ID: 545443
Sample Name: L0mddDYjoL
Cookbook: default.jbs
Time: 17:16:10
Date: 26/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

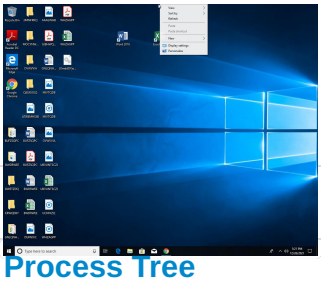
Windows Analysis Report L0mddDYjoL

Overview

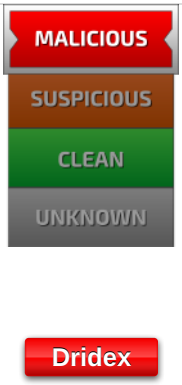
General Information

Sample Name:	L0mddDYjoL (renamed file extension from none to dll)
Analysis ID:	545443
MD5:	0d9cc367aa4abc…
SHA1:	cb6db576bbe636..
SHA256:	1bd2e431f2631a5.
Tags:	32 dll Dridex exe trojan
Infos:	

Most interesting Screenshot:



Detection

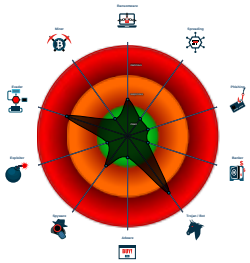


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- Uses 32bit PE files
- Found a high number of Window / Us…
- AV process strings found (often use…
- Sample file is different than original …
- One or more processes crash

Classification



Process Tree

- **System is w10x64**
- loaddll32.exe (PID: 6976 cmdline: loaddll32.exe "C:\Users\user\Desktop\L0mddDYjoL.dll" MD5: 7DEB5DB86C0AC789123DEC286286B938)
  - cmd.exe (PID: 7052 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\L0mddDYjoL.dll",#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 7132 cmdline: rundll32.exe "C:\Users\user\Desktop\L0mddDYjoL.dll",#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
      - WerFault.exe (PID: 5584 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7132 -s 740 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
  - rundll32.exe (PID: 7116 cmdline: rundll32.exe C:\Users\user\Desktop\L0mddDYjoL.dll,Wgpomsdeeomtunmdrt MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
    - WerFault.exe (PID: 2456 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 7116 -s 812 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
00000003.00000000.737237461.000000006E731000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000004.00000002.770102151.000000006E731000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000004.00000000.731296114.000000006E731000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000001.00000002.1175187257.000000006E731000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
00000003.00000000.739970824.000000006E731000.00000020.00020000.sdmp	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
Click to see the 1 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.0.rundll32.exe.6e730000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
4.0.rundll32.exe.6e730000.5.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
3.0.rundll32.exe.6e730000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
4.2.rundll32.exe.6e730000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
1.2.loaddll32.exe.6e730000.2.unpack	JoeSecurity_Dridex_1	Yara detected Dridex unpacked file	Joe Security	
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicious Call by Ordinal

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Dridex unpacked file

System Summary:

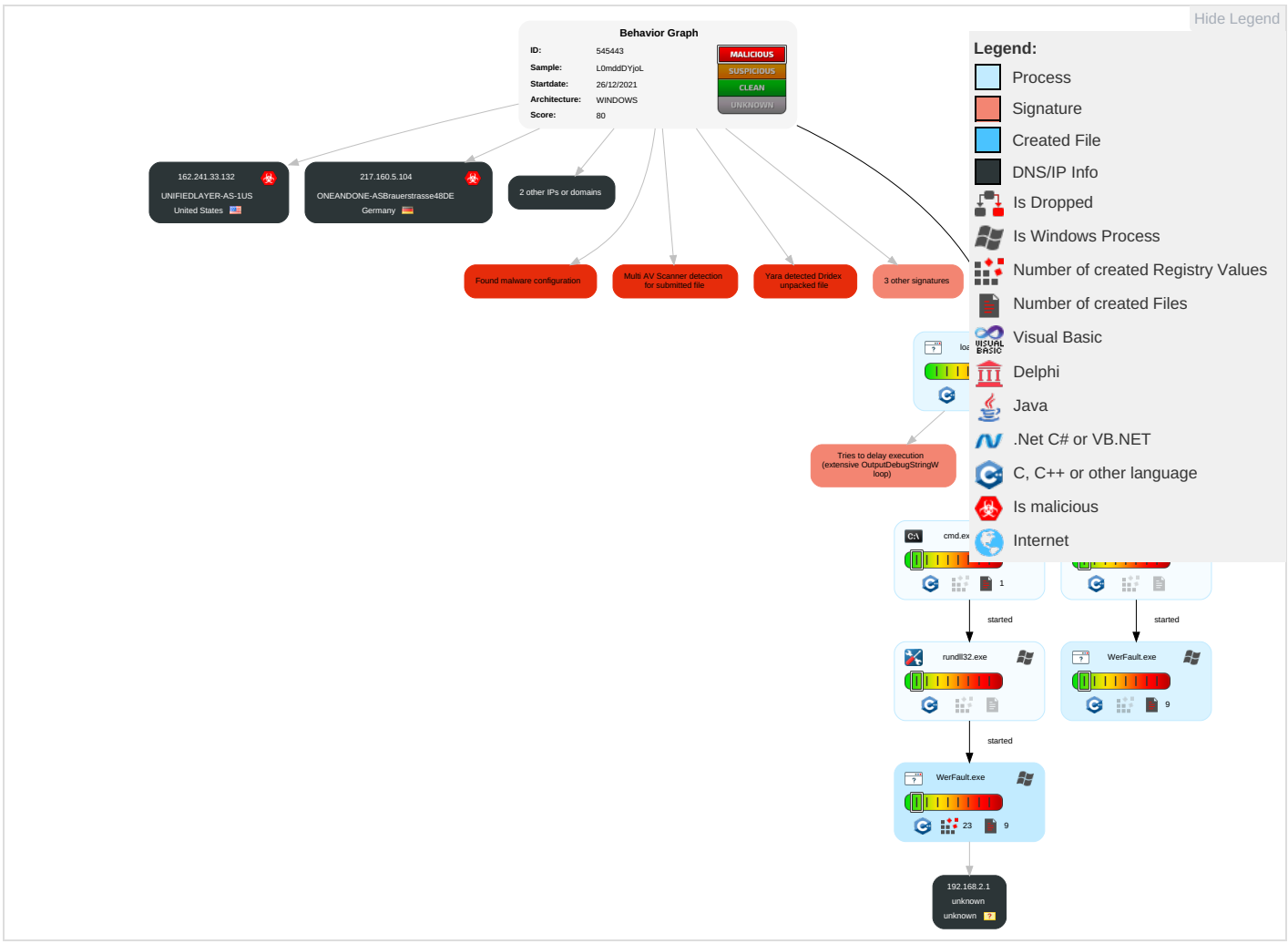
Malware Analysis System Evasion:

Tries to delay execution (extensive OutputDebugStringW loop)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	DLL Side-Loading 1	Process Injection 1 2	Virtualization/Sandbox Evasion 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Process Injection 1 2	LSASS Memory	Security Software Discovery 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 Redirect PI Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rundll32 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	Account Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming o Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Owner/User Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-I Access Poi
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Information Discovery 1 3	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cell Base Statio

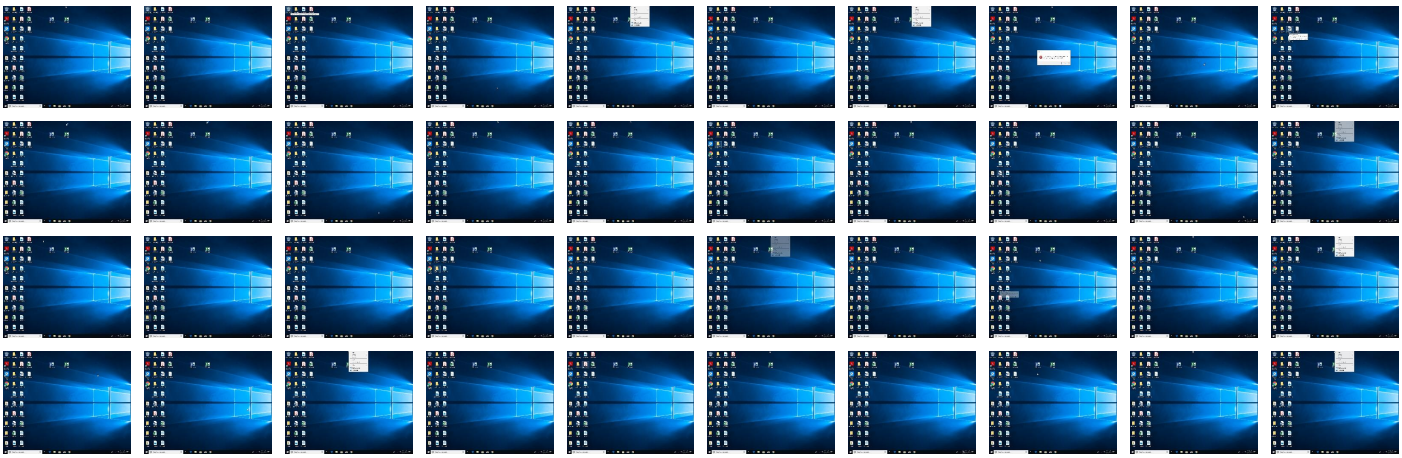
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
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
3.0.rundll32.exe.3430000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.0.rundll32.exe.900000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.0.rundll32.exe.6e730000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
3.0.rundll32.exe.3430000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.loaddll32.exe.6e730000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
3.2.rundll32.exe.3430000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.rundll32.exe.6e730000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
1.2.loaddll32.exe.10d0000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.0.rundll32.exe.6e730000.2.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
4.0.rundll32.exe.6e730000.5.unpack	100%	Avira	HEUR/AGEN.1144420		Download File

