ID: 575240
Sample Name: dry.dll
Cookbook: default.jbs
Time: 08:19:09
Date: 20/02/2022
Version: 34.0.0 Boulder Opal

Table of Contents

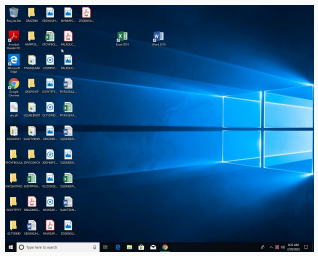
Windows Analysis Report

dry.dll

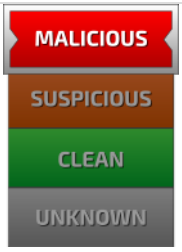
Overview

General Information

Sample Name:	dry.dll
Analysis ID:	575240
MD5:	4bec705de3584b..
SHA1:	b29ff37578ef950..
SHA256:	13aa6bed5b3a65.
Tags:	dll dridex exe
Infos:	



Detection



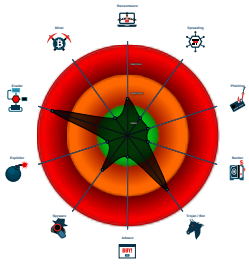
Dridex

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…
- Malicious sample detected (through…
- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Changes memory attributes in foreig…
- Machine Learning detection for sam…
- Queues an APC in another process …
- Contains functionality to inject code…
- Sigma detected: Suspicious Call by…
- Machine Learning detection for drop…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 6572 cmdline: loaddll64.exe "C:\Users\user\Desktop\dry.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 6612 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\dry.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 4484 cmdline: rundll32.exe "C:\Users\user\Desktop\dry.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5792 cmdline: rundll32.exe C:\Users\user\Desktop\dry.dll,CreateXmlReader MD5: 73C519F050C20580F8A62C849D49215A)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - consent.exe (PID: 4904 cmdline: C:\Windows\system32\consent.exe MD5: 74D31E4F51873160D91B1F80E0C472D0)
      - consent.exe (PID: 3576 cmdline: C:\Users\user\AppData\Local\DLKXiO\consent.exe MD5: 74D31E4F51873160D91B1F80E0C472D0)
      - SysResetErr.exe (PID: 4676 cmdline: C:\Windows\system32\SysResetErr.exe MD5: 6A3F2F3C36FE45A87E3BFA80B6D92E07)
      - SysResetErr.exe (PID: 2064 cmdline: C:\Users\user\AppData\Local\s8hTTPzEx\SysResetErr.exe MD5: 6A3F2F3C36FE45A87E3BFA80B6D92E07)
      - consent.exe (PID: 6440 cmdline: C:\Windows\system32\consent.exe MD5: 74D31E4F51873160D91B1F80E0C472D0)
      - consent.exe (PID: 4740 cmdline: C:\Users\user\AppData\Local\dfAZPUGwQ\consent.exe MD5: 74D31E4F51873160D91B1F80E0C472D0)
      - rdpshell.exe (PID: 6520 cmdline: C:\Windows\system32\rdpshell.exe MD5: 4994A0ADA359924026FE631E54FC7A5D)
      - cmstp.exe (PID: 4628 cmdline: C:\Windows\system32\cmstp.exe MD5: 2A9828E0C405422D166E0141054A04B3)
      - cmstp.exe (PID: 6000 cmdline: C:\Users\user\AppData\Local\y1c6p\cmstp.exe MD5: 2A9828E0C405422D166E0141054A04B3)
      - SystemPropertiesComputerName.exe (PID: 5732 cmdline: C:\Windows\system32\SystemPropertiesComputerName.exe MD5: BEE134E1F23AFD3AE58191D265BB9070)
      - DWWIN.EXE (PID: 5392 cmdline: C:\Windows\system32\DWWIN.EXE MD5: 3C21F944D5FF44E45BC753919F6AE445)
      - DWWIN.EXE (PID: 4336 cmdline: C:\Users\user\AppData\Local\oudoiG\DWWIN.EXE MD5: 3C21F944D5FF44E45BC753919F6AE445)
      - SystemPropertiesDataExecutionPrevention.exe (PID: 4940 cmdline: C:\Windows\system32\SystemPropertiesDataExecutionPrevention.exe MD5: 1A34577AEDE83993615D7F2E37024D4D)
      - sppsvc.exe (PID: 5788 cmdline: C:\Windows\system32\sppsvc.exe MD5: FEEC8055C5986182C717DD888000AEF6)
      - sppsvc.exe (PID: 5012 cmdline: C:\Users\user\AppData\Local\GsjW\sppsvc.exe MD5: FEEC8055C5986182C717DD888000AEF6)
      - SndVol.exe (PID: 3156 cmdline: C:\Windows\system32\SndVol.exe MD5: CDD7C7DF2D0859AC3F4088423D11BD08)
      - SndVol.exe (PID: 5664 cmdline: C:\Users\user\AppData\Local\0rPbJb\SndVol.exe MD5: CDD7C7DF2D0859AC3F4088423D11BD08)
  - rundll32.exe (PID: 568 cmdline: rundll32.exe C:\Users\user\Desktop\dry.dll,CreateXmlReaderInputWithEncodingCodePage MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5456 cmdline: rundll32.exe C:\Users\user\Desktop\dry.dll,CreateXmlReaderInputWithEncodingName MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000001B.00000002.448574954.00007FFC6E291000.00000020.00000001.01000000.0000000C.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
0000001B.00000002.448574954.00007FFC6E291000.00000020.00000001.01000000.0000000C.sdmp	crime_win64_dridex_bot_hook	Detects latest Dridex bot hook	@VK_Intel	• 0x37e93:$code: E8 38 5D 00 00 8B 5C 24 5C 48 8D 95 70 01 00 00 44 2B F3 48 8D 4D 70 41 B8 04 00 00 00 41 83 EE 05 44 89 B5 70 01 00 00 E8 10 5D 00 00 BA CD 9C FF 56 B9 CB 69 E2 6A 8B F3 48 89 5D A8 48 C7 45 ...
00000008.00000002.305054509.00007FFC68291000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000008.00000002.305054509.00007FFC68291000.00000020.00000001.01000000.00000003.sdmp	crime_win64_dridex_bot_hook	Detects latest Dridex bot hook	@VK_Intel	• 0x37e93:$code: E8 38 5D 00 00 8B 5C 24 5C 48 8D 95 70 01 00 00 44 2B F3 48 8D 4D 70 41 B8 04 00 00 00 41 83 EE 05 44 89 B5 70 01 00 00 E8 10 5D 00 00 BA CD 9C FF 56 B9 CB 69 E2 6A 8B F3 48 89 5D A8 48 C7 45 ...
00000006.00000002.296790826.00007FFC68291000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
Click to see the 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.rundll32.exe.7ffc68290000.2.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
4.2.rundll32.exe.7ffc68290000.2.unpack	crime_win64_dridex_bot_hook	Detects latest Dridex bot hook	@VK_Intel	• 0x38293:$code: E8 38 5D 00 00 8B 5C 24 5C 48 8D 95 70 01 00 00 44 2B F3 48 8D 4D 70 41 B8 04 00 00 00 41 83 EE 05 44 89 B5 70 01 00 00 E8 10 5D 00 00 BA CD 9C FF 56 B9 CB 69 E2 6A 8B F3 48 89 5D A8 48 C7 45 ...
8.2.rundll32.exe.7ffc68290000.2.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
8.2.rundll32.exe.7ffc68290000.2.unpack	crime_win64_dridex_bot_hook	Detects latest Dridex bot hook	@VK_Intel	• 0x38293:$code: E8 38 5D 00 00 8B 5C 24 5C 48 8D 95 70 01 00 00 44 2B F3 48 8D 4D 70 41 B8 04 00 00 00 41 83 EE 05 44 89 B5 70 01 00 00 E8 10 5D 00 00 BA CD 9C FF 56 B9 CB 69 E2 6A 8B F3 48 89 5D A8 48 C7 45 ...
3.2.rundll32.exe.7ffc68290000.2.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
Click to see the 13 entries				

Sigma Signatures

System Summary

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

E-Banking Fraud

Yara detected Dridex unpacked file

System Summary

Malicious sample detected (through community Yara rule)

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)

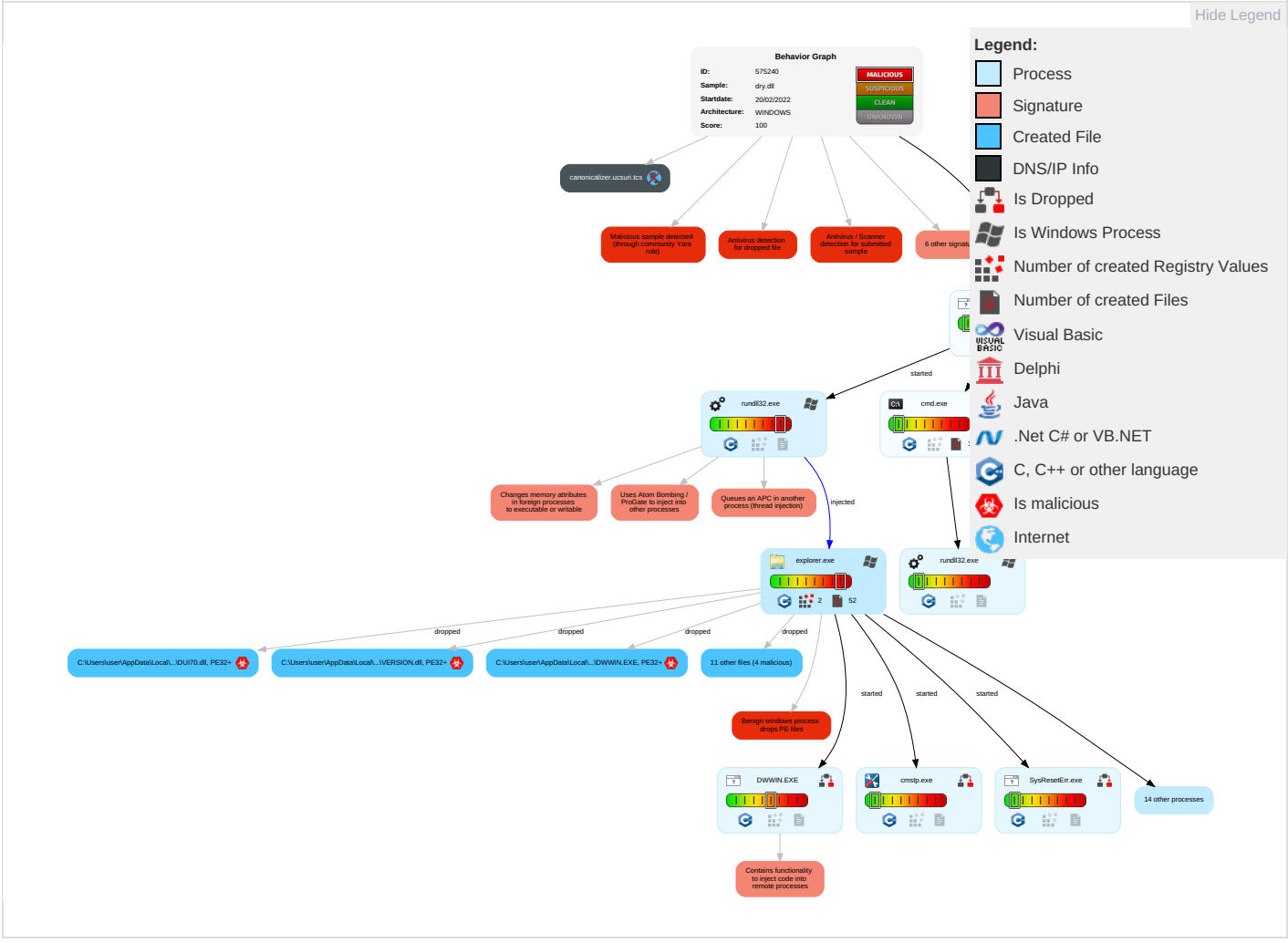
Contains functionality to inject code into remote processes

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
1 Valid Accounts	2 Command and Scripting Interpreter	1 Valid Accounts	1 Valid Accounts	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	2 Service Execution	1 Windows Service	1 1 Access Token Manipulation	1 Valid Accounts	LSASS Memory	3 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Native API	Logon Script (Windows)	1 Windows Service	1 1 Access Token Manipulation	Security Account Manager	3 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 Exploitation for Client Execution	Logon Script (Mac)	4 1 2 Process Injection	4 1 2 Process Injection	NTDS	1 Account 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 Deobfuscate/Decode Files or Information	LSA Secrets	1 System Owner/User 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	3 Obfuscated Files or Information	Cached Domain Credentials	2 File and Directory 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 Rundll32	DCSync	3 5 System Information 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	2 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Timestomp	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

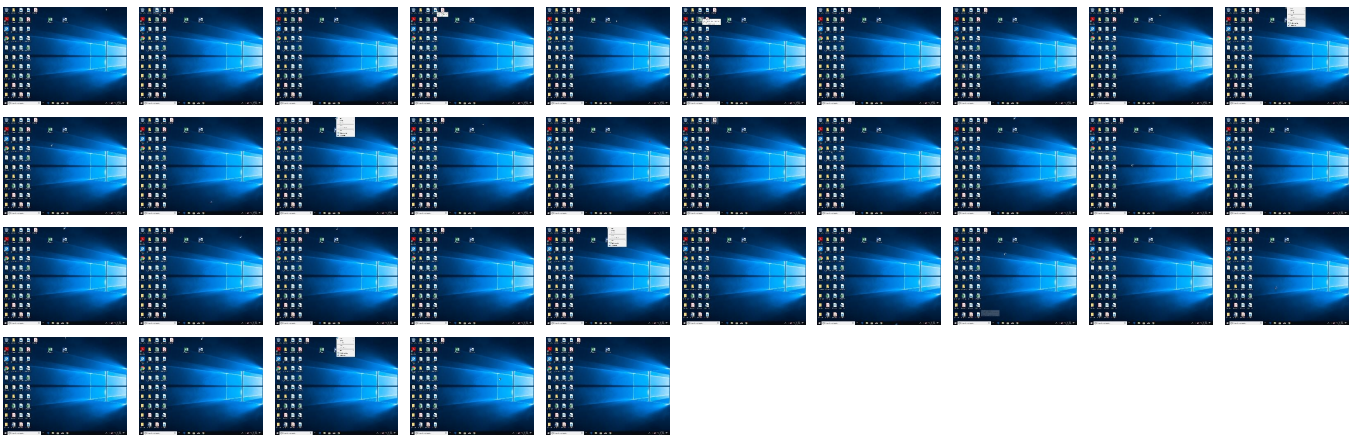
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
dry.dll	71%	Virustotal		Browse
dry.dll	56%	Metadefender		Browse
dry.dll	82%	ReversingLabs	Win64.Infostealer.Dridex	
dry.dll	100%	Avira	TR/Crypt.XPACK.Gen7	
dry.dll	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\oudoiG\VERSION.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\oudoiG\VERSION.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\0rPbJb\UxTheme.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\dfAZPUGwQ\WINSTA.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\s8hTTPzEx\DUI70.dll	100%	Avira	TR/Crypt.XPACK.Gen4	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\GsjW\XmlLite.dll	100%	Avira	TR/Crypt.XPACK.Gen7	
C:\Users\user\AppData\Local\DLKXiO\WMsgAPI.dll	100%	Avira	TR/Crypt.XPACK.Gen7	
C:\Users\user\AppData\Local\oudoiG\VERSION.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\oudoiG\VERSION.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\0rPbJb\UxTheme.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\dfAZPUGwQ\WINSTA.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\s8hTTPzEx\DUI70.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\GsjW\XmlLite.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\DLKXiO\WMsgAPI.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\0rPbJb\SndVol.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\0rPbJb\SndVol.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\0rPbJb\SndVol.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\DLKXiO\consent.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\DLKXiO\consent.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\GsjW\sppsvc.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\GsjW\sppsvc.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\dfAZPUGwQ\consent.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\dfAZPUGwQ\consent.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
27.2.cmstp.exe.7ffc6e290000.3.unpack	100%	Avira	HEUR/AGEN.1138339		Download File
8.2.rundll32.exe.7ffc68290000.2.unpack	100%	Avira	HEUR/AGEