ID: 545443
Sample Name: L0mddDYjoL.dll
Cookbook: default.jbs
Time: 17:25:20
Date: 26/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

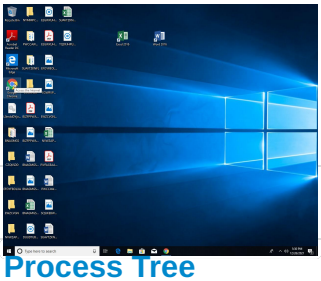
Windows Analysis Report L0mddDYjoL.dll

Overview

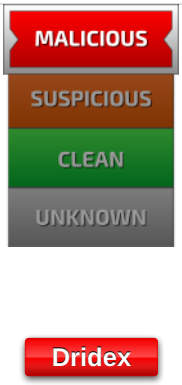
General Information

Sample Name:	L0mddDYjoL.dll
Analysis ID:	545443
MD5:	0d9cc367aa4abc…
SHA1:	cb6db576bbe636..
SHA256:	1bd2e431f2631a5.
Tags:	32 dll Dridex exe trojan
Infos:	

Most interesting Screenshot:



Detection

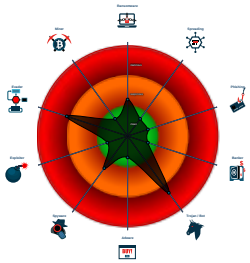


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected Dridex unpacked file
- Multi AV Scanner detection for subm…
- Sigma detected: Suspicious Call by …
- Tries to delay execution (extensive O…
- C2 URLs / IPs found in malware con…
- Machine Learning detection for samp…
- Creates a DirectInput object (often fo…
- Uses 32bit PE files
- Found a high number of Window / Us…
- AV process strings found (often use…
- Sample file is different than original …

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6400 cmdline: loaddll32.exe "C:\Users\user\Desktop\L0mddDYjoL.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 5696 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\L0mddDYjoL.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 4988 cmdline: rundll32.exe "C:\Users\user\Desktop\L0mddDYjoL.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 5924 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4988 -s 728 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 6340 cmdline: rundll32.exe C:\Users\user\Desktop\L0mddDYjoL.dll,Wgpomsdeeomtunmdrt MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 5652 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 6340 -s 848 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
00000005.00000000.371795691.000000006E9A1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000005.00000000.369759856.000000006E9A1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000006.00000000.363470341.000000006E9A1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000006.00000002.389367218.000000006E9A1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000001.00000002.685190249.000000006E9A1000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
Click to see the 1 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.0.rundll32.exe.6e9a0000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
6.0.rundll32.exe.6e9a0000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
6.0.rundll32.exe.6e9a0000.5.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
1.2.loaddll32.exe.6e9a0000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
5.0.rundll32.exe.6e9a0000.5.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:

