ID: 492758
Sample Name: 2JlIMkLNXh
Cookbook: default.jbs
Time: 00:33:58
Date: 29/09/2021
Version: 33.0.0 White Diamond

Table of Contents

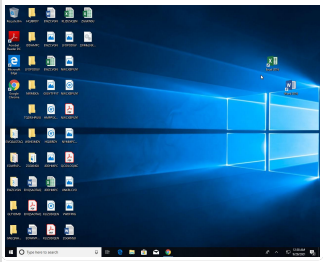
Windows Analysis Report 2JlIMkLNXh

Overview

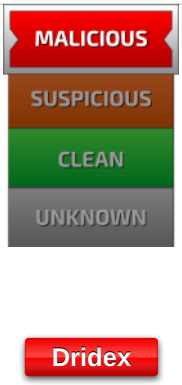
General Information

Sample Name:	2JlIMkLNXh (renamed file extension from none to dll)
Analysis ID:	492758
MD5:	fe213638baba7c7.
SHA1:	e463b86c2e5735..
SHA256:	27f32618162b8a5.
Tags:	Dridex exe
Infos:	

Most interesting Screenshot:



Detection

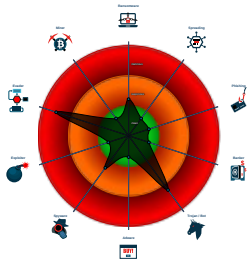


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected Dridex unpacked file
- Multi AV Scanner detection for subm…
- Benign windows process drops PE f…
- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Changes memory attributes in foreig…
- Machine Learning detection for samp…
- Queues an APC in another process …
- Machine Learning detection for dropp…
- Uses Atom Bombing / ProGate to in…
- Queries the volume information (nam…
- Uses code obfuscation techniques (…
- PE file contains sections with non-s…
- Queries the installation date of Wind…
- Detected potential crypto function

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 576 cmdline: loaddll64.exe 'C:\Users\user\Desktop\2JlIMkLNXh.dll' MD5: E0CC9D126C39A9D2FA1CAD5027EBBD18)
  - cmd.exe (PID: 4192 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\2JlIMkLNXh.dll',#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 3240 cmdline: rundll32.exe 'C:\Users\user\Desktop\2JlIMkLNXh.dll',#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 4656 cmdline: rundll32.exe C:\Users\user\Desktop\2JlIMkLNXh.dll,CreateXmlReader MD5: 73C519F050C20580F8A62C849D49215A)
    - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - mstsc.exe (PID: 6340 cmdline: C:\Windows\system32\mstsc.exe MD5: 3FBB5CD8829E9533D0FF5819DB0444C0)
      - mstsc.exe (PID: 6412 cmdline: C:\Users\user\AppData\Local\fJxx4Zu\mstsc.exe MD5: 3FBB5CD8829E9533D0FF5819DB0444C0)
      - tcmsetup.exe (PID: 6516 cmdline: C:\Windows\system32\tcmsetup.exe MD5: 0DDA495155D552D024593C4B3246C8FA)
      - tcmsetup.exe (PID: 6564 cmdline: C:\Users\user\AppData\Local\YTBx\tcmsetup.exe MD5: 0DDA495155D552D024593C4B3246C8FA)
  - rundll32.exe (PID: 4920 cmdline: rundll32.exe C:\Users\user\Desktop\2JlIMkLNXh.dll,CreateXmlReaderInputWithEncodingCodePage MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 1320 cmdline: rundll32.exe C:\Users\user\Desktop\2JlIMkLNXh.dll,CreateXmlReaderInputWithEncodingName MD5: 73C519F050C20580F8A62C849D49215A)
- rundll32.exe (PID: 6476 cmdline: C:\Windows\System32\rundll32.exe C:\Windows\System32\shell32.dll,SHCreateLocalServerRunDll {9aa46009-3ce0-458a-a354-715610a075e6} -Embedding MD5: 73C519F050C20580F8A62C849D49215A)
- explorer.exe (PID: 6880 cmdline: explorer.exe MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
00000005.00000002.251743405.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000008.00000002.257720074.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000016.00000002.374374689.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000004.00000002.342710737.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
0000000A.00000002.266384036.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
Click to see the 2 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

E-Banking Fraud:

Yara detected Dridex unpacked file

HIPS / PFW / Operating System Protection Evasion:

Benign windows process drops PE files

Changes memory attributes in foreign processes to executable or writable

Queues an APC in another process (thread injection)

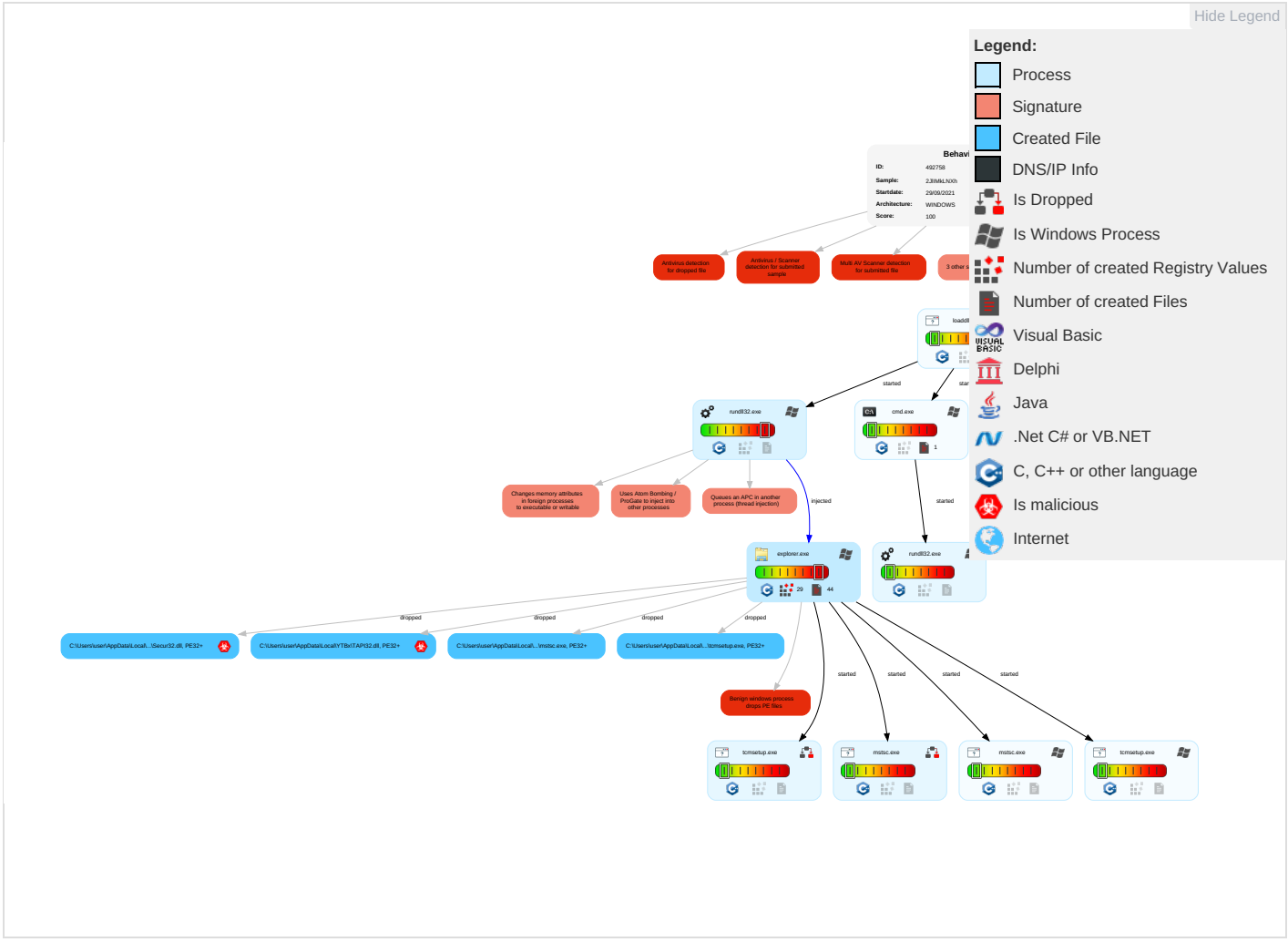
Uses Atom Bombing / ProGate to inject into other processes

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	Native API 1	Startup Items 1	Startup Items 1	Masquerading 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop Insecure Network Communic

