ID: 544521
Sample Name:
triage_dropped_file
Cookbook: default.jbs
Time: 15:41:11
Date: 23/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

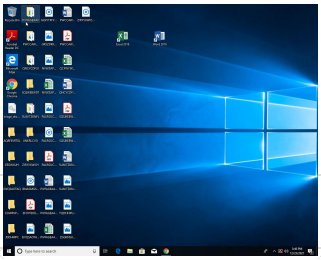
Windows Analysis Report triage_dropped_file

Overview

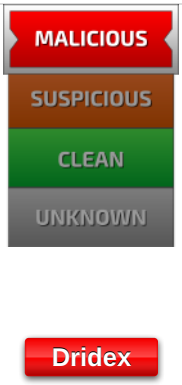
General Information

Sample Name:	triage_dropped_file (renamed file extension from none to dll)
Analysis ID:	544521
MD5:	e95ef0e572a9b18.
SHA1:	dec119bc3ac328…
SHA256:	7c86d999e3b4df3.
Tags:	22201 dll dridex
Infos:	

Most interesting Screenshot:



Detection

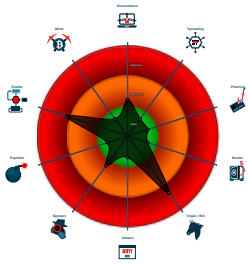


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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: 6128 cmdline: loaddll32.exe "C:\Users\user\Desktop\triage_dropped_file.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 5968 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\triage_dropped_file.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 4000 cmdline: rundll32.exe "C:\Users\user\Desktop\triage_dropped_file.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 3568 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4000 -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",
    "hnk63OiMfIbUqQnY7gkPwplwC0UeSZkZBYMCTYTjntqX7zsy9OvtNUlthJZXRtFF6P52Zbz6R5"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.310193138.000000006EBC1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000000.287871322.000000006EBC1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000000.00000002.808180663.000000006EBC1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000002.00000000.286654390.000000006EBC1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
2.0.rundll32.exe.6ebc0000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
2.0.rundll32.exe.6ebc0000.5.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
2.2.rundll32.exe.6ebc0000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
0.2.loaddll32.exe.6ebc0000.2.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:

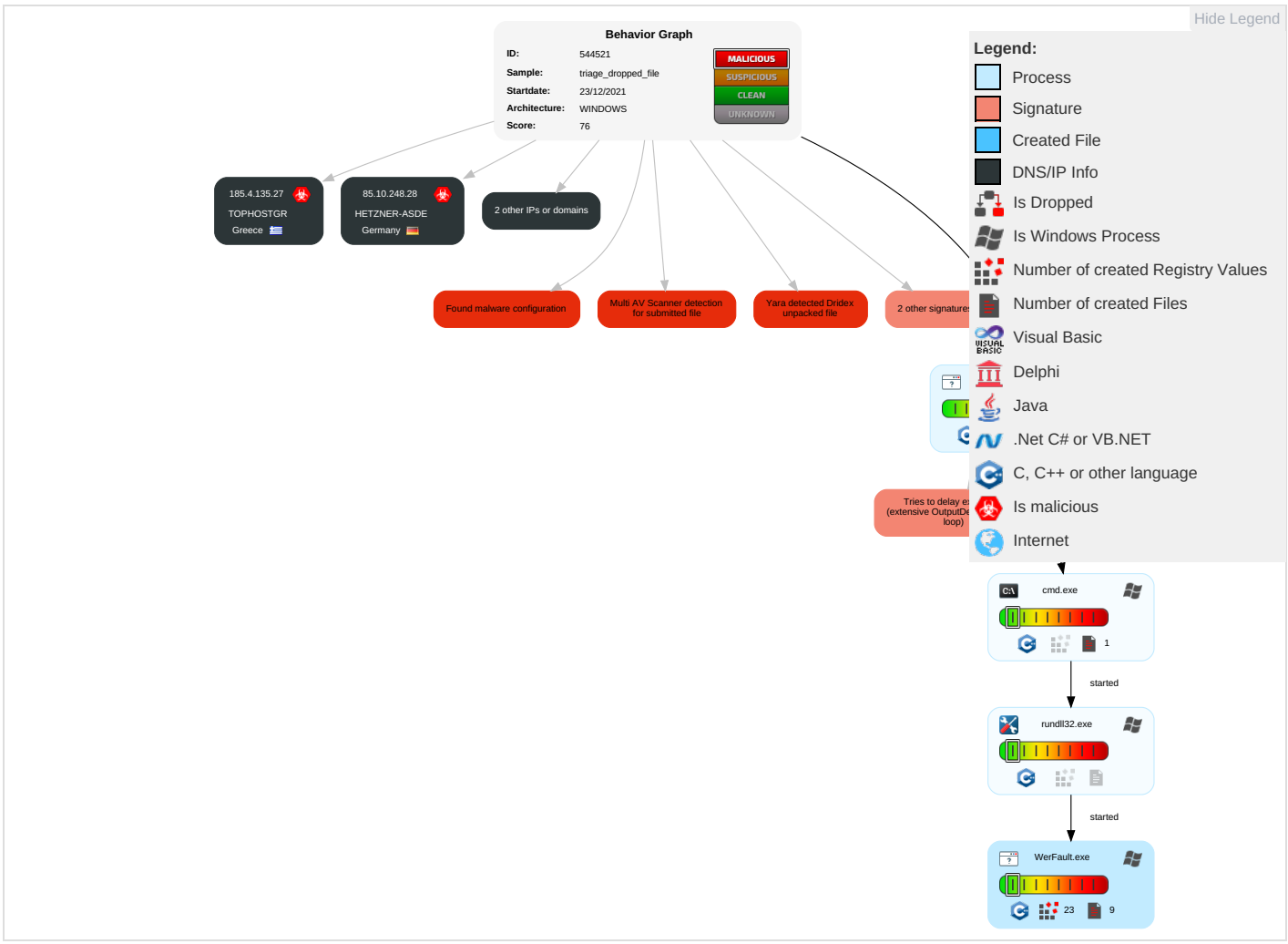
Malware Analysis System Evasion:

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

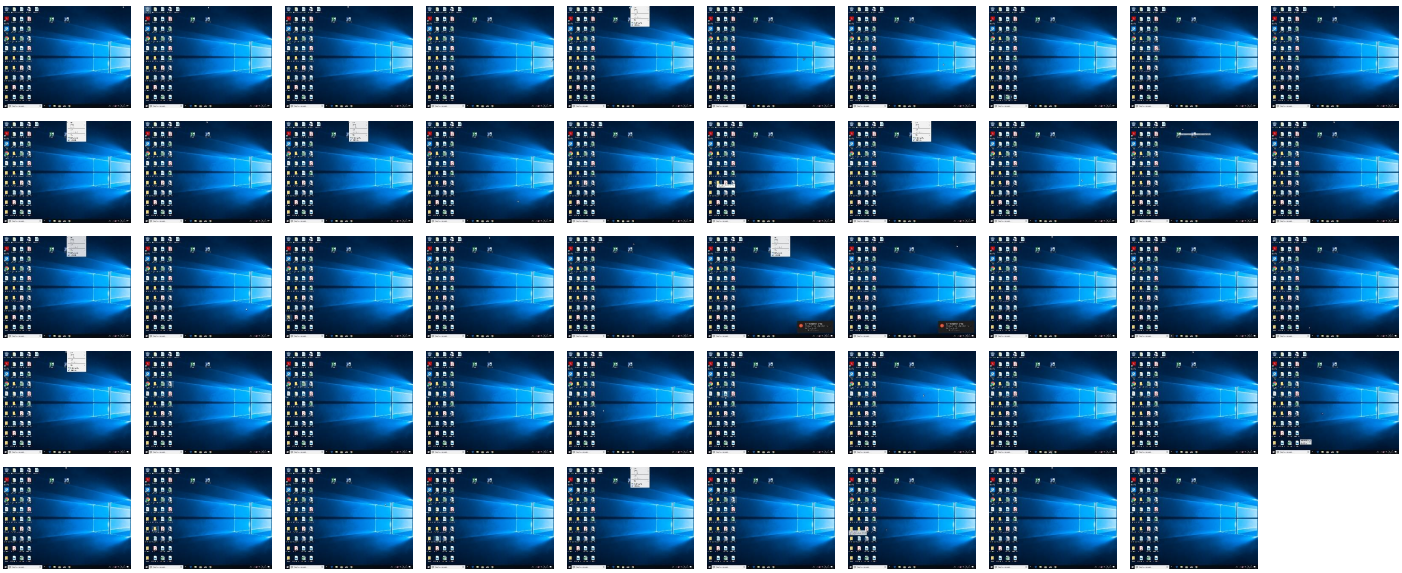
Behavior Graph



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	19%	ReversingLabs	Win32.Worm.Cridex	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.loaddll32.exe.6ebc0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
2.0.rundll32.exe.6ebc0000.5.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
0.2.loaddll32.exe.5f0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.rundll32.exe.2980000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.rundll32.exe.2980000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.rundll32.exe.6ebc0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
2.2.rundll32.exe.2980000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.rundll32.exe.6ebc0000.2.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:	544521
Start date:	23.12.2021
Start time:	15:41:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 46s
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:	29
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: 95.8% (good quality ratio 93.8%) • Quality average: 79.6% • Quality standard deviation: 25.2%
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
15:42:16	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_3e2aba14ae6839fafa2e423496d524d852da7165_82810a17_0cfc6ceb\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):	0.9145295751866201
Encrypted:	false
SSDEEP:	192:KoqiR0oXRm/HBUZMX4jed+9T/u7sIS274ItWc:AifXg/BUZMX4je0/u7sIX4ItWc
MD5:	7FD6435C602BD7E08973C8968953B87D
SHA1:	E91C943C78187709410FF7A2D5F32A11C4CC1B4F
SHA-256:	C9776CF688D0355A7F16DF3418C726CAA6F3FC7BCD90F02395CC5F98977F8EE8
SHA-512:	B9C6227C75F01C5313BFE1E4049B102E5C270D1CCE7A6FACD5CF35AB814309A13251D99754647B94A4E6E41B23852FDCEFB6D6A5F28ED7E848B306112D1ECBB
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.=.1.3.2.8.4.7.7.6.5.3.0.9.9.8.4.3.4.2.....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.=.1.3.2.8.4.7.7.6.5.3.5.3.1.0.9.1.4.8.....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.=.a.1.6.2.6.a.1.6.-.3.d.b.e.-.4.e.3.a.-.b.d.8.1.-.0.9.3.a.3.7.a.0.c.d.4.7.....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.f.d.b.e.d.e.3.