ID: 492776
Sample Name: 1zdJLxxTnh
Cookbook: default.jbs
Time: 01:05:07
Date: 29/09/2021
Version: 33.0.0 White Diamond

Table of Contents

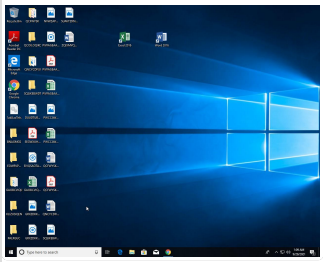
Windows Analysis Report 1zdJLxxTnh

Overview

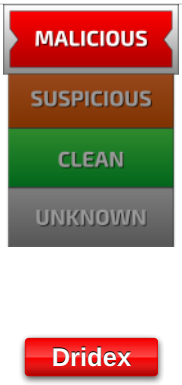
General Information

Sample Name:	1zdJLxxTnh (renamed file extension from none to dll)
Analysis ID:	492776
MD5:	784adf3295b7eaf..
SHA1:	c79da77a4d00ec..
SHA256:	69af86da86fc2f9…
Tags:	Dridex exe
Infos:	

Most interesting Screenshot:



Detection

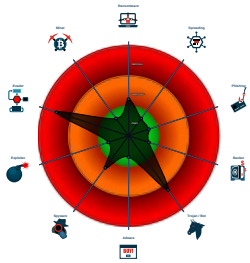


Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- Queues an APC in another process …
- Machine Learning detection for dropp…
- Uses Atom Bombing / ProGate to in…
- Queries the volume information (nam…
- Contains functionality to check if a d…
- 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: 7152 cmdline: loaddll64.exe 'C:\Users\user\Desktop\1zdJLxxTnh.dll' MD5: E0CC9D126C39A9D2FA1CAD5027EBBD18)
  - cmd.exe (PID: 5808 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\1zdJLxxTnh.dll',#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 1012 cmdline: rundll32.exe 'C:\Users\user\Desktop\1zdJLxxTnh.dll',#1 MD5: 73C519F050C20580F8A62C849D49215A)
      - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - ProximityUxHost.exe (PID: 5800 cmdline: C:\Windows\system32\ProximityUxHost.exe MD5: E7F0E9B3779E54CD271959C600A2A531)
        - ProximityUxHost.exe (PID: 4896 cmdline: C:\Users\user\AppData\Local\fk8bXjSn\ProximityUxHost.exe MD5: E7F0E9B3779E54CD271959C600A2A531)
        - rstrui.exe (PID: 492 cmdline: C:\Windows\system32\rstrui.exe MD5: 3E8AFFA54035412F86663C8B44CAA2E5)
        - irftp.exe (PID: 4740 cmdline: C:\Windows\system32\irftp.exe MD5: F1C2D10CA8161DB689CD4FDE756E2DBB)
        - irftp.exe (PID: 6684 cmdline: C:\Users\user\AppData\Local\94LPZAU0\irftp.exe MD5: F1C2D10CA8161DB689CD4FDE756E2DBB)
        - SystemPropertiesComputerName.exe (PID: 5792 cmdline: C:\Windows\system32\SystemPropertiesComputerName.exe MD5: BEE134E1F23AFD3AE58191D265BB9070)
        - sessionmsg.exe (PID: 5252 cmdline: C:\Windows\system32\sessionmsg.exe MD5: 1F7CEA0216DE48B877C16F95C7DA1F0F)
        - sessionmsg.exe (PID: 5724 cmdline: C:\Users\user\AppData\Local\nPqx0Ph\sessionmsg.exe MD5: 1F7CEA0216DE48B877C16F95C7DA1F0F)
        - WindowsActionDialog.exe (PID: 6136 cmdline: C:\Windows\system32\WindowsActionDialog.exe MD5: 991359EE1E9C1958EB5D0F7314774123)
        - WindowsActionDialog.exe (PID: 1840 cmdline: C:\Users\user\AppData\Local\buYWmbl3\WindowsActionDialog.exe MD5: 991359EE1E9C1958EB5D0F7314774123)
        - irftp.exe (PID: 4592 cmdline: C:\Windows\system32\irftp.exe MD5: F1C2D10CA8161DB689CD4FDE756E2DBB)
        - irftp.exe (PID: 6252 cmdline: C:\Users\user\AppData\Local\hJiut\irftp.exe MD5: F1C2D10CA8161DB689CD4FDE756E2DBB)
        - osk.exe (PID: 6228 cmdline: C:\Windows\system32\osk.exe MD5: 88B09DE7D0DF1D2E9BCA9BAE1346CB23)
  - rundll32.exe (PID: 5904 cmdline: rundll32.exe C:\Users\user\Desktop\1zdJLxxTnh.dll,??0?$PatternProvider@VExpandCollapseProvider@DirectUI@@UIExpandCollapseProvider@@$00@DirectUI@@QEAA@XZ MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6588 cmdline: rundll32.exe C:\Users\user\Desktop\1zdJLxxTnh.dll,??0?$PatternProvider@VGridItemProvider@DirectUI@@UIGridItemProvider@@$01@DirectUI@@QEAA@XZ MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5848 cmdline: rundll32.exe C:\Users\user\Desktop\1zdJLxxTnh.dll,??0?$PatternProvider@VGridProvider@DirectUI@@UIGridProvider@@$02@DirectUI@@QEAA@XZ MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.304569547.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
0000000C.00000002.289547097.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000003.00000002.365405591.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
0000000D.00000002.296819494.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000024.00000002.491095361.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
Click to see the 5 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 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