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Default Accounts	Exploitation for Client Execution 1	Registry Run Keys / Startup Folder 2	Process Injection 3 1 2	Virtualization/Sandbox Evasion 1	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	DLL Side-Loading 1	Registry Run Keys / Startup Folder 2	Process Injection 3 1 2	Security Account Manager	Security Software Discovery 2 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)	DLL Side-Loading 1	Obfuscated Files or Information 2	NTDS	Virtualization/Sandbox Evasion 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Rundll32 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 2	Cached Domain Credentials	Application Window 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	Timestomp 1	DCSync	File and Directory Discovery 2	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	DLL Side-Loading 1	Proc Filesystem	System Information Discovery 2 5	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

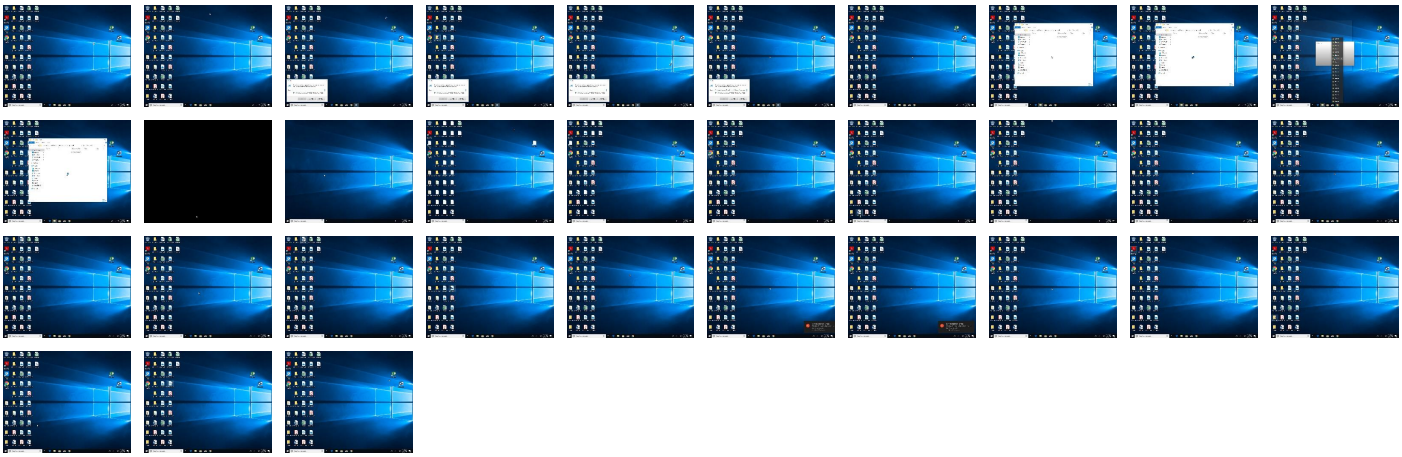
Behavior Graph



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
2JIIMkLNXh.dll	69%	Virustotal		Browse
2JIIMkLNXh.dll	78%	ReversingLabs	Win64.Infostealer.Dridex	
2JIIMkLNXh.dll	100%	Avira	HEUR/AGEN.1114452	
2JIIMkLNXh.dll	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\fJxx4Zu\Secur32.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\YTBx\TAPI32.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\fJxx4Zu\Secur32.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\YTBx\TAPI32.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\YTBx\tcmsetup.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\YTBx\tcmsetup.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\YTBx\tcmsetup.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\fJxx4Zu\mstsc.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\fJxx4Zu\mstsc.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\fJxx4Zu\mstsc.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
26.2.tcmsetup.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.2.mstsc.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.loaddll64.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://schemas.microso	0%	URL Reputation	safe	
http://schemas.microsoft.c	0%	URL Reputation	safe	
http://schemas.miC	0%	Avira URL Cloud	safe	
http://schemas.microsoft.co	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond

Analysis ID:	492758
Start date:	29.09.2021
Start time:	00:33:58
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	2JlIMkLNXh (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:	41
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:	mal100.troj.evad.winDLL@21/5@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 20.8% (good quality ratio 14.1%) • Quality average: 50.1% • Quality standard deviation: 41.2%
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
00:35:44	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\GU
00:35:45	API Interceptor	1326x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\YTBx\tcmsetup.exe	oB4wShoM81.dll	Get hash	malicious	Browse	
	5s7H5yP0YA.dll	Get hash	malicious	Browse	
	wr3PdlRKjL.dll	Get hash	malicious	Browse	
	PSnPApRPsG.dll	Get hash	malicious	Browse	
	N37wjZ34KC.dll	Get hash	malicious	Browse	
	e75OHzYF9S.dll	Get hash	malicious	Browse	
	Z3Asq5R56C.dll	Get hash	malicious	Browse	
	Y7KrNvSxWx.dll	Get hash	malicious	Browse	
	8yQieH8k8q.dll	Get hash	malicious	Browse	
	5pG7H5XLEj.dll	Get hash	malicious	Browse	
	40TWLYCrEf.dll	Get hash	malicious	Browse	
	BUal7Z7t7a.dll	Get hash	malicious	Browse	
	mmM8TEnV8t.dll	Get hash	malicious	Browse	
	d3bWgdGpkZ.dll	Get hash	malicious	Browse	
	0oSZeHvzK2.dll	Get hash	malicious	Browse	
	neTLYArwd7.dll	Get hash	malicious	Browse	
	hDeUA0Ag8C.dll	Get hash	malicious	Browse	
	gKibedwOnl.dll	Get hash	malicious	Browse	
	b2e1YcSctb.dll	Get hash	malicious	Browse	
	l7ytx2QXnx.dll	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\YTBx\TAPI32.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1949696
Entropy (8bit):	3.847240274529997
Encrypted:	false
SSDEEP:	12288:aVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:HfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	2DB379C0F1D84F594F99640DF0EC1C86
SHA1:	276A4C43DE33BE489DC83520FF470CB24D959205
SHA-256:	16B57B8D107E0E5C08D74FA5B3B63D346415E85301B121186D2CED0A0D5F407E
SHA-512:	6AD20F570B6038397DDCFCC5AFD2CECD8D17F0E12337F90602595CC7350D57584A52546EA49E6490E167736E4F93DC820E1154CAB138AD3D14622E05508FF51
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.4 ..DN^....." .....p.....@.....@lx}..b.....V....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\YTBx\tcmsetup.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	4.999998588063228
Encrypted:	false
SSDEEP:	192:DIzBdu2Mhf/+G1jQ0pwPYqLmdO0O7RgZiLtzADWO4hxDcUh6UdBndOvfSWG0oW:GMVJjQ0dg0O7yk5ciJcUhLiSWG0oW
MD5:	0DDA495155D552D024593C4B3246C8FA
SHA1:	7501A7AD5DAA41462BEFF9127154BAF261A24A5B
SHA-256:	D3074CBD29678CA612C1F8AA93DE1F5B75108BE8187F0F2A2331BC302AD48CD9
SHA-512:	9159D8AF457591256BA87443E89ECE942DE40B8FF39586116C2026330B8AE9C20F96905547E87D98508951D2B4687069EFD018CC9E4A6C94A6C26D4B587F41B3
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Local\YTBx\tcmsetup.exe

Joe Sandbox View:	• Filename: oB4wShoM81.dll, Detection: malicious, Browse • Filename: 5s7H5yP0YA.dll, Detection: malicious, Browse • Filename: wr3PdlRKjL.dll, Detection: malicious, Browse • Filename: PSnPApRPsG.dll, Detection: malicious, Browse • Filename: N37wjZ34KC.dll, Detection: malicious, Browse • Filename: e75OHzYF9S.dll, Detection: malicious, Browse • Filename: Z3Asq5R56C.dll, Detection: malicious, Browse • Filename: Y7KrNvSxWx.dll, Detection: malicious, Browse • Filename: 8yQieH8k8q.dll, Detection: malicious, Browse • Filename: 5pG7H5XLEj.dll, Detection: malicious, Browse • Filename: 40TWLYCrEf.dll, Detection: malicious, Browse • Filename: BUal7Z7t7a.dll, Detection: malicious, Browse • Filename: mmM8TEnV8t.dll, Detection: malicious, Browse • Filename: d3bWgdGpkZ.dll, Detection: malicious, Browse • Filename: 0oSZeHvzK2.dll, Detection: malicious, Browse • Filename: neTLYArwd7.dll, Detection: malicious, Browse • Filename: hDeUA0Ag8C.dll, Detection: malicious, Browse • Filename: gKibedwOnl.dll, Detection: malicious, Browse • Filename: b2e1YcSctb.dll, Detection: malicious, Browse • Filename: l7ytx2QXnx.dll, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Z...Z...Z..[...Z..[...Z..[...Z..[...Z...Z...Z..[...Z.:Z...Z..[...ZRich...Z.. .....PE..d....E.H.....".....,..... .....@.....`..... .....9..x....p..P....`..D..... ....5..T.....0.....1.. .....text..... ..`.rdata..&....0.....@..@.data... ....P.....0.....@....pdata..D....`.....2.....@..@.rsrc...P....p.....4..... ....@..@.reloc.. .....>.....@..B..... .....