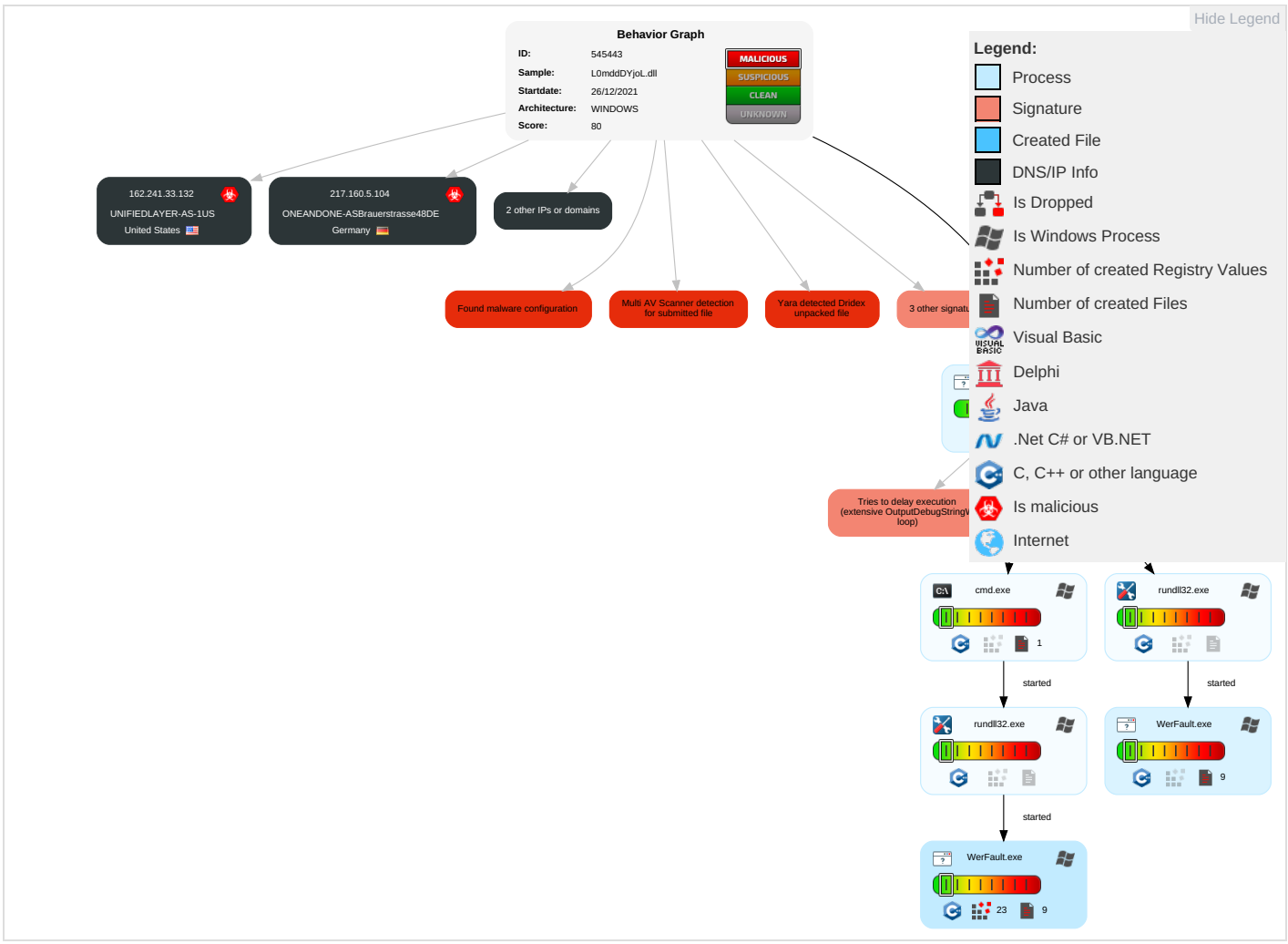
Malware Analysis System Evasion:

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	Input Capture 1	Security Software Discovery 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop (Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Process Injection 1 2	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rundll32 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poir
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

