

JOeSandbox Cloud BASIC



ID: 595308

Sample Name: eWlldJYfLc

Cookbook: default.jbs

Time: 15:46:03

Date: 23/03/2022

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report eWldJYfLc	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Yara Signatures	5
Memory Dumps	5
Unpacked PEs	5
Sigma Signatures	5
System Summary	5
Joe Sandbox Signatures	5
AV Detection	5
Exploits	5
E-Banking Fraud	6
System Summary	6
HIPS / PFW / Operating System Protection Evasion	6
Mitre Att&ck Matrix	6
Behavior Graph	7
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	9
Unpacked PE Files	9
Domains	10
URLs	10
Domains and IPs	10
Contacted Domains	10
URLs from Memory and Binaries	10
World Map of Contacted IPs	12
General Information	12
Warnings	13
Simulations	13
Behavior and APIs	13
Joe Sandbox View / Context	13
IPs	13
Domains	13
ASNs	14
JA3 Fingerprints	14
Dropped Files	14
Created / dropped Files	14
C:\Users\user\AppData\Local\409p1cGN\dxpsrvr.exe	14
C:\Users\user\AppData\Local\409p1cGN\dwmap.dll	14
C:\Users\user\AppData\Local\EQ0DjT2sP\CameraSettingsUIHost.exe	14
C:\Users\user\AppData\Local\EQ0DjT2sP\DU170.dll	15
C:\Users\user\AppData\Local\Nz4mnM\SndVol.exe	15
C:\Users\user\AppData\Local\Nz4mnM\UxTheme.dll	15
C:\Users\user\AppData\Local\O0z6Mm4\XmLite.dll	16
C:\Users\user\AppData\Local\O0z6Mm4\ddodiag.exe	16
C:\Users\user\AppData\Local\R7Mg9\CloudNotifications.exe	17
C:\Users\user\AppData\Local\R7Mg9\UxTheme.dll	17
C:\Users\user\AppData\Local\ajcBg\DeviceEnroller.exe	17
C:\Users\user\AppData\Local\ajcBg\XmLite.dll	18
C:\Users\user\AppData\Local\bj1HT\MFPlat.DLL	18
C:\Users\user\AppData\Local\bj1HT\mfpmmp.exe	18
C:\Users\user\AppData\Local\n0R5g\Secur32.dll	18
C:\Users\user\AppData\Local\n0R5g\mstsc.exe	19
C:\Users\user\AppData\Local\wFRJtv0CU\ACTIVEDS.dll	19
C:\Users\user\AppData\Local\wFRJtv0CU\SppExtComObj.Exe	19
C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\414045e2d09286d5db2581e0d955d358_d06ed635-68f6-4e9a-955c-4899f5f57b9a	20
Static File Info	20
General	20
File Icon	20
Static PE Info	21
General	21
Entrypoint Preview	21
Data Directories	22
Sections	23
Resources	25

Imports	25
Exports	25
Version Infos	26
Possible Origin	27
Network Behavior	27
Statistics	27
Behavior	27
System Behavior	27
Analysis Process: loadll64.exePID: 7088, Parent PID: 668	27
General	27
File Activities	28
Analysis Process: cmd.exePID: 7112, Parent PID: 7088	28
General	28
File Activities	28
Analysis Process: rundll32.exePID: 7120, Parent PID: 7088	28
General	28
File Activities	29
File Read	29
Analysis Process: rundll32.exePID: 7132, Parent PID: 7112	29
General	29
File Activities	29
File Read	29
Analysis Process: explorer.exePID: 3968, Parent PID: 7120	29
General	29
File Activities	29
File Created	29
File Deleted	31
File Written	32
File Read	40
Registry Activities	42
Key Created	42
Key Value Created	43
Analysis Process: rundll32.exePID: 5384, Parent PID: 7088	46
General	46
File Activities	46
File Read	46
Analysis Process: rundll32.exePID: 3156, Parent PID: 7088	46
General	46
File Activities	47
File Read	47
Analysis Process: svchost.exePID: 5604, Parent PID: 568	47
General	47
Analysis Process: sdclt.exePID: 3960, Parent PID: 3968	47
General	47
Analysis Process: CloudNotifications.exePID: 5876, Parent PID: 3968	47
General	47
Analysis Process: CloudNotifications.exePID: 2928, Parent PID: 3968	48
General	48
File Activities	48
File Read	48
Analysis Process: systemreset.exePID: 6544, Parent PID: 3968	48
General	48
Analysis Process: Dxpserver.exePID: 3500, Parent PID: 3968	48
General	48
Analysis Process: Dxpserver.exePID: 1740, Parent PID: 3968	49
General	49
File Activities	49
File Read	49
Analysis Process: mfpmp.exePID: 5604, Parent PID: 3968	49
General	49
Analysis Process: mfpmp.exePID: 3464, Parent PID: 3968	49
General	49
File Activities	50
File Read	50
Analysis Process: msra.exePID: 1908, Parent PID: 3968	50
General	50
Analysis Process: mstsc.exePID: 7132, Parent PID: 3968	50
General	50
Analysis Process: mstsc.exePID: 3176, Parent PID: 3968	50
General	50
Analysis Process: SndVol.exePID: 5936, Parent PID: 3968	51
General	51
Analysis Process: SndVol.exePID: 5900, Parent PID: 3968	51
General	51
Disassembly	51

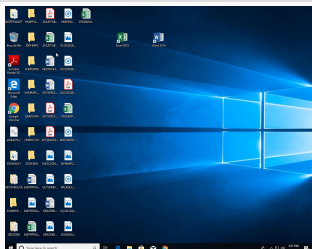
Windows Analysis Report

eWlldJYfLc

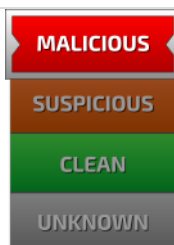
Overview

General Information

Sample Name:	eWldJyflC (renamed file extension from none to dll)
Analysis ID:	595308
MD5:	d098d01cbea52f..
SHA1:	952ce9cd899108..
SHA256:	82c89b2a758177..
Tags:	Dridex exe
Infos:	      



Detection



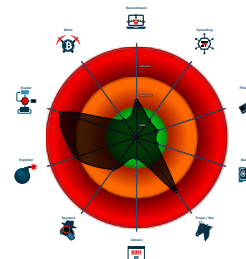
Dridex

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 foreign...
- Machine Learning detection for sam...
- Sigma detected: Suspicious Svchos...
- Queues an APC in another process ...
- Sigma detected: Suspicious Call by...
- Machine Learning detection for drop...
- Accesses ntoskrnl, likely to find offs...

Classification



Process Tree

- System is w10x64
-  **loadll64.exe** (PID: 7088 cmdline: loadll64.exe "C:\Users\user\Desktop\WlIdJYflc.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
-  **cmd.exe** (PID: 7112 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\WlIdJYflc.dll",#1 MD5: 4E2AC4F48A396486AB4268C94A6A245F)
 -  **rundll32.exe** (PID: 7132 cmdline: rundll32.exe "C:\Users\user\Desktop\WlIdJYflc.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
-  **rundll32.exe** (PID: 7120 cmdline: rundll32.exe C:\Users\user\Desktop\WlIdJYflc.dll,IsInteractiveUserSession MD5: 73C519F050C20580F8A62C849D49215A)
 -  **explorer.exe** (PID: 3968 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C968AB0E1D)
 -  **svchost.exe** (PID: 5604 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
 -  **sdclt.exe** (PID: 3960 cmdline: C:\Windows\system32\sdclt.exe MD5: 0632A8402C6504CD541AC93676AAD0F5)
 -  **CloudNotifications.exe** (PID: 5876 cmdline: C:\Windows\system32\CloudNotifications.exe MD5: D9FF4C8DBC1682E0508322307CB89C0F)
 -  **CloudNotifications.exe** (PID: 2928 cmdline: C:\Users\user\AppData\Local\R7Mg9\CloudNotifications.exe MD5: D9FF4C8DBC1682E0508322307CB89C0F)
 -  **systemreset.exe** (PID: 6544 cmdline: C:\Windows\system32\systemreset.exe MD5: 872AE9FE08ED1AA78208678967BE2FEF)
 -  **Dxpserver.exe** (PID: 3500 cmdline: C:\Windows\system32\Dxpserver.exe MD5: DCCB1D350193BE0A26CEAFF602DB848E)
 -  **Dxpserver.exe** (PID: 1740 cmdline: C:\Users\user\AppData\Local\O9p1cGN\Dxpserver.exe MD5: DCCB1D350193BE0A26CEAFF602DB848E)
 -  **mfmpmp.exe** (PID: 5604 cmdline: C:\Windows\system32\mfmpmp.exe MD5: 7C3D09D6DB5D4A272FCF4C1BB3986BD)
 -  **mfmpmp.exe** (PID: 3464 cmdline: C:\Users\user\AppData\Local\bj1HT\mfmpmp.exe MD5: 7C3D09D6DB5D4A272FCF4C1BB3986BD)
 -  **msra.exe** (PID: 1908 cmdline: C:\Windows\system32\msra.exe MD5: 3240CC226FB8AC41A0431A8F3B9BD770)
 -  **mstsc.exe** (PID: 7132 cmdline: C:\Windows\system32\mstsc.exe MD5: 3FB85CD8829E9533D0FF5819DB0444C0)
 -  **mstsc.exe** (PID: 3176 cmdline: C:\Users\user\AppData\Local\In0R5\mstsc.exe MD5: 3FB85CD8829E9533D0FF5819DB0444C0)
 -  **SndVol.exe** (PID: 5936 cmdline: C:\Windows\system32\SndVol.exe MD5: CDD7C7DF2D0859AC3F4088423D11BD08)
 -  **SndVol.exe** (PID: 5900 cmdline: C:\Users\user\AppData\Local\Nz4mnM\SndVol.exe MD5: CDD7C7DF2D0859AC3F4088423D11BD08)
 -  **rundll32.exe** (PID: 5384 cmdline: rundll32.exe C:\Users\user\Desktop\WlIdJYflc.dll,QueryActiveSession MD5: 73C519F050C20580F8A62C849D49215A)
 -  **rundll32.exe** (PID: 3156 cmdline: rundll32.exe C:\Users\user\Desktop\WlIdJYflc.dll,QueryUserToken MD5: 73C519F050C20580F8A62C849D49215A)
 - cleanup

Malware Configuration

 No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.274772551.00007FFC670C1000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_Dride x_2	Yara detected Dridex unpacked file	Joe Security	
00000000.00000002.280898080.00007FFC670C1000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_Dride x_2	Yara detected Dridex unpacked file	Joe Security	
00000023.00000002.574221343.00007FFC74C21000.00000020.00000001.01000000.00000013.sdmp	JoeSecurity_Dride x_2	Yara detected Dridex unpacked file	Joe Security	
00000014.00000002.430869317.00007FFC74C21000.00000020.00000001.01000000.0000000A.sdmp	JoeSecurity_Dride x_2	Yara detected Dridex unpacked file	Joe Security	
00000002.00000002.382839680.00007FFC670C1000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_Dride x_2	Yara detected Dridex unpacked file	Joe Security	

Click to see the 5 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
33.2.mstsc.exe.7ffc74c20000.3.unpack	JoeSecurity_Dride x_2	Yara detected Dridex unpacked file	Joe Security	
35.2.SndVol.exe.7ffc74c20000.3.unpack	JoeSecurity_Dride x_2	Yara detected Dridex unpacked file	Joe Security	
20.2.CloudNotifications.exe.7ffc74c20000.3.unpack	JoeSecurity_Dride x_2	Yara detected Dridex unpacked file	Joe Security	
8.2.rundll32.exe.7ffc670c0000.2.unpack	JoeSecurity_Dride x_2	Yara detected Dridex unpacked file	Joe Security	
2.2.rundll32.exe.7ffc670c0000.2.unpack	JoeSecurity_Dride x_2	Yara detected Dridex unpacked file	Joe Security	

Click to see the 5 entries

Sigma Signatures

System Summary



Sigma detected: Suspicious Svchost Process

Sigma detected: Suspicious Call by Ordinal

Joe Sandbox Signatures

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

Exploits



Exploits



Accesses ntoskrnl, likely to find offsets for exploits

E-Banking Fraud



Yara detected Dridex unpacked file

System Summary



PE file contains section with special chars

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)

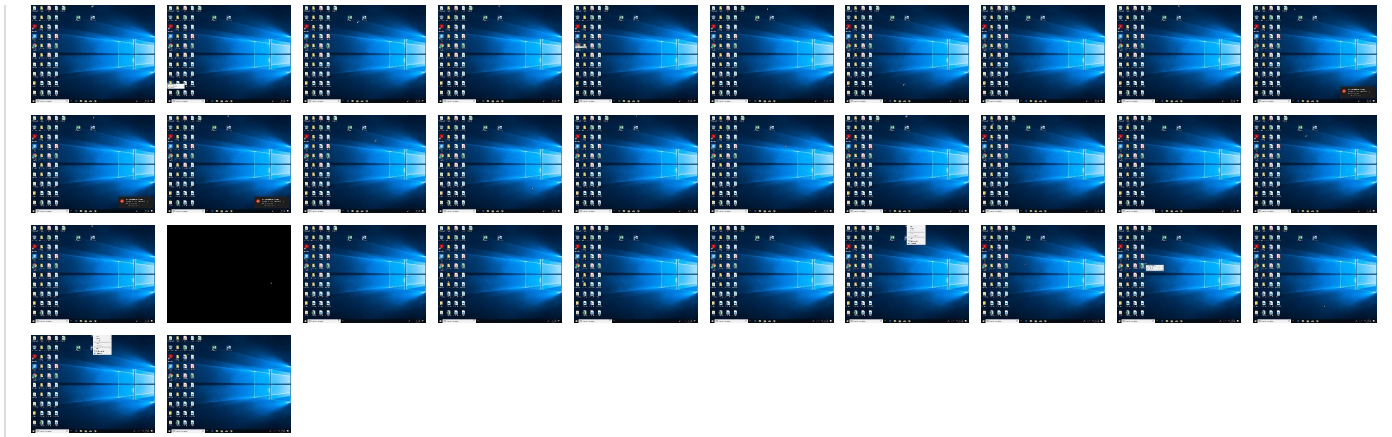
Contains functionality to automate explorer (e.g. start an application)