C:\Users\user\AppData\Local\fJxx4Zu\Secur32.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1945600
Entropy (8bit):	3.837322257119322
Encrypted:	false
SSDEEP:	12288:6VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:nfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	05BACE1B34170BF867B1462BD982E0C6
SHA1:	657AF7B197381CCA16204428730E105DB9F42BA7
SHA-256:	92D65FB15281A70FC6749A5ECC43BBC4B680497AEFA7E82182018F05DED98826
SHA-512:	5E45E93763FFB8A3E83BE512F55DDF2C75CF6B6B654A849735AE1049A8F0115AD01E19011ACF9D62C7175FC30B003659E43659A18991F5D1205DA95F0102A830
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.4 ..DN^....." .....p.....@.....@lx}..b.....#....c.....h.....$#..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\fJxx4Zu\mstsc.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	3640832
Entropy (8bit):	5.884402821447862
Encrypted:	false
SSDEEP:	98304:q8yNOTNEpZxGb+ZPgN6tYDNBMe+8noqvEYw0n2WFfZT+xgsLOsMg:q8yNOTNEpZxk+ZIN6tYDNBMe+8noqvEB
MD5:	3FBB5CD8829E9533D0FF5819DB0444C0
SHA1:	A4A6E4E50421E57EA4745BA44568B107A9369447
SHA-256:	043870DBAB955C1851E1710D941495357383A08F3F30DD3E3A1945583A85E0CA
SHA-512:	349459CCF4DDFB0B05B066869C99088BA3012930D5BBC3ED1C9E4CF6400687B1EFE698C5B1734BF6FF299F6C65DD7A71A2709D3773E9E96F6FDE659F5D883F4
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... w.dN$.dN$.dN$..M%.dN$..J%.dN$..K%.dN$..O%.dN$.dO$ TfN$..G%.eN$...$.dN$..L%.dN$Rich.dN$.....PE..d.....Y.....".....$....%.....p.....@.....7.....K8...`.....].....p..H>!.....`..... ..7. *..P...T.....`.....`.....\..`.....text....".....$..... ..`.rdata...\...@...^...(.....@..@.data...P(.....@....pdata..`..... ....@..@.didat..(....`..... .....@....rsrc...H>!..p...@!..".....@..@.reloc.. *....7.,...b7.....@..B..... .....

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\89dad5d484a9f889a3a8dfca823edc3e_d06ed635-68f6-4e9a-955c-4899f5f57b9a

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\89dad5d484a9f889a3a8dfca823edc3e_d06ed635-68f6-4e9a-955c-4899f5f57b9a

Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	4447
Entropy (8bit):	5.480585654433585
Encrypted:	false
SSDEEP:	48:JcwUc3+5j2KMXDFaQwSluTIQcvVJ6cwUcAx54iurf/BjbJxjIxlPcuZJYmm:Jjzgj+TFmWuyyjcD0z/lNx0vg
MD5:	8F8C26181663A67A34214741DE21A3D0
SHA1:	6582F9AC92CDED35B3F82538E11A5D20957FA931
SHA-256:	A77369687E9FC82C8208FD8415EEC9D98CD332011C772CCDADA93F9202D11E63
SHA-512:	6DD67B4D5E94B76FB54BB17423CFD91D90B8451D0B137622A94717C29B27433F2E25BECD057C4DEFD1EA75DC0C8F3401CFF7D223784930E580F881763C4F1FF
Malicious:	false
Preview:	.....user.....user.....RSA1.....Y..uEZ..b^.....V...q..3..wO_q.....E_~.=.=g....A...m...z...H.-..Nc..>..*...._X.....,.. .cD+..%..7...7k.U=.h....1...0.`!.....z..O.....I..)..L.tMN.p.....,...C.r.y.p.t.o.A.P.I. .P.r.i.v.a.t.e. .K.e.y....f..... .....n....7.$Y...5..k.c.Q./.4u_..... ...q3_3.,!.m.6...s.at.) .....il.9y....V.?q.....>...p7.dO.'i.d^<)g.Ws.....~....{..f._#.....Zm..c.....Z...e....e.S2....]$f....6.7....VFy7....\a.iSW..w...q..H.x.....-.}.q.....P|.U....LpK..G)P.]....E..X<..1...`.... ..4...PX.UF...'p....N..W._Y.g.I.O.@..Ih.Ht..L..j.0Z..y!..w.s@.{AF\.S.m.z..+.H..*...ch....R}.3.W.R.....(.o..}.....[5.R...-m%.[....o...F.Z7d..,.....8.:..T.7.4.....Bo#.z.W- 9.6| .....m.....s.....z.k..p..++....5b/d.~..,If....P..(.....u.....Q.:.E#.w.R....VHF..EX..d.u&XWOm8..-....]%9./..}.~.-.}j..H..

Static File Info

General

File type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Entropy (8bit):	3.831979748392846
TrID:	• Win64 Dynamic Link Library (generic) (102004/3) 86.43% • Win64 Executable (generic) (12005/4) 10.17% • Generic Win/DOS Executable (2004/3) 1.70% • DOS Executable Generic (2002/1) 1.70% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	2JlIMkLNXh.dll
File size:	1941504
MD5:	fe213638baba7c73e9addd779b4f078a
SHA1:	e463b86c2e573569643c5e24668bd291d7c2e6b0
SHA256:	27f32618162b8a522fc5fb8fb832848acb724cf2ac0c03b8488b2c405c582d6a
SHA512:	2bafcee6542db5f32c4a181ed745c7a6944382d2b3a730c4444b6d8ce8d81f195c2c7c3c7d2b492db3de815e2b50f690455f0c86ba3595667da27d1ff0f3582e
SSDEEP:	12288:RVl0W/TtlPLfJCm3WlYxJ9yK5lQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:gfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....|...|...|....K.#}...'...}.....{}....X.#}....f..|....g..}..*...a|.....}....N..}..*...E}..[.I.E|...'..U}....N.+}..[.K.P|.

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x140041070
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x140000000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA

General

Time Stamp:	0x5E4E44CC [Thu Feb 20 08:35:24 2020 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:	6668be91e2c948b183827f040944057f

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x40796	0x41000	False	0.776085486779	data	7.73364605679	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x42000	0x64fd0	0x65000	False	0.702390160891	data	7.86574512659	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa7000	0x178b8	0x18000	False	0.0694580078125	data	3.31515306295	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0xbf000	0x12c	0x1000	False	0.06005859375	PEX Binary Archive	0.581723022719	IMAGE_SCN_TYPE_DSECT, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0xc0000	0x880	0x1000	False	0.139892578125	data	1.23838501563	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc1000	0x2324	0x3000	False	0.0498046875	data	4.65321444248	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.qkm	0xc4000	0x74a	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.cvjb	0xc5000	0x1e66	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tlmkv	0xc7000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.wucsxe	0xc8000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.fltwtj	0x10e000	0x1267	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.sfplio	0x110000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rpg	0x111000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bewzc	0x157000	0x1124	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vksvaw	0x159000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.wmhg	0x15a000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.kswemc	0x15c000	0x36d	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.kaxfk	0x15d000	0x197d	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pjf	0x15f000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.retjqj	0x160000	0x7fd	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.mizn	0x161000	0x9cd	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrub	0x162000	0x197d	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.susbqq	0x164000	0x6cd0	0x7000	False	0.00177873883929	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.jeojcw	0x16b000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vwl	0x16c000	0xae7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.mub	0x16d000	0x6cd0	0x7000	False	0.00177873883929	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.xwxpmb	0x174000	0x573	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.aea	0x175000	0x7fd	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.lwpch	0x176000	0x7fd	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.nzgp	0x177000	0x1f7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.qimx	0x178000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.jbqbr	0x179000	0x1f7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.kxxxil	0x17a000	0xbf6	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.drpaa	0x17b000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.lepjc	0x17c000	0x1f7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ywrsat	0x17d000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ialjct	0x17e000	0x103	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ujrqkf	0x17f000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.lwaoje	0x181000	0x1af	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pces	0x182000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.zuizg	0x183000	0x6cd0	0x7000	False	0.00177873883929	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.upz	0x18a000	0x3ba	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.wxuh	0x18b000	0xbf6	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.fsdfq	0x18c000	0x5a7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.xxlo	0x18d000	0x1f7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.hcxtgl	0x18e000	0x1e66	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.owbx	0x190000	0xf9	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.php	0x191000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.trmoj	0x192000	0x1ee	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.zaixaf	0x193000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.myzf	0x1d9000	0x13e	0x1000	False	0.046142578125	data	0.645779984281	IMAGE_SCN_CNT_INITIALIZED_DATA, 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

