ID: 492503
Sample Name: DC2zX44MQr
Cookbook: default.jbs
Time: 19:13:08
Date: 28/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Windows Analysis Report DC2zX44MQr

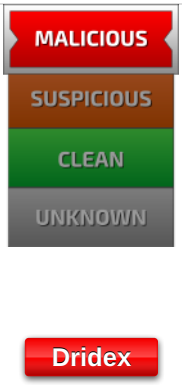
Overview

General Information

Sample Name:	DC2zX44MQr (renamed file extension from none to dll)
Analysis ID:	492503
MD5:	94f8317b419e947.
SHA1:	f2b03dd4441f380..
SHA256:	2f10b593a5e0450.
Tags:	Dridex exe
Infos:	

Most interesting Screenshot:

Detection

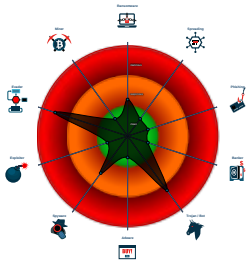


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- Contains functionality to check if a d…

Classification



- **System is w10x64**
- loaddll64.exe (PID: 6552 cmdline: loaddll64.exe 'C:\Users\user\Desktop\DC2zX44MQr.dll' MD5: E0CC9D126C39A9D2FA1CAD5027EBBD18)
  - cmd.exe (PID: 6576 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\DC2zX44MQr.dll',#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 6600 cmdline: rundll32.exe 'C:\Users\user\Desktop\DC2zX44MQr.dll',#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6584 cmdline: rundll32.exe C:\Users\user\Desktop\DC2zX44MQr.dll,DisplaySYSDMCPL MD5: 73C519F050C20580F8A62C849D49215A)
    - explorer.exe (PID: 3292 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - DmNotificationBroker.exe (PID: 3476 cmdline: C:\Windows\system32\DmNotificationBroker.exe MD5: 1643D5735213BC89C0012F0E48253765)
      - DmNotificationBroker.exe (PID: 6464 cmdline: C:\Users\user\AppData\Local\EwdQnyo\DmNotificationBroker.exe MD5: 1643D5735213BC89C0012F0E48253765)
      - RdpSa.exe (PID: 4488 cmdline: C:\Windows\system32\RdpSa.exe MD5: 0795B6F790F8E52D55F39E593E9C5BBA)
      - RdpSa.exe (PID: 2152 cmdline: C:\Users\user\AppData\Local\zLYZkwYH\RdpSa.exe MD5: 0795B6F790F8E52D55F39E593E9C5BBA)
      - Utilman.exe (PID: 2884 cmdline: C:\Windows\system32\Utilman.exe MD5: C91CCEF3884CFDE746B4BAEF5F1BC75C)
      - Utilman.exe (PID: 3596 cmdline: C:\Users\user\AppData\Local\KbLvcSLVf\Utilman.exe MD5: C91CCEF3884CFDE746B4BAEF5F1BC75C)
      - EaseOfAccessDialog.exe (PID: 6104 cmdline: C:\Windows\system32\EaseOfAccessDialog.exe MD5: F87F2E5EBF3FFBA39DF1621B5F8689B5)
      - EaseOfAccessDialog.exe (PID: 6128 cmdline: C:\Users\user\AppData\Local\rm4w0\EaseOfAccessDialog.exe MD5: F87F2E5EBF3FFBA39DF1621B5F8689B5)
      - DevicePairingWizard.exe (PID: 5024 cmdline: C:\Windows\system32\DevicePairingWizard.exe MD5: E23643C785D498FF73B5C9D7EA173C3D)
      - DevicePairingWizard.exe (PID: 4804 cmdline: C:\Users\user\AppData\Local\mJLa\DevicePairingWizard.exe MD5: E23643C785D498FF73B5C9D7EA173C3D)
      - wermgr.exe (PID: 4896 cmdline: C:\Windows\system32\wermgr.exe MD5: FF214585BF10206E21EA8EBA202FACFD)
      - wermgr.exe (PID: 5600 cmdline: C:\Users\user\AppData\Local\xIPP\wermgr.exe MD5: FF214585BF10206E21EA8EBA202FACFD)
      - mstsc.exe (PID: 6664 cmdline: C:\Windows\system32\mstsc.exe MD5: 3FBB5CD8829E9533D0FF5819DB0444C0)
      - mstsc.exe (PID: 6636 cmdline: C:\Users\user\AppData\Local\pZCYq8TUy\mstsc.exe MD5: 3FBB5CD8829E9533D0FF5819DB0444C0)
  - rundll32.exe (PID: 6676 cmdline: rundll32.exe C:\Users\user\Desktop\DC2zX44MQr.dll,EditEnvironmentVariables MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6808 cmdline: rundll32.exe C:\Users\user\Desktop\DC2zX44MQr.dll,EditUserProfiles MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000023.00000002.498301124.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000026.00000002.525725102.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000003.00000002.252587929.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000000.00000002.272674434.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000006.00000002.258809816.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
Click to see the 7 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)