Contains functionality to prevent local Windows debugging

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	Remote Service Effects	Impact
Valid Accounts	2 Native API	1 DLL Side-Loading	1 Exploitation for Privilege Escalation	1 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Exploitation for Client Execution	Boot or Logon Initialization Scripts	4 1 2 Process Injection	1 Virtualization/Sandbox Evasion	LSASS Memory	2 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 DLL Side-Loading	4 1 2 Process Injection	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 Obfuscated Files or Information	NTDS	3 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Rundll32	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Software Packing	Cached Domain Credentials	1 Account Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Timestomp	DCSync	1 System Owner/User Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 DLL Side-Loading	Proc Filesystem	1 File and Directory Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue



Antivirus, Machine Learning and Genetic Malware Detection				
Initial Sample				
Source	Detection	Scanner	Label	Link
eWldJYfLc.dll	67%	Virustotal		Browse
eWldJYfLc.dll	60%	Metadefender		Browse
eWldJYfLc.dll	88%	ReversingLabs	Win64.Trojan.Occamy	

Source	Detection	Scanner	Label	Link
eWldJYfLc.dll	100%	Avira	TR/Crypt.ZPACK. Gen	
eWldJYfLc.dll	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\lvFRJtv0CU\ACTIVEDS.dll	100%	Avira	TR/Crypt.ZPACK. Gen	
C:\Users\user\AppData\Local\4O9p1cGN\dwmapl.dll	100%	Avira	TR/Crypt.XPACK. Gen7	
C:\Users\user\AppData\Local\Nz4mnMUxTheme.dll	100%	Avira	TR/Crypt.ZPACK. Gen	
C:\Users\user\AppData\Local\O0z6Mm4\XmlLite.dll	100%	Avira	TR/Crypt.XPACK. Gen7	
C:\Users\user\AppData\Local\O0z6Mm4\XmlLite.dll	100%	Avira	TR/Crypt.XPACK. Gen7	
C:\Users\user\AppData\Local\bj1HT\MFPlat.DLL	100%	Avira	TR/Crypt.XPACK. Gen7	
C:\Users\user\AppData\Local\EQ0DJT2sP\DIUI70.dll	100%	Avira	TR/Crypt.XPACK. Gen4	
C:\Users\user\AppData\Local\Nz4mnMUxTheme.dll	100%	Avira	TR/Crypt.ZPACK. Gen	
C:\Users\user\AppData\Local\n0R5g\Secur32.dll	100%	Avira	TR/Crypt.ZPACK. Gen	
C:\Users\user\AppData\Local\lvFRJtv0CU\ACTIVEDS.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\4O9p1cGN\dwmapl.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Nz4mnMUxTheme.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\O0z6Mm4\XmlLite.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\O0z6Mm4\XmlLite.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\bj1HT\MFPlat.DLL	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\EQ0DJT2sP\DIUI70.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Nz4mnMUxTheme.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\n0R5g\Secur32.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\4O9p1cGN\Dxpserver.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\4O9p1cGN\Dxpserver.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\EQ0DJT2sP\CameraSettingsUIHost.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\EQ0DJT2sP\CameraSettingsUIHost.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Nz4mnM\SndVol.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Nz4mnM\SndVol.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\O0z6Mm4\ddodiag.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\O0z6Mm4\ddodiag.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
33.2.mstsc.exe.7ffc74c20000.3.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
8.2.rundll32.exe.7ffc670c0000.2.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
20.2.CloudNotifications.exe.7ffc74c20000.3.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
35.2.SndVol.exe.7ffc74c20000.3.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
33.2.mstsc.exe.15f26e10000.0.unpack	100%	Avira	HEUR/AGEN.12 15493		Download File
29.2.mfmp.exe.1cdaa1c0000.0.unpack	100%	Avira	HEUR/AGEN.12 15493		Download File
0.2.loaddll64.exe.16b476e0000.0.unpack	100%	Avira	HEUR/AGEN.12 15493		Download File
26.2.Dxpserver.exe.7ffc74c20000.3.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
2.2.rundll32.exe.7ffc670c0000.2.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
26.2.Dxpserver.exe.19273270000.0.unpack	100%	Avira	HEUR/AGEN.12 15493		Download File

Source	Detection	Scanner	Label	Link	Download
29.2.mfmp.exe.7ffc74c20000.3.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
6.2.rundll32.exe.7ffc670c0000.2.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
6.2.rundll32.exe.28586ab0000.0.unpack	100%	Avira	HEUR/AGEN.12 15493		Download File
20.2.CloudNotifications.exe.2953cdf0000.1.unpack	100%	Avira	HEUR/AGEN.12 15493		Download File
8.2.rundll32.exe.2541e150000.0.unpack	100%	Avira	HEUR/AGEN.12 15493		Download File
2.2.rundll32.exe.16bb42f0000.0.unpack	100%	Avira	HEUR/AGEN.12 15493		Download File
3.2.rundll32.exe.17f7c0b0000.0.unpack	100%	Avira	HEUR/AGEN.12 15493		Download File
0.2.loadall64.exe.7ffc670c0000.2.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File
35.2.SndVol.exe.1c1733a0000.0.unpack	100%	Avira	HEUR/AGEN.12 15493		Download File
3.2.rundll32.exe.7ffc670c0000.2.unpack	100%	Avira	TR/Crypt.XPAC K.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://schemas.mi	0%	URL Reputation	safe	
http://https://login.windows.net-%s	0%	Avira URL Cloud	safe	
http://schemas.micr	0%	URL Reputation	safe	
http://https://dynamic.t	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dynamic.t0.tiles.ditu.live.com/comp/gen.ashx	svchost.exe, 0000000B.00000003.320641560 .000001BB8E651000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://schemas.mi	explorer.exe, 00000004.00000000.32443615 8.000000000DA7E000.00000004.00000001.000 20000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://login.windows.net-%s	DeviceEnroller.exe.4.dr	false	Avira URL Cloud: safe	low
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdv ?pv=1&r=	svchost.exe, 0000000B.00000003.320980194 .000001BB8E646000.00000004.00000020.0002 0000.00000000.sdmp, svchost.exe, 0000000 B.00000003.320872446.000001BB8E641000.00 000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Routes/	svchost.exe, 0000000B.00000002.321807705 .000001BB8E63E000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Driving	svchost.exe, 0000000B.00000003.320641560 .000001BB8E651000.00000004.00000020.0002 0000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/comp/gen .ashx	svchost.exe, 0000000B.00000002.321807705 .000001BB8E63E000.00000004.00000020.0002 0000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://dev.ditu.live.com/REST/v1/Traffic/Incidents/	svchost.exe, 0000000B.00000002.321834175.000001BB8E64C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.320766530.000001BB8E64A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Transit/Stops/	svchost.exe, 0000000B.00000003.320495277.000001BB8E669000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.321905396.000001BB8E66B000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.tiles.ditu.live.com/tiles/gen	svchost.exe, 0000000B.00000002.321768696.000001BB8E629000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/	svchost.exe, 0000000B.00000002.321807705.000001BB8E63E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Traffic/Incidents/	svchost.exe, 0000000B.00000002.321768696.000001BB8E629000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gdi?pv=1&r=	svchost.exe, 0000000B.00000003.298657798.000001BB8E630000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Routes/Walking	svchost.exe, 0000000B.00000003.320641560.000001BB8E651000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Transit/Stops/	svchost.exe, 0000000B.00000003.298657798.000001BB8E630000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?	svchost.exe, 0000000B.00000002.321834175.000001BB8E64C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.320766530.000001BB8E64A000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.320872446.000001BB8E641000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gd?pv=1&r=	svchost.exe, 0000000B.00000002.321807705.000001BB8E63E000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.321751772.000001BB8E613000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/HumanScaleServices/GetBubbles.ashx?n=	svchost.exe, 0000000B.00000002.321820678.000001BB8E643000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.321051969.000001BB8E642000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.320872446.000001BB8E641000.00000004.00000020.00020000.00000000.sdmp	false		high
http://schemas.micr	explorer.exe, 00000004.00000000.324436158.000000000DA7E000.00000004.00000001.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://dev.ditu.live.com/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000000B.00000002.321768696.000001BB8E629000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Locations	svchost.exe, 0000000B.00000003.298657798.000001BB8E630000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.320641560.000001BB8E651000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/mapcontrol/mapconfiguration.ashx?name=native&v=	svchost.exe, 0000000B.00000003.298657798.000001BB8E630000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/mapcontrol/logging.ashx	svchost.exe, 0000000B.00000003.320641560.000001BB8E651000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/mapcontrol/logging.ashx	svchost.exe, 0000000B.00000003.320641560.000001BB8E651000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Imagery/Copyright/	svchost.exe, 0000000B.00000002.321768696.000001BB8E629000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.320766530.000001BB8E64A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/webservices/v1/LoggingService/LoggingService.svc/Log?entry=	svchost.exe, 0000000B.00000003.298657798.000001BB8E630000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://t0.ssl.ak.dynamic.tiles.virtualearth.net/odvs/gri?pv=1&r=	svchost.exe, 0000000B.00000003.298657798.000001BB8E630000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdi?pv=1&r=	svchost.exe, 0000000B.00000002.321834175.000001BB8E64C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.320766530.000001BB8E64A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000B.00000002.321834175.000001BB8E64C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.320766530.000001BB8E64A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Transit/Schedules/	svchost.exe, 0000000B.00000002.321820678.000001BB8E643000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.321051969.000001BB8E642000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.320872446.000001BB8E641000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.t	svchost.exe, 0000000B.00000003.320872446.000001BB8E641000.00000004.00000020.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://dev.virtualearth.net/REST/v1/Routes/Transit	svchost.exe, 0000000B.00000003.320641560.000001BB8E651000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://t0.ssl.ak.tiles.virtualearth.net/tiles/gen	svchost.exe, 0000000B.00000003.298657798.000001BB8E630000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.321244735.000001BB8E63A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gdv?pv=1&r=	svchost.exe, 0000000B.00000002.321834175.000001BB8E64C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.320766530.000001BB8E64A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/mapcontrol/roadshield.ashx?bucket=	svchost.exe, 0000000B.00000003.298657798.000001BB8E630000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.bingmapsportal.com	svchost.exe, 0000000B.00000002.321751772.000001BB8E613000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/Locations	svchost.exe, 0000000B.00000003.320641560.000001BB8E651000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 0000000B.00000002.321768696.000001BB8E629000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.298657798.000001BB8E630000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://ecn.dev.virtualearth.net/REST/v1/Imagery/Copyright/	svchost.exe, 0000000B.00000003.298657798.000001BB8E630000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000002.321807705.000001BB8E63E000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dev.ditu.live.com/REST/v1/JsonFilter/VenueMaps/data/	svchost.exe, 0000000B.00000002.321834175.000001BB8E64C000.00000004.00000020.00020000.00000000.sdmp, svchost.exe, 0000000B.00000003.320766530.000001BB8E64A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://dynamic.api.tiles.ditu.live.com/odvs/gd?pv=1&r=	svchost.exe, 0000000B.00000003.320766530.000001BB8E64A000.00000004.00000020.00020000.00000000.sdmp	false		high

World Map of Contacted IPs
No contacted IP infos

General Information	
Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	595308

Start date and time:	2022-03-23 14:46:03 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	eWldJYfLc (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:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winDLL@46/19@0/0
EGA Information:	• Successful, ratio: 90%
HDC Information:	• Successful, ratio: 29% (good quality ratio 17.8%) • Quality average: 41% • Quality standard deviation: 39%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, www.bing.com, client.wns.windows.com, fs.microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com, arc.msn.com
- Execution Graph export aborted for target mfpmp.exe, PID 3464 because there are no executed function
- Not all processes were analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtEnumerateKey calls found.

Simulations

Behavior and APIs

 No simulations

Joe Sandbox View / Context

IPs

 No context

Domains

 No context

ASNs
 No context

JA3 Fingerprints
 No context

Dropped Files
 No context

Created / dropped Files	
C:\Users\user\AppData\Local\409p1cGN\Dxpserver.exe 	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	304640
Entropy (8bit):	5.920357039114308
Encrypted:	false
SSDEEP:	6144:SidsFxbUPoT/FPriCEe+oiXoGJm7JwQ9oWxDEHZwj:xaFxbFDBsBo6maPWxDcwj
MD5:	DCCB1D350193BE0A26CEAFF602DB848E
SHA1:	02673E7070A589B5BF6F217558A06067B388A350
SHA-256:	367CEA47389B6D5211595AE88454D9589AA8C996F5E765904FFEDE434424AF22
SHA-512:	ECD3C32E2BED31FC6328CA4B171B5D2503A2795324667F67FF48A67DF7C8B88760A62C0119A173487B9886E6AF3994025A85E42B064BEA38A466A6848AF65541
Malicious:	false
Antivirus:	- Antivirus: Metadefender, Detection: 0%, Browse - Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....9. E}.N}.N}.N...M..~.N...J.d.N...K.{N...O.X.N}.O.F.N...G.[N....].N... .L .N.Rich}.N.....PE..d...z....."......`.....@.....`.....0..H.....p...`..T.....<..... .....=.....text...<.....`..rdata..6.....@..@.data.....@...pdata.....@...@.rsrc...H...0..... ...@...@.reloc..p.....@..B.....