Source	Detection	Scanner	Label	Link	Download
3.0.rundll32.exe.6e730000.5.unpack	100%	Avira	HEUR/AGEN.1144420		Download File
4.0.rundll32.exe.900000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.rundll32.exe.900000.1.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

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	545443
Start date:	26.12.2021
Start time:	17:16:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	L0mddDYjoL (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:	23
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal80.troj.evad.winDLL@9/10@0/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 99.8% (good quality ratio 98.4%) • Quality average: 79.7% • Quality standard deviation: 24.4%
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
17:17:57	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_929199edf0b5e1a671cd932c57bd132abfcfef1_82810a17_08c67057\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):	0.9993867188590722
Encrypted:	false
SSDEEP:	192:jDi80oXDHVzOMjed+p8/u7sUS274It7c:jDiaXDVzOMjeP/u7sUX4It7c

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_rundll32.exe_929199edf0b5e1a671cd932c57bd132abfcfef1_82810a17_08c67057\Report.wer	
MD5:	210C57A511E71E606A4E046E586BBDB5
SHA1:	E06AFE803A93B2CE89C70769A4CC5DEC34D165BD
SHA-256:	24B889162903E167F88442A155D86C8D452A1DBFE758380BDEB7FEBCF62B4CDD
SHA-512:	0BA15DEA3A0A19EA19DBC80AC8FAF40BC7460FC7162A19315EF2728A1A1B810ED1158F2487D271A7FA6E6B1947940D3B700CAEB374AB5402A47087027CBE045B
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.B.E.X.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.5.0.0.9.0.6.8.9.3.8.0.9.5.0.....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.=.e.0.b.5.a.8.0.4.-.0.0.6.2.-.4.c.d.4.-.b.4.a.7.-.e.8.5.5.5.2.0.c.3.2.1.5.....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.=.9.4.9.a.9.8.7.c.-.7.c.a.c.-.4.7.f.1.-.9.2.d.3.-.5.3.0.7.9.2.6.7.a.b.b.9.....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.b.c.c.-.0.0.0.1.-.0.0.1.b.-.3.4.7.a.-.6.f.0.5.7.4.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_148e72c8\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):	0.9649633348399153
Encrypted:	false
SSDEEP:	192:SUCiv0oXuCHBUZMX4jed+JU/u7sUS274ItWc:iiRX1BUZMX4je//u7sUX4ItWc
MD5:	9A4C1465EAE84BA6885C5330631F0286
SHA1:	BE13493CE3C6576BF82B23AA5CF3B4E69B9AA83F
SHA-256:	F3340F0302157D25952C360C23FFCB3436C60F49C7EBB165180917D0631560B3
SHA-512:	FAEFC5F3BE5801A6480E7F5E4F8E4A6071FB5F6381546CC624714A55E9527DDDB260E86298BB0F90E2AF81B40A143E8BA530073D32759EDB6C2C014795178FFF
Malicious:	false
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.8.5.0.0.9.0.6.4.5.5.2.8.4.1.8.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.8.5.0.0.9.0.7.3.9.9.0.3.2.2.8.....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.=.7.d.7.3.d.8.2.b.-.a.b.e.e.-.4.7.0.5.-.a.4.0.6.-.a.f.a.3.2.3.f.c.6.1.9.d.....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.=.e.3.1.1.8.d.d.5.-.3.7.4.6.-.4.1.9.2.-.8.3.e.7.-.6.c.a.6.c.4.d.7.4.b.e.d.....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.b.d.c.-.0.0.0.1.-.0.0.1.b.-.5.6.9.b.-.7.2.0.5.7.4.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\WER3F35.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 14 streams, Sun Dec 26 16:17:46 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	47378
Entropy (8bit):	2.1001310880250115
Encrypted:	false
SSDEEP:	384:3P3Mvj5LbMOTXtX9+1Nquc9sk4ynLRlsBeX:KjVbjTXtX9i2WQnLYBe
MD5:	E43EECD3B23FCAD44D11879196A2B0C3
SHA1:	02177C17F9BD6798B55D26E54F01EF1426D668BC
SHA-256:	5693B40D8399DB0EFF4E49EC6D75FB81C659D1DC0B74251B8873A246ED93885F
SHA-512:	688CC731DC24528ECDEB04EF32F2C045E7D60735F6587833D9BE1FD85A3D3B1AA3D9564E2DF6F9CB06643A312FCE558A0AD4FB35D26B062DEFBF5E4D8A134DBC
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....a.....`.....1.....T.....8.....T.....p.....U.....B..... .....GenuineIntelW.....T.....a.....0..=.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e.....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4735.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8272
Entropy (8bit):	3.6923779779217307
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiCj6F6Ybo6UVgmfT4DSX+prG89bPqsfVFm:RrlsNie6F6Y06UVgmfTMSMPJfG
MD5:	6561E96FD83370A68540817569A21DC4