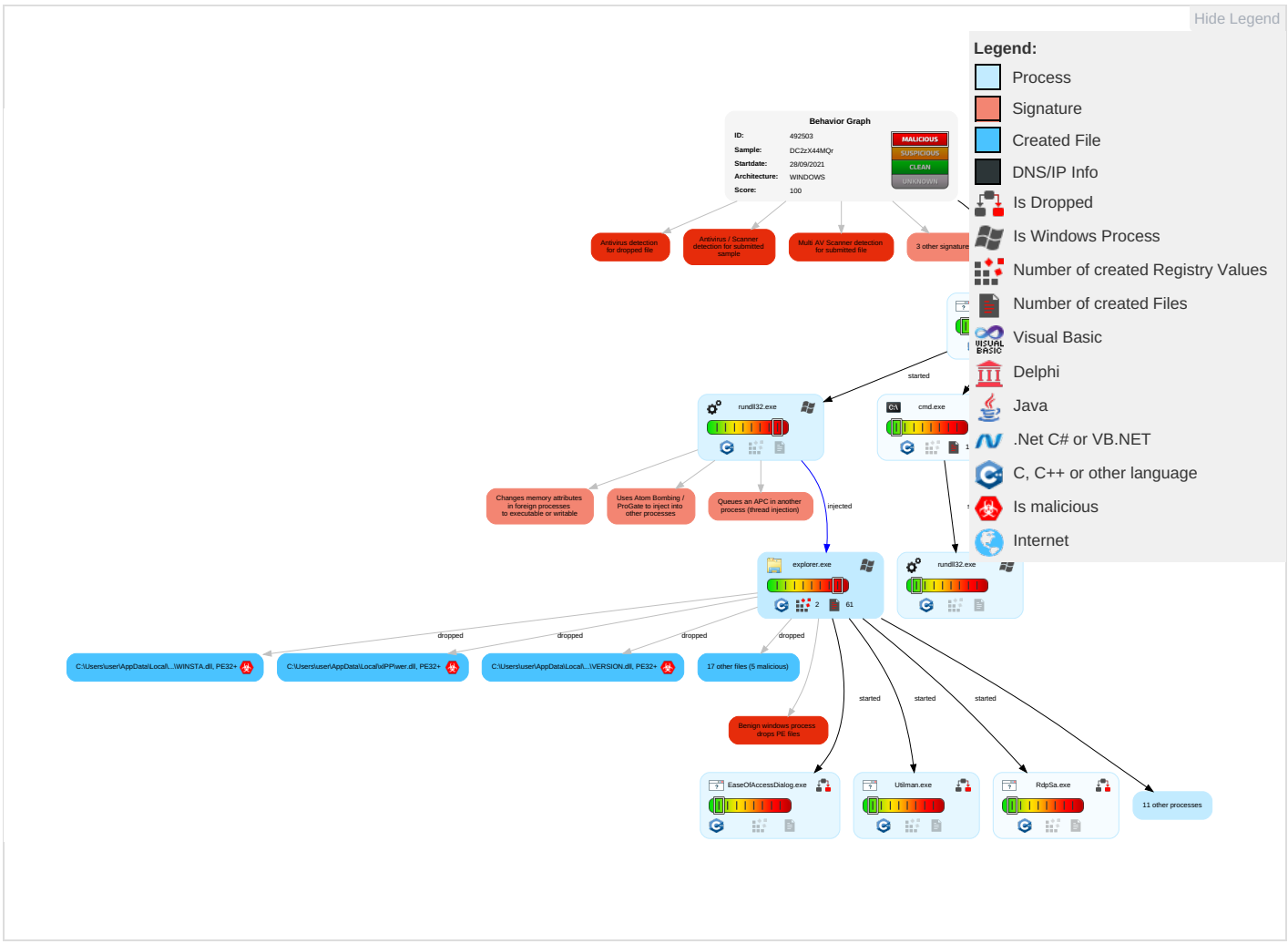
Uses Atom Bombing / ProGate to inject into other processes

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	Windows Service 1	Windows Service 1	Masquerading 1	Input Capture 1	System Time Discovery 1 1	Remote Services	Input Capture 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	Boot or Logon Initialization Scripts	Process Injection 3 1 2	Virtualization/Sandbox Evasion 1	LSASS Memory	Security Software Discovery 2 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Junk Data	Exploit SS Redirect Pl Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 3 1 2	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Process Discovery 3	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	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 2	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	Timestomp 1	DCSync	System Owner/User Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi- Access Poi
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	File and Directory 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 3 5	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cell Base Static