C:\Users\user\AppData\Local\409p1cGN\dwmapl.dll  	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1372160
Entropy (8bit):	5.073965259759853
Encrypted:	false
SSDEEP:	12288:vZgJtlQepQn+NDo7nlYegQCLDF/B9wvj/cLvVZFuw:vZK6F7n5eRmDFJivohZVF
MD5:	76657995BEE544EFB7B57F3ADE10CACC
SHA1:	AFD9BC6AAEF6E67ABEB32C4111B61F39412D8DCA
SHA-256:	E4FAF63C9DF8C711816BDD85DED07539FC7F425EFFBAFDD680EFE01E45DCD26
SHA-512:	BEF755E7AE0D4C82D7F0A86A881FBDAFC565C990C821EBA88B1D5C208B1A94097E3BC74A9AFA58B11146658CC68CECE1F615E28FC891852FB99FA4D703829670
Malicious:	true
Antivirus:	- Antivirus: Avira, Detection: 100% - Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....X..Z.qb..qb.a...jqb.s...qb.9...qb.s...(qb.....qb.#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb..(c..qb.;...qb../.Tqb.....Zqb.....qb.z.. ..Bqb.....nqb.....[qb.....qb.;...{qb.....qb..#...qb...f.oqb...hqb.z...qb.....qb.;...tqb.Rich.qb.....PE..d=...}^....."\$.....@.....`.....&...\$..<.....0..(.....text..... .. .....@.....`..rdata..Co...0...p...0...0..@Co.....@..@.data.....;.....@.....@.....@.....@.....pdata..8.....@8.....@...@.rsrc.....@.....@...@.reloc..1.....@1.....@..B.vxl.....@.....@..@..@.qwubgr.\$...0... ..0...0..@\$.....@..@.eer...

C:\Users\user\AppData\Local\EQ0DJT2sP\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:HYxSW1tZfJtM2mpgc8WtCpZswKro1PDg:HhAhty8WteuwKrwPDg
MD5:	34F32BC06CDC7AF56607D351B155140D
SHA1:	88EF25BC91BCC908AF743ECA254D6251E5564283
SHA-256:	47238D9ED75D01FD125AC76B500FEEF7F8B27255570AD02D18A4F049B05DF3BD
SHA-512:	D855414779125F4E311ACF4D5EFC8ACA4452323CABD1694798CA90FD5BD76DC70B5D06790A2AE311E7DD19190DCCB134F6EF96AB1B7CF5B8A40AD642B72D544
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...Y.N.....".....*...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\EQ0DjTzSP\DUI70.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1654784
Entropy (8bit):	5.506546408859127
Encrypted:	false
SSDEEP:	12288:tZgJtlQepQn+NDo7nlYegQCLDF/B9wvj/cLvVZFuwmsNRt:tZK6F7n5eRmDFJivohZFVmu
MD5:	72722E89BA0B4F6CAD054811AB8BB33C
SHA1:	84099E5B7CF14C99D301AADAD9934E8981C019EB
SHA-256:	27DBA4A57AD9F0CA7678B55C851F17E1A2CAE742FCFD041D8503080831E93520
SHA-512:	08CF3ABE10557F284B0427849A4CEF2F111E67E6371F79C3B477F659CC36B438E6C9E541C2DD10C290C6A43E963EBE1B4A7BEF89910C7C98A6099E6E04F8A9EC
Malicious:	true
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....X.Z.qb.qb.qb.a...jqb.s....qb.9...\qb.s...(qb.....qb.#.. qb./b.qb.....qb....Hqb.(c/qb.r.f.qb..(c.qb.;...qb../..Tqb.....Zqb.....qb.z.. ..Bqb.....nqb....[qb....qb;.{qb....qb.#...qb..f.oqb....hqb.z...qb.....qb;...tqb.Rich.qb.....PE.d.=...}^....."\$......@.....@.....@.....dQ.\$.<.....0..(..text.......@.....`..rdata..Co..0...p..0...0.@Co.....@..@..@.data.....;.....@.....@.....@.....pdata..8.....@8.....@..@..@.rsrc.....@.....@..@..@.reloc..1.....@1.....@..B.vxl.....@.....@.....@..@.qwubgr.\$..0....0...0.@\$.....@..@..eef....

C:\Users\user\AppData\Local\Nz4mnM\SndVol.exe  	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	259904
Entropy (8bit):	5.955701055747905
Encrypted:	false
SSDEEP:	3072:UFYIZJbRydnidilSnGvLqeD358rwW39nuyHjVozZcxSHfcBL1ljBeyB7Hbla+:Uf9JonidFnqLV358rNnJqcRcy10/
MD5:	CDD7C7DF2D0859AC3F4088423D11BD08
SHA1:	128789A2EA904F684B5DF2384BA6EEF4EB60FB8E
SHA-256:	D98DB8339EB1B93A7345EECAC2B7290FA7156E3E12B7632D876BD0FD1F31EC66
SHA-512:	A093BF3C40C880A80164F2CAA87DF76DCD854375C5216D761E60F3770DFA04F4B02EC0CA6313C32413AC99A3EBDC081CF915A7B468EE3CED80F9B1ECF4B49104
Malicious:	true
Antivirus:	- Antivirus: Metadefender, Detection: 0%, Browse - Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!L!This program cannot be run in DOS mode...\$.....<BL]..L]..E%...].#9..O].#9..U].#9..F].#9..W].L].\..#9..o].#9k.M].#9..M].RichL].....PE..d...wJSn.....".....@.....@.....p....@.....@+...0....U..T.....t&...(p%.....&...P.....text.....`imrsiv.....rdata.....@..@.data.....@..pddata.....@..@.didat.....@...rsrc...@.....@..@.reloc...0.....@..B.....

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1372160
Entropy (8bit):	5.07954324475136
Encrypted:	false
SSDEEP:	12288:2ZgJtlQepQn+NDo7nlYegQCCLDF/B9wvj/cLvVZFuw:2ZK6F7n5eRmDFJivohZfV
MD5:	AA4563F3E285E21921818923EEC1AB27
SHA1:	F36D24960356D6CCB49EF189025B9366324851D9
SHA-256:	33736F3A5EB68B07C19FDA12C97A3A17120719FA53FFF3B74EB4B5BCA81ED86E
SHA-512:	26BBE92AF58E8B574BA3C4673938F48BF12AFA872FDE65BC3E4A48C590C20BD03B9F1DA460E9F5EB8D5410272E0741D8C4EC3B068CFA4D78595E0A8042E5E488
Malicious:	true
Antivirus:	- Antivirus: Avira, Detection: 100% - Antivirus: Avira, Detection: 100% - Antivirus: Joe Sandbox ML, Detection: 100% - Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....X.Z.qb.qb.qb.a...qb.9...\qb.s...(qb.....qb.#..qb./b..qb.....qb.....Hqb.(c./qb.r.f.qb.(c..qb.;...qb./..Tqb.....Zqb.....qb.z..Bqb.....nqb.....[qb.....qb;...{qb.....qb.#...qb..f.oqb...hqb.z...qb.....qb;...tqb.Rich.qb.....PE.d=...}^.....".....\$.....@.....`.....\$...<.....0..(.....text.....@.....`..r.data.Co..0...p..0...0.@Co.....@..@.data.....@.....@.;.....@.....@..pdata..8.....@8.....@..@.rsrc.....@.....@.....@..@.reloc..1.....@1.....@..B.vxl.....@.....@..@.qwubgr.\$..0....0...0.@\$.....@..@.eer...

C:\Users\user\AppData\Local\00z6Mm4\XmlLite.dll  	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1372160
Entropy (8bit):	5.066544233417286
Encrypted:	false
SSDEEP:	12288:CZgJtlQepQn+ND07nlYegQCLDF/B9wvj/cLvVZFuw:CZK6F7n5eRmDFJivohZFV
MD5:	CFC069A16E13B366B0F56BD27F5BC600
SHA1:	CD6DF254F7B0550B0CC2524F4592571C9EC3F7B1
SHA-256:	1A044F24CC8B8D583E66F577C90C92FF15FF4F3D1FE8096A38B5032C1F8B8D6B
SHA-512:	55F44E15EB12F94804DFE947774B2078DCCD13E0A98EEB9963F90BC0289BD7345F90063DCD29530D161C0B411613FAA6323C53F1C5C7595D19004C117
Malicious:	true
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....X.Z.qb.qb.qb.a...jqb.s....qb.9...\qb.s...(qb.....qb.#..qb../b..qb.....qb.....Hqb.(c./qb.r.f.qb.(c..qb;...qb../.Tqb.....Zqb.....qb.z.. ..Bqb.....nqb....[qb....qb;...{qb....qb.#..qb..f.oqb...hqb.z...qb....qb;...tqb.Rich.qb.....PE..d=...}^....."\$....@.....@.....\$.<.....0..(.....text..@.....@......rdata..Co..0..p..0..0..@Co.....@..@.data.....;.....@.....@.....@.....pdata..8.....@8.....@..@..rsrc.....@.....@.....@.....@..@..@.reloc..1.....@1.....@..B.vxl.....@.....@..@..@qwubgr\$.0....0..0..@\$......@..@..eef....

C:\Users\user\AppData\Local\00z6Mm4\ddodiag.exe 	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	37888
Entropy (8bit):	5.0324146638870335
Encrypted:	false
SDDEEP:	768:ii5tlKBaheiGK/hc3aZkLmMgMaouZI6i9Kott/D:/C0heiGK/hc3aZkLmMgMaouZI6i9t/D
MD5:	3CE911D7C12A2EFA9108514013BD17FE
SHA1:	2F739BD7731932A0BF13A3B8526FC867EC41C63E
SHA-256:	FC55CB5FF243496B039D3DB181BD846BDD38D11C7D52E4BA20D882B65FBE1C3B
SHA-512:	33F4FD94916DB3F0BC4E138DD88125D9B45108F7EECFDE0A54BE1901F4BE3F1966BC0FE9278A919A3D94AEC53A8269ACA9451EBA7D53C82BF64CC215522AD78E
Malicious:	false
Antivirus:	- Antivirus: Metadefender, Detection: 0%, Browse - Antivirus: ReversingLabs, Detection: 0%

Preview:	MZ.....@.....!.L!This program cannot be run in DOS mode...\$......X.=...S...S...S.s.P...S.s.W...S.s.V...S.s.R...S...R.\$S.s.Z...S.s...S.s.Q...S.Rich..S.....PE..d...~3.....*.....&...p.....p/.....@.....q.....`.....~.....d.....p.....(.....Z..T.....E.....F.....text..P%.....&.....`..rdata.."D...@...F...*.....@...@..data.....p.....@....pdata.....@...@.rsrc...p.....@...@.reloc..(.....@..B.....
----------	---

C:\Users\user\AppData\Local\R7Mg9\CloudNotifications.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	77072
Entropy (8bit):	6.115516882753233
Encrypted:	false
SSDEEP:	1536:PBw6bK5qGy2vbnG4bhimIHw28N6GgJpdNtgdNttP+O1K9dr3uhyZb3NnPg5:FbK522vDfnp28a+O1AdCoZxno5
MD5:	D9FF4C8DBC1682E0508322307CB89C0F
SHA1:	52FF480ABF6A6CE9BC32BD3B467C028C35849C6F
SHA-256:	E99A6238FDF53700DE8588E1C1128D52680C1DCAAD4E32B38EF2170395495D29
SHA-512:	C068F98855514994AA7CD66ED02E3FD05B7E81EAD714F83CC158B65AAC6DE12A1D324375C41FEC5C1B6A3F1D6D8639EBFF71D510A720148A33E645ED066DAF2C
Malicious:	false
Preview:	MZ.....@.....!.L!This program cannot be run in DOS mode...\$......=.....e.....Q.....Rich.....PE..d.....".....@.....p.....*.....p.....@... ..L.....%...`.....P...T.....`.....text.....`..imrsiv.....rdata..W.....X.....@...@..data..x.....@....pdata..L.....@...@.didat.....0.....@....rsrc....@.....@...@.reloc.....`.....@..B.....