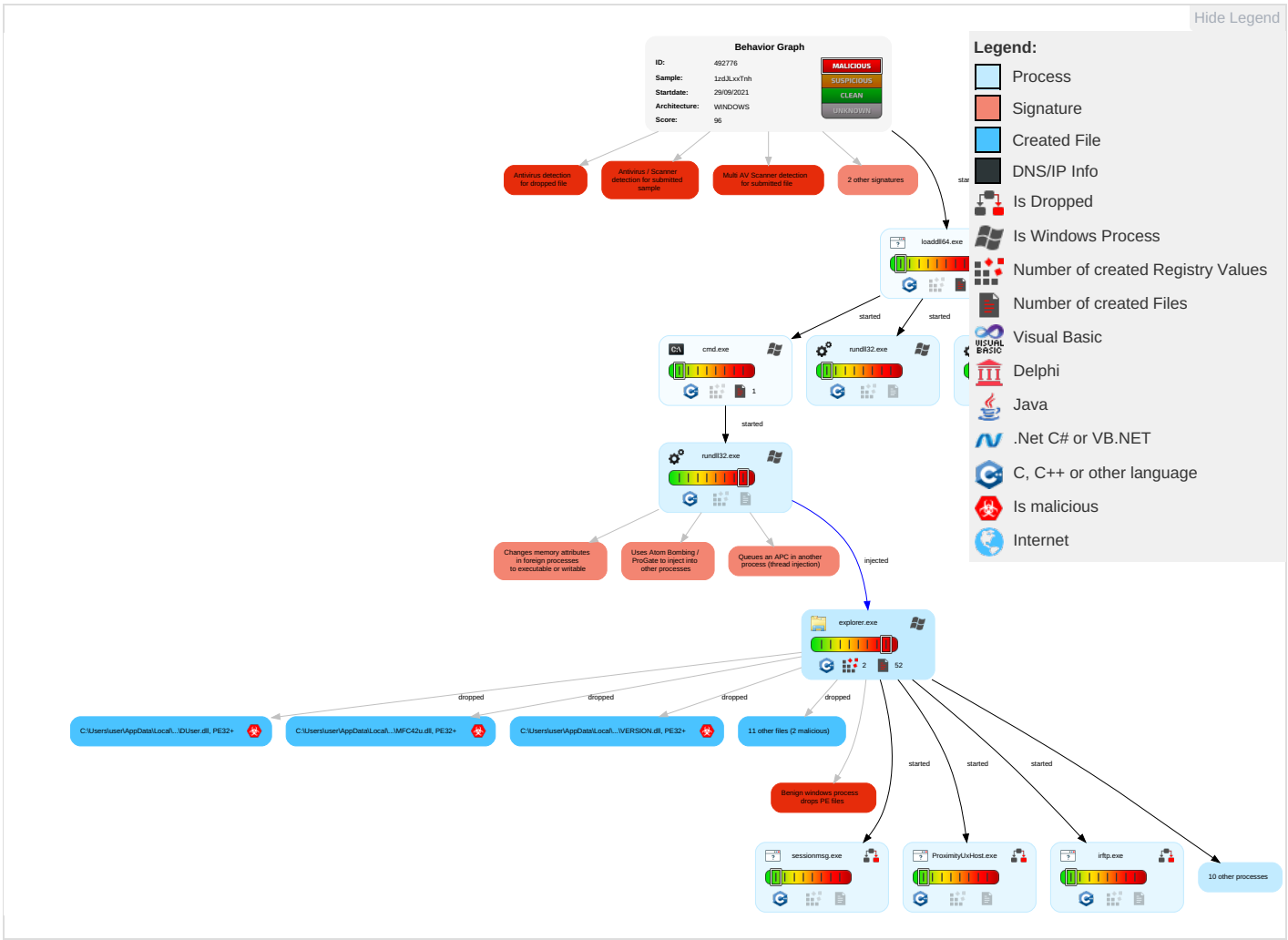
Queues an APC in another process (thread injection)

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	Remot Servic Effect
Valid Accounts	Exploitation for Client Execution 1	Path Interception	Process Injection 3 1 2	Masquerading 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remot Track Withou Author
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 3 1 2	LSASS Memory	Security Software Discovery 3 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS	Remot Wipe D Withou Author
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backu
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rundll32 1	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 2	LSA Secrets	System Information Discovery 2 5	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Timestomp 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