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4735.tmp.WERInternalMetadata.xml	
SHA1:	E0AE0E9610CFD348C961D1675F0984D7F37AB4DF
SHA-256:	6F4A2B67EFAFF56850388920A6A1C75875C14E3A9013095DEE46E5C956DF1868
SHA-512:	749CCD7301B62FC7695E5FC9935BFE42DF0DD12B7C02A3D930A31F2C933960BA4218BDD8DF750DD7CE4FC83814FEF9323E44B974A08BA9BF5749623F76C3408
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.>.7.1.3.2.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER4AFE.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):	4.456079303878735
Encrypted:	false
SSDEEP:	48:cvIwSD8zs9JgtWI9U9kWSC8Bsz8fm8M4JCdsKDFe+q8/bnb4SrSCd:uITfXv99SNLJJGDWCd
MD5:	7EC1B268F8282E11C57A629D5ABECB25
SHA1:	7032FD3A5DCC932999614F13A6D82E17BDED7207
SHA-256:	3017365A7BD5E29C5ABFBCF61288D781891F9F0E984EBCAA9CF765F185A21F7E
SHA-512:	5BA5366A688FC9808CE6B41A7F63D5BD4725793F485C574D4B440F03E74BF6F826AB7D89CE6EF7356F7B2DFE6284B0C55AC5F5F93CD29CE635C40C89A67C3FD2
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="1314808" />.. <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\WER505B.tmp.dmp	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	Mini DuMP crash report, 15 streams, Sun Dec 26 16:17:50 2021, 0x1205a4 type
Category:	dropped
Size (bytes):	49590
Entropy (8bit):	2.186914958849693
Encrypted:	false
SSDEEP:	192:5siH1POn05+vxO5SkbQOq7JSFVCMNVK+h8gFAPk3VsthyeLn99gn:V2Q+M5Lb4LgxVML99
MD5:	4ACD96B9B5339AB7128F3CAE7F6D867F
SHA1:	91A705408232BDDFD63C6AF1FAB805A0B2BD60A8
SHA-256:	EF69CCCC427F52D48529077720B50BD14182E44795AFCCA7DAECC4AD26EF142A
SHA-512:	1F9245886DCAB6C13884BA71D9B9E0DA45FC813E217A02DEB0621CC3DF00F8427F9AEFE1020ED856E3AC9182D34674800B052336B81C0CB0E5E184B4F3F8B06
Malicious:	false
Reputation:	low
Preview:	MDMP..... .....a.....|.....$...$ .....4.....`.....8.....T....."....."....H .....4".....U.....B.....".... ..GenuineIntelW.....T.....a.....0..=.....W... .E.u.r.o.p.e. .S.t.a.n.d.a.r.d. .T.i.m.e.....W... .E.u.r.o.p.e. .D.a.y.l.i.g.h.t. .T.i.m.e. .....1.7.1.3.4...1...x.8.6.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4..... ....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B1A.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\SysWOW64\WerFault.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	8352
Entropy (8bit):	3.6863170526836
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiEn6V6Y8O6Zgmf8xSc+pB/89bROFWsfzbm:RrlsNiM6V6YN6Zgmf8xSyROfu
MD5:	D9648DB992C76ECCBE56DB5E98DCB007
SHA1:	FBABA5C4093DF8D79BD3A9A541138DCC507D38C9
SHA-256:	CE1771BB3F5D413A463EE1588084A2719D4E77CC5FA4993C1FC895F11CD659EE
SHA-512:	80E8CFA7702B032B796007004105F8F4D85A23125C0CA1F8E4AC9472E5CC6F2B8F7873C1F54EEA11424354985CBBB14BAAC38801E1B77B5C6A7C5632D3DF8B7