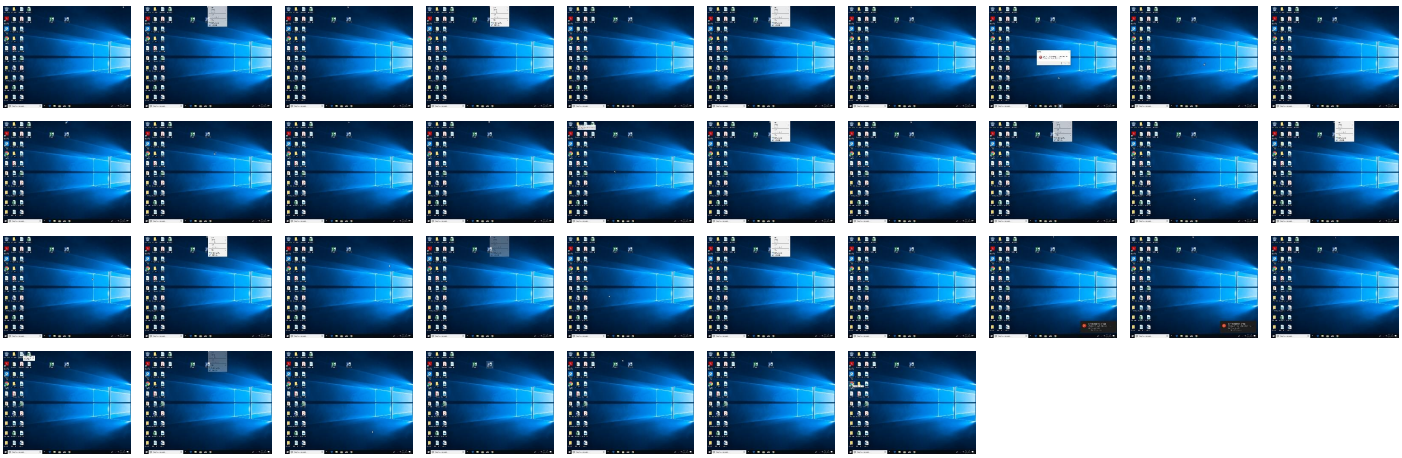
Behavior Graph



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
L0mddDYjoL.dll	63%	Virustotal		Browse
L0mddDYjoL.dll	67%	ReversingLabs	Win32.Infostealer.Dridex	
L0mddDYjoL.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.rundll32.exe.bf0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.loaddll32.exe.6e9a0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
5.0.rundll32.exe.2f40000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.0.rundll32.exe.6e9a0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
5.0.rundll32.exe.6e9a0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
5.0.rundll32.exe.2f40000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.0.rundll32.exe.bf0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.rundll32.exe.2f40000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.0.rundll32.exe.6e9a0000.5.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
5.0.rundll32.exe.6e9a0000.5.unpack	100%	Avira	HEUR/AGEN.1144420		Download File

Source	Detection	Scanner	Label	Link	Download
6.2.rundll32.exe.6e9a0000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
6.0.rundll32.exe.bf0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.loaddll32.exe.960000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

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

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	545443
Start date:	26.12.2021
Start time:	17:25:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	L0mddDYjoL.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:	28
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: 99.8% (good quality ratio 94.2%) • Quality average: 77.3% • Quality standard deviation: 28.8%
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_929199edf0b5e1a671cd932c57bd132abfcfef1_82810a17_17b46e91\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):	0.9969512980665527
Encrypted:	false
SSDEEP:	192:JPiH0oXLHVzOMjed+J8/u7sxS274lt7c:JPi5XrVzOMjev/u7sxX4lt7c
MD5:	F0033206EB8AD55F047E545A9482C4FC
SHA1:	357E0C8E4966FF45179AAC1B2267E469617BED27
SHA-256:	580F1B6638CEC90D96D129D4E7A81C7E883052527FE33312E54BFB08D649C554
SHA-512:	370829816F6CE02BFECEAB66EB118811EBC23CA0B3DB680DDA85A44564D359B8889AD726836260EA81E40E44BE74CE906E17477BECAA1804A113A452B27EBC E