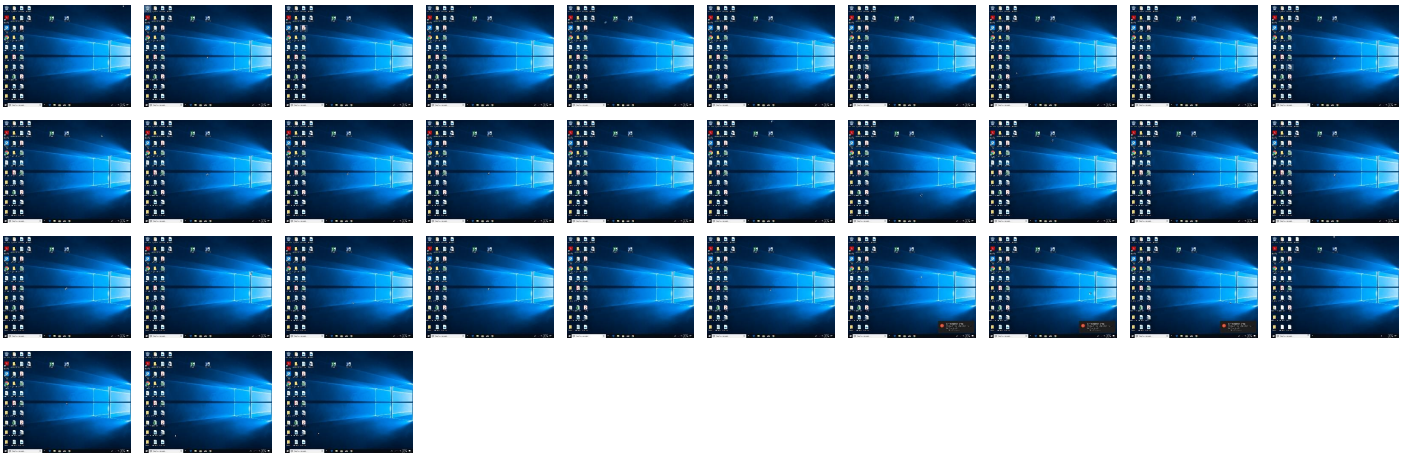
Behavior Graph



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
1zdJLxxTnh.dll	63%	Metadefender		Browse
1zdJLxxTnh.dll	78%	ReversingLabs	Win64.Infostealer.Dridex	
1zdJLxxTnh.dll	100%	Avira	HEUR/AGEN.1114452	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\XVzc21m9h\DUI70.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\94LPZAU0\WINMM.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\hJiut\MFC42u.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\nPqx0Ph\DUser.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\cp4nWp\VERSION.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\XVzc21m9h\DUI70.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\XVzc21m9h\DUI70.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\XVzc21m9h\DUI70.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\94LPZAU0\WINMM.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\hJiut\MFC42u.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\nPqx0Ph\DUser.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\cp4nWp\VERSION.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\XVzc21m9h\DUI70.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\XVzc21m9h\DUI70.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\94LPZAU0\irftp.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\94LPZAU0\irftp.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\XVzc21m9h\CameraSettingsUIHost.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\XVzc21m9h\CameraSettingsUIHost.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.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
12.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.2.irftp.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
36.2.WindowsActionDialog.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.loaddll64.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.2.ProximityUxHost.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
38.2.irftp.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
33.2.sessionmsg.exe.140000000.0.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

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	492776

Start date:	29.09.2021
Start time:	01:05:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1zdJLxxTnh (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:	mal96.troj.evad.winDLL@44/15@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 38% (good quality ratio 20.7%) • Quality average: 40.3% • Quality standard deviation: 42.3%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32
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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\94LPZAU0\irftp.exe	kVNcnRiK3f.dll	Get hash	malicious	Browse	
	y5ByLDz3o1.dll	Get hash	malicious	Browse	
	6jxIVk0kA7.dll	Get hash	malicious	Browse	
	QqfX0oJvWr.dll	Get hash	malicious	Browse	
	3zec70XUHT.dll	Get hash	malicious	Browse	
	9kiaVokmF5.dll	Get hash	malicious	Browse	
	N37wjZ34KC.dll	Get hash	malicious	Browse	
	f8YMzujfAD.dll	Get hash	malicious	Browse	
	siaHBnlRS5.dll	Get hash	malicious	Browse	
	Yz2OIFLI6N.dll	Get hash	malicious	Browse	
	P7n0h6OhYp.dll	Get hash	malicious	Browse	
	fyOtZmdc67.dll	Get hash	malicious	Browse	
	4keq2VSf0C.dll	Get hash	malicious	Browse	
	FFeeEo1mVe.dll	Get hash	malicious	Browse	
	m8ob3WN42p.dll	Get hash	malicious	Browse	
	rJyP5pxSI7.dll	Get hash	malicious	Browse	
	5pG7H5XLEj.dll	Get hash	malicious	Browse	
	0oSZeHvzK2.dll	Get hash	malicious	Browse	
	OAn9UHAhxa.dll	Get hash	malicious	Browse	
	AMlHS3s1sj.dll	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\94LPZAU0\WINMM.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2076672
Entropy (8bit):	3.638584417742171
Encrypted:	false
SSDEEP:	12288:tVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:0fP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	DE6B90EF400CA7533F969DAB0E573346
SHA1:	24B2B6E4E03023D8654BDC636E2BF78E5BC66175
SHA-256:	ABEE6BEE9DAEC86C44CA0BC43CAE8BCD52D192C5F5B8F7CFFCC053002579ED2A
SHA-512:	C10D42A295FFD0C4524109EE5ABEE659A82270F924F62539B2222515B198C207B91F21961128200C48927C603DBA85B41FF45E54A3F6523955174005AF717B96
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.$ ..DN^..... " .....p.....@.....@lx}..b.....h....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\94LPZAU0\irftp.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	184832
Entropy (8bit):	5.862106385432374
Encrypted:	false
SSDEEP:	3072:gzPq/xfWlkWmvIGaYLZ4yjchpChlyelcU4uuh0SEslWsXxgCzX0Fhf8LL8FT7:Eq5fWlkjuYLLtHyeFSEiXxZzb8FT
MD5:	F1C2D10CA8161DB689CD4FDE756E2DBB
SHA1:	C41E86E9755824D3775E2AD6CAC9A46C7AA1C417
SHA-256:	8854450FEAD134B24FABF4B805434FCFDDF25D2179048410728F8901E0FE0906
SHA-512:	5EBB1AD4261C689E22FE34CFB0C18D71451DD4F3694D8F521D181EB42FF90582D8EF8C8AB43BFC59D224452944D9602DB1030B633856E139442EEF0C2F4428F5
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Local\94LPZAU0\irftp.exe