-.2.3.d.4.-.4.f.7.c.-.a.0.6.4.-.a.8.7.9.1.f.3.f.e.0.0.8.....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.=.0.0.0.0.0.f.a.0.-.0.0.0.1.-.0.0.1.c.-.0.e.9.a.-.e.7.b.0.5.6.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\WER5675.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Thu Dec 23 23:42:12 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	43954
Entropy (8bit):	2.153938265643367
Encrypted:	false
SSDEEP:	192:458pHEc6e5C0zdZnO5SkbmGsyo7S/zpUwDP1iPgpYG:xN+MZO5Lb3lNzplDP1k
MD5:	62679E32234FCD9B0C336CBFB27CDE8E
SHA1:	1DC7B8FC9659ED0BB69F8B29F822EA8867C8B9E4
SHA-256:	ECC26AFE2B4B4BF647269FF4450C860F7593D99B6CA851EEC5F1B2521C370076
SHA-512:	984DC983F4520FFE2CEE2206098A20D0CF9DC534DC9BDC65038571BEB291FDB64F65C6AEA676BB9D50A01B0ADB19BFD190B82A34BBB16471B5AACFE8AB52518B
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....T..a.....-.....T.....8.....T.....U.....B..... .....GenuineIntelW.....T.....L..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\WER5EB3.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):	3.6926922388463868
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi5867z7Me6YBXa6CgmfT+PSNzCprK89b0Csf0OVcm:RrlsNiC6R6YBK6CgmfTGSC0Bfv
MD5:	01763B43E3A0821D6CC879204780C984
SHA1:	30415EF138A952B8947AB3CAD8EF3D048683F684
SHA-256:	DCA0FC6EAE971634A72EE41A1FFAAF3ED63DC95B7241345D2241DEA63913717E
SHA-512:	1FEA82AD59C9BC769F9D515AF3DF430E4BCD8D489392CEF634B5977D517C66EB8291FFFD7BB3F9677D1531AB174E01FE022005F706F9AC59ADB646D1C2E6D36
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.4.0.0.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER60D7.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):	4.463207964222361
Encrypted:	false
SSDEEP:	48:cvIwSD8zsrJgtWI9XOjjYWSC8B38fm8M4JCdsFv2hFk+q8/iJKBfZ4SrSZd:uITfFuOjjRSNGJjPdQZDWZd
MD5:	340243A8285D55C6E0119BCE93BB9DA4
SHA1:	F925A38C7884A814EFECE181BAB42C5D1638E874
SHA-256:	950D73354BC3780991AC2AF8F3D78B2BEBB2FF6D80069DD3D9A969917E2B1682
SHA-512:	10F1DAAFBFD26C93D0697E0989F05F066354DB39E8123B3AAB53CC1BC30F6AD5CF5938EDE9FFF2559C594028E54AFCC1EB2A7ECB582FA24ADE5BC400F3BA489
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="1310932" />.. <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