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_929199edf0b5e1a671cd932c57bd132abfcfef1_82810a17_17b46e91\Report.wer	
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.5.0.4.2.0.6.7.8.3.8.8.6.0.4.....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.=.1.f.5.8.1.8.f.d.-.3.f.c.6.-.4.8.d.b.-.8.4.9.0.-.d.1.9.4.1.4.3.1.0.1.f.9.....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.=.8.3.e.f.3.0.8.9.-.3.2.f.a.-.4.6.0.8.-.8.2.6.c.-.e.1.7.6.1.2.c.e.b.f.6.0.....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.c.4.-.0.0.0.1.-.0.0.1.c.-.2.3.d.c.-.a.a.d.a.c.0.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\ReportQueue\AppCrash_rundll32.exe_fb9152841665ded0dbf17d9a73851f865888cee_82810a17_168461a0\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):	0.9651697352998475
Encrypted:	false
SSDEEP:	192:7dv6iD0oXPCHBUZMX4jed+JU/u7sxS274ltWc:Rv6idXSBUZMX4je//u7sxX4ltWc
MD5:	D599339891655D6254BF62FE10A78944
SHA1:	4FAF72D52A6FB4F891A9ABD30EC3909AE7A878D0
SHA-256:	90151AC6D1A756A1E8D302CADFA11C67F9C1356E188C11CA62012DD49AD9AFC0
SHA-512:	D21BA0B4483D38A3EBD255D5E0E6F9283158E3DCA1AA29C5A8D479E1632B95D7F0B27EA68EEB1031733699B6F9AC83A3EC86CD633E45EF77F2A047DE6C64394
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.5.0.4.2.0.6.3.8.7.1.2.2.8.4.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.8.5.0.4.2.0.6.8.4.1.8.0.8.8.9.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.7.a.9.1.e.f.f.0.-.e.3.a.9.-.4.b.a.9.-.b.6.9.e.-.0.a.a.4.2.7.d.b.6.c.0.3.....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.=.4.d.6.3.7.2.9.0.-.2.c.2.e.-.4.6.6.b.-.b.9.f.b.-.3.7.3.7.3.9.0.d.7.5.1.e.....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.=.0.0.0.0.1.3.7.c.-.0.0.0.1.-.0.0.1.c.-.1.a.9.7.-.a.e.d.a.c.0.f.a.d.7.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.0.f.5.1.9.f.e.e.c.4.8.6.d.e.8.7.e.d.7.3.c.b.9.2.d.3.c.a.c.8.0.2.4.0.0.0.0.0.0.0.0.!.0.0.0.0.b.c.c.5.d.c.3.2.2.2.0.3.4.d.3.f.2.5.7.f.1.f.d.3.5.8.8.9.e.5.b.e.9.0.f.0.9.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4A30.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Mon Dec 27 01:27:45 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	47434
Entropy (8bit):	2.089972974158097
Encrypted:	false
SSDEEP:	192:QjuMBqmBiU0zx+IbO5SkbuGssI+uOksRyWfJ9BRYf4ynhVGkoFbE0mnrK:gq5UG+15LbuGssIk9g4ynTGkyHmnrK
MD5:	1DFA4E8F9E2D879586116D458E321E87
SHA1:	3F7F518F7C55A9BCFBECE1ACF9FA8E2DF6EE7838
SHA-256:	EB14E0288F47EAE18EFEC8D3849AAF1BEF74CBF03C9C50CCB0211F0A3D113096
SHA-512:	BCE1008E74F16A52EA535CA4EEE287CFDB97EC00EB19C79B8A6339EBC7812138C2D86DA2868FAFE2295843E4DD9D7052A81EE505A09D653935238B1FA052BCB
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....a.....`.....1.....T.....8.....T.....R.....U.....B..... .....GenuineIntelW.....T.....|...h..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\WER5201.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8270
Entropy (8bit):	3.693943868682352
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNi466B6Y3s6fB2gmfT4DS7Cpry89b95psfCQX5m:RrlsNi96B6Yc6p2gmfTMSY95CfCI0
MD5:	1FF324457E7728C5BE90DF5B2613103E
SHA1:	827B125771E315405BD68CA1CE4AF1B194830E01
SHA-256:	1F9FF71BF40348304DD8F27406FF2DF60F5004F4ACB80E9EC8807B8A12FFC37B
SHA-512:	58DAB421D51B90EDF3676C663CDD4B36CCEC92FCA5061798F07B86FDC0E207DA846263C4E412B34250B8D48B52799AD6824A22BBFA6E2793CEF42BADB07DC57