Joe Sandbox View:	• Filename: kVNcnRiK3f.dll, Detection: malicious, Browse • Filename: y5ByLDz3o1.dll, Detection: malicious, Browse • Filename: 6jxIVk0kA7.dll, Detection: malicious, Browse • Filename: QqfX0oJvWr.dll, Detection: malicious, Browse • Filename: 3zec70XUHT.dll, Detection: malicious, Browse • Filename: 9kiaVokmF5.dll, Detection: malicious, Browse • Filename: N37wjZ34KC.dll, Detection: malicious, Browse • Filename: f8YMzujfAD.dll, Detection: malicious, Browse • Filename: siaHBnlRS5.dll, Detection: malicious, Browse • Filename: Yz2OIFLI6N.dll, Detection: malicious, Browse • Filename: P7n0h6OhYp.dll, Detection: malicious, Browse • Filename: fyOtZmdc67.dll, Detection: malicious, Browse • Filename: 4keq2VSf0C.dll, Detection: malicious, Browse • Filename: FFeeEo1mVe.dll, Detection: malicious, Browse • Filename: m8ob3WN42p.dll, Detection: malicious, Browse • Filename: rJyP5pxSI7.dll, Detection: malicious, Browse • Filename: 5pG7H5XLEj.dll, Detection: malicious, Browse • Filename: 0oSZeHvzK2.dll, Detection: malicious, Browse • Filename: OAn9UHAhxa.dll, Detection: malicious, Browse • Filename: AMlHS3s1sj.dll, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PU...4}..4}..4}.{P~..4}.{Py..4}.{Px..4}.{P|..4}..4|.c5}.{Pt.74}.{P...4}.{P...4}.Rich.4}.....PE..d....v.4.....".....6.....4.....@.....`..... .....T...,....p..0....`..t.....p.....T..... .....@i.....@j.....text....4.....6..... ..`.rdata.....P.....:.....@..@.data....|.....@....pdata..t....`.....@..@.rsrc. ..0....p.....@..@.reloc.....p.....@..B. .....

C:\Users\user\AppData\Local\XVzc21m9h\CameraSettingsUIHost.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	32104
Entropy (8bit):	6.224595599643794
Encrypted:	false
SSDEEP:	768:HYxSW1tZfZjtM2mpgc8WtCpZswKro1PDg:HhAhty8WteuwKrwPDg
MD5:	34F32BC06CDC7AF56607D351B155140D
SHA1:	88EF25BC91BCC908AF743ECA254D6251E5564283
SHA-256:	47238D9ED75D01FD125AC76B500FEEF7F8B27255570AD02D18A4F049B05DF3BD
SHA-512:	D855414779125F4E311ACF4D5EFC8ACA4452323CABD1694798CA90FD5BD76DC70B5D06790A2AE311E7DD19190DCCB134F6EF96AB1B7CF5B8A40AD642B72D5 44
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....._Lp..-...-...-U...-..tl...-..tl...-..tl...-..tl...-..-..-K-..tl...-..tl..-..tl...-..Rich.- .....PE..d....\YN.....".....*...2.....0.....@..... ..... ._.....Z..h#.....X..T.....`S..(...`R..... .....S.....text....(.....*..... ..`.imrsiv.....@.....rdata.....P.....@..@.data.....p.....J.....@....pdata.....L..... .....@..@.rsrc.....P.....@..@.reloc.....X.....@..B. .....