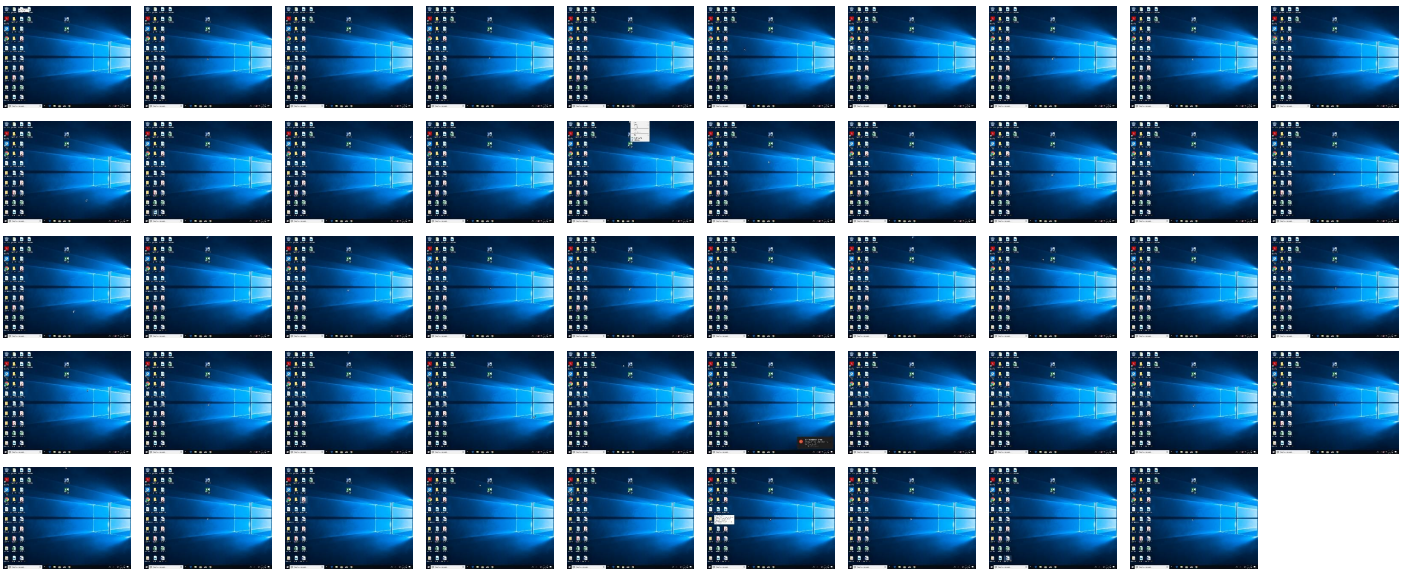
Behavior Graph



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
DC2zX44MQr.dll	68%	Virustotal		Browse
DC2zX44MQr.dll	80%	ReversingLabs	Win64.Infostealer.Dridex	
DC2zX44MQr.dll	100%	Avira	HEUR/AGEN.1114452	
DC2zX44MQr.dll	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\sBx0fm\VERSION.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\xlPP\wer.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\pZCYq8TUy\credui.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\zLYZkwYH\WINSTA.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\EwdQnyo\DUI70.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\EwdQnyo\DUI70.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\bQkmObl\WTSAPI32.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\EwdQnyo\DUI70.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\mJLa\MFC42u.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\rm4w0\OLEACC.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\sBx0fm\VERSION.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\xlPP\wer.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\pZCYq8TUy\credui.dll	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\zLYZkwYH\WINSTA.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\EwdQnyo\DUI70.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\EwdQnyo\DUI70.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\bQkmObl\WTSAPI32.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\EwdQnyo\DUI70.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\mJLa\MFC42u.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\rm4w0\OLEACC.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\EwdQnyo\DmNotificationBroker.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\EwdQnyo\DmNotificationBroker.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\EwdQnyo\DmNotificationBroker.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\KbLvcSLVf\Utilman.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\KbLvcSLVf\Utilman.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\WkAB\PasswordOnWakeSettingFlyout.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\WkAB\PasswordOnWakeSettingFlyout.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\bQkmObl\RDVGHelper.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\bQkmObl\RDVGHelper.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
33.2.EaseOfAccessDialog.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.DmNotificationBroker.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
38.2.wermgr.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
25.2.RdpSa.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
40.2.mstsc.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
35.2.DevicePairingWizard.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.rundll32.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
28.2.Utilman.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

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond

Analysis ID:	492503
Start date:	28.09.2021
Start time:	19:13:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DC2zX44MQr (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@45/21@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 39.2% (good quality ratio 25.9%) • Quality average: 52.1% • Quality standard deviation: 43.6%
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

No context

Created / dropped Files

C:\Users\user\AppData\Local\EwdQnyo\DUI70.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1523712
Entropy (8bit):	5.861496486431302
Encrypted:	false
SSDEEP:	12288:ZVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1sr:YfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	C63D9096C976C275357356F7A08F8CDE
SHA1:	1C35F2161C931B04E8A41D42C9CD1CA76D8FE41E
SHA-256:	AF746CDAE49B2A4E18F9BCC2517DA92AD8FEED1FE1F4D96EE15B1D6E003C8852
SHA-512:	84944B6F7E59E957437EC02B3E555AC0833163DC1F19EBC0DE518AF89245310E49EF4C87396641C0B41A73E1DF352D4BA8831EDE20AD424365F4AAFC4D8C134
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\EwdQnyo\DmNotificationBroker.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	32256
Entropy (8bit):	5.250876383836324
Encrypted:	false
SSDEEP:	768:ghunFhykO4aAvnsvpzte5+Ql0/iqmjjn:58kO4asshu+Q+/Ojjn
MD5:	1643D5735213BC89C0012F0E48253765
SHA1:	D076D701929F1F269D34C8FD7BD1BAB4DAF42A9D
SHA-256:	4176FA24D56BB870316D07BD7211BC8A797394F77DCC12B35FFEBAA0326525D2
SHA-512:	F0BD45FE66EDC6F615C0125C1AE81E657CA26544544769651AB0623DD3C724F96D9D78835EF6B1D15083D1BB9D501F6DC48487DDA5C361CAFA96022D5F33A4
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....$.....j.?H..lH..lH..lAs.lT..l'o.mJ..l'o.m[..lH..l...l'o.mC..l'o.mA..l'o.mA..l'ohll..l'o.ml..lRichH..l.....PE..d.....".....*...V.....&.....@.....n3..... .....x..... .....Po..T.....]..... ^..p.....text....(.....*..... ..`.imrsiv.....@.....rdata..P8...P...:.....@..@.data...(.....h.....@...pdata.....j.....@..@.rsrc... .....n.....@..@.reloc.....z.....@..B.....