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5201.tmp.WERInternalMetadata.xml	
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.>.4.9.8.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER54C1.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):	4.459475558463607
Encrypted:	false
SSDEEP:	48:cvIwSD8zsYJgtWI9acWSC8BCM8fm8M4JCdsKDF3L+q8/bnV4SrSVd:uITfeZVSNMxJQLgDWVd
MD5:	F799FB0FD596A725DDCC1D3DF9DAACED
SHA1:	4A271A3432B71581C010D8EF7A7DA366E70F7DC4
SHA-256:	DAFF5ED97F257E6F2453BFA4A13FFF11D1C25C5283D6ADAF89140123618E3496
SHA-512:	3477196C7F55DFD8BB24B0DE3043D85F699DE43086BD2B896721250138427A64287143A7545521C357A5E753A7BDBAA42C6C7A04F3F72596E40AB8861ED9577B
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="1315358" />.. <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\WER59B1.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Mon Dec 27 01:27:50 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	50532
Entropy (8bit):	2.124326452281166
Encrypted:	false
SSDEEP:	192:29ugbqVKFhV2vj/Ef5O5SkbqiloDkqHmHMvGWj3HcUcW5+:LVSsr/q85LbqSneG6ncWg
MD5:	91E23ED71E3B58E5EF808982D171F677
SHA1:	3DE1EECA62BBBD8E51C878405D3990187071C11D
SHA-256:	0575CC672BFEAEB4E346D305AA36BEDE2B30CEF9B754FBA610BE09079D2CF221
SHA-512:	4EE5E844265C64C72D5720CF296E05E8D55FAF1E2F0012139CADDF94D0B79A674ACFA35F4056FCD73CA46037906FA10FDB925BB8EA45CF0E30F6030B10A11E2B
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....a.....|.....$...$ .....4.....`.....8.....T.....H".....H .....4".....U.....B....."...GenuineIntelW.....T.....h..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\WER656A.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8350
Entropy (8bit):	3.68971409405603
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNikF6i6YI66Qvgmf8xSwCpB789b9nysfxAXnm:RrlsNie6i6Yt6Ygmf8xSW9nxfam
MD5:	0332A2E72E7BB508D64678E5061D1AE0
SHA1:	0373BF515A54A7AD057E99FC6521431EEABEBCE3
SHA-256:	809AF7D048EDD6CEA31973B7F677488127587C25BBD63FE091CD76EA418F5DB5
SHA-512:	0E7C000A802F9B539D507CFAF42505007C60DFACF353853568328C6FFF9B8066F067A8736046605DEF2D03EF1A57A2F5D2C4D343E8BE078A359027464B18A302
Malicious:	false
Reputation:	low

C:\ProgramData\Microsoft\Windows\WER\Temp\WER656A.tmp.WERInternalMetadata.xml	
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.>.6.3.4.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER68B7.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):	4.443766600628613
Encrypted:	false
SSDEEP:	48:cvIwSD8zsYJgtWI9acWSC8BI8fm8M4JCdsK7Ff8+q8vjsKp4SrSSd:uITfeZVSNbJvKzDWSd
MD5:	62007515FD1454403F933BA85C3AA38F
SHA1:	29C81AC3A501EB2C35CECA757B81906E2EB4F3B3
SHA-256:	5F16E55D31CA10A5B32119D1D0BD5F704BA780663729BE82C5B8CD50D0D48BB8
SHA-512:	CC4A38E56C4F4D60D4FCB312E5719877C3A319D56C41B3AA33D843C8738C2766824F60A66925A67507AE576D2114A785896723F0F4A8017B606B31BCDF82938A
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="1315358" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Windows\appcompat\Programs\Amcache.hve	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.278251829968785
Encrypted:	false
SSDEEP:	12288:LveNC46gDrh7xM5E+mHAzjA4/yfMhdTjXOH0K3QZGRAXWv0BhcLJnW:reNC46gDrh7xM5IR
MD5:	F1EEDE3884835CB30D08C5C778213538
SHA1:	88A6A24CC0A2C596276DAB87A052ED38B49E5651
SHA-256:	2D5815003642357A42A131ECC5B8975053D7F77170AC1E664A222F1BB92AEB2A
SHA-512:	E7F01F2222C0D6F0841D4E58DFA26463E77230DED5A48BD95D5562B6AE9125EF0B10F7D6883B4A55389FF73D64C518DB2C37901D03074173F7FA8DE600DA1A1
Malicious:	false
Preview:	regfZ...Z...p.\..,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtm&"..... .....k..... .....