C:\Users\user\AppData\Local\R7Mg9\UxTheme.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1372160
Entropy (8bit):	5.079630029271723
Encrypted:	false
SSDEEP:	12288:qZgJtlQepQn+NDo7nlYegQCLDF/B9wvj/cLvVZFuw:qZK6F7n5eRmDFJivohZfV
MD5:	EEEEA0804F1E5EB7827FD942423AC682D
SHA1:	09CD42B0D6B83B896B61016364BCAE0FDB729FA2
SHA-256:	EC50BADCD4F4E021A341A08A03FA8A72D4496A5B71BA1BBF6C4F49F79EA61F45
SHA-512:	0C58E87B0716CBB5A0D7DE3A0463C4AF9E09C28EE99543F5A4130A7658B2BB8EB8A88F5BEE0B6877DC9224B6AA0988850C83BF5EB48CB4A22FBEEEF79EBBE E6C
Malicious:	false
Preview:	MZ.....@.....X..Z.qb..qb..qb.a...jqb.s....qb.9...\qb.s...(qb.....qb.#.. qb../b..qb.....qb.....Hqb..(c./qb.r.f..qb..(c..qb.;...qb../..Tqb....Zqb.....qb.z..Bqb.....nqb....[qb....qb.;{qb.....qb..#...qb...f.oqb....hqb.z....qb....qb;...qb.Rich.qb.....PE..d.=...}^....." \$......@.....`.....\$.<.....0..(.....text.....@.....`..rdata..Co...0...p...0...0.@Co.....@...@..data...;.....@.....@.....@....pdata..8.....@8.....@...@.rsrc.....@.....@...@.reloc..1.....@1.....@..B.vxl.....@.....@...@.qwubgr.\$...0... ..0..0.@\$......@...@.eer...

C:\Users\user\AppData\Local\ajcBg\DeviceEnroller.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	359936
Entropy (8bit):	6.00535524532166
Encrypted:	false
SSDEEP:	6144:NXYgu80D0GEiHJb3r/mrKqfNF3Ne8xQOQ2UyQPyHS:Nok0DTHJrr/MKqfNPRyyQI
MD5:	53688BC273A0CB9FD174F809FB56F866
SHA1:	F69901D480530661A3342E567C2F789D3361851D
SHA-256:	D39F1DE499FFD7D8E12ADEA0979AA70FB291C8BD9061019AA0045A247A4B948B
SHA-512:	2233B66D79042C2C1F8B10228FAEE3698FA2C54396B0331F7352DC087F23493BDEB89CECD7E23A1B2CFBD124D9ADB483413DC55DDA813C4F49B18120A702AE5
Malicious:	false
Preview:	MZ.....@.....!.L!This program cannot be run in DOS mode...\$......(.....e.2.0....0.....t.....a.....G.....^m.....m..Richl.....PE..d.....{.....".....ON.....@.....pE...@...\$......h...#.T.....0...(.....X...(.....text...{.....`..rdata.....@...@..data.....@....pdata...\$.@...&.....@...@.didat.....p.....0.....@...rsrc...pE.....F...2.....@...@.reloc..h.....x.....@..B.....

C:\Users\user\AppData\Local\JcB\XmlLite.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1372160
Entropy (8bit):	5.0665476710905875
Encrypted:	false
SSDEEP:	12288:qZgJtlQepQn+ND07nlYegQCLDF/B9wvj/cLvVZFuw:qZK6F7n5eRmDFJivohZfV
MD5:	5A3E479CD2E6CE8BF8B95EB1B9473DF7C
SHA1:	E006DC68DA1C26A263DA0FF6D1B3B6E5E8E5A657
SHA-256:	0D7E29272223CE36DAA5CAA7DCDADBAED9CE393E26FF9A8C7BE5382A072B7EDF
SHA-512:	932974FAD53CD8F754758A2F6712140217369C207CEEDB00A7A34A606C43095DCB4C979151077BBE39C9EF4390E9F1FEB926CEFCDA7D765860B1FB0A3BC8D54
Malicious:	false
Preview:	MZ.....@.....X..Z.qb..qb.a...jqb.s...qb.9...qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb..(c..qb.;...qb../..Tqb.....Zqb.....qb.z.. ..Bqb.....nqb.....[qb.....qb.;...{qb.....qb..#...qb..f.oqb...hqb.z...qb.....qb;...tqb.Rich.qb.....PE..d.=...}^....."\$......@.....`.....\$..<.....0..(.....text....... .....@.....`..rdata..Co...0...p...0...0.@Co.....@..@.data.....@.....@.;.....@..pdata..8.....@8.....@..@.rsrc.....@.....@..@.reloc..1.....@1.....@..B.vxl.....@.....@..@.qwubgr.\$...0... ..0..0.@\$......@..@.eer...

C:\Users\user\AppData\Local\bj1HT\MFPlat.DLL

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1376256
Entropy (8bit):	5.093356085119384
Encrypted:	false
SSDEEP:	12288:3ZgJtlQepQn+ND07nlYegQCLDF/B9wvj/cLvVZFuw:3ZK6F7n5eRmDFJivohZfV
MD5:	094F25E8EE0B130D03AE8565EC8BF099
SHA1:	5988CCA553B95A1D599AF1409602270FC2E97713
SHA-256:	B738ACDF220BAB43ED0EF6E0ABBBEDF3037FA9B654626C526393ECADB11D756B
SHA-512:	485AF608EE610ECD4AE8471415EEBBA38A47A1312CDBE8A5B9E3E5DC6D40707570D37C819B572E25F59199ED645D75B973BA042C049302AF39BF77CBB2B808D
Malicious:	true
Antivirus:	- Antivirus: Avira, Detection: 100% - Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....X..Z.qb..qb.a...jqb.s...qb.9...qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb..(c..qb.;...qb../..Tqb.....Zqb.....qb.z.. ..Bqb.....nqb.....[qb.....qb.;...{qb.....qb..#...qb..f.oqb...hqb.z...qb.....qb;...tqb.Rich.qb.....PE..d.=...}^....."\$......@.....`.....\$..<.....0..(.....text....... .....@.....`..rdata..Co...0...p...0...0.@Co.....@..@.data.....@.....@.;.....@..pdata..8.....@8.....@..@.rsrc.....@.....@..@.reloc..1.....@1.....@..B.vxl.....@.....@..@.qwubgr.\$...0... ..0..0.@\$......@..@.eer...

C:\Users\user\AppData\Local\bj1HT\mfmpmp.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	49688
Entropy (8bit):	6.083384253651048
Encrypted:	false
SSDEEP:	768:vcqpeHowVxW4zmjjJF686T/5Le12fBetjEWI9Wuhu3H1PcSP:vcEoVxJodg/tfiEAhu3VPcSP
MD5:	7C3D09D6DB5DB4A272FCF4C1BB3986BD
SHA1:	F0C392891B6D73EADB20F669A29064910507E55E
SHA-256:	E459FF6CBA8C93589B206C07BDCCD2E6C57766BE6BB4754F2FB1DEF9EF2E3BDE
SHA-512:	6CFE325CD0A78D6ACC9473BA51069E234CB0F9A47F285A6204EE787902C77005491B41C301DD38602CC387329F214E700F9203E4ECE5077E58D30276821640E4
Malicious:	true
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode...\$......0.._Q`..Q`..Q`..)...Q`..5c..Q`..5d..Q`..Qa..Q`..5a..Q`..5e..Q`.. ..5n..Q`..5...Q`..5b..Q`.Rich.Q`.....PE..d..^A.....".....R..V.....P).....@.....s.....h.....`.....\$..... ...`z..T.....Pq.....`r.....H...`.....text...Q.....R.....`..rdata..T...p.....V.....@..@.data.....@.....pdata.....@..@.didat..0.....@.....rsrc...`.....@.....@..@.reloc.....@.....@..B.....

C:\Users\user\AppData\Local\n0R5g\Secur32.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	577024
Entropy (8bit):	7.365924302927238
Encrypted:	false
SSDEEP:	12288:KEpKNOQ/1mgFgnHF+2ryqfut4iob3vBzx4PQplQbwhsi:lpKbbFgl+2Oqfuqjob3JUfs
MD5:	809E11DECADAEBE2454EFEDD620C4769
SHA1:	A121B9FC2010247C65CE8975FE4D88F5E9AC953E
SHA-256:	8906D8D8BCD7C8302A3E56EA2EBD0357748ACC9D3FDA91925609C742384B9CC2
SHA-512:	F78F46437C011C102A9BCEC2A8565EDC75500C9448AC17457FF44D3C8DB1980F772C0D1546F1DEE0F8A6F2C7273A5A915860B768DE9BB24EBEFE2907CE18B0F
Malicious:	false
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....%.].a.3.a.3.a.3.h.u.3..6.`3...7.t.3...2.n.3.a.2...3...=.r.3...0.e.3... ..3...1.`3.Richa.3.....PE..d...b.....".....0.....@.....CS P.....3.....Y..h.....J.....T..... ..S.....z.`.....text.....`?g_Encry~.....`..rdata..._.....`.....@..@.data.....p.....V.....@....pdata...J..... L..d.....@..@.rsrc.....@..@.reloc.....@..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):	1450
Entropy (8bit):	7.341856001318595
Encrypted:	false
SSDEEP:	24:Uk1KaW6dGUcke/TZTy9hu yg1FxVOJ8Mk20PrbBuN1rnbzQcR8Yw76s80c+:UwKZBUckerYh/g19u8F2Ub8N1NXQcGYO
MD5:	464F2980E43A11D0B043075EFE6C5BF4
SHA1:	41A667A8B3E476E64CB9C026908057E9FD420507
SHA-256:	EF19B78322AB9FF8DF1F08E2936B698BD7A57E490EA7E40E675421D60344EDF6
SHA-512:	162D82A7F9C8B2F152331CDA46B34A428B329F506FE854B6203653F99A0E1125D664ADE6C08E878216C9E957606314323251B6B7ED3ABC82884E243F7E094A5F
Malicious:	false
Preview:	user.....RSA1.....a>.(p_{..E..%.....Lr...z...\$f...y7)b<...b.....0.....s..`).F.g.t.....o<..j.n..X.R...XqM.....~?..... .....z..O.....w...L.al...?E.....C.r.y.p.t.o.A.P.I..P.r.i.v.a.t.e..K.e.y....f.....u/.O.Y..U;...{5}.y..9MFX..l.....G`.....hj.Lwi.....Zu2.V.fl.....)z#.##...@..U...j.. {C.Z.Ufd..mX.Q%.2.^7.J/<.'0..m....m%.[g...D.Ky...y..0."...R.IB.X..H.W...T.+X..)....*.4.....SY..7..Leb.^...6=j.....N.b_5.eqA..%.Xp.....H{7..A..71.Pe.f.V%...O#.cR..zC..t.X..~e2X..d....V<.....H@.qE....r`..00_....;U...A..w.....^ID.IY...].Fm;Nfj7.f....Dw{jc...<...:pC~.Ke'iL..p5...Z.b.n..Zz..J <<&d..\$i.lf.....*{9^J.j{.+.....5.b.u.g..w.{ q.O.....d....=T.....8P.....)\\$.1.....z....V.~*.]m`bV.g.!4....z.~Gl...[3...V?#...;bg.A...n.....*\$O..{+o".bm!J.p..H..@..&wIT..Jn..1GAT.....

Static File Info	
General	
File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	5.088449668278153
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:	eWlIdJYfLc.dll
File size:	1368064
MD5:	d098d01cbea52f858bce6d0d9faa5b26
SHA1:	952ce9cd899108c2821bf488b98387b6db8424b8
SHA256:	82c89b2a758177c7cfb7c1763b0444281c6b670deef015a886c866f18dbd8370
SHA512:	ca6b21d580689b8e50b55277d9630e972da202270800c3820c060782f464115220674cfcf78fb3253c5d4607cebf23f087a5281a7a324f94aa75b97a8329f702
SSDEEP:	12288:LZgJtlQepQn+NDo7nlYegQCCLDF/B9wvj/cLvZFw:LZK6f7n5eRmDFJivohZfV
File Content Preview:	MZ.....@.....X.Z.qb..qb..qb.a..jqb.s....qb.9...qb.s...(qb.....qb..#.qb../b..qb.....qb.....Hqb.(c./qb.r.f..qb.. (c..qb.;...qb../.Tqb.....Zqb.....qb.z...Bqb.....nqb....[qb.....qb.;...qb.....qb

File Icon



Icon Hash:

74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1400424b0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x140000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x5E7D9D05 [Fri Mar 27 06:28:21 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:	4a2e61e1749a0183eccadb9c4ef6ec2

Entrypoint Preview

Instruction

```
dec eax
mov dword ptr [00070639h], ecx
dec eax
lea ecx, dword ptr [FFFFFF2F2h]
dec esp
mov dword ptr [0007064Bh], eax
dec esp
mov dword ptr [00070654h], edi
dec esp
mov dword ptr [00070655h], esi
dec eax
xor eax, eax
dec eax
inc eax
dec eax
add ecx, eax
dec esp
mov dword ptr [00070655h], esp
dec eax
dec ecx
dec eax
mov dword ptr [00070653h], esi
dec eax
test eax, eax
je 00007F13CCA7C10Dh
dec eax
mov dword ptr [0007060Fh], esp
dec eax
mov dword ptr [00070600h], ebp
dec eax
mov dword ptr [00070649h], ebx
dec eax
```

Instruction
mov dword ptr [0007063Ah], edi
dec eax
test eax, eax
je 00007F13CCA7C0ECh
dec esp
mov dword ptr [000705FEh], ecx
dec esp
mov dword ptr [0007060Fh], ebp
dec eax
mov dword ptr [000705D0h], edx
jmp ecx
dec eax
add edi, ecx
retn 0008h
ud2
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push esi
dec eax
sub esp, 00000080h
dec eax
mov dword ptr [esp+78h], 58225FC8h
mov dword ptr [esp+60h], 2DFAE652h
mov al, byte ptr [esp+77h]
mov dl, al
add dl, FFFFFFF85h
mov byte ptr [esp+77h], dl
mov word ptr [esp+5Eh], 3327h
dec esp
mov eax, dword ptr [esp+78h]
inc esp
mov ecx, dword ptr [esp+64h]

Data Directories			
Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x14d010	0x8ee	.pmeh
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa9924	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbf000	0x3d8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x1000	0x0	.text
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc0000	0xefc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IAT	0x43000	0x28	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections								
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x418cc	0x42000	False	0.781412760417	data	7.78392111205	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x43000	0x66f43	0x67000	False	0.700320938258	data	7.87281050709	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.data	0xaa000	0x13ba7	0x14000	False	0.0782836914062	data	2.51707039551	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0xbe000	0x138	0x1000	False	0.061279296875	PEX Binary Archive	0.599172422844	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.rsrc	0xbf000	0x69e	0x1000	False	0.123291015625	data	1.07831823765	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc0000	0xf31	0x1000	False	0.416748046875	data	5.36145191459	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.vxl	0xc1000	0x14d4	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.qwubgr	0xc3000	0x1124	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.eer	0xc5000	0x1e66	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.xwwauf	0xc7000	0x9cd	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.pkc	0xc8000	0x42a	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.npkda	0xc9000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.vhs	0xca000	0x1af	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.iaywj	0xcb000	0x1455	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.nasi	0xcd000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.zhvprh	0xce000	0x6cd0	0x7000	False	0.00177873883929	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.yatdsp	0xd5000	0x543	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.njso	0xd6000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.lgliat	0xd8000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.ntqjh	0xd9000	0xbf6	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.sucsek	0xda000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.qsxjui	0xdb000	0x9cd	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.twctcm	0xdc000	0x1124	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.nms	0xde000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.ogj	0xdf000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.vrkgb	0xe1000	0x706	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.gikfw	0xe2000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.ktl	0xe3000	0x9cd	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.crcn	0xe4000	0x5a7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.wtfr	0xe5000	0x1ee	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.hep	0xe6000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.ywg	0xe7000	0xd33	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.sqsp	0xe8000	0x2da	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.gzb	0xe9000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.fatlss	0xea000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.plqa	0xeb000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.vzt	0xec000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.dsbyd	0xed000	0x1e66	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.cdelc	0xef000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.qkhkj	0xf0000	0x5a7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.mnzegr	0xf1000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.krw	0xf2000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.jvsmn	0xf3000	0x389	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.bygpq	0xf4000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.kzdbu	0xf6000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.mwxorn	0xf7000	0x3fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.raf	0xf8000	0x389	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.zcyw	0xf9000	0x2da	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.zeczh	0xfa000	0x128f	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.pvv	0xfc000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.lug	0xfd000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.ski	0x143000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.japjd	0x144000	0x128f	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.mwtzml	0x146000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.vgssf	0x147000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.gsroye	0x148000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.vcmr	0x14a000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.ufki	0x14b000	0x389	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.btl	0x14c000	0x2da	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ
.pmeh	0x14d000	0x8fe	0x1000	False	0.25537109375	data	3.73292380196	IMAGE_SCN_CNT_INITIALIZE D_DATA, IMAGE_SCN_MEM_READ

Resources					
Name	RVA	Size	Type	Language	Country
RT_VERSION	0xbf0a0	0x2dc	data	English	United States
RT_MANIFEST	0xbf380	0x56	ASCII text, with CRLF line terminators	English	United States

Imports	
DLL	Import
ADVAPI32.dll	GetServiceDisplayNameW
KERNEL32.dll	LoadLibraryA, HeapUnlock

Exports		
Name	Ordinal	Address
IsInteractiveUserSession	1	0x14001b188
QueryActiveSession	2	0x14002de80
QueryUserToken	3	0x140021f90
RegisterUserTokenForNoWinlogon	4	0x140037744
WTSCloseServer	5	0x140001e84
WTSCConnectSessionA	6	0x1400128ec
WTSCConnectSessionW	7	0x14003b464
WTSCreateListenerA	8	0x14003ca60
WTSCreateListenerW	9	0x140016670
WTSDisconnectSession	10	0x14002e280
WTSEnableChildSessions	11	0x14001d394
WTSEnumerateListenersA	12	0x140008b14

Name	Ordinal	Address
WTSEnumerateListenersW	13	0x14000ae90
WTSEnumerateProcessesA	14	0x140006aa4
WTSEnumerateProcessesExA	15	0x140036e0c
WTSEnumerateProcessesExW	16	0x14003dd78
WTSEnumerateProcessesW	17	0x1400040c8
WTSEnumerateServersA	18	0x140035160
WTSEnumerateServersW	19	0x140038de0
WTSEnumerateSessionsA	20	0x140031ca8
WTSEnumerateSessionsExA	21	0x14000d828
WTSEnumerateSessionsExW	22	0x14001fae0
WTSEnumerateSessionsW	23	0x1400287b8
WTSFreeMemory	24	0x14002b15c
WTSFreeMemoryExA	25	0x140029c60
WTSFreeMemoryExW	26	0x14000a54c
WTSGetChildSessionId	27	0x140037034
WTSGetListenerSecurityA	28	0x140010070
WTSGetListenerSecurityW	29	0x14002dea0
WTSIsChildSessionsEnabled	30	0x14002b160
WTSLogoffSession	31	0x14002f53c
WTSOpenServerA	32	0x140026a74
WTSOpenServerExA	33	0x140028860
WTSOpenServerExW	34	0x14002380c
WTSOpenServerW	35	0x14002aa8c
WTSQueryListenerConfigA	36	0x140019714
WTSQueryListenerConfigW	37	0x1400401a4
WTSQuerySessionInformationA	38	0x140030ae4
WTSQuerySessionInformationW	39	0x140024f78
WTSQueryUserConfigA	40	0x14002490c
WTSQueryUserConfigW	41	0x14003dda8
WTSQueryUserToken	42	0x140004d64
WTSRegisterSessionNotification	43	0x140008d84
WTSRegisterSessionNotificationEx	44	0x14001a96c
WTSSendMessageA	45	0x14003dd78
WTSSendMessageW	46	0x14000a2cc
WTSSetListenerSecurityA	47	0x140037dec
WTSSetListenerSecurityW	48	0x140033d00
WTSSetRenderHint	49	0x1400309e8
WTSSetSessionInformationA	50	0x140027a8c
WTSSetSessionInformationW	51	0x140020908
WTSSetUserConfigA	52	0x140013664
WTSSetUserConfigW	53	0x14002f130
WTSShutdownSystem	54	0x1400234cc
WTSStartRemoteControlSessionA	55	0x14002f0b0
WTSStartRemoteControlSessionW	56	0x140040e90
WTSStopRemoteControlSession	57	0x14000daec
WTSTerminateProcess	58	0x1400270d8
WTSUnRegisterSessionNotification	59	0x14002c144
WTSUnRegisterSessionNotificationEx	60	0x140035390
WTSVirtualChannelClose	61	0x140042810
WTSVirtualChannelOpen	62	0x140035678
WTSVirtualChannelOpenEx	63	0x14002dff4
WTSVirtualChannelPurgeInput	64	0x14000e808
WTSVirtualChannelPurgeOutput	65	0x14003aacc
WTSVirtualChannelQuery	66	0x1400235d4
WTSVirtualChannelRead	67	0x140041888
WTSVirtualChannelWrite	68	0x14000c228
WTSWaitSystemEvent	69	0x140038334

Version Infos

Description	Data
LegalCopyright	Microsoft Corporation. All rights
InternalName	dphnup
FileVersion	1.56
CompanyName	Microsoft C
ProductName	Sysinternals Streams
ProductVersion	6.1
FileDescription	Thai K
OriginalFilename	dphnupnp.d
Translation	0x0409 0x04b0

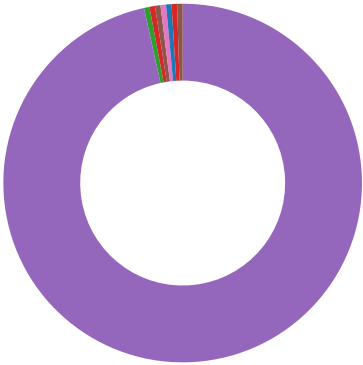
Possible Origin		
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

 No network behavior found

Statistics

Behavior



- loaddll64.exe
- cmd.exe
- rundll32.exe
- rundll32.exe
- explorer.exe
- rundll32.exe
- rundll32.exe
- svchost.exe
- sdclt.exe
- CloudNotifications.exe
- CloudNotifications.exe
- systemreset.exe
- Dxpserver.exe
- Dxpserver.exe
- mfmp.exe
- mfmp.exe
- msra.exe
- mstsc.exe
- mstsc.exe
- SndVol.exe
- SndVol.exe

 Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: 7088, Parent PID: 668

General

Target ID:	0
Start time:	15:47:10
Start date:	23/03/2022

Path:	C:\Windows\System32\loadll64.exe
Wow64 process (32bit):	false
Commandline:	loadll64.exe "C:\Users\user\Desktop\WlldJYfLc.dll"
Imagebase:	0x7ff72e730000
File size:	140288 bytes
MD5 hash:	4E8A40CAD6CCC047914E3A7830A2D8AA
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: 00000000.00000002.280898080.00007FFC670C1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	moderate

File Activities							
There is hidden Windows Behavior. Click on Show Windows Behavior to show it.							
File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
File Path	Offset	Length	Completion	Count	Source Address	Symbol	

Analysis Process: cmd.exe PID: 7112, Parent PID: 7088	
General	
Target ID:	1
Start time:	15:47:11
Start date:	23/03/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\WlldJYfLc.dll",#1
Imagebase:	0x7ff64ce50000
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	
There is hidden Windows Behavior. Click on Show Windows Behavior to show it.	
File Path	Access Attributes Options Completion Count Source Address Symbol

Analysis Process: rundll32.exe PID: 7120, Parent PID: 7088	
General	
Target ID:	2
Start time:	15:47:12
Start date:	23/03/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\WlldJYfLc.dll,IsInteractiveUserSession
Imagebase:	0x7ff7ef960000
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: 00000002.00000002.382839680.00007FFC670C1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\WldJYfLc.dll	unknown	1368064	success or wait	1	7FFC6711F8D6	ReadFile

Analysis Process: rundll32.exe PID: 7132, Parent PID: 7112

General

Target ID:	3
Start time:	15:47:12
Start date:	23/03/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\WldJYfLc.dll",#1
Imagebase:	0x7ff7ef960000
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: 00000003.00000002.260901088.00007FFC670C1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\WldJYfLc.dll	unknown	1368064	success or wait	1	7FFC6711F8D6	ReadFile

Analysis Process: explorer.exe PID: 3968, Parent PID: 7120

General

Target ID:	4
Start time:	15:47:14
Start date:	23/03/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6b8cf0000
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

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
-----------	--------	------------	---------	------------	-------	----------------	--------

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\kz7HdNSL5oE	read data or list directory synchronize	device compressed	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	14005F2F5	CreateDirect oryW
C:\Users\user\AppData\Local\R7Mg9\	read data or list directory synchronize	device compressed	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	14005F2F5	CreateDirect oryW
C:\Users\user\AppData\Local\R7Mg9\UxTheme.dll	read attributes synchronize generic read generic write	device compressed	synchronous io non alert non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\R7Mg9\CloudNotifications.exe	read attributes synchronize generic read generic write	device compressed	synchronous io non alert non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\4O9p1cGN\	read data or list directory synchronize	device compressed	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	14005F2F5	CreateDirect oryW
C:\Users\user\AppData\Local\4O9p1cGN\dwmapi.dll	read attributes synchronize generic read generic write	device compressed	synchronous io non alert non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\4O9p1cGN\Dxpserver.exe	read attributes synchronize generic read generic write	device compressed	synchronous io non alert non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\bj1HT\	read data or list directory synchronize	device compressed	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	14005F2F5	CreateDirect oryW
C:\Users\user\AppData\Local\bj1HT\MFplat.DLL	read attributes synchronize generic read generic write	device compressed	synchronous io non alert non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\bj1HT\mfmp.exe	read attributes synchronize generic read generic write	device compressed	synchronous io non alert non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\4n0R5g\	read data or list directory synchronize	device compressed	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	14005F2F5	CreateDirect oryW
C:\Users\user\AppData\Local\4n0R5g\Secur32.dll	read attributes synchronize generic read generic write	device compressed	synchronous io non alert non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\4n0R5g\mstsc.exe	read attributes synchronize generic read generic write	device compressed	synchronous io non alert non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\Nz4mnM\	read data or list directory synchronize	device compressed	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	14005F2F5	CreateDirect oryW
C:\Users\user\AppData\Local\Nz4mnM\UxTheme.dll	read attributes synchronize generic read generic write	device compressed	synchronous io non alert non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\Nz4mnM\SndVol.exe	read attributes synchronize generic read generic write	device compressed	synchronous io non alert non directory file	success or wait	1	14005F6CE	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\laJcBg\	read data or list directory synchronize	device compressed	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	14005F2F5	CreateDirectoryW
C:\Users\user\AppData\Local\laJcBg\XmlLite.dll	read attributes synchronize generic read generic write	device compressed	synchronous io non alert non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\laJcBg\DeviceEnroller.exe	read attributes synchronize generic read generic write	device compressed	synchronous io non alert non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\EQ0DjT2sP\	read data or list directory synchronize	device compressed	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	14005F2F5	CreateDirectoryW
C:\Users\user\AppData\Local\EQ0DjT2sP\UI70.dll	read attributes synchronize generic read generic write	device compressed	synchronous io non alert non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\EQ0DjT2sP\CameraSettingsUIHost.exe	read attributes synchronize generic read generic write	device compressed	synchronous io non alert non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\lVRJtv0CU\	read data or list directory synchronize	device compressed	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	14005F2F5	CreateDirectoryW
C:\Users\user\AppData\Local\lVRJtv0CU\ACTIVEDS.dll	read attributes synchronize generic read generic write	device compressed	synchronous io non alert non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\lVRJtv0CU\SppExtComObj.Exe	read attributes synchronize generic read generic write	device compressed	synchronous io non alert non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\O0z6Mm4\	read data or list directory synchronize	device compressed	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	14005F2F5	CreateDirectoryW
C:\Users\user\AppData\Local\O0z6Mm4\XmlLite.dll	read attributes synchronize generic read generic write	device compressed	synchronous io non alert non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\O0z6Mm4\ddodiag.exe	read attributes synchronize generic read generic write	device compressed	synchronous io non alert non directory file	success or wait	1	14005F6CE	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\R7Mg9\CloudNotifications.exe	cannot delete	16	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\R7Mg9\UxTheme.dll	cannot delete	16	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\R7Mg9\CloudNotifications.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\R7Mg9\UxTheme.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\4O9p1cGN\dwmapl.dll	cannot delete	6	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\4O9p1cGN\Dxpserver.exe	cannot delete	6	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\4O9p1cGN\dwmapl.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\4O9p1cGN\Dxpserver.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\bj1HT\MFPlat.DLL	cannot delete	16	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\bj1HT\mfpmpl.exe	cannot delete	16	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\bj1HT\MFPlat.DLL	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\bj1HT\mfpmpl.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\n0R5g\mstsc.exe	cannot delete	26	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\n0R5g\Secur32.dll	cannot delete	26	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\n0R5g\mstsc.exe	success or wait	1	14005FB70	DeleteFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\409p1cGN\dwmapi.dll	0	1372160	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 fd 01 00 00 58 10 0c 5a 1c 71 62 09 1c 71 62 09 1c 71 62 09 61 08 fd 09 6a 71 62 09 73 07 fd 09 18 71 62 09 39 06 fd 09 5c 71 62 09 73 07 fd 09 28 71 62 09 fd 15 fd 09 0b 71 62 09 11 23 fd 09 20 71 62 09 fd 2f 62 08 07 71 62 09 15 09 fd 09 09 71 62 09 07 fd fd 09 48 71 62 09 fd 28 63 08 2f 71 62 09 72 2c 66 08 0b 71 62 09 fd 28 63 08 10 71 62 09 3b fd fd 09 2c 71 62 09 fd 2f fd 09 54 71 62 09 fd fd fd 09 5a 71 62 09 fd fd fd 09 1e 71 62 09 7a fd fd 09 42 71 62 09 fd fd fd 09 6e 71 62 09 fd 15 fd 09 5b 71 62 09 9d fd 09 1b 71 62 09 3b fd 0c 09 7b 71 62 09 1f 09 fd 09 7f 71 62	MZ@XZqbqbajqbsqb9\ qbs(qbqb# qb/bqbqbHqb(c/qbr,fqb(c qb;,qb/ TqbZqbqbzBqbnqb[qbqb; {qbqb	success or wait	1	14005F160	WriteFile
C:\Users\user\AppData\Local\409p1cGN\Dxpserver.exe	0	304640	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 39 fd 20 45 7d fd 4e 16 7d fd 4e 16 7d fd 4e 16 12 fd 4d 17 7e fd 4e 16 12 fd 4a 17 64 fd 4e 16 12 fd 4b 17 7b fd 4e 16 12 fd 4f 17 58 fd 4e 16 7d fd 4f 16 46 fd 4e 16 12 fd 47 17 5b fd 4e 16 12 f1 16 7c fd 4e 16 12 fd 4c 17 7c fd 4e 16 52 69 63 68 7d fd 4e 16 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06 00 fd 7a fd fd 00 00 00 00 00 00 00 fd 00 22 00 0b 02 0e 0c 00 fd 02	MZ@!L!This program cannot be run in DOS mode.\$9 E}N}N}NM~NJd NK{NOXN}OFNG[N]NL[N Rich}NPedz"	success or wait	1	14005F160	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\EQ ODjT2sP\DIU70.dll	0	165478 4	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 fd 01 00 00 58 10 0c 5a 1c 71 62 09 1c 71 62 09 1c 71 62 09 61 08 fd 09 6a 71 62 09 73 07 fd 09 18 71 62 09 39 06 fd 09 5c 71 62 09 73 07 fd 09 28 71 62 09 fd 15 fd 09 0b 71 62 09 11 23 fd 09 20 71 62 09 fd 2f 62 08 07 71 62 09 15 09 fd 09 09 71 62 09 07 fd fd 09 48 71 62 09 fd 28 63 08 2f 71 62 09 72 2c 66 08 0b 71 62 09 fd 28 63 08 10 71 62 09 3b fd fd 09 2c 71 62 09 fd 2f fd 09 54 71 62 09 fd fd fd 09 5a 71 62 09 fd fd fd 09 1e 71 62 09 7a fd fd 09 42 71 62 09 fd fd fd 09 6e 71 62 09 fd 15 fd 09 5b 71 62 09 9d fd 09 1b 71 62 09 3b fd 0c 09 7b 71 62 09 1f 09 fd 09 7f 71 62	MZ@XZqbqbqbajqbsqb9\ qbs(qbqb# qb/bqbqbHqb(c/qbr,fqb(c qb;,qb/ TqbZqbqbzBqbnqb[qbqb; {qbqb	success or wait	1	14005F160	WriteFile
C:\Users\user\AppData\Local\EQ ODjT2sP\CameraSettingsUIHost.exe	0	32104	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 5f 4c 70 fd 1b 2d 1e fd 1b 2d 1e fd 1b 2d 1e fd 12 55 fd fd 11 2d 1e fd 74 49 1d fd 19 2d 1e fd 74 49 1a fd 08 2d 1e fd 74 49 1b fd 1c 2d 1e fd 74 49 1f fd 16 2d 1e fd 1b 2d 1f fd 4b 2d 1e fd 74 49 17 fd 19 2d 1e fd 74 49 fd 1a 2d 1e fd 74 49 1c fd 1a 2d 1e fd 52 69 63 68 1b 2d 1e fd 00 50 45 00 00 64 fd 07	MZ@!L!This program cannot be run in DOS mode.\$_Lp---U-tl-tl-tl-- K-tl-tl-tl-Rich-PEd	success or wait	1	14005F160	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\MBR2GPT.EXE	unknown	808960	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\sdclt.exe	unknown	1210880	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\TCPSVCS.EXE	unknown	12288	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\lcsEntitlementHost.exe	unknown	35328	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\setsnp.exe	unknown	29184	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\CloudNotifications.exe	unknown	77072	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\luxtheme.dll	unknown	599040	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\ComputerDefaults.exe	unknown	72192	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\UevAppMonitor.exe	unknown	55808	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\setuppugc.exe	unknown	127488	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\timeout.exe	unknown	30720	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\systemreset.exe	unknown	506184	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\lsdiagnhost.exe	unknown	25088	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\calc.exe	unknown	27648	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\prevhost.exe	unknown	28160	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\baaupdate.exe	unknown	112640	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\RmClient.exe	unknown	17408	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\lcofire.exe	unknown	23552	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\xbgmsvc.exe	unknown	59512	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\printui.exe	unknown	64000	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\Dxpserver.exe	unknown	304640	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\dwmapl.dll	unknown	146840	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\sort.exe	unknown	27136	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\lqappsrv.exe	unknown	24064	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\lmpnotify.exe	unknown	19456	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\curl.exe	unknown	424448	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\loaddll64.exe	unknown	140288	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\lvmfmp.exe	unknown	49688	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\lvmplat.dll	unknown	1947816	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\AppHostRegistrationVerifier.exe	unknown	110080	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\lmsra.exe	unknown	600064	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\PrintBrmUi.exe	unknown	71168	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\MuiUnattend.exe	unknown	100352	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\lvenotify.exe	unknown	173568	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\lmtsc.exe	unknown	3640832	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\secur32.dll	unknown	27648	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\pcwrun.exe	unknown	15872	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\Defrag.exe	unknown	185856	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\lfhmanagew.exe	unknown	139264	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\WSManHTTPConfig.exe	unknown	32256	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\runonce.exe	unknown	57856	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\plasrv.exe	unknown	10752	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\SndVol.exe	unknown	259904	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\PrintIsolationHost.exe	unknown	76288	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\query.exe	unknown	16896	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\UIMgrBroker.exe	unknown	35840	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\reg.exe	unknown	72704	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\lquser.exe	unknown	24576	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\lPnPUnattend.exe	unknown	59392	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\WorkFolders.exe	unknown	103936	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\ApplyTrustOffline.exe	unknown	1034632	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\DeviceEnroller.exe	unknown	359936	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\xmlite.dll	unknown	227840	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\CameraSettingsUIHost.exe	unknown	32104	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\dui70.dll	unknown	1719808	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\wuapihost.exe	unknown	10752	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\ldcomcnfg.exe	unknown	11776	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\cipher.exe	unknown	46080	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\lrstrui.exe	unknown	266752	success or wait	2	14005F8D6	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\SppExtComObj.Exe	unknown	577024	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\activeds.dll	unknown	263680	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\unarchiver.exe	unknown	10752	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\runas.exe	unknown	19456	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\CompMgmtLauncher.exe	unknown	90112	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\charmap.exe	unknown	188928	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\aitstatic.exe	unknown	2856448	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\Locator.exe	unknown	10752	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\ksetup.exe	unknown	37376	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\CIDiag.exe	unknown	30208	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\ddodiag.exe	unknown	37888	success or wait	3	14005F8D6	ReadFile

Registry Activities					
Key Created					
Key Path	Completion	Count	Source Address	Symbol	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{9F16F3A5-E10E-4F5D-0952-ED348BFD2785}	success or wait	1	14006340A	RegCreateKeyExW	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{9F16F3A5-E10E-4F5D-0952-ED348BFD2785}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{BC715C51-4336-812E-2F6A-D8A684FC8688}	success or wait	1	14006340A	RegCreateKeyExW	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{BC715C51-4336-812E-2F6A-D8A684FC8688}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{E8285A23-2463-C83F-F962-201551F0C4A4}	success or wait	1	14006340A	RegCreateKeyExW	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{E8285A23-2463-C83F-F962-201551F0C4A4}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{3C881BE8-E385-BB1F-9622-BB449A1E17A1}	success or wait	1	14006340A	RegCreateKeyExW	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{3C881BE8-E385-BB1F-9622-BB449A1E17A1}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{07E44A99-3038-C75F-7B90-595B5B1F5413}	success or wait	1	14006340A	RegCreateKeyExW	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{07E44A99-3038-C75F-7B90-595B5B1F5413}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{BCE418A1-321B-A640-5575-AC08B7F3F725}	success or wait	1	14006340A	RegCreateKeyExW	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{BCE418A1-321B-A640-5575-AC08B7F3F725}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{58CBDCE0-3983-6A95-86C1-8F391F2316E7}	success or wait	1	14006340A	RegCreateKeyExW	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{58CBDCE0-3983-6A95-86C1-8F391F2316E7}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{0A1DAC31-8F47-D454-A702-975F9CB2BCFF}	success or wait	1	14006340A	RegCreateKeyExW	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{0A1DAC31-8F47-D454-A702-975F9CB2BCFF}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{AE9ACCD9-10EC-D8A7-9FEA-972D6257C8CC}	success or wait	1	14006340A	RegCreateKeyExW	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{AE9ACCD9-10EC-D8A7-9FEA-972D6257C8CC}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{1EEA80CD-E4D6-F285-3A76-982709B296C5}	success or wait	1	14006340A	RegCreateKeyExW	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{1EEA80CD-E4D6-F285-3A76-982709B296C5}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{F971B9BB-3837-8E42-602F-C6DA18E248D8}	success or wait	1	14006340A	RegCreateKeyExW	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{F971B9BB-3837-8E42-602F-C6DA18E248D8}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{50FB222D-D8BB-6301-C7F5-DCAF6DF7C1A2}	success or wait	1	14006340A	RegCreateKeyExW	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{50FB222D-D8BB-6301-C7F5-DCAF6DF7C1A2}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{86259FDD-7636-FF91-9A41-AFCA8FEAD43C}	success or wait	1	14006340A	RegCreateKeyExW	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{86259FDD-7636-FF91-9A41-AFCA8FEAD43C}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW	

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{D9A8C8C7-A497-39A3-61C3-1730A6FBCDC0}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{D9A8C8C7-A497-39A3-61C3-1730A6FBCDC0}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{F5FEE91B-F170-CB05-61DC-067139B1F0EE}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{F5FEE91B-F170-CB05-61DC-067139B1F0EE}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{695DFACB-9FCB-6697-D55B-0DB74A0FA584}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{695DFACB-9FCB-6697-D55B-0DB74A0FA584}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{8C952134-F88E-1118-8535-F1539661BCCB}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{8C952134-F88E-1118-8535-F1539661BCCB}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{160BFC5A-4D9E-6A61-B115-25D81E8ABC87}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{160BFC5A-4D9E-6A61-B115-25D81E8ABC87}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW

Key Value Created								
Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{F971B9BB-3837-8E42-602F-C6DA18E248D8}\ShellFolder	{10A77711-7431-5C48-2D8C-EEB99DF5A872}	binary	73 32 A8 61 01 F2 48 59 20 07 7E C5 49 07 5C 33 C5 F0 36 B2 49 DD DF 29 2E 32 D1 6C 15 3D 06 FE E5 EA A1 92 51 0C 8A B1 56 DB 58 7D 37 04 C5 FA 14 92 46 1F AF D8 D1 8F 8B FE 9D D6 26 C9 E4 E6 48 C4 6E 76 A5 27 DF	success or wait	1	140062470	RegSetValueExA	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{AE9ACCD9-10EC-D8A7-9FEA-972D6257C8CC}\ShellFolder	{B3423271-AEFB-C732-77C8-82413DD14B0C}	binary	67 E1 2E 4B A5 1C D0 56 2B B5 70 38 98 B5 1B 8C B2 B3 9F 3C AE 41 28 99 57 90 92 4A 0B 9E 40 22 86 0D 17 06 6D 8A 60 AB 01 BF 02 09 A9 69 27 A5 BC F3 37 4B 55 D0 8C 67 2E 78 69 3C 28 F5 83 E6 90 CC 13 72 D5 C3 DA 2B 5D 9A 75 78 BA A4 46 CA 13 B0 91 50 59 C1 91 81 B1 F5 59 EC	success or wait	1	140062470	RegSetValueExA	
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{F971B9BB-3837-8E42-602F-C6DA18E248D8}\ShellFolder	{32683374-3DBE-53CB-ECD6-C9577D1E6A36}	binary	11 3B 8C 81 3F 65 93 96 3E 12 0A 6D 8B C8 FF 94 B0 6A F8 33 D0 28 EB E6 AF 7F B8 60 E0 97 2D 4E 46 00 2E 84 27 9B 00 1B 4D 50 9D A8 22 82 81 D9 3F 92 8B 69 3C F3 6B 51 CA C0 11 52 68 A0 49 D1 0B 00 A0 A9 5A D6 57 45 A9 C1 EC E0 92 56 80 38 74 AB 85 05 1B 7A B8 F3 79 21 F3 28 0E 02 A4 1F E4 AC 9A 99 10 02 CF F8 7A 50 31 46 AE 70 84 58 50 4F A4 D9 73 7F BC 30 B8 2A 6E 2F 3B F5 3E 9A 11 8E 89 E9 89 05 8E 83 5A F1 D4 E2 3F 8B 0E E1 F7 E2 03 EA C2 B0 FF 42 24 AD E7 72 56 14 8A 4E 82 B3 A0 85 B4 8E C2 6C E7 25 7B 45 67 AF F7 79 D1 C8 63 5D 69 4D 99 B7 B8 0B 56 0C 31 4B 7D 24 31 C9 40 0C E4 AD 1D 73 70 96 70 7A A8 3B 74 69 D8 25 E7 61 BA 55 E6 D1 7B C1 FD ED 1E 8A 10 B4 DC BC 34 BE 2A 5A B4 07 02 F4 41 6B 26 5B F6 85 E5 4F 60 10 CF 76 4E 74 C3 57 7A 51 6A 69 1C 49 A2 6F 47 98 36 D4 A5 CF C7 4F F5 7A 29 60 01 BA 62 37 08 2B 05 93 6C 88 6C E0 7D A6 84 B3 02 17 72 89 2C F3 56 8C 38 F1 8F 44 98 01 ED A8 8F B8 46 19 BB 38 87 7F 42 97 81 AF E1 B4 6C A1 56 A2 2E 56 88 BE 7A F8 FD 7E 53 44 5B 6D F8 20 11 7A D2 17 85 5B 92 08 6A 41 BB B0 0A C0 A3 A0 BE 29 65 E3 A6 05 B2 B8 71 8B 4A 85 0C D0 C4 0A B6 06 F6 2E 1E 1D B1 84 73 C3 0A D5 7E CA 5C 39 1D B6 23 72 0A 2B EF A5 16 A9 3A C1 C4 9F 20 05 A2 D7 63 F7 48 E7 2D 0A 96 DB 77 8B 5F 83 61 F2 F6 0D 6C E3 41 FB 9A 47 B6 5A FA 61 7D 7D D0 21 DF 40 DB DA 72 A7 EC 5C DE 3B AF ED CF 92 A7 BD 45 CB 52 A5 63 88 63 30 B0 CE 53 A6 AC 85 69 AA 32 1E 25 DF DC	success or wait	1	140062470	RegSetValueExA	

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			99 C F 00 6B 89 E0 BF BA C0 DF E9 32 6F CA A5 12 A1 3E E8 9C 25 CF 97 5F B6 61 46 3A E8 2B BA F5 ED F6 A0 49 A6 A0 5D 00 19 9C 12 97 B2 06 10 38 FE 32 61 2B 40 57 AC 30 93 F9 9D C0 D5 1E A8 D7 85 37 39 C2 AA 33 B7 1D 08 61 6E BF 09 04 35 50 C8 21 9C 9E 8F F5 9F FA 30 20 54 FF 2E CD 59 0B F7 8D 3C 2B 68 83 3C 2D FE 12 07 81 31 01 32 C2 C4 11 DB D6 80 75 94 02 F2 C9 8A 3B EC 5F 13 DD 3E B8 53 B2 48 ED 86 2C EB C5 83 06 B7 3E 18 58 1F 9E 47 CF F7 B4 71 29 9D 2E D6 B3 BA CE EF 17 4A E3 09 11 D9 D6 EB DD DB EF 83 84 A7 CE EF F4 B6 88 E9 51 98 81 95 00 C9 CD 20 FF 58 5D CD C7 75 76 35 90 74 9C 47 B8 96 2C C2 D1 1C 37 58 13 3A 8F 08 9E 8A 5B BB FB D2 A4 02 1F 13 1A A6 FC ED 7F BD 2A 0E A9 83 2B 2E 2B 99 7D 99 A2 B4 F7 F8 5D E3 93 5B 0F 0B A6 46 C0 32 F4 CD 87 22 96 54 C3 73 BB E9 BC 2A BE 4F 62 E2 8E 1F 46 C0 6A 79 F4 CC 5F B4 5B 49 54 09 62 99 E4 DC 0B AA 16 B9 D4 EB 6A FA 29 B8 09 3C EA 8F A4 FB D8 AC 64 21 EE 4A F9 5D E0 3A 4D 66 C9 C5 99 DE AE 5D B1 24 0E F8 AA 16 4F D4 D5 6C 59 96 CA 3B 84 E5 00 99 87 41 3A 99 0B 96 BF B1 36 ED F2 DE 8A 2B 11 8F 85 4F D8 9F 71 47 7B CD 47 AE E3 37 83 C5 36 3F D0 22 D3 CE 5F 0B 85 6E 36 E9 BB E2 D7 AC 6B 72 A4 5E A2 7D 92 39 81 D9 7D 24 CE DC C9 B7 DC 4E 49 F6 0A E4 2D 36 D5 81 24 27 28 F0 BB 85 E3 B6 B8 44 AA E1 11 B7 33 87 19 CE 06 EB 5E 51 4A 91 64 DE 8E 5A 98 40 F6 AD 01 17 10 C4 E2 A0 69 37 77 AF 37 9C 5F 0C 16 60 AE 03 31 67 AD 14 54 52 45 82 C6 FF 5A AA D6 E1 28 67 A4 7C A1 52 63 FB 22 20 AC 82 5F F9 66 B2 F8 5A 2A 56 BC 1C 21 3B 06 4F 57 00 6F DE 2A E6 39 30 33 97 38 0F D9 71 57 74 DA DC F7 86 15 76 62 6E 57 DB 29 4E 9D 15 3D 1E 9B 37 89 21 BD 37 9F 96 BE 4B 54 F0 DF E7 85 64 D8 E5 3B CF D5 50 E8 B6 9B 9E 21 40 B1 9F F7 62 CF ED C5 FC 9F 75 2A 56 80 3E 59 2E 05 0C 4E 1C 05 68 67 C5 E7 78 00 64 4B E3 4C 23 48 AB 4B 02 65 6D D8 41 63 A9 2C C3 77 D1 5B C9 61 F8 4F 44 16 71 35 A3 27 74 C4 95 84 34 E1 AE AE 1C 82 87 E4 29 69 FA 52 6F 91 32 AB BE 9B E9 E1 E5 C1 91 CB A6 B4 BB 51 D0 24 1B B9 BB 62 8F 61 CF 96 0D 42 F4 60 15 91 99 15 A1 CD BE A0 49 3E 4D 3B 9A 9F F6 47 EE 50 4D C0 28 60 83 F0 6E 8F 23 F1 83 1E B1 08 B1 E4 FC DA 39 55 E7 52 97 E3 E2 1A E0 2D D5 5C 17 2F B8 2F AA 7B C5 F6 FD 7F D7 F9 6E C4 AC 9B C9 A3 EE 1A 35 EF 59 3D F3 5F FE 2A 62 F4 76 16 59 34 C9 C5 A4 F0 43 CA 1B 76 48 D0 91 32 56 1E AC 3F 0E 59 40 EA 1A C8 AA 74 C1 94 84 72 86 E7 E5 BD F2 4A 06 CF 66 37 CE D5 CD 8B 11 71 C6 C4 07 65 22 25 77 E9 6C 13 77 01 E1 21 27 E2 3E C3 31 D9 7D CC 5D E5 4B 15 66 7B D6 A6 B6 38 D3 CB 25 8D 51 84 B0 EE 4E D3 5D 3F 29 C2 A4 9B C5 4C 78 6C C1 F3 0D D4 86 7E C4 2F A5 61 1D 37 B5 A1 83 4D E7 EE B3 E4 03 83 77 4C 6C C7 9A 45 FE 67 32 FD 98 DD 7E ED 55 14 2E 6B E7 8D AC 73 62 56 45 92 0B D4 E3 82 6A BC 5E DE 71 06 BE 53 FE 22 F3 2E 80 4F 29 CB 1D C8 F1 43 60 9B 53 06 70 0E 56 BE D0 08 B8 25 E1 88 F4 2C 03 4E 6D 40 84 B5 FA 82 8E FE AA 6B 6A 16 5C 6A 66 B9 C9 DC 52 63 DA 95 F1 39 F3 9A 3C 72 E3 59 06 0D A9 AC 77 D6 CF 60 81 7F 4F 6D 1E 06 0C 87 C6 24 58 22 70 0A 0B C9 0E 80 83 30 B3 2A 3A A8 99 25 81 72 E4 CB 1F A2 4E 0B 92 96 B4 93 33 F1 39 D4 0F 63 BD FF B8 55 AA 2F A1 FA 71				

Key Path	Name	Type	Completion	Count	Source Address	Symbol
			DAtāB 13 00 5D 97 95 AA 3E B0 3C D0 5C B7 A3 97 75 8F 49 06 F7 70 0B D1 9F 19 9C F8 9B F3 E1 26 6A 63 57 4E F9 1F 53 41 EE FA 18 15 90 2D 22 8D A2 91 6D 0B DE C7 F7 50 39 F6 D2 28 1B CD 84 0A 2B 74 AB 47 71 18 4C 82 9E 0C 06 E4 04 2C 9A A5 78 12 6C 23 5A 1A C5 FF 4F 8E 9E F3 13 55 05 94 A1 A1 0E 2F CA 5C FF BA CA 7D 11 E5 06 9D 7D CD 1E 0C 87 CE B0 F6 FD E6 F7 F9 96 3A A5 D1 86 DE 49 B2 AF 90 F0 9B B3 BA A5 EA 78 59 04 5D 8A 66 34 42 61 5D 14 DE 03 6D AA B2 B6 81 D2 61 FA E1 51 A1 B1 66 09 6A 1D 50 56 CE F2 F4 6A D6 63 A4 9E AC 3E FC F3 B6 C9 50 D0 9F A9 03 AF 7F 11 01 53 78 EB 34 44 33 45 F4 9B 92 EA 07 68 33 7D 41 5C 4A BC C0 53 73 5C 96 94 17 96 FD 2D 58 31 1E AC E7 22 F1 D3 FE D7 A9 4C 69 82 C1 7C 2B 65 50 7A 6F FC 4E 40 31 AA 0F 93 6A 5D 0F 85 E0 BF EB 50 B8 3B 3A 18 C7 56 8A BF 45 A0 4E 3A 5D A3 AB 58 A9 D3 65 19 6B 5C D2 5D CD 32 FB DC 87 20 0E 91 5D 22 AD 40 55 AA 4C CB 27 2C C5 B7 A3 21 AD 0D 52 42 71 10 26 7F D8 5B 6C 40 95 A1 63 8E EC 73 12 5F 93 9B F6 D1 D2 01 F7 BA 50 12 FC 64 BD 89 07 83 62 45 6D D4 1B 52 6C CB 62 F2 4A D0 AE A9 75 D4 F7 F0 A7 74 BC 13 03 F9 F3 C7 68 C1 E1 C9 F2 8B F1 B7 72 DA 4B 9B D8 D4 5C E4 94 F8 AC B0 F9 2D 55 61 A3 A0 85 2D 8F FB 27 4B D2 1A F4 F6 69 15 B3 17 30 61 5C DB 21 AB D0 42 DB E2 B4 70 F3 7C E4 22 DA 16 FB 67 54 46 EA 71 B8 F7 B7 FC 5F 1B A4 9C 4E 55 D9 95 95 DB CE 63 0C C5 BB 4F 22 CD BD CC 06 A2 B6 30 CD 90 F9 2D D7 32 E9 50 AE C4 BB 52 EB F3 DD 65 B9 46 C7 AC 4E B6 93 A4 46 20 8A 9F C2 03 59 01 35 4A 50 2E C5 87 CA E0 C5 81 D1 98 87 CE 93 81 76 11 26 FF 2A A8 B6 A6 BB 1A E6 9A 10 CE 5C 62 C0 60 24 32 48 25 91 7A A8 DB 1D AB 5A 76 03 B5 DA F1 AF 07 6B C9 27 71 5C 86 CC 6F 0E D8 6B B1 A2 AC E1 F0 57 87 59 1B 33 84 EE 55 8B 1E 2B C0 43 13 5C 93 48 8F 9A F9 8A 6B 17 27 06 32 26 90 82 3C 5C 37 80 40 BF 45 9E 22 BF 57 62 00 8B 12 6F 00 FB 6F F8 65 72 5D AA 1F E5 64 F6 4F D5 64 78 1C 0D E3 E4 B9 27 D3 11 E8 9D 74 81 38 26 BC 20 6C 13 2B 20 03 9A 09 38 D3 28 1C E2 1F D3 91 AD E5 7D 43 38 1E E5 0A 82 F1 04 D5 71 44 29 30 3B E0 66 C5 30 6A 2E DD 2E 9E E9 81 15 AE 5C A3 2A 19 77 78 52 FA 46 7F FD 0E 4D 5C AF 9F AD FE A8 B0 2C 99 65 3B B8 E3 AA FB FE F5 97 00 AF 21 4D 13 94 B6 C1 93 B8 ED 5A 96 E4 2E 5F 87 DB 68 0C F2 2B AC 9B 43 8E 36 A9 38 69 D6 D6 94 B1 62 0B E3 1A DC 58 6F 4E FF 21 0D 2F 90 30 B9 8E 98 D9 D2 F7 30 A2 1A 1F C6 D1 28 C9 13 25 2B 14 51 08 20 95 FF 33 A1 94 9F C7 E6 AB 27 0C 73 29 6A 49 46 D0 16 FE C3 A1 57 20 EF 5C DC 3C 6E 22 5C 5D 7D D7 AD 17 2D 19 00 57 AC 87 C4 98 05 4C 1D 36 81 7E 09 A7 FC 71 DE 13 81 E6 FE 2F CD 98 2C F3 1D E6 A8 5D 8B 4A A7 1C EB DC 1F A9 55 54 8F 7F 67 75 8E C1 89 53 64 59 75 85 0A A7 E3 6F 97 51 E5 8F 2F 75 86 64 4A 07 02 30 3B F5 3C 6B 7A 94 54 32 77 27 DF F2 D4 11 AF 71 0F 08 F9 08 A8 21 6B 26 4D EC B6 99 28 88 A8 EA 92 5C 75 9A 21 15 E0 2B 7E ED FD 08 E5 5D 89 C8 8B A1 4A A2 EA 6C 32 A3 6B 5C 11 47 79 B2 35 5B 7A 99 97 76 EB F2 6E 6C 8F 0B 7E 4C 65 7E AF D6 ED 30 C8 7A EE 0C 4E 43 18 C3 BC 57 CC BA B2 6A CF B6 D8 2F D0 D5 7E 63 78 B4 D8 FE 8E 8A 61 CF 27 D1 4F 55 D1 49 99 04 44 13 EC 34 4D 3B FC 62 77 7B 37 77 D6 A8 28 B7 A2 4A DE 4C 68 71 BA DE			

Key Path	Name	Type	Date	Completion	Count	Source Address	Symbol
			A9 29 B7 A3 4A DE 4C 09 71 BA DE 04 68 68 FC 58 D2 0D BD 4D E1 F6 84 CC 3B 43 F0 99 5F 28 D7 59 8B 37 66 13 7F D3 77 C2 5E 5D 01 F7 5E 00 11 BC 73 9D 19 03 79 DB 91 76 03 A7 4B 77 7E 27 62 8B CD AC DC DF E3 A0 1D 4E 2B AF B0 2C 5C 46 4D AB 90 1B 4F C0 D1 B6 62 84 77 9B 3E C9 C9 94 92 34 7E 2F AB 3A E0 3D DA 1E E0 14 77 E4 10 31 B0 5D 27 82 7F F8 2A 21 DE 55 39 36 A9 DA B3 41 D3 AC 5B B5 C2 92 51 91 66 E7 14 8F E4 FC EB C4 23 83 EA 49 54 1C 4A E8 3C 3F 58 70 E1 CB 10 9D 30 23 5A 4D 81 AD 5E 17 72 5F 00 3A D7 BA 9E 7C FC A4 A6 DB 03 F1 C2 5B 0C 3C BE AC D6 3A 3A A3 03 26 38 48 DD 84 4F EF 02 41 45 CB C2 CE 8C 3C 1C A2 6A 2F 9D C8 37 00 D8 92 A3 AE E6 A6 11 27 A2 9F 6A 5E EE AA 07 7A 87 2F 0B C7 F9 FF CA 22 A7 9B B4 E3 41 FD 76 8B 10 11 CD 23 89 C9 63 2F 4B 97 D1 2A 68 8F 23 C7 1E D4 50 37 5D 00 12 5D 43 25 AE 13 56 77 2E DC 98 EF AD 56 5B 7B FB F8 9D EB 7D 83 E5 F3 34 61 77 BD B7 00 D9 02 1F E4 B4 99 98 F7 04 CD 6B 14 F8 41 FA 1F 4C 86 CD 7F E5 2E 40 C1 80 23 9B 62 67 90 78 1A 85 90 AB 7B 79 60 AF CD 6B DC B7 65 2B 44 33 5C DB 1E EA 59 B0 55 B9 8D F2 D9 C1 2D 29 8E 6C 43 5A 13 B6 F7 34 23 53 BB 1D 6B 87 50 A9 43 30 BF CD BC 95 9F 85 7F 63 92 75 32 49 1C 67 80 6F 42 6D DC				

Analysis Process: rundll32.exe PID: 5384, Parent PID: 7088	
General	
Target ID:	6
Start time:	15:47:15
Start date:	23/03/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\WldJYfLc.dll,QueryActiveSession
Imagebase:	0x7ff7ef960000
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: 00000006.00000002.267568902.00007FFC670C1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities							
File Read							
File Path	Offset	Length	Completion	Count	Source Address	Symbol	
C:\Users\user\Desktop\WldJYfLc.dll	unknown	1368064	success or wait	1	7FFC6711F8D6	ReadFile	

Analysis Process: rundll32.exe PID: 3156, Parent PID: 7088	
General	
Target ID:	8
Start time:	15:47:18
Start date:	23/03/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false

Commandline:	rundll32.exe C:\Users\user\Desktop\WldJYfLc.dll,QueryUserToken
Imagebase:	0x7ff7ef960000
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: 00000008.00000002.274772551.00007FFC670C1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities						
File Read						
File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\WldJYfLc.dll	unknown	1368064	success or wait	1	7FFC6711F8D6	ReadFile

Analysis Process: **svchost.exe** PID: 5604, Parent PID: 568

General	
Target ID:	11
Start time:	15:47:30
Start date:	23/03/2022
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff73c930000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: **sdclt.exe** PID: 3960, Parent PID: 3968

General	
Target ID:	18
Start time:	15:48:17
Start date:	23/03/2022
Path:	C:\Windows\System32\sdclt.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\sdclt.exe
Imagebase:	0x7ff60bf90000
File size:	1210880 bytes
MD5 hash:	0632A8402C6504CD541AC93676AAD0F5
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: **CloudNotifications.exe** PID: 5876, Parent PID: 3968

General	
Target ID:	19
Start time:	15:48:18

Start date:	23/03/2022
Path:	C:\Windows\System32\CloudNotifications.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\CloudNotifications.exe
Imagebase:	0x7ff793190000
File size:	77072 bytes
MD5 hash:	D9FF4C8DBC1682E0508322307CB89C0F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: CloudNotifications.exe PID: 2928, Parent PID: 3968

General

Target ID:	20
Start time:	15:48:20
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\R7Mg9\CloudNotifications.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\R7Mg9\CloudNotifications.exe
Imagebase:	0x7ff740780000
File size:	77072 bytes
MD5 hash:	D9FF4C8DBC1682E0508322307CB89C0F
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: 00000014.00000002.430869317.00007FFC74C21000.00000020.00000001.01000000.0000000A.sdmp, Author: Joe Security

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\R7Mg9\UxTheme.dll	unknown	1372160	success or wait	1	7FFC74C7F8D6	ReadFile

Analysis Process: systemreset.exe PID: 6544, Parent PID: 3968

General

Target ID:	22
Start time:	15:48:33
Start date:	23/03/2022
Path:	C:\Windows\System32\systemreset.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\systemreset.exe
Imagebase:	0x7ff764df0000
File size:	506184 bytes
MD5 hash:	872AE9FE08ED1AA78208678967BE2FEF
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: Dxpserver.exe PID: 3500, Parent PID: 3968

General

Target ID:	25
------------	----

Start time:	15:48:34
Start date:	23/03/2022
Path:	C:\Windows\System32\Dxpserver.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\Dxpserver.exe
Imagebase:	0x7ff7a7db0000
File size:	304640 bytes
MD5 hash:	DCCB1D350193BE0A26CEAFF602DB848E
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: Dxpserver.exe PID: 1740, Parent PID: 3968

General

Target ID:	26
Start time:	15:48:38
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\4O9p1cGN\Dxpserver.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\4O9p1cGN\Dxpserver.exe
Imagebase:	0x7ff7540f0000
File size:	304640 bytes
MD5 hash:	DCCB1D350193BE0A26CEAFF602DB848E
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: 0000001A.00000002.465961019.00007FFC74C21000.00000020.00000001.01000000.0000000C.sdmp, Author: Joe Security
Antivirus matches:	- Detection: 0%, Metadefender, Browse - Detection: 0%, ReversingLabs

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\4O9p1cGN\dwmapl.dll	unknown	1372160	success or wait	1	7FFC74C7F8D6	ReadFile

Analysis Process: mfpmp.exe PID: 5604, Parent PID: 3968

General

Target ID:	28
Start time:	15:48:49
Start date:	23/03/2022
Path:	C:\Windows\System32\mfpmp.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\mfpmp.exe
Imagebase:	0x7ff6cc190000
File size:	49688 bytes
MD5 hash:	7C3D09D6DB5DB4A272FCF4C1BB3986BD
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: mfpmp.exe PID: 3464, Parent PID: 3968

General

Target ID:	29
Start time:	15:48:51
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\bj1HT\mfmp.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\bj1HT\mfmp.exe
Imagebase:	0x7ff670a40000
File size:	49688 bytes
MD5 hash:	7C3D09D6DB5DB4A272FCF4C1BB3986BD
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: 0000001D.00000002.500951495.00007FFC74C21000.00000020.00000001.01000000.0000000E.sdmp, Author: Joe Security

File Activities

File Read						
File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\bj1HT\MFPlat.DLL	unknown	1376256	success or wait	1	7FFC74C7F8D6	ReadFile

Analysis Process: msra.exe PID: 1908, Parent PID: 3968

General	
Target ID:	30
Start time:	15:49:06
Start date:	23/03/2022
Path:	C:\Windows\System32\msra.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msra.exe
Imagebase:	0x7ff7a2430000
File size:	600064 bytes
MD5 hash:	3240CC226FB8AC41A0431A8F3B9DD770
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: mstsc.exe PID: 7132, Parent PID: 3968

General	
Target ID:	31
Start time:	15:49:06
Start date:	23/03/2022
Path:	C:\Windows\System32\mstsc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\mstsc.exe
Imagebase:	0x7ff633000000
File size:	3640832 bytes
MD5 hash:	3FBB5CD8829E9533D0FF5819DB0444C0
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: mstsc.exe PID: 3176, Parent PID: 3968

General

Target ID:	33
Start time:	15:49:08
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\n0R5g\lmtsc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\n0R5g\lmtsc.exe
Imagebase:	0x7ff7b8700000
File size:	3640832 bytes
MD5 hash:	3FBB5CD8829E9533D0FF5819DB0444C0
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: 00000021.00000002.543380049.00007FFC74C21000.00000020.00000001.01000000.00000011.sdmp, Author: Joe Security

Analysis Process: SndVol.exe PID: 5936, Parent PID: 3968

General

Target ID:	34
Start time:	15:49:25
Start date:	23/03/2022
Path:	C:\Windows\System32\SndVol.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SndVol.exe
Imagebase:	0x7ff62b390000
File size:	259904 bytes
MD5 hash:	CDD7C7DF2D0859AC3F4088423D11BD08
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: SndVol.exe PID: 5900, Parent PID: 3968

General

Target ID:	35
Start time:	15:49:27
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\Nz4mnM\SndVol.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Nz4mnM\SndVol.exe
Imagebase:	0x7ff742cd0000
File size:	259904 bytes
MD5 hash:	CDD7C7DF2D0859AC3F4088423D11BD08
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: 00000023.00000002.574221343.00007FFC74C21000.00000020.00000001.01000000.00000013.sdmp, Author: Joe Security
Antivirus matches:	- Detection: 0%, Metadefender, Browse - Detection: 0%, ReversingLabs

Disassembly

 No disassembly