C:\Users\user\AppData\Local\KbLvcSLVf\DUI70.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1523712
Entropy (8bit):	5.861475842348347
Encrypted:	false
SSDEEP:	12288:5VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ12Bh:4fP7fWsK5z9A+WGAW+V5SB6Ct4bnb2
MD5:	1B515CB5B54D379E258F3BE018F2DCC5
SHA1:	448821262C4B6775152F3D1FC3F70A125A7A4A78
SHA-256:	65E9D5DC7D6ECAB9FEB419B641726C56772C951270750ECC51317C305AB62CAC
SHA-512:	5A0A16531FFEE2A563933EE571C913D1EF2557D3C57EC177D27F8798438062C828EC7D4BFACD32E315F5D150239A3029B67C1B99D6B391461F3C1E6E88E6A7E
Malicious:	false

C:\Users\user\AppData\Local\KbLvcSLVf\DUI70.dll	
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\KbLvcSLVf\Utilman.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	98304
Entropy (8bit):	5.996546491031358
Encrypted:	false
SSDEEP:	1536:3bo99g4+4G8mMM+nCA+o6UJMUHznV80KCt1p7Gx:LXH4GvNKAUHR80KCt/G
MD5:	C91CCEF3884CFDE746B4BAEF5F1BC75C
SHA1:	9A7E17BA64FE1842E904D4019D9BB9B005E61E55
SHA-256:	E6C9C88491EF6FB4B4DAFAC3276C8E2A3B2BC3C4D7825F4EAA3AC99E1801195B
SHA-512:	431754EC35871B2ED1F5E9FC621F24B6187720C0562D0ABDC9232A063DA1E8419A07CDC1740A3B433A80BA15FF25F0EAE0E5B331985A7B8ABC9CE8E73CBC21E
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....D.....@..@..@..8@..@o..A..@o..A..@o..A..@o..A..@..@4.@o..A..@o.T@..@o..A..@Rich..@.....PE..d....0.....".....@.....R..... .....L.,.....x.....d...p...T.....text..... ..`.imrsiv.....rdata...x.....z.....@..@.data.....P.....@....pdata.....Z.....@..@.rsrc...x.....d.....@..@.reloc..d.....~.....@..B.....

C:\Users\user\AppData\Local\WkAB\DUI70.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1523712
Entropy (8bit):	5.861361447985384
Encrypted:	false
SSDEEP:	12288:cVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1m5:pfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	0E2C09A45BC0ED953B1A20E3DDD9D186
SHA1:	80317AB8392B224A9091359C0A16DA40D35053F5
SHA-256:	2E2F9B6F590F13C1834BA38AFFE06DAA48AA7A0994EEE493D5011B336B0CC6A9
SHA-512:	9F9EA4D4E62D0863212B227B2DF45BFD751D43BC5E674BADD730DDB1FD0E67AC9F99D0B4F8B209B0B4AA73467DDCEB29075E6BEFA7C9620A3CA056E00DD0C8F5
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\WkAB\PasswordOnWakeSettingFlyout.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	43472
Entropy (8bit):	6.224421457593777
Encrypted:	false
SSDEEP:	768:+pH9d9NT4uJO0qK/lEbrDGe2gfBTDxxsg652PIBmRncHiDgcZd3cxe1PIc:EzNT4GpHaTDvst2gmRnVdZVcgPIc
MD5:	F0C8675F98E397383A112CC8ED5B97DA
SHA1:	644A87D9CEE0BC576402573224F6695AA45196D3
SHA-256:	0E9C85E4833BB1BF45CB66AA3B021A2CDA6074333C2217F8FFB5360B63719374
SHA-512:	ABF6B2BB5BB48C1C2E54C01656D3C448E8CD4159686F285D67CFF805A757FFAF6B0D7D9DD579786B739AD90ECB1FB6D43A181CBEBBC27FEA3504D48B61C105C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Local\WkAB\PasswordOnWakeSettingFlyout.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....h.....J...J...J.q_J...J.m.K...J.m.K...J.m.K...J.m.K...J...J...J.m.K...J .m3J...J.m.K...JRich...J.....PE..d....Z.....".....B...F.....I.....@.....*}..... .....@.....,.....#.....|..T..... .....0q.....0r.....text....A.....B..... ..`.imrsiv.....`.....rdata..8$...p...&...F.....@..@.data.....I.....@....pdata. .,.....n.....@..@.rsrc.....t.....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\bQkmObl\RDVGHelper.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	107008
Entropy (8bit):	6.213211715541241
Encrypted:	false
SSDEEP:	1536:jZPv9YEIT8g15BZNWNBWNK5/FzUJmufD6o6ffv+Difx1P4dirH+Z3sUS+CvilU/s:lPBLBBbWDwff22J1Puq+y+HUk
MD5:	0BF1E2262C95164A0B244174167FBD85
SHA1:	81BD08AD31BF2665F298406F843924588BB7606B
SHA-256:	6B35C354C480D232A96EF73EABA268EF7D94F30A3D3A1161B69081B048A27E29
SHA-512:	FD01664A377359E72A67F52E8DFFDD237E24F8ACC158B3A478F71CAAC1CE2EDDB19B15E1FC66CB73E77DDED564D6A98FD3064BDA20419D8C949505457721BI 5C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....L.....g.....g.....g.....g.....g.....g.w....g.....Rich..... ....PE..d.....o.....".....B...b.....`G.....@.....`..... .....T.....$.....T.....g.....h..... .....text....@.....B..... ..`.rdata...A...`...B...F.....@..@.data.....@....pdata..T.....@..@.rsrc.....@..@.r eloc..$.....@..B..... .....

C:\Users\user\AppData\Local\bQkmObl\WTSAPI32.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1241088
Entropy (8bit):	5.503813896207835
Encrypted:	false
SSDEEP:	12288:hVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:QfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	F2A29CC94479DC03351404004C40E18A
SHA1:	778E570E30ABD2DCAEFEDCC2D24F35F81D56AC5E
SHA-256:	BB734D97EF436A89FC93C426141CDE1A5A73C73B7E10CBEB667105C44823CA5E
SHA-512:	7758DDA6DC6D6E1AE63A6F7D84C1EBA50470DAD48052A4AA7609BDF4AB33BF5253FB7368F0A78747F78D19F4D77E0ACD7DE9DE53B42C3863159513ABB03198 A
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}..'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.(..DN^..... " .....p.....@.....@\|x}..b.....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\mJLa\DevicePairingWizard.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	92160
Entropy (8bit):	5.664138088677901
Encrypted:	false
SSDEEP:	1536:D/BmrFjio5/vzDSPwiEKi3xGyibqZ3qOT3:9mp5SwiEKWZiTo3
MD5:	E23643C785D498FF73B5C9D7EA173C3D
SHA1:	56296F1D29FC2DCBFAA1D991C87B10968C6D3882
SHA-256:	40F423488FC0C13DED29109F8CC1C0D2CCE52ECB1BD01939EF774FE31014E0F4
SHA-512:	22E29A06F19E2DA941A707B8DA7115E0F5962617295CC36395A8E9B2A98F0239B6519B4BF4AB1DC671DEF8CD558E8F59F4E50C63130D392D1E085BBF6B710914
Malicious:	false

C:\Users\user\AppData\Local\mJLa\DevicePairingWizard.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%...a...a...a...h...o.....b.....r.....i.....j...a.....c.....j.`.....`...Richa..... .....PE..d...x.1".....".....\.....b.....@.....H...`..... .....|..T.....`r.....`s..8 .....text....[.....\..... ..`.rdata...-...p.....`.....@..@.data... .....@....pdata.....@..@.rsrc.....@..@.re loc.....f.....@..B..... .....

C:\Users\user\AppData\Local\mJLa\MFC42u.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1265664
Entropy (8bit):	5.5179792497477465
Encrypted:	false
SSDEEP:	12288:0VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1hBB:xfP7fWsK5z9A+WGAW+V5SB6Ct4bnb7
MD5:	ACAA18F0CA1472EBA6752C43A76F63D4
SHA1:	1BD14A5CB0788853667F25EE5DC84DBABFB1E69A
SHA-256:	7BBCEA1DD21373D8A86FD2A6048971967CA3E410A7D5799222474DF7A97D66AB
SHA-512:	FA56F548843551898F932B285D83ED3238138F246E0FA642EC6719C5886DDF4B71A1D65A04707EA0301B767543CB8C8EA3DAA478C98D4039B5FAB35183B0E57B
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.(..DN^....." .....0.....p.....@.....P.....@\|x}..b.....\|...c.....h.....$#..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\pZCYq8TUy\credui.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1241088
Entropy (8bit):	5.497178010630534
Encrypted:	false
SSDEEP:	12288:kVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:BfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	092BC1900DB5A3970E41A4A850EC783E
SHA1:	D89437CB8A48260E34A0D0C44768F7662CAEB2F4
SHA-256:	F151BAEF206217841A78357977495815717409F349365DB9FFD4DB6166E83CDD
SHA-512:	414B9DFE04E94B275A48EFE03DA688A0AAF80B0DFF9B461A29C92E4D8E5799371A937F5B13F520B16ABD465E29F1D38713DB1C825F4BB282CC9BAF1868C6F51 B
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.(..DN^....." .....p.....@.....@\|x}..b.....c.....h.....$#..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\pZCYq8TUy\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:	043870DBAB955C1851E1710D9414953573 83A08F3F30DD3E3A1945583A85E0CA
SHA-512:	349459CCF4DDFB0B05B066869C99088BA3012930D5BBC3ED1C9E4CF6400687B1EFE698C5B1734BF6FF299F6C65DD7A71A2709D3773E9E96F6FDE659F5D883F4
Malicious:	false
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\Local\rm4w0\EaseOfAccessDialog.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	304640
Entropy (8bit):	6.843015704242449
Encrypted:	false
SSDEEP:	6144:E/Odkrq1AlGra6uFz2LJGRg4kLNnei36cw:As5+FCdUc
MD5:	F87F2E5EBF3FFBA39DF1621B5F8689B5
SHA1:	B4E358BF1BE0DF6D341CA1BC949867D94F13EC07
SHA-256:	06780477637707BEA6317AE81D059A4D75B101542ADFA6DC855287EAEDFC822A
SHA-512:	6E8D60C17396260791898A2914422AFFF2921A4C3D924F56C83ED117B683D3F3AEFB15E234600F3B5375A47C0C6A13F6160B0638CA91663D29DC56067EB5E5B7
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....)..8m..km..km..kd.Hki..k...jn..k...j{..k...j`..k...jv..km..k3..k...jx..k ..$kl..k...jl..kRichm..k.....PE..d...1.(i....."....@.....L}...`..... .....(0.,.....5.....X.....T..... .....text..... ..`.rdata.....@..@.data...0....p.....X.....@....pdata.....b.....@..@.rsrc....5.... ...6...l.....@..@.reloc..X.....@..B..... .....

C:\Users\user\AppData\Local\rm4w0\OLEACC.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1241088
Entropy (8bit):	5.496643926580779
Encrypted:	false
SSDEEP:	12288:QVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:VfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	D3FE50240DC0CB29FD1626AD60D27A33
SHA1:	4CDC09987F4ED88D1A133E384A150AA6B079A9A0
SHA-256:	7AEAAA41996A44EA2A028D695DF30580802B65D8D4B9A3FB26CAE91EFA00E3CF
SHA-512:	70903C4596F5AE1CE905E3CACCCAB75F82A5148766CD002ED4414C63179CDECB34898DF791FF439BB56F20571453057CCB443F93B19A9101D6E3C7FCF7C7905
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\sBx0fm\VERSION.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1241088
Entropy (8bit):	5.4946364596901
Encrypted:	false
SSDEEP:	12288:RVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:gfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	5361D083DFF1152C4481BAA13FFA6689
SHA1:	68DACC124F275798E5511A815304311F4CC17014
SHA-256:	67DB65C41FEFBE51F18ED9F1A8C6BC09BDEEE7D5507F82446CFA5B7EB8E83F8F
SHA-512:	D500FB3985B472D0AC44A1E78D855FD52CBD5607063D5D451F3DEBA1B6D26FA486B90289E71847D0E3E6F1ECBFD374740656FF3DFB94765FCD092EE0CB64FC 5
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\sBx0fm\psr.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	600576

C:\Users\user\AppData\Local\sBx0fm\psr.exe	
Entropy (8bit):	6.4861677167766665
Encrypted:	false
SSDEEP:	12288:B2mS50ICmAX+ASa8wd9Nkmw6cD8pellpco//EH1:B2mlmeFSa8wd9NStApeCoXEH
MD5:	3B8262EB45E790BF7FA648CEE2CCCB7B
SHA1:	EDDD81D1B3FD2EE99E42A43B25BD74D39BB850BC
SHA-256:	D1225E9FD2834BD2EF84EADAA4126020D20F4A0F50321440190C3896E69BD5D8
SHA-512:	A3709D39372CDB6D9C9E58932144CE8BA437C2134EFC9BCD2531708C1515CBAEA5929C220DF25D76785F7594BC5F8541E6ED5330EA3CA12E87C4DA5A2171C45
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....}.....x.....x.....x.....x...x.....x.....xR.....x.....Rich..... ....PE..d....S.....".....`.....@.....h....`..... .....7.,.....L.....D.....T..... .....X...8....7..@. .....text...5..... ..`.rdata.....@..@.data....m...`.....H.....@....pdata..L.....T.....@..@.didat.....j.....@....rsrc..... .....I.....@..@.reloc..D.....&.....@..B.....

C:\Users\user\AppData\Local\xlPP\wer.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1245184
Entropy (8bit):	5.502578344059862
Encrypted:	false
SSDEEP:	12288:8VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:JfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	9E94BC8A0688A10E6CEA3FD9A924C09E
SHA1:	11342B809DF3914361510FE0FE1734804CA268DB
SHA-256:	7984FB0BE2E6A704A2C2299A0519AA14A3CB475B95DEC8C836D054FB8783984A
SHA-512:	0A8BED06C8D8C732AF3639D5261BDDF96895521BA7C2A523B4F7377FA53CE94DF06F2AAD9B47E1B0619A320462BD487DFC32194869E72E0F81FBE822690129D
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.(..DN^.....".....p.....@.....@\|x}..b.....W....c.....h.....$#..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\xlPP\wermgr.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	209312
Entropy (8bit):	6.796289498157116
Encrypted:	false
SSDEEP:	6144:swTMBboFMSuc/9NPXWPJROo/wVJyB60OHyLC7vs:swTMB02SD/mXO64c2Hyw
MD5:	FF214585BF10206E21EA8EBA202FACFD
SHA1:	1ED4AE92D235497F62610078D51105C4634AFADE
SHA-256:	C48C430EB07ACC2FF8BDDD6057F5C9F72C2E83F67478F1E4A1792AF866711538
SHA-512:	24073F60B886C58F227769B2DD7D1439DF841784E43E753265DA761801FDA58FBEEDAC4A642E0A6ABDA40A6263153FAA1A9540DF6D35E38BF0EE5327EA55B4FE
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....(j.Jl..jl..jl..c1...l...-..il...-..ql..jl...H...-..mI...-..`I...-..KI...-..kI...-..kI..Rich jl.....PE..d...p.....".....,.....`(.....@.....p.....`..... ... ..0:.....I...`..\...@...T.....`Q.....`R.. ...t.....text...++.....,..... ..`.imrsiv.....@.....rdata.....P.....0.....@..@.data...X.....@....pdata.....@. .@.didat..@.....@....rsrc...0:... ...<.....@..@.reloc..\....`.....@..B.....

C:\Users\user\AppData\Local\zLYZkwYH\RdpSa.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	43008
Entropy (8bit):	5.898730459072675
Encrypted:	false
SSDEEP:	768:2nweYBCOBU+khtTMstnGUEqbfynaDWVVVFZ5i7t4AYRyF:TiaU+1qDya6VV7Z5SudyF
MD5:	0795B6F790F8E52D55F39E593E9C5BBA
SHA1:	6A9991A1762AAC176E3F47AB210CC121E038E4F9