C:\Users\user\AppData\Local\XVzc21m9h\DUI70.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2355200
Entropy (8bit):	4.163841194314587
Encrypted:	false
SSDEEP:	12288:1VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ10+:sfP7fWsK5z9A+WGAW+V5SB6Ct4bnb0
MD5:	DF9A26EBFD0E77955639B4C28CDBCEED
SHA1:	D11A7BDC5C6E5C9C3F3CF4D2F37424A51B56F0E8
SHA-256:	1F6373350BC6604ACBD20A05AF002A90D9EA3D5B91846E9CC2246C58DD6F489E
SHA-512:	F4CCBA5DEA29E8F1597D85F894284286DC11AA18C82CFACAD79F519D3572DB51931402723F1E70B587BF74007E272D2D7079E7291187CCF26351456460985AB1
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|....\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.$ ..DN^....." .....p.....@.....#.....@lx}..b.....dQ...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\buYWmbl3\DUI70.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2355200
Entropy (8bit):	4.163717824294011
Encrypted:	false
SSDEEP:	12288:iVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ18tr:/fP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	EEDAC2477895922DC82316E94D049F45
SHA1:	91ACC4000617F625D237FEFF2978816483250E7B
SHA-256:	67CF8B8F250FCA4EE30D3E2EDFB59193EDCCC021100F4E36B8B2CA69C5CBD6F2
SHA-512:	C3E07B53406D9938B94FB8559232B544AB2A187B600EE9072BA0729FA65DF475239A475791EAC457FFD700899437036DE7A912E60495AC85650B5DE2069D0DF7
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.$ ..DN^....." .....p.....@.....#.....@lx}..b.....dQ...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\buYWmbl3\WindowsActionDialog.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	59392
Entropy (8bit):	5.897489723280295
Encrypted:	false
SSDEEP:	1536:VgSmVr7b1rKOX4TfOwQaq1WWhrIWSNJy8e:eZVrAThqLfSNwV
MD5:	991359EE1E9C1958EB5D0F7314774123
SHA1:	6456AEA32407B0AEEDD347AFAE5BB12BAB781863
SHA-256:	9F8E465348DBB165B7B0E6A72FCC78D2CE79FB897B1514490CD0DDAB021EA500
SHA-512:	EE6D10A0B75829AAAB55CB9F9EDA967D763F7CACD09F944A9C40B8E5ADDD6BBB6970F069FC64FA1807B547134B3558667A680174AB0366D11A068C6DD70BC3F3
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... .%.A.v.A.v.A.v.9Wv.A.v.%.w.A.v.%.w.A.v.%.w.A.v.%.w.A.v.A.v.A.v.%.w.A.v.%;v.A.v.%.w.A.vRich.A.v.....PE..d....i.....".....j.....@.....@.....'..... .....h.... .....0... ...p...T.....H.....text..... ..`.imrsiv.....rdata...H.....J.....@..@.data.....@ ....pdata.....@..@.rsrc..... .....@..@.reloc.....0.....@..B..... .....

C:\Users\user\AppData\Local\cp4nWp\PresentationHost.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	259072
Entropy (8bit):	6.5074250085194665
Encrypted:	false
SSDEEP:	6144:8kfs4/kfxzJTbHfyH5KNXwy3Odjp19k5KNXf:fs4ixzJTbHmKVwy3OdLaKV
MD5:	E3053C73EA240F4C2F7971B3905A91CF
SHA1:	1848AD66BD55E5484616FB85E80BA58BE1D5BA4B
SHA-256:	0BACCDB2B5ACB7B3C2E90856554575329 64CAFFF1AE250016CE1A80E839B820C
SHA-512:	167BCC3E2552286F7D985A65674DA2FF0D0AA6A7F0C4C3B43193943B606E0133C06EEB33656EFBB8B827AC9221FB1BA00A49ADCC2489BD4F38DF62A015806DE3
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3/.]\|.]\|.]\|...\|.]\|...\|..]\|..^}.]\|..Y}.]\|.\|..]\|..\}.]\|..T}..]\|..X}.]\|..\|.]\|..._}.]\|Rich.]\|. .....PE..d..../.....".....&.....@.....0.....`..... .....p.....j.....l..... ..,....d..T.....#..... .....$.....text...o..... ..`.rdata.....@..@.data.....r.....@....pdata..l.....t.....@..@.rsrc....j.....l...~..... ...@..@.reloc..,... .....@..B..... .....

C:\Users\user\AppData\Local\cp4nWp\VERSION.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2072576
Entropy (8bit):	3.6295467008086466
Encrypted:	false
SSDEEP:	12288:sVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:ZfP7fWsK5z9A+WGAW+V5SB6Ct4bnb

C:\Users\user\AppData\Local\cp4nWp\VERSION.dll	
MD5:	C0296097264DDCD2F205CF026F6156EE
SHA1:	62ADC91C6B674EFD2EA562829802BD1EF8100BDF
SHA-256:	0CDB374DD9EAF41D87A617D8CBF4BCB21EEFF618A31FCCAB6EA9C66FA8251906
SHA-512:	DD745FD15C16F44D9C171680729536B98A415D550B9B41106198C0DE5B187EB9FBA437FA8BBD4CE54337666F5044EA8FC313CAEE4B3E4FC03809710F7F9E4A0
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.$ ..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\fk8bXjSn\DUI70.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2355200
Entropy (8bit):	4.163555502778555
Encrypted:	false
SSDEEP:	12288:2VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ17:rfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	97899DD22E7099CBD89B24E779B35EF5
SHA1:	765C86A0789108B5301B2A6F5BA847A80F7CF488
SHA-256:	1CD2F440043C296AE7EDAA2F97BCDC6E3F75A563DB30CF26376DC5BE1F536016
SHA-512:	CD3508D410CBC89B8D7B6B2E45348F62C86DDF9FE9A2BF020B7006C1BF1EFEFD632D469BA62D58224BD3920A6B1A84144DDFB0D27CB08E751D9AFCD901A89B9
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.$ ..DN^..... ....p.....@.....#.....@lx}..b.....dQ...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\fk8bXjSn\ProximityUxHost.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	264480
Entropy (8bit):	6.478365286411354
Encrypted:	false
SSDEEP:	6144:xSt+s2GFGbqEuzhJONjx9UVuCuHpwqr/vt9r+ULJBaBpcIFz:xStzFGbGhoPgMHpwqrHthUB6IF
MD5:	E7F0E9B3779E54CD271959C600A2A531
SHA1:	8006E2D1AA91798E48D8BFDE1EBF94A2D6BA6C0A
SHA-256:	155CE33E0E145314FE9D8911BE69B8CBBD2AC09B7B6D98363F9BAA277C71954E
SHA-512:	E10C3FD9C5F34260323CEC9E8EEDF2290F40254F0FFDCA582DB57D113B32871793CDFFF03D55941EF5E79FA8141803AB353BA4938357A4555233F2D090045338
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B..B..B..K.`.&..-..A..-...U..-...K..-..U..B..t..-...]..-...C..-..C..RichB..... .....PE..d...;.*Q....."..... .....@..... .....&..... .....H.....T..... +.....Pa..T.....p3..(...p2.....3. .....text..... ..`.imrsiv.....rdata..... .....@..@.data...x.....@....pdata..T.....@..@. rsrc...H.....@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\hJiut\MFC42u.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2097152
Entropy (8bit):	3.6697318639322516
Encrypted:	false
SSDEEP:	12288:CVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1f+:ffP7fWsK5z9A+WGAW+V5SB6Ct4bnbf
MD5:	6BCACDA8CFA448613A0451AE796AE5C6
SHA1:	64A461FDFE4E9A7F8396360BB20E76621F29E84D
SHA-256:	FE69D758AF8D1751485661FBBBEF32774E6AC762A530ACE05A0588892A979D4E
SHA-512:	214B6361D9677ED81E0CE82470DBB81C831F5A90B7AEC3BF933B955DFBDFB41037EACBE20F08453492C5D0C361D217596E61CE52B5E405B4C24B7192C8B87B0
Malicious:	**true**