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5B1A.tmp.WERInternalMetadata.xml	
Malicious:	false
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.>.7.1.1.6.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5FBF.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):	4.4420030678612346
Encrypted:	false
SSDEEP:	48:cvIwSD8zs9JgtWI9U9kWSC8BsZH8fm8M4JCdsK7Ffu+q8vjsKQ4SrSVd:uITfXv99SNcMJpKuDWVd
MD5:	DBBBE16CDAECA4FB3845C0840E0C758B
SHA1:	D4C41993E07E9AACDAB18A78B85C37C9564BD350
SHA-256:	260BC90B516B16369B22172D6C9D25C3658260BA94AD15A8C7A699BDCB7A857F
SHA-512:	F0959E9EC3BF7559C78C69B1181397E6AD5E92DFF3C24F488A572E5151C947905585346CD8CE280B296F5C3F207FA48610E40A6FB3DD384B818D53A0C9FA0667
Malicious:	false
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="1314808" />.. <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):	4.2416359039463964
Encrypted:	false
SSDEEP:	12288:sAWdSUOP+weKfjSdLI9uHvap6Qvt/BFqp4hsNJTVY4Y9eyFp:7WdSUOP+weejSdb06
MD5:	D80199F332C8BD4168AEF930B4D179F4
SHA1:	BBC2007D99EE7E6C4B0251D07498449C663D28A5
SHA-256:	E999B65715AEA8C45A68C0F3515B4C950D42F6F36A89E8B711D613DE289393F0
SHA-512:	C6D63BDDF131BC40E961548553AB4AA25DC80F758229C3B1F817F905B278A3139C27D773FCE65752C7393130F7BBC75775802AAF775208086D8CB5401A3ADFDI
Malicious:	false
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.rmtmB`J.t..... .....vYNA..... .....

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):	3.4098731481025215
Encrypted:	false
SSDEEP:	384:nozn8Q5K5VPv4EgnVVeeDzeq1NKZtjCT8Gpwe1E33SYd:gXKpg/eeDzekNYtj/Gpwe8SY
MD5:	E154A74DC10E538854C76A8F41A498F6
SHA1:	F4B56ED7C23481A17464B53BD524106D7EA4B4B8
SHA-256:	BB6E33880350BA61C43A6EDF69B2DFC3637FC2A21DB9C2D851625E691796FC3F
SHA-512:	7A7B89EB6ADDB225C58F2753A236379D223AD3381FEB3751C2920D9BB7D6383EBA7890EF3B5A0F7B2C2ED4452E7061DF4177DF731115B207D8FAD828B6C66E4E
Malicious:	false
Preview:	regfG...G...p.\.,..... .....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtmB`J.t..... .....pYNAHvLE.N.....G.....@..|..w.t..ml},..... ..hbin.....p.\.,.....nk,...L.t.....@..... .....&...{ad79c032-a2ea-f756-e377-72fb9332c3ae}.....nk ...L.t..... ....Z.....Root.....lf.....Root....nk ...L.t..... .....*.....DeviceCensus..... ....vk.....WritePermissionsCheck.....p...

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: 6976 Parent PID: 6104

General

Start time:	17:17:03
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:	0x190000
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: 00000001.00000002.1175187257.000000006E731000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 7052 Parent PID: 6976

General

Start time:	17:17:04
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:	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: 7116 Parent PID: 6976

General

Start time:	17:17:04
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:	0xab0000
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: 00000003.00000000.737237461.000000006E731000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000003.00000000.739970824.000000006E731000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

Analysis Process: rundll32.exe PID: 7132 Parent PID: 7052

General

Start time:	17:17:04
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:	0xab0000
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: 00000004.00000002.770102151.000000006E731000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000004.00000000.731296114.000000006E731000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Dridex_1, Description: Yara detected Dridex unpacked file, Source: 00000004.00000000.730291590.000000006E731000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: WerFault.exe PID: 5584 Parent PID: 7132

General

Start time:	17:17:42
Start date:	26/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7132 -s 740
Imagebase:	0x1060000
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: 2456 Parent PID: 7116

General

Start time:	17:17:46
Start date:	26/12/2021
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 7116 -s 812
Imagebase:	0x1060000

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