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: 576 Parent PID: 1860

General

Start time:	00:34:56
Start date:	29/09/2021
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe 'C:\Users\user\Desktop\2JlIMkLNXh.dll'
Imagebase:	0x7ff7a0630000
File size:	1136128 bytes
MD5 hash:	E0CC9D126C39A9D2FA1CAD5027EBBD18
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000001.00000002.272046081.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 4192 Parent PID: 576

General

Start time:	00:34:57
Start date:	29/09/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\2JlIMkLNXh.dll',#1
Imagebase:	0x7ff7eef80000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
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: 4656 Parent PID: 576

General

Start time:	00:34:57
Start date:	29/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\2JlIMkLNXh.dll,CreateXmlReader
Imagebase:	0x7ff6ab530000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000004.00000002.342710737.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 3240 Parent PID: 4192

General

Start time:	00:34:57
Start date:	29/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe 'C:\Users\user\Desktop\2JlIMkLNXh.dll',#1
Imagebase:	0x7ff6ab530000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000005.00000002.251743405.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3472 Parent PID: 4656

General

Start time:	00:34:59
Start date:	29/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
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

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: rundll32.exe PID: 4920 Parent PID: 576

General

Start time:	00:35:01
Start date:	29/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\2JIIMkLNXh.dll,CreateXmlReaderInputWithEncodingCodePage
Imagebase:	0x7ff797770000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000008.00000002.257720074.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 1320 Parent PID: 576

General

Start time:	00:35:04
Start date:	29/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\2JIIMkLNXh.dll,CreateXmlReaderInputWithEncodingName
Imagebase:	0x7ff6ab530000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000000A.00000002.266384036.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: mstsc.exe PID: 6340 Parent PID: 3472

General

Start time:	00:35:43
Start date:	29/09/2021
Path:	C:\Windows\System32\mstsc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\mstsc.exe
Imagebase:	0x7ff6a77f0000
File size:	3640832 bytes
MD5 hash:	3FBB5CD8829E9533D0FF5819DB0444C0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: mstsc.exe PID: 6412 Parent PID: 3472

General

Start time:	00:35:45
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\fJxx4Zu\mstsc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\fJxx4Zu\mstsc.exe
Imagebase:	0x7ff660310000
File size:	3640832 bytes
MD5 hash:	3FBB5CD8829E9533D0FF5819DB0444C0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000016.00000002.374374689.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 6476 Parent PID: 792

General

Start time:	00:35:55
Start date:	29/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\rundll32.exe C:\Windows\System32\shell32.dll,SHCreateLocalServerRunDll {9aa46009-3ce0-458a-a354-715610a075e6} -Embedding
Imagebase:	0x7ff6ab530000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: tcmsetup.exe PID: 6516 Parent PID: 3472

General

Start time:	00:35:57
Start date:	29/09/2021
Path:	C:\Windows\System32\tcmsetup.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\tcmsetup.exe
Imagebase:	0x7ff65de30000
File size:	16384 bytes
MD5 hash:	0DDA495155D552D024593C4B3246C8FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: tcmsetup.exe PID: 6564 Parent PID: 3472

General

Start time:	00:35:58
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\YTBx\tcmsetup.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\YTBx\tcmsetup.exe
Imagebase:	0x7ff6193b0000
File size:	16384 bytes
MD5 hash:	0DDA495155D552D024593C4B3246C8FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000001A.00000002.394057525.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 6880 Parent PID: 564

General

Start time:	00:36:05
Start date:	29/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	explorer.exe
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Disassembly

Code Analysis