ID: 544526
Sample Name:
triage_dropped_file.dll
Cookbook: default.jbs
Time: 15:58:24
Date: 23/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

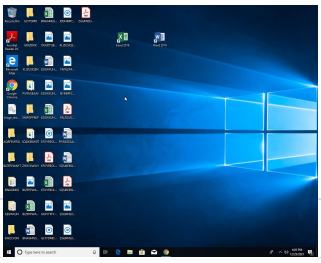
Windows Analysis Report triage_dropped_file.dll

Overview

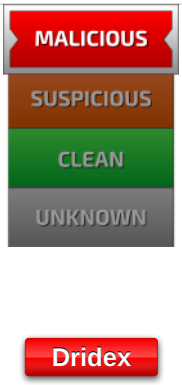
General Information

Sample Name:	triage_dropped_file.dll
Analysis ID:	544526
MD5:	7d424a845f21f90..
SHA1:	129162c1750520..
SHA256:	7f62e9d0e2cb735.
Tags:	22201 dll dridex
Infos:	

Most interesting Screenshot:



Detection

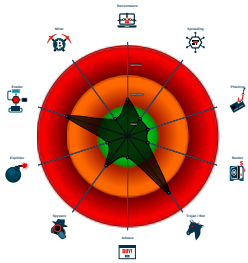


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 2332 cmdline: loaddll32.exe "C:\Users\user\Desktop\triage_dropped_file.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 4700 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\triage_dropped_file.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 6376 cmdline: rundll32.exe "C:\Users\user\Desktop\triage_dropped_file.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 1460 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6376 -s 672 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
00000000.00000002.694559765.000000006EB21000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000000.296075681.000000006EB21000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000002.00000002.324884043.000000006EB21000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000002.00000000.298180742.000000006EB21000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000002.00000001.292482173.000000006EB20000.00000004.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.rundll32.exe.6eb20000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
2.1.rundll32.exe.6eb20000.0.raw.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
2.1.rundll32.exe.6eb20000.0.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
2.0.rundll32.exe.6eb20000.5.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
2.0.rundll32.exe.6eb20000.2.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

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Dridex unpacked file

System Summary:

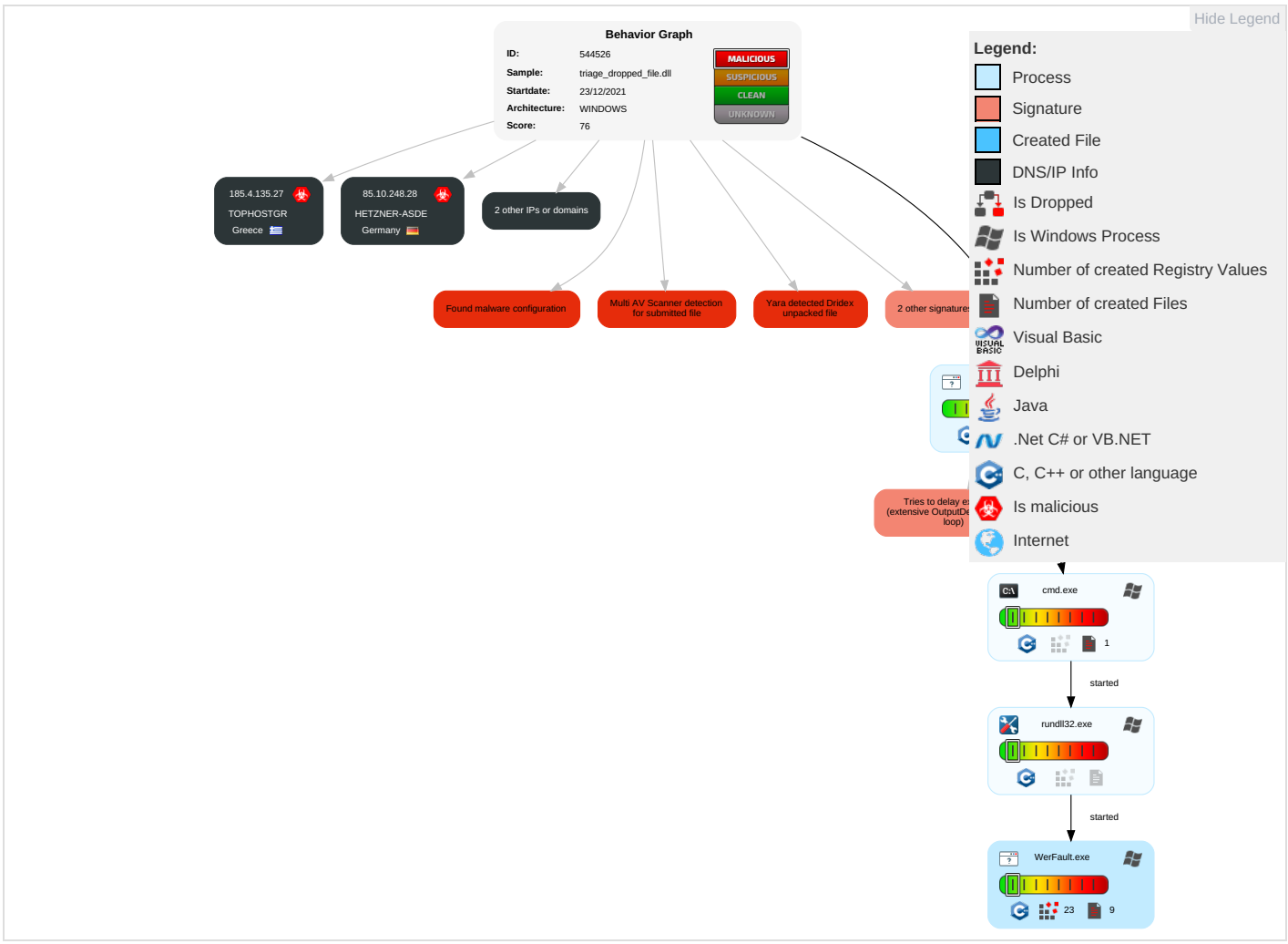
Malware Analysis System Evasion:

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

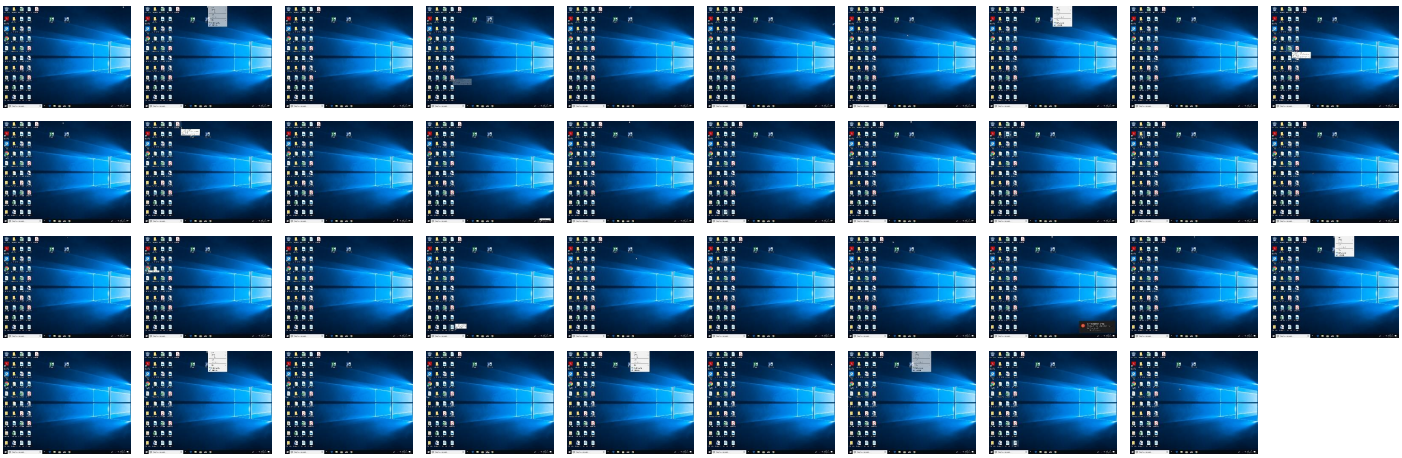
Behavior Graph



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
triage_dropped_file.dll	19%	ReversingLabs	Win32.Worm.Cridex	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.6eb20000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
2.0.rundll32.exe.1260000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.rundll32.exe.6eb20000.5.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
2.0.rundll32.exe.1260000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.rundll32.exe.6eb20000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
2.2.rundll32.exe.1260000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.1.rundll32.exe.6eb20000.0.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
0.2.loaddll32.exe.760000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.rundll32.exe.6eb20000.2.unpack	100%	Avira	HEUR/AGEN.1144420		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:	544526
Start date:	23.12.2021
Start time:	15:58:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	triage_dropped_file.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:	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: 95% (good quality ratio 92.4%) • Quality average: 78.8% • Quality standard deviation: 26.2%
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_3e2aba14ae6839fafa2e423496d524d852da7165_82810a17_041bce1d\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):	0.914992745908544
Encrypted:	false
SSDEEP:	192:CcXi390oX7m/HBUZMX4jed+9T/u7s6S274ltWc+:lXi3TXi/BUZMX4je0/u7s6X4ltWc+
MD5:	FFC283118AA06FE416FAFB456382ABA0
SHA1:	9A144EDE4DB5AF94BED38F4CBC76907AAAF22074
SHA-256:	8E42A49718BFB041FCDFEC95F0CB56404C26673C16E3CA3FD277D7FE700F6D98
SHA-512:	B7E5796FA394342342B7198665C186379D6F45ACB685F8738F9E5967007BA346851C21BFC6CD7E3D96B73B19154D3888F21F78971F1BEB3C414DB2F09D786095
