA48BA66FCDD7D8413603B536A059E9431
SHA-512:	93B87F21C32F2BF80ED38233F9D46A62FDF3190A7F1E71E9D41CE010DBE97D23E9EFE0AC65DF1ED03FD9ED39B77526A4936ECADEE4EAAA70B063C6155F35E3E
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="1314817" />.. <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\WERF6D6.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sun Dec 26 16:27:06 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	48114
Entropy (8bit):	2.214478850648368
Encrypted:	false
SSDEEP:	192:spSTPOAweBQ1yPO5Skb0n5F8OAJBMhY7Cic64tYqRd:5R7Wp5LbauJJ7oOqf
MD5:	CDA1D8C55F50A313FF3D2A7329EBCAE7
SHA1:	96F7234CF1C8F68C220804F09D1C3AB22382D81C
SHA-256:	9CC5AF8951F9F570166671864ABC67DE2093209CC54F3495DB89B9CF96745D06
SHA-512:	BD069989775B4E5CCF8727CAA79E413D20F3E216E5888F247981A90785D42FF1D9C4A072A60324871F09DC0DB4600BC0F5C30CEC714BDCB7135A872A27442213
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF6D6.tmp.dmp	
Preview:	MDMP..... .....a.....|.....$...$ .....4.....`.....8.....T.....".....H .....4".....U.....B.....".... ..GenuineIntelW.....T.....`.....a.....0..=.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .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\WERF9.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):	8352
Entropy (8bit):	3.6888277131607947
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiwo6L6YnY6Dgmf8ZSY+pB789bI9ssf/ulm:RrlsNiX6L6YY6Dgmf8ZSKI9/f2o
MD5:	C67D9D1CFEB29DE16FC73541620A6BCC
SHA1:	2FA1A6B3F4D4FC257A7BC337F10061B33109CEAA
SHA-256:	C3D56890FC63DA7B18860D0C3C9B9761FD843466BB42707F6C7B418EA11FEEBF
SHA-512:	D9FEA34D57691311F930763F5BFAABCCE36CE3705337A9783152197E3E002F14DB5292B832B316D9D2D12FB6FA5CE99195AA3A85B06BD43AD8C47A9818561675
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.>.6.4.9.6.</.P.i.d.>.....

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):	4.240225930170385
Encrypted:	false
SSDEEP:	12288:vq9elvRGZTfXh9g7lg9YTkV8gUnsMhEhczXfTDaT6toEwdfj:S9elvRGZTfR9g7vhg
MD5:	B33794E3C6B1BEB6D6B2581831709E4D
SHA1:	BC9BB5B86AE5D7EC84E8F45ED0B93F5C03A27AE3
SHA-256:	2AC4F58765C291C6D51B5C2CA28421A9996607457DD0D05F8BF5275FC7F28759
SHA-512:	55DD41010C8783E6CE731A7FD38AB9A3897756A759264C7157E61F65DEC3E22B5ADE92CCE1564447005E2FB65E744C4F4B1B0867B8874A00C009F09EFEF43CA
Malicious:	false
Reputation:	low
Preview:	regfH...H...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^Z_gu..... ....kc[:..... .....

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):	3.407583074430547
Encrypted:	false
SSDEEP:	384:OH5GY5K5PPv4EgnVVeeDzeQ1NKZtjoT8GpwL1033SYH:ipKjg/eeDzeuNYtjpGpwLkSY
MD5:	3A7B0EC19DB89A30EB62BF9891DF07F8
SHA1:	95EA4D60CA49F5DB36207E645B5EB1B936190159
SHA-256:	1771EAB3A5D72F77997C3029E5900693DFDC0057DB2038548A9702B74864B397
SHA-512:	D355B50B97CBF4C65894924B0A115B91A5487AB96685FFB3F23349EC9E3F6214A24CFDC58DFDBBECADC5489A0E8C196FF039183A75052AB46C4639CB7CCBA6C
Malicious:	false
Preview:	regfG...G...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^Z_gu..... ....mc[:HvLE.N.....G.....-..{k!.dhS..... ..hbin.....p.\..,.....nk,..agu..... .....&...{ad79c032-a2ea-f756-e377-72 fb9332c3ae}.....nk ..agu..... ....Z.....Root.....lf.....Root....nk ..agu..... .....*.....DeviceCensus..... vk.....WritePermissionsCheck.....p...

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:	e4db910a4147ac44bef76f71e6b0d6bd193b89a6268dda35f3b1c210cc111fe4
SHA512:	c99e35f6313aa75f24b7bdb1cc9e91eb7246dd7cd79de9c18f50d1f6ee27984ff075c108d1025e16dbd6d03087d11bcb6f927c5773e8a03d7bdd02c204782a42
SSDEEP:	6144:4KMImhktm7mnmvetmzK/kxwv4Zm7mREqZzdazdULd54f3X0kdVtL8faGAPIX:49hXAg5aX0CL8fI
File Content Preview:	MZ.....@.....P.....E;...;...;.....Xl.....2.4.^....uh.{...6.F.....Xl.....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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.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: 6380 Parent PID: 5204

General

Start time:	17:26:21
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:	0xc30000
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: 00000000.00000002.1054100443.000000006E471000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6376 Parent PID: 6380

General

Start time:	17:26:21
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:	0x11d0000
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: 6496 Parent PID: 6380

General

Start time:	17:26:22
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:	0xa50000
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: 00000002.00000000.740603075.000000006E471000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000002.00000000.742949248.000000006E471000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 6484 Parent PID: 6376

General

Start time:	17:26:22
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:	0xa50000
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: 00000003.00000002.831692261.000000006E471000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000003.00000000.733407707.000000006E471000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000003.00000000.734461323.000000006E471000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 5728 Parent PID: 6484

General

Start time:	17:26:57
Start date:	26/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6484 -s 740
Imagebase:	0x2b0000
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: 4864 Parent PID: 6496

General

Start time:	17:27:01
Start date:	26/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6496 -s 864
Imagebase:	0x2b0000
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