C:\Windows\appcompat\Programs\Amcache.hve	
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.2769153201685866
Encrypted:	false
SSDEEP:	12288:oRJk7B3tKO1oYipLoRNQalCxPtSEYeGXuTyxq6ms7ExFHPWfExp/th:qJk7B3tKO1oYipbZ
MD5:	AED9403D47618427407BABA250362EAB
SHA1:	912FB922E00821D80DCA7FB90906185 51B095695
SHA-256:	4315DD9C14317137FD0341F0D0DB47AEDBAA190F3629D8DE24D99E15262CCF0E
SHA-512:	06DDDC19ADFA942109AB6C65BFCEEAA7AB9274D1AC1CD0E2315D5B27EAA08BA4C05A05E2435CB1FC7BC3BF1C9F47AD5AB9E61982E613A056F030DC3F79F5E9BE
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.rmtmn .V..... ....xk..... .....

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):	4.032274875706708
Encrypted:	false
SSDEEP:	384:sKRz5Rftx1APJ4X3sFcnE7kzPBqXwSeq5QMVyi6+/Gl4Lk4TZd1DoXznxXvwvK:rRNRftx1WJ4X8FcE7sBqXDeq5QMVyi6C
MD5:	F9BAEE3671339D97B56361E9C7CF5629
SHA1:	0433770FD143178E0C91760EC44B781325385288
SHA-256:	00673A62F7F1F37E4E208A54F48A719C89B4E639F4773B35E6A3EAA2FD04708A
SHA-512:	60C9856032F3CAB00EB18205B908FAE69C320D6F65AF222645617BC36CEE67BEEE9C9185CEA425DEFD01941DE857F0F35E34F882F9992D0FFE2FD7D84FC2326
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.rmtmn .V..... ....~k..HvLE.^.....Y.....e. ..(..RK.....0..... ..hbin.....p.\.,.....nk,..E.V..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ..E.V..... ....Z.....Root.....lf.....Root....nk ..E.V.....}..... .....*.....DeviceCensus..... .....vk.....WritePermissionsCheck...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.341977764373263
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:	e95ef0e572a9b18fdb848cfe2c56d3e5
SHA1:	dec119bc3ac328ce0f914731182d2109381d6d0a
SHA256:	7c86d999e3b4df3541fda635146705484b6216ae82cf614a3b576441e4092246
SHA512:	44071dff18f49dd9b6bd243ef61ab5d9b3c41d3f399acc48da1e9e465d32aab07e488161b9b01ea75fa2e2fe36f512863518c3a5df0927a99b300f2c45710f9c
SSDEEP:	12288:qGBK1zWlDqhPUVpqF9q9FAfPWvF+r3qTFCX1za7EV8RgfQOOvDC93:qNkIu2KAGIOwZ+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

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	0.389997209821	data	4.4630822385	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x79c1d	0x7a000	False	0.303941070056	data	7.45740090867	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x82000	0x6178	0x5000	False	0.246435546875	data	5.05789801748	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x89000	0x2f0	0x1000	False	0.090087890625	data	0.791740378228	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8a000	0x1d22	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: 6128 Parent PID: 3120

General

Start time:	15:42:04
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:	0x1000000
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: 00000000.00000002.808180663.000000006EBC1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 5968 Parent PID: 6128

General

Start time:	15:42:04
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: 4000 Parent PID: 5968

General

Start time:	15:42:05
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:	0x880000
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: 00000002.00000002.310193138.000000006EBC1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000002.00000000.287871322.000000006EBC1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000002.00000000.286654390.000000006EBC1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 3568 Parent PID: 4000

General

Start time:	15:42:08
Start date:	23/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4000 -s 672
Imagebase:	0x1180000
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