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.=.1.3.2.8.4.7.7.7.7.3.1.8.9.7.6.4.9.2.....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.=.1.3.2.8.4.7.7.7.7.3.6.2.4.1.3.6.3.3.....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.=.0.5.9.2.2.a.6.c.-.4.b.f.a.-.4.d.0.2.-.9.2.e.6.-.a.f.3.0.f.0.5.3.b.c.7.3.....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.=.b.9.1.f.8.5.5.8.-.4.4.8.f.-.4.1.e.1.-.a.6.1.1.-.d.9.c.8.a.0.1.e.0.2.5.f.....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.=.0.0.0.0.1.8.e.8.-.0.0.0.1.-.0.0.1.c.-.2.f.9.e.-.d.5.7.c.5.9.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\WERB361.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Fri Dec 24 00:02:13 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	43206
Entropy (8bit):	2.189975589605877
Encrypted:	false
SSDEEP:	192:J2ZlWZxL5EcqNLO5SkbmAx//Cz8X+tH+Z/ift9yb7mNgR1n5:Jz9N5Lb2HZU/iV9ybIQ5
MD5:	4DED7EA4DBDB77A88A5165D62BA5657E
SHA1:	5745929C3EEE8276778432A70358FD7D21C3440D
SHA-256:	E5B50B049B76A84A855932293C56ABEECA7F0FB914C2162D151A98E2D50E1DC0
SHA-512:	DC346283D3067A695798153E6A8255320E667BB1388E95EE72C6CCB04576CA46C8AB2226978E01D1946B83C4E64E1C313D80D84B2386CFBCAC27EA33E2AC155
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....a.....-.....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\WERBB03.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):	8276
Entropy (8bit):	3.6904332711477816
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiBy67zHs9x6Y4R6CgmfT+PSuCprC89bOosfJ6m:RrlsNiU6Q6Ye6CgmfTGSNObf1
MD5:	483B84C6B648D40698425111147992D6
SHA1:	58ABB6F98BCD71702EC2A80684CE0501B6627801
SHA-256:	E8CE58DE9BC83D21AF4A6397844B5AFC072F30F413EAC882B41533FA9485EB8E
SHA-512:	E34A0A4C81750B458A29C38EEFB6B46D9DE207DB8604ED717067DFA7A9C42DA0D91561984940EAE82907919CCEF50CA39F931F8D1D684C1C1B3AEC6045B0734
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.>.6.3.7.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBD27.tmp.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4648
Entropy (8bit):	4.463350423834014
Encrypted:	false
SSDEEP:	48:cvIwSD8zsRJgtWI9ECWSC8BE8fm8M4JCdsFv2hFtUw+q8/iJKB4a4SrSzd:uITfjDDSN7Ja1dTaDWzd
MD5:	9387DBD51C297B4F39DAF45EC8D36822
SHA1:	9086AEFE076B0FA2C449CE254A1AAE33BB1544A4
SHA-256:	1A37AA5BFB91650D5CB1D5FC29A59425F5785443B44BC8AA287952D399476C1A
SHA-512:	5F0E05DC0D687197E864470F3CF740519CABD87ED809A4A77CAC03EC2226C8D4A6B34D0D4D8A512DD634CA05EE247C7B0FD1755B7B1FBACCB29FB2D35E09288
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="1310952" />.. <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

C:\Windows\appcompat\Programs\Amcache.hve	
Size (bytes):	1572864
Entropy (8bit):	4.278196954406433
Encrypted:	false
SSDEEP:	12288:TCcdS461PHcyy3k6a1i86+nhM/XdsVR9yVSxkKS0qulM19mvM1deCR:WcdS461PHcyy3kzj
MD5:	FEA865E0FCCBC94F2979F3F94AFE6133
SHA1:	BBC47B1C701145F06D00725B4D7B09404EC37A10
SHA-256:	24E3B616F120054E0D538D7DF9004BFA8694C18AE92E03769B3FB3D6B1AED83A
SHA-512:	D92F82E82D241B2DEE62C1E7BA019323FEC1F5D69A466B46D1D79848402EEC8F891CBEB0F4041D63784884B9CCD04165DD9E72F67151F8F3F9F4158B28BB6D9
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.A..Y..... ..... "..... .....

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):	4.035954912109526
Encrypted:	false
SSDEEP:	384:GEbK5Rftx1CPJ4XRsFcnE7k9PBqXSSeq5QMVyi6+/zl4Lk4uZd1DoXzn+XvwvL:DbURftx14J4XmFcE7yBqXxeq5QMVyi6B
MD5:	BAE518626246B42FE89E91F61E190EC2
SHA1:	35AB5793F7D83F7BD1B390C6E33CE36AF484C7A2
SHA-256:	53CEBE5670D00B7441257A65A6590732102309D73F210972C0F106A4BF303144
SHA-512:	D21040190C28A362F34EBDB8D62F65E73336F9E5ECE07328D9177011A6020781B3354CCCB88678F391A6CE578750C2B8B81BEEE97C284FAA32AFBB76BD1F033
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.A..Y..... ...."HvLE.^.....Y.....Bj-M...T....cR.....0..... ..hbin.....p.\..,.....nk,..A..Y..... ....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk .....Y..... ....Z.....Root.....lf.....Root....nk .....Y.....}..... .....*.....DeviceCensus..... .....vk.....WritePermissionsCheck...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.341748728708058
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:	triage_dropped_file.dll
File size:	565248
MD5:	7d424a845f21f905b17fb1e4ece26bc4
SHA1:	129162c17505204008b8c6345f78d8bd8e9d9548
SHA256:	7f62e9d0e2cb7358202052b4b20f43cec7eed7db11c57cfb372f8fddfb9307a3
SHA512:	abc7141739ffb23ba3e982796e697e33a5c3108fa7910cf97ca4fc6a1e9dbdadbd10b27665da4829f753794df3f0d2a79adfc9aee91863d60ec70042309bc6a6
SSDEEP:	12288:nGBK1zWlDqhPUVpqF9q9FAfPWvF+r3qTFCX1za7EV8RgfQOOvDC93:nNkIu2KAGIOwZ+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	0.389334542411	data	4.45862860296	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x7929c	0x7a000	False	0.303943071209	data	7.45743598814	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x82000	0x6b66	0x5000	False	0.246435546875	data	5.05789801748	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x89000	0x5dc	0x1000	False	0.090087890625	data	0.791740378228	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8a000	0x1834	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: 2332 Parent PID: 2144

General

Start time:	16:02:05
Start date:	23/12/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\triage_dropped_file.dll"
Imagebase:	0xa50000
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: 00000000.00000002.694559765.000000006EB21000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 4700 Parent PID: 2332

General

Start time:	16:02:05
Start date:	23/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\triage_dropped_file.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: 6376 Parent PID: 4700

General

Start time:	16:02:06
Start date:	23/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\triage_dropped_file.dll",#1
Imagebase:	0x1350000
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: 00000002.00000000.296075681.000000006EB21000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000002.00000002.324884043.000000006EB21000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000002.00000000.298180742.000000006EB21000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000002.00000001.292482173.000000006EB20000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 1460 Parent PID: 6376

General

Start time:	16:02:09
Start date:	23/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6376 -s 672
Imagebase:	0x220000
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