C:\Users\user\AppData\Local\hJiut\MFC42u.dll	
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.$ ..DN^....." .....p.....@..... .....@lx}..b.....l...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\hJiut\irftp.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	184832
Entropy (8bit):	5.862106385432374
Encrypted:	false
SSDEEP:	3072:gzPq/xfWlkWmvlGaYLZ4yjchpChlyelcU4uuh0SEslWsXxgCzX0Fhf8LL8FT7:Eq5fWlkjuYLLtHyeFSEiXxZzb8FT
MD5:	F1C2D10CA8161DB689CD4FDE756E2DBB
SHA1:	C41E86E9755824D3775E2AD6CAC9A46C7AA1C417
SHA-256:	8854450FEAD134B24FABF4B805434FCFDDF25D2179048410728F8901E0FE0906
SHA-512:	5EBB1AD4261C689E22FE34CFB0C18D71451DD4F3694D8F521D181EB42FF90582D8EF8C8AB43BFC59D224452944D9602DB1030B633856E139442EEF0C2F4428F5
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PU...4}..4}..4}.{P~..4}.{Py..4}.{Px..4}.{P|..4}..4|.c5}.{Pt.74}.{P...4}. {P...4}.Rich.4}.....PE..d....v.4....."....6.....4.....@.....`..... .....T...,....p..0....`..t.....p.....T..... .....@i.....@j.....text....4.....6..... ..`.rdata.....P.....:.....@..@.data....|.....@....pdata..t...`.....@..@.rsrc. ..0....p.....@..@.reloc.....p.....@..B..... .....

C:\Users\user\AppData\Local\nPqx0Ph\DUser.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2076672
Entropy (8bit):	3.637582444744564
Encrypted:	false
SSDEEP:	12288:gVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:FfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	A9531A4FBBE843891F8C095078E00403
SHA1:	0C85EFD8F60C8E4ABE9DE5F75E6B4C06D282D7EA
SHA-256:	D7CDF51766A2963B345787D3DB99D39A09F40EC03C522F21D386D920C58BA35F
SHA-512:	881BDDED76845E38AD6426D75700C7E8C5873D783E7360C6B71E7CA4BA75F18B66EC508B17507132AD1015AC29B812C64E398DCE20675ECB285B8068FB6C039
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.$ ..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\nPqx0Ph\sessionmsg.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	74440
Entropy (8bit):	6.20617662830101
Encrypted:	false
SSDEEP:	1536:uC9DVLLFwi//NFlWPP0mTluh1AzxJIdqqP86mSsrvNJYKPd:L3FR/F7+0mTwhswdqqk6mS4RF
MD5:	1F7CEA0216DE48B877C16F95C7DA1F0F
SHA1:	BBF654AC3D1EEC107CF18B9A7AF15FA1ED0F6075
SHA-256:	0E585A4A11586B921D103433AFA215EC419A5ED2940EFD084A47B871F43CC786
SHA-512:	3E724732D4EAA863263D2D4259FF2DF8132486418D23DBBE572E72B766416F2F7100C54EC5F776085F3EB04C33521D50895DDA1DE2947814AB67FEED55E89F50
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....:...[...[...[..?...[..?...[..?...[..?...[...[...[..?...[..?<..[..?...[..Rich.[..... .....PE..d.....#E....."....\|.....y.....@.....s,..... .....P..`....@..l.....$...p.....`...T..... .....text....{....|..... ..`.imrsiv.....rdata...Y.....Z.....@..@.data....0.....@....pdata..l....@.....@..@.rs rc...`....P.....@..@.reloc.....p.....@..B..... .....

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\414045e2d09286d5db2581e0d955d358_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	4442
Entropy (8bit):	5.478783838366747
Encrypted:	false
SSDEEP:	48:FB5UgQRPrFgsq9CQktB5Unb3q92Wxrdwp6BHCribUY3k:FB5a13QuB50ba9RSpILX3k
MD5:	B2DC6B85154F81B3DD4677C710BD887B
SHA1:	B5A3862164A608B9E4616191876DD21B48F7A3D6
SHA-256:	3438E62E88D5193A7CE2948C465034883BA92EB335F5E8C6A9AFB60C43853BD1
SHA-512:	49318BA9C0F9E53718906521E2029B405E58CF700531CCC53BBEB63E298F8205F49267AD8D1533A514E4EFAF4770138F5F30E7B5923B1495F1F4F1C6479123D4
Malicious:	false
Preview:	.....user.....user.....RSA1.....V.l4...&..O.5|z\.C...:h.N./.....J.....U...u.R..y0.ZW%.....u..k.0_.U.d...#..t+..I..F}I..E'...pw.s..C.ke.....&.s.....z..O.....A\..1..F..:M...F....,...C.r.y.p.t.o.A.P.I. .P.r.i.v.a.t.e. .K.e.y....f..... ....Xf..1..?.8..Xn8m.o..{/.R6U..... .....d.[Dpg....X .P.@qXU....+mP.....T.....JI.ts7...d.r....'.t#...."S....|.....R.a{.\0.i,..Y.XF't.).Cl<...*.U.y.R..$b..m1P..=.pS...X% ...J.z?I.....t@..xi.rWQ..Y.=..b`<..0....2>...;...eT.Y.c{$. .' Jdw`...O$.Q.....^r1.S...8V.E.-S+=?*x...-s...(^.+.S .....T.i.\|f...1.m....}.!.....X3.....y....^.!.....U..9.)...zbg....V.....X.....=...+,./.;....*k7t.....f)..c^o..s....Z....<.~.N.p .!.Y9....`.0. B..WL.7.....+W..)&...$.,.F....q.....?..3..>...}..~I..:.$/09..hgtb.A;.B.T.r&u...z.....h.Gof.GZ...'.v.....,5.#..s..0..rH.O.w..A.....

Static File Info

General

File type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Entropy (8bit):	4.624276841986733
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:	1zdJLxxTnh.dll
File size:	2068480
MD5:	784adf3295b7eafe53aa80da302b1b5d
SHA1:	c79da77a4d00ec47594e007f9a174de43b5028d3
SHA256:	69af86da86fc2f9639f010e0b729b1c2ce33a272d199aeedc4c873d98a2b83b4
SHA512:	3fbc71e7f7de7526acd525f98fc18c8af2cef28a44e0b08b0f789f758ca96ce4c631d94b76c85513c2954ea9fa0dd6bbcbf07143ab86861a720b89a018a29860
SSDEEP:	12288:YVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1qxgI:NfP7fWsK5z9A+WGAW+V5SB6Ct4bnbg
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	0x64f2c	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
.tblq	0x110000	0x5a7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.hcmjm	0x111000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.nagyk	0x157000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.jrucz	0x158000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rnr	0x159000	0x3fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rdc	0x15a000	0x45174	0x46000	False	0.0010498046875	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
.umrigl	0x1a0000	0x543	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.nepl	0x1a1000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.akkqh	0x1a2000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.cvbwr	0x1a3000	0x15a	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ftrk	0x1a4000	0x3ba	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ubbf	0x1a5000	0x1f7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ulwqi	0x1a6000	0x5a7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.imcflb	0x1a7000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.hgmkm	0x1a8000	0x3ba	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.cnoij	0x1a9000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.qgdv	0x1aa000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.hsbye	0x1ac000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.cdn	0x1ad000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.hte	0x1af000	0x389	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vcnknm	0x1b0000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.thfe	0x1b1000	0x1f7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tat	0x1b2000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.xqltbd	0x1b3000	0x451c2	0x46000	False	0.218523297991	data	5.76006812667	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

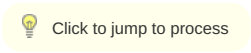
Network Port Distribution

UDP Packets

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: loaddll64.exe PID: 7152 Parent PID: 4336

General

Start time:	01:05:58
Start date:	29/09/2021
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe 'C:\Users\user\Desktop\1zdJLxxTnh.dll'
Imagebase:	0x7ff62eae0000
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: 00000000.00000002.304569547.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 5808 Parent PID: 7152

General

Start time:	01:05:59
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\1zdJLxxTnh.dll',#1
Imagebase:	0x7ff6637d0000
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: 1012 Parent PID: 5808

General

Start time:	01:05:59
Start date:	29/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe 'C:\Users\user\Desktop\1zdJLxxTnh.dll',#1
Imagebase:	0x7ff79cf00000
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: 00000003.00000002.365405591.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 5904 Parent PID: 7152

General

Start time:	01:05:59
Start date:	29/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\1zdJLxxTnh.dll,??0?$PatternProvider@VExpandCollapseProvider@DirectUI@@UIExpandCollapseProvider@@$00@DirectUI@@QEAA@XZ
Imagebase:	0x7ff79cf00000
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: 00000004.00000002.283056136.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3352 Parent PID: 1012

General

Start time:	01:06:01
Start date:	29/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff720ea0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
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: 6588 Parent PID: 7152

General

Start time:	01:06:02
Start date:	29/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\1zdJLxxTnh.dll,??0?$PatternProvider@VGridItemProvider@DirectUI@@UIGridItemProvider@@$01@DirectUI@@QEAA@XZ
Imagebase:	0x7ff79cf00000
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: 0000000C.00000002.289547097.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 5848 Parent PID: 7152

General

Start time:	01:06:06
Start date:	29/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\1zdJLxxTnh.dll,??0?$PatternProvider@VGridProvider@DirectUI@@UIGridProvider@@$02@DirectUI@@QEAA@XZ
Imagebase:	0x7ff79cf00000
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: 0000000D.00000002.296819494.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: ProximityUxHost.exe PID: 5800 Parent PID: 3352

General

Start time:	01:06:41
Start date:	29/09/2021
Path:	C:\Windows\System32\ProximityUxHost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\ProximityUxHost.exe
Imagebase:	0x7ff7a7f60000
File size:	264480 bytes
MD5 hash:	E7F0E9B3779E54CD271959C600A2A531
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ProximityUxHost.exe PID: 4896 Parent PID: 3352

General

Start time:	01:06:46
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\fk8bXjSn\ProximityUxHost.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\fk8bXjSn\ProximityUxHost.exe
Imagebase:	0x7ff7a3c80000
File size:	264480 bytes
MD5 hash:	E7F0E9B3779E54CD271959C600A2A531
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000016.00000002.402800394.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities Show Windows behavior

File Read

Analysis Process: rstrui.exe PID: 492 Parent PID: 3352

General

Start time:	01:06:58
Start date:	29/09/2021
Path:	C:\Windows\System32\rstrui.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\rstrui.exe
Imagebase:	0x7ff7515b0000
File size:	266752 bytes
MD5 hash:	3E8AFFA54035412F86663C8B44CAA2E5
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: irftp.exe PID: 4740 Parent PID: 3352

General

Start time:	01:06:58
Start date:	29/09/2021
Path:	C:\Windows\System32\irftp.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\irftp.exe
Imagebase:	0x7ff669c40000
File size:	184832 bytes
MD5 hash:	F1C2D10CA8161DB689CD4FDE756E2DBB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: irftp.exe PID: 6684 Parent PID: 3352

General

Start time:	01:06:59
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\94LPZAU0\irftp.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\94LPZAU0\irftp.exe
Imagebase:	0x7ff7edb50000
File size:	184832 bytes
MD5 hash:	F1C2D10CA8161DB689CD4FDE756E2DBB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000001C.00000002.430835734.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

File Activities

Show Windows behavior

File Read

Analysis Process: SystemPropertiesComputerName.exe PID: 5792 Parent PID: 3352

General

Start time:	01:07:10
Start date:	29/09/2021
Path:	C:\Windows\System32\SystemPropertiesComputerName.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SystemPropertiesComputerName.exe
Imagebase:	0x7ff70aa30000
File size:	83968 bytes
MD5 hash:	BEE134E1F23AFD3AE58191D265BB9070
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: sessionmsg.exe PID: 5252 Parent PID: 3352

General

Start time:	01:07:11
Start date:	29/09/2021
Path:	C:\Windows\System32\sessionmsg.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\sessionmsg.exe
Imagebase:	0x7ff75e520000
File size:	74440 bytes
MD5 hash:	1F7CEA0216DE48B877C16F95C7DA1F0F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: sessionmsg.exe PID: 5724 Parent PID: 3352

General

Start time:	01:07:12
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\nPqx0Ph\sessionmsg.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\nPqx0Ph\sessionmsg.exe
Imagebase:	0x7ff679360000
File size:	74440 bytes
MD5 hash:	1F7CEA0216DE48B877C16F95C7DA1F0F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000021.00000002.459843217.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Read

Analysis Process: WindowsActionDialog.exe PID: 6136 Parent PID: 3352

General

Start time:	01:07:24
Start date:	29/09/2021
Path:	C:\Windows\System32\WindowsActionDialog.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WindowsActionDialog.exe
Imagebase:	0x7ff6dc520000
File size:	59392 bytes
MD5 hash:	991359EE1E9C1958EB5D0F7314774123
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: WindowsActionDialog.exe PID: 1840 Parent PID: 3352

General

Start time:	01:07:27
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\buYWmbl3\WindowsActionDialog.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\buYWmbl3\WindowsActionDialog.exe
Imagebase:	0x7ff6a5e00000
File size:	59392 bytes
MD5 hash:	991359EE1E9C1958EB5D0F7314774123
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000024.00000002.491095361.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: irftp.exe PID: 4592 Parent PID: 3352

General

Start time:	01:07:39
Start date:	29/09/2021
Path:	C:\Windows\System32\irftp.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\irftp.exe
Imagebase:	0x7ff669c40000
File size:	184832 bytes
MD5 hash:	F1C2D10CA8161DB689CD4FDE756E2DBB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: irftp.exe PID: 6252 Parent PID: 3352

General

Start time:	01:07:46
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\hJiut\irftp.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\hJiut\irftp.exe
Imagebase:	0x7ff65a340000

File size:	184832 bytes
MD5 hash:	F1C2D10CA8161DB689CD4FDE756E2DBB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000026.00000002.532861365.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: osk.exe PID: 6228 Parent PID: 3352

General

Start time:	01:07:59
Start date:	29/09/2021
Path:	C:\Windows\System32\osk.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\osk.exe
Imagebase:	0x7ff64ff30000
File size:	622592 bytes
MD5 hash:	88B09DE7D0DF1D2E9BCA9BAE1346CB23
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

Code Analysis