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):	4.036587068153938
Encrypted:	false
SSDEEP:	384:D+1XJ5Rftx1pPJ4XmsFcnE7kKPBqXZSeq5QMVyi6+/gl4Lk49Zd1DoXznwXvwvo:K1XXRftx15J4XjFcE77BqXAeq5QMVyic
MD5:	186F9B0626F31F86600410AD679039E4
SHA1:	530359F4036224E5A0178952A2C3FC2124F07216
SHA-256:	6B0EB4872D3040CF239052A380E1EA8F00A942970D2D4C4D9531604F4F972B38
SHA-512:	1B91DFC012C93AD2A8AA17C9E7F0DEBA46579A85C438F15E498C51E53E4A8A9C89CABEC3F350CC0AE6A27B0F03870FECEE46DE7B3A37236C306D8BD71FEE0614
Malicious:	false
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&"..... .....k..HvLE.^.....Y.....y..l.l..q.....0..... ..hbin.....p.\..,.....nk,.s..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk .s..... ....Z.....Root.....lf.....Root....nk .s.....}..... .....*.....DeviceCensus..... ..vk.....WritePermissionsCheck...

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.269389698652151
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:	L0mddDYjoL.dll
File size:	536576
MD5:	0d9cc367aa4abc5620b6fcf8e9272f53
SHA1:	cb6db576bbe636a895d0ad3e3136483d0ec777be
SHA256:	1bd2e431f2631a5bfc21a9e244bb28d4230dad825b9d639 6afcd32458923fb0a
SHA512:	f827b80e02a9fd180c6bc6d4261c1ce09d42f301f313742 0942b8308688de5bbc6ed9d5945388f3ba5ac877f2211b5 088b48fb72c8db10b97b81f0fdf60eb655
SSDEEP:	6144:yKMImhktm7mnmvetmzK/kxwv4Zm7mREqZzdaz dULd54f3X0kdVtL8faGAPlX:y9hXAg5aX0CL8fI
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	0.360137939453	data	4.61046868402	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x9000	0x6fb7f	0x70000	False	0.311187744141	data	7.37787835354	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	0x2f0	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: 6400 Parent PID: 2924

General

Start time:	17:27:03
Start date:	26/12/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe "C:\Users\user\Desktop\L0mddDYjoL.dll"
Imagebase:	0x1320000
File size:	116736 bytes
MD5 hash:	7DEB5DB86C0AC789123DEC286286B938
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000001.00000002.685190249.000000006E9A1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 5696 Parent PID: 6400

General

Start time:	17:27:03
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\L0mddDYjoL.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: 6340 Parent PID: 6400

General

Start time:	17:27:04
Start date:	26/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\L0mddDYjoL.dll,Wgpomsdeeomtunmdrt
Imagebase:	0xeb0000
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: 00000005.00000000.371795691.000000006E9A1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000005.00000000.369759856.000000006E9A1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 4988 Parent PID: 5696

General

Start time:	17:27:04
Start date:	26/12/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe "C:\Users\user\Desktop\L0mddDYjoL.dll",#1
Imagebase:	0xeb0000
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: 00000006.00000000.363470341.000000006E9A1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000006.00000002.389367218.000000006E9A1000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000006.00000000.365127503.000000006E9A1000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 5924 Parent PID: 4988

General

Start time:	17:27:41
Start date:	26/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4988 -s 728
Imagebase:	0x1000000
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: 5652 Parent PID: 6340

General

Start time:	17:27:44
Start date:	26/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 6340 -s 848
Imagebase:	0x1000000
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