C:\Users\user\AppData\Local\zLYZkwYH\RdpSa.exe	
SHA-256:	DF5B698983C3F08265F2FB0B74046CD7E68568190F329C8331CCA4761256D33B
SHA-512:	72D332EBDD1B9B40E18F565DACC200E5B710A91D803D536A0CF127C74622EED12A5EC855B9040F4A1FA8A44584E4E97E7E6C490B88DB3BDAFE61EA3FBF26AE59
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....-.G.i.).i.).i.).`..o.)...*.k.)...-.}.)....,j.)...(.|.).i.(..)... .}.).....h.)...+.h.).Richi.)..... .....PE..d.....".....j...@.....q.....@.....|.....`..... .....<.....@...T.....@..... .....@.....text....h.....j..... ..`.rdata..n'.....(...n.....@..@.data.....@....pdata..<.....@..@.rsrc..... .....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\zLYZkwYH\WINSTA.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1245184
Entropy (8bit):	5.512898849354316
Encrypted:	false
SSDEEP:	12288:4VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:tfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	4CD034EF892E4ACE84DE2EDF40C5C4F8
SHA1:	6DC79223A1CBE044E2E4071A301980B19FA3C9BC
SHA-256:	3C508E30EA6B7182E35ADCBC610F7B434B658859871082F4E63F56E7F1A44E2F
SHA-512:	5D7955CBFC760BA57987ABD973CFCED4C8EFE48BD753A25357285041AEF3D4CA2159407BFAB63CE291BFBC791A098CE903E440DE39AC44822C2A5FD41D3AD0A
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.(..DN^....." .....p.....@.....@\|x}..b.....m....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#.... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\eb42b1a5c308fc11edf1ddbdd25c8486_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	4462
Entropy (8bit):	5.486322521408924
Encrypted:	false
SSDEEP:	48:eBYynUf3KN7ms4dD24d7eDM36jhJQM4BYynU2QMR6CTj5iJWo49pYCUzMmKpH1:eusI3KN2D24ZeDkiwus3/R6WwIo6vo8V
MD5:	E6110DEC2D5794F12E28864B52AA17DF
SHA1:	35BB21C92A1977140B7EC8A0F80AC6FD1947B230
SHA-256:	48CEBC917B864CB68722E1960DDB91D86D4BBAB294CC735FD1FB834B5759E03E
SHA-512:	4E24FF2F1DAEF75435B1BF9F9D3EC1E3B2BFD1FAA4C2C2811FF518E5FA531235F07E47281A33A6D75FB363AF4A0221E512FE9CD565402FEFF1DFC1ED529D1625
Malicious:	false
Preview:	.....user.....user.....RSA1.....mL..\...m.k.N..2.....,y$}=...S.....Z.D\...CM.]..."[.....b.0Rt.>.`.u..N.n..dK...K&...{..>.{B...^.....h?.R}.....z..O.....!p..N...<..8.....,...C.r.y.p.t.o.A.P.I. .P.r.i.v.a.t.e. .K.e.y.....f..... .....?.o..t8.....U..dh..8.I..`l..... ...$.B....u?...I.c...x.N.s..t....I.....7.L.....A...*.>r.....;.a..... #b9|T*f(..'...|.^?..r..o..:~eM.....x.....Y..:.P.;w\..h...[.....{...~<lB.Yb...-.....D...D.n..t..~...u..0....p...~.}.r..b5..v.zW..3.A..5_#;..]Sg...D8.....V"{:i.,...P..Z....$..X.*.x...V.d.)...M.~I.',..s.%.....r.).....:...J.....P..0fa.....ySA}...HF(.i.C.@^@U.s0.E... .....D...G...j..l.:.hT....;.f,....(....].\...IBU..oq...XM.3.].h.....eg.:.o1.T...R...$%.?s.K.n/.....K..8.....7...`...{.a...RC[.....3..u.m...b..@..J..yq2.K..f....^....q..NNV#.9..G#.M

Static File Info

General

File type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Entropy (8bit):	5.507980268942348
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%

General

File name:	DC2zX44MQr.dll
File size:	1236992
MD5:	94f8317b419e9476120b14a29d9b05d2
SHA1:	f2b03dd4441f3808468bdbb8b26273cfb41b5298
SHA256:	2f10b593a5e04506d8050ebe39e28619199958a4f4bae0b9f3a1ee2af3d74862
SHA512:	73edd03df050bf72249dafdc8e0c71884d236e713b871c5e8ce9c825937ba1c8447ae791e39400a1d7b5af77aa5ec5d01b6db356003e9616ed7d24e7f78b24a3
SSDEEP:	12288:+VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:jfP7fWsK5z9A+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
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	0x64fcb	0x65000	False	0.702262047494	data	7.86510283498	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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.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
.wnx	0x10e000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.weqy	0x10f000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.yby	0x110000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ormx	0x112000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.dhclu	0x113000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.xmiul	0x114000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tlwcxe	0x115000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.get	0x116000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.hzrd	0x117000	0x1124	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.qzu	0x119000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.nhglos	0x11a000	0x1af	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.itzo	0x11b000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.nmsaom	0x11c000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rvhi	0x11d000	0x1af	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ucrzce	0x11e000	0x389	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ijc	0x11f000	0xbf6	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ohvs	0x120000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rlvrc	0x121000	0x1ee	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.yjv	0x122000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.clbcyy	0x123000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.xcyn	0x124000	0x8fe	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
.boqx	0x125000	0x389	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rnlia	0x126000	0x389	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ctip	0x127000	0x5a7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.fkv	0x128000	0x1124	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pczrv	0x12a000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ibglr	0x12b000	0x3fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.uirkq	0x12c000	0x3ba	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.xmo	0x12d000	0x1af	0x1000	False	0.070068359375	data	0.884469413236	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: 6552 Parent PID: 4924

General

Start time:	19:14:06
Start date:	28/09/2021
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe 'C:\Users\user\Desktop\DC2zX44MQr.dll'
Imagebase:	0x7ff7eaf80000
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: 00000000.00000002.272674434.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6576 Parent PID: 6552

General

Start time:	19:14:06
Start date:	28/09/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\DC2zX44MQr.dll',#1
Imagebase:	0x7ff7bf140000
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: 6584 Parent PID: 6552

General

Start time:	19:14:07
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\DC2zX44MQr.dll,DisplaySYSDMCPL
Imagebase:	0x7ff775bc0000

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: 00000002.00000002.330302590.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 6600 Parent PID: 6576

General

Start time:	19:14:07
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe 'C:\Users\user\Desktop\DC2zX44MQr.dll',#1
Imagebase:	0x7ff775bc0000
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: 00000003.00000002.252587929.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3292 Parent PID: 6584

General

Start time:	19:14:08
Start date:	28/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff662bf0000
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: 6676 Parent PID: 6552

General

Start time:	19:14:10
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\DC2zX44MQr.dll,EditEnvironmentVariables
Imagebase:	0x7ff775bc0000
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: 00000006.00000002.258809816.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities — Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 6808 Parent PID: 6552

General

Start time:	19:14:14
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\DC2zX44MQr.dll,EditUserProfiles
Imagebase:	0x7ff775bc0000
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: 00000008.00000002.266253941.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities — Show Windows behavior

File Read

Analysis Process: DmNotificationBroker.exe PID: 3476 Parent PID: 3292

General

Start time:	19:14:46
Start date:	28/09/2021
Path:	C:\Windows\System32\DmNotificationBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\DmNotificationBroker.exe
Imagebase:	0x7ff67baa0000
File size:	32256 bytes
MD5 hash:	1643D5735213BC89C0012F0E48253765
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: DmNotificationBroker.exe PID: 6464 Parent PID: 3292

General

Start time:	19:14:51
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\EwdQnyo\DmNotificationBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\EwdQnyo\DmNotificationBroker.exe
Imagebase:	0x7ff686900000
File size:	32256 bytes
MD5 hash:	1643D5735213BC89C0012F0E48253765
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: 00000013.00000002.366691390.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: RdpSa.exe PID: 4488 Parent PID: 3292

General

Start time:	19:15:03
Start date:	28/09/2021
Path:	C:\Windows\System32\RdpSa.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\RdpSa.exe
Imagebase:	0x7ff794d50000
File size:	43008 bytes
MD5 hash:	0795B6F790F8E52D55F39E593E9C5BBA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: RdpSa.exe PID: 2152 Parent PID: 3292

General

Start time:	19:15:03
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\zLYZkwYH\RdpSa.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\zLYZkwYH\RdpSa.exe
Imagebase:	0x7ff644d50000
File size:	43008 bytes
MD5 hash:	0795B6F790F8E52D55F39E593E9C5BBA
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: 00000019.00000002.393120079.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Read

Analysis Process: Utilman.exe PID: 2884 Parent PID: 3292

General

Start time:	19:15:16
Start date:	28/09/2021
Path:	C:\Windows\System32\Utilman.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\Utilman.exe
Imagebase:	0x7ff728540000
File size:	98304 bytes
MD5 hash:	C91CCEF3884CFDE746B4BAEF5F1BC75C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: Utilman.exe PID: 3596 Parent PID: 3292

General

Start time:	19:15:20
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\KbLvcSLVf\Utilman.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\KbLvcSLVf\Utilman.exe
Imagebase:	0x7ff719840000
File size:	98304 bytes
MD5 hash:	C91CCEF3884CFDE746B4BAEF5F1BC75C
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: 0000001C.00000002.429090698.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

File Activities

Show Windows behavior

File Read

Analysis Process: EaseOfAccessDialog.exe PID: 6104 Parent PID: 3292

General

Start time:	19:15:34
Start date:	28/09/2021
Path:	C:\Windows\System32\EaseOfAccessDialog.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\EaseOfAccessDialog.exe
Imagebase:	0x7ff6cc0e0000
File size:	304640 bytes
MD5 hash:	F87F2E5EBF3FFBA39DF1621B5F8689B5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: EaseOfAccessDialog.exe PID: 6128 Parent PID: 3292

General

Start time:	19:15:34
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\rm4w0\EaseOfAccessDialog.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\rm4w0\EaseOfAccessDialog.exe
Imagebase:	0x7ff792c30000
File size:	304640 bytes
MD5 hash:	F87F2E5EBF3FFBA39DF1621B5F8689B5
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: 00000021.00000002.459149344.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Read

Analysis Process: DevicePairingWizard.exe PID: 5024 Parent PID: 3292

General

Start time:	19:15:46
Start date:	28/09/2021
Path:	C:\Windows\System32\DevicePairingWizard.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\DevicePairingWizard.exe
Imagebase:	0x7ff74a2d0000
File size:	92160 bytes
MD5 hash:	E23643C785D498FF73B5C9D7EA173C3D
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language

Analysis Process: DevicePairingWizard.exe PID: 4804 Parent PID: 3292

General

Start time:	19:15:52
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\mJLa\DevicePairingWizard.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\mJLa\DevicePairingWizard.exe
Imagebase:	0x7ff6cb020000
File size:	92160 bytes
MD5 hash:	E23643C785D498FF73B5C9D7EA173C3D
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: 00000023.00000002.498301124.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: wermgr.exe PID: 4896 Parent PID: 3292

General

Start time:	19:16:04
Start date:	28/09/2021
Path:	C:\Windows\System32\wermgr.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wermgr.exe
Imagebase:	0x7ff62a2c0000
File size:	209312 bytes
MD5 hash:	FF214585BF10206E21EA8EBA202FACFD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: wermgr.exe PID: 5600 Parent PID: 3292

General

Start time:	19:16:05
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\xlPP\wermgr.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\xlPP\wermgr.exe
Imagebase:	0x7ff776fa0000
File size:	209312 bytes
MD5 hash:	FF214585BF10206E21EA8EBA202FACFD
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: 00000026.00000002.525725102.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: mstsc.exe PID: 6664 Parent PID: 3292

General

Start time:	19:16:17
Start date:	28/09/2021
Path:	C:\Windows\System32\mstsc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\mstsc.exe
Imagebase:	0x7ff7f3970000
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: 6636 Parent PID: 3292

General

Start time:	19:16:18
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\pZCYq8TUy\mstsc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\pZCYq8TUy\mstsc.exe
Imagebase:	0x7ff7a40d0000
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: 00000028.00000002.555665664.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Disassembly

Code Analysis