ID: 544201
Sample Name:
triage_dropped_file
Cookbook: default.jbs
Time: 20:30:19
Date: 22/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

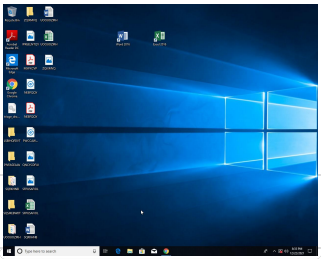
Windows Analysis Report triage_dropped_file

Overview

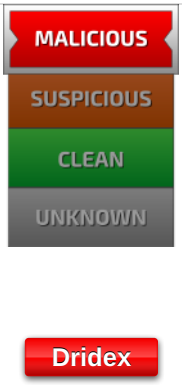
General Information

Sample Name:	triage_dropped_file (renamed file extension from none to dll)
Analysis ID:	544201
MD5:	232a73868213c0..
SHA1:	2de77f30b087dfb..
SHA256:	47738cc4c2025a…
Tags:	22201 dll dridex
Infos:	

Most interesting Screenshot:



Detection

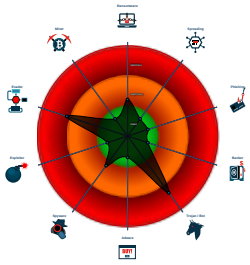


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 4388 cmdline: loaddll32.exe "C:\Users\user\Desktop\triage_dropped_file.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 2920 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\triage_dropped_file.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 5340 cmdline: rundll32.exe "C:\Users\user\Desktop\triage_dropped_file.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 5112 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 5340 -s 684 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

Threatname: Dridex


```
{
  "Version": 22201,
  "C2 list": [
    "144.91.122.102:443",
    "85.10.248.28:593",
    "185.4.135.27:5228",
    "80.211.3.13:8116"
  ],
  "RC4 keys": [
    "3IC8sFlUX9XZuoBQY9u5LhcZnHsV7E5r",
    "hnk63OiMfIbUqQnY7gkPwplwC0UeSZkZBYMCTYTjntqX7zsy9OvtNUlthJZXRtFF6P52Zbz6R5"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000000.669892514.000000006E7C1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000000.672146465.000000006E7C1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000000.00000002.1189977007.000000006E7C1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000003.00000002.703106750.000000006E7C1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
3.0.rundll32.exe.6e7c0000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
3.0.rundll32.exe.6e7c0000.5.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
3.2.rundll32.exe.6e7c0000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
0.2.loaddll32.exe.6e7c0000.2.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:

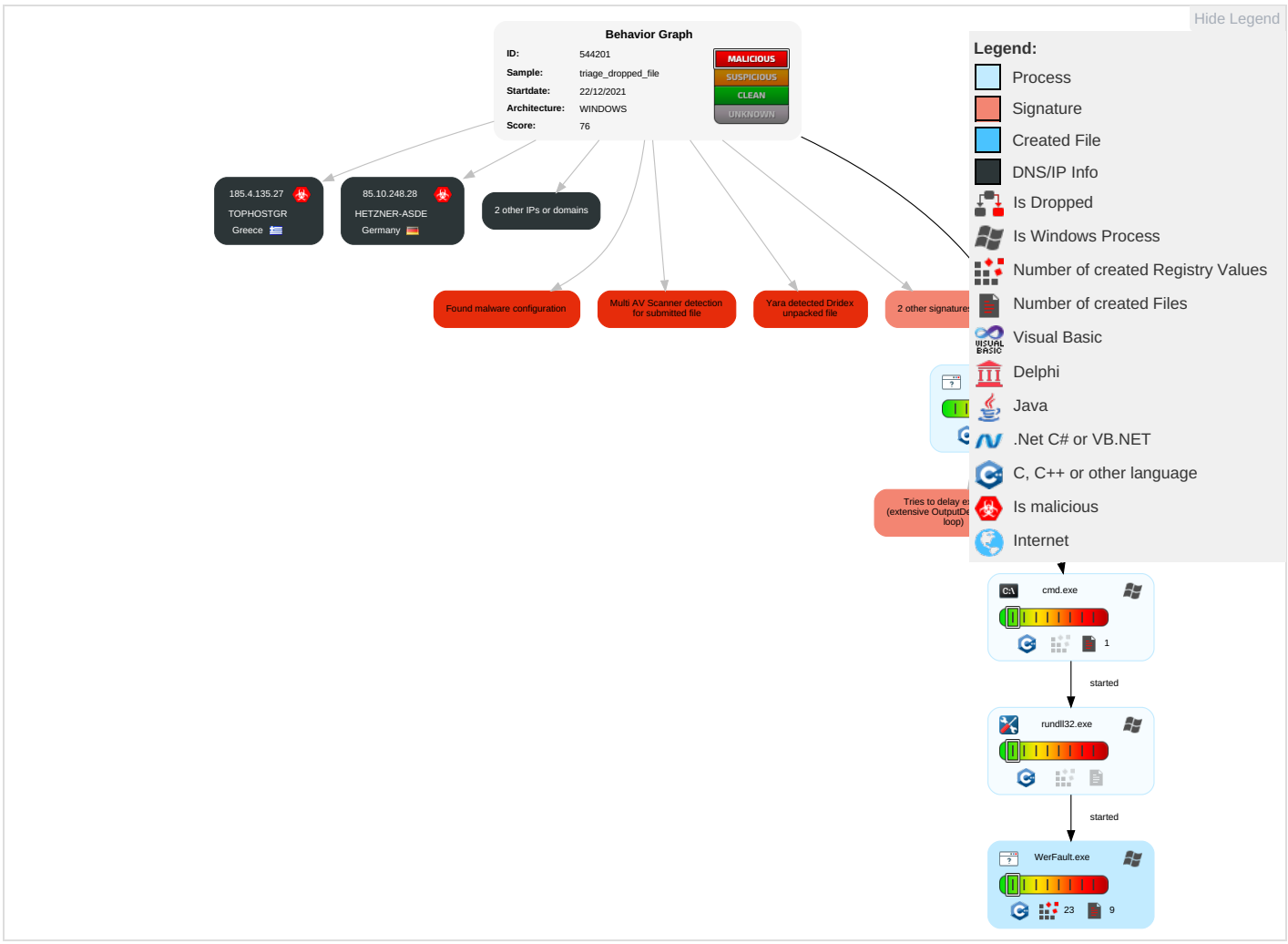
Malware Analysis System Evasion:

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

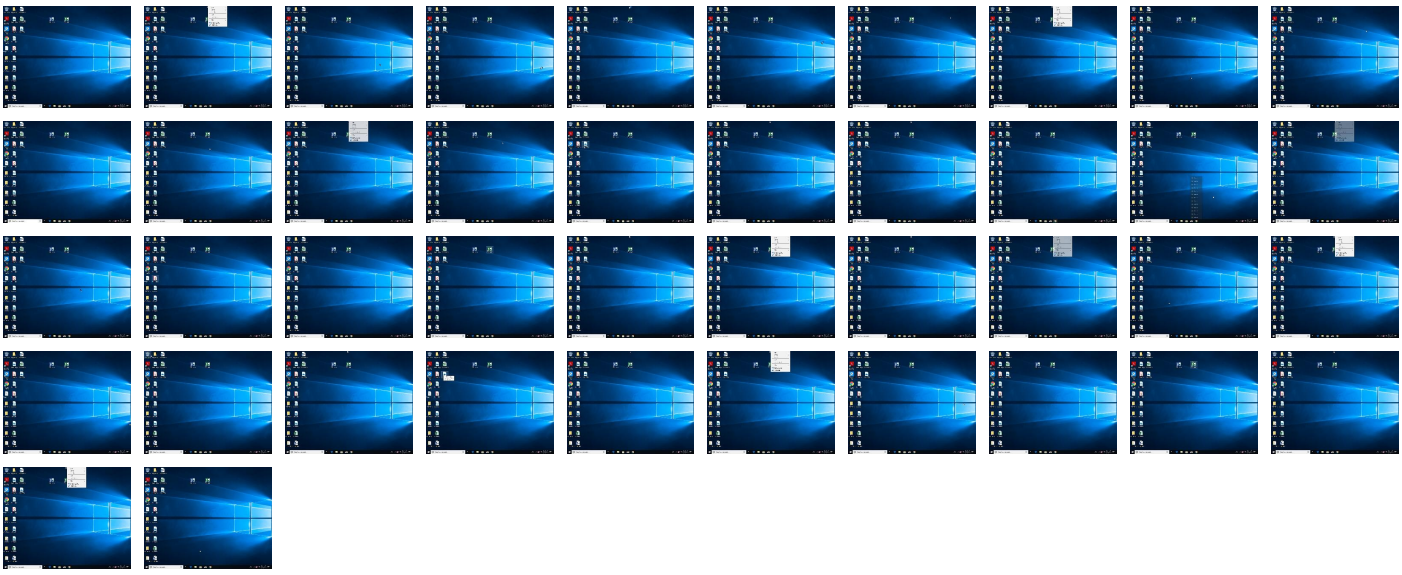
Behavior Graph



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
triage_dropped_file.dll	21%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.6e7c0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
3.0.rundll32.exe.6e7c0000.5.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
0.2.loaddll32.exe.e80000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.rundll32.exe.2fe0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.rundll32.exe.2fe0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.rundll32.exe.6e7c0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
3.2.rundll32.exe.2fe0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.loaddll32.exe.6e7c0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.forex-broker.websiteDVarFileInfo$	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:	544201
Start date:	22.12.2021
Start time:	20:30:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	triage_dropped_file (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:	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: 99.8% (good quality ratio 96.9%) • Quality average: 79.5% • Quality standard deviation: 26.1%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
20:31:35	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_ec6115aeb189d7d59bb1a88bf53c0a942c0e358_82810a17_1240230c\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):	0.9152035705418007
Encrypted:	false
SSDEEP:	192:OCpic0oXuF/HBUZMX4jed+9T/u7skS274ltWc:ti6Xq/BUZMX4je0/u7skX4ltWc
MD5:	B42CE31931FA6A0E0BF6D515319A6CCA
SHA1:	B1A7EF8C7B8C45A96775DE9D6228E820E07EA4CB
SHA-256:	8A81B01C2521FDBB80EFF7E0697995196337CEC627BC9CF68CD07E1385359275
SHA-512:	4BAC6D0CE3409052889C6C836377B5FAC669B83D06F6FDA4DE1209FD7F44B88D167441F2124F5572964A342290FB8C717422BC1A561B1CFA549B82A772B9F2CA
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.=.1.3.2.8.4.6.7.5.0.8.7.9.7.8.2.8.7.3.....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.=.1.3.2.8.4.6.7.5.0.9.3.8.8.4.5.0.5.4.....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.=.6.1.5.7.3.6.1.a.-.8.c.d.f.-.4.6.6.1.-.b.7.4.9.-.2.6.c.9.a.0.8.b.d.4.3.b.....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.=.2.8.8.2.3.8.c.b.-.3.7.6.c.-.4.e.0.e.-.8.8.d.9.-.4.8.6.4.6.9.4.2.c.8.c.6.....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.=.0.0.0.0.1.4.d.c.-.0.0.0.1.-.0.0.1.b.-.e.1.6.e.-.2.b.8.0.6.a.f.7.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\WER110D.tmp.xml

C:\ProgramData\Microsoft\Windows\WER\Temp\WER110D.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):	4.457245636674434
Encrypted:	false
SSDEEP:	48:cvIwSD8zsfJgtWI9+bkWSC8Bo8fm8M4JCdsFVhFTG+q8/ixBG4SrS0d:uITfBRb9SNjJRGuDW0d
MD5:	BD4C4D1C2D178201B210F3232F579AA7
SHA1:	4054FBB95D1509647774AF7861759C4957300668
SHA-256:	5BE01AEB609502CD0D3F0B665280555FEC363519E488364BDF1478A5708B98AB
SHA-512:	C40D72AA25519BCE50E1EC334622A7F92298443E8BD4D537AA1CC87CB3E4A68AF49410B7F5D863E3DBC4D428CF216A5AFFF3346590DECF1F9B5E1C2FC38EF0 59
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="1309242" />.. <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\WER747.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Wed Dec 22 19:31:29 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	43998
Entropy (8bit):	2.154852029864072
Encrypted:	false
SSDEEP:	192:LHWEIZVOdmO5SkbmRPHWu7tEXJZkRrcTpKIsp4YPQlKC2:6EIW5LbWHOEqpmhPQlS
MD5:	81784F986C251801998945F25F9F1596
SHA1:	9A1C1617CD8EEE41D6FCB0196E2228F267456999
SHA-256:	5F145465162E5568CCDAADA9B232D48CA439B2BBAA54033664A841EA983211EE
SHA-512:	92DC53A2B6C111CBD593AFE3CD1126F8C0D79D6A05AA2A417F2BC505F8443419C63978AB201AB4F6D1C5BC5B3E486C90D22AC5CEB8F9B3616BFD5AE46E6E2 68
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....}.a.....-.....T.....8.....T.....@.....U.....B..... .....GenuineIn telW.....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\WERE4D.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):	8278
Entropy (8bit):	3.6919358880255273
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi3o67zzL06YSj6ngmfT+KS4rs+prm89bZ1sf7zm:RrlsNi46U6Y26ngmfTrS0ZOf+
MD5:	7A305581E9CD501E9E74F1F75A83494C
SHA1:	F78406D8117B4E4ACA3464EB31C18F6E756BC5D7
SHA-256:	D9E3B50901899C276A4DAFC281D5F601FDEEF9497AEFE4DD9A81BB726CCAB894
SHA-512:	61C510D79CCF3842E361F227E59C3A3BBF3DA463B5B9ABC3BAD9FD763B4095CCF9CC543AF127104F078177AAA8F2FE94AF5A9D2F833C30D6E9EA2054633E15 B
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.>.5.3.4.0.<./.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

C:\Windows\appcompat\Programs\Amcache.hve	
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.24513602723487
Encrypted:	false
SSDEEP:	12288:I7+oXtLSfBiusoJGm+9JnHHNapijT2+KXAostH6LmWYYGOuh:M+oXtLSfBiVoJGjNa
MD5:	B7EF2E84C38B892A92DAFFA1CF79B2DC
SHA1:	72CB6C55844EB597F91ED0E344A76A040F2883A6
SHA-256:	5037295BF78701F84932B0E003DC5BAE82DD24C8C88F2CFA3EF1B8C38C156BE8
SHA-512:	D97E3AC086DAAB4BCAF8471149704DB2A8A5E6F010D0D3126744CBB51E82EDA4C246575F22123082B514DFE7C5326B1977D83805799D613147F309DCEE535A4
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*..j..... ....

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):	3.410465000893189
Encrypted:	false
SSDEEP:	384:8bf5K5KPv4EgnVVeeDze11NKZtjtT8Gpwe1b33SYd:EhKig/eeDzePNYtjSGpwetSY
MD5:	5A328D1BCB75D088428D8FBFC4F31E0D
SHA1:	E931C0C197B38575BDCEA151CB5F42250721DE8F
SHA-256:	5F9A3CDC8BFEDF1710693C4F00387FB64D144AF4336BBF12AC7A22C44E5EB122
SHA-512:	CA960CF2EE982A27EFD8464AE90FABD8ACB564F9BCBA2E94920B777D38AC1E3935A87257F16F3A2904C12F21292ECBB8FA7A47B766813FC057713F6E0E55F119
Malicious:	false
Reputation:	low
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*..j..... ....HvLE.N.....G.....D.....e=..... ..hbin.....p.\.....nk,.x@.j..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk .x@.j..... ....Z.....Root.....lf.....Root....nk .x@.j..... .....*.....DeviceCensus..... vk.....WritePermissionsCheck.....p...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.220126206743121
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:	232a73868213c05f54359f7d7c5d349f
SHA1:	2de77f30b087dfb182e414c341c6d6426e752fd9
SHA256:	47738cc4c2025a2f4655695777fabde7c80bf272406b4dd89efbfab34ff5780b
SHA512:	4d01ebbf6745ba652109459634916b283c3fb00017f23e9b40aff690107a75b4348aebd920ef80a912b866e55b339547fb0ec151f446b8e5ddb6987147d63a33
SSDEEP:	12288:snYoMi8KFy86zc86boq67oy6zq86xoG6V2C6FoE69oI6Vo8mHo06zo8knoz5fU56:sil0+2OJljTR
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

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10004cd0
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:	0x61C34004 [Wed Dec 22 15:11:00 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:	6c630f89c340001062a2ada6a2273a4d

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x1000	0x66be	0x7000	False	0.380684988839	data	4.37366562379	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x7916e	0x7a000	False	0.283385229892	data	7.33168362555	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x82000	0x634f	0x5000	False	0.247509765625	data	5.01040935971	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x89000	0x2f0	0x1000	False	0.09033203125	data	0.788492020975	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8a000	0x1d9a	0x2000	False	0.242309570312	data	4.16996433109	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: 4388 Parent PID: 1444

General

Start time:	20:31:21
Start date:	22/12/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\triage_dropped_file.dll"
Imagebase:	0x10c0000
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: 00000000.00000002.1189977007.000000006E7C1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 2920 Parent PID: 4388

General

Start time:	20:31:21
Start date:	22/12/2021
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:	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: 5340 Parent PID: 2920

General

Start time:	20:31:22
Start date:	22/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\triage_dropped_file.dll",#1
Imagebase:	0xf70000
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: 00000003.00000000.669892514.000000006E7C1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000003.00000000.672146465.000000006E7C1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000003.00000002.703106750.000000006E7C1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 5112 Parent PID: 5340

General

Start time:	20:31:25
Start date:	22/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 5340 -s 684
Imagebase:	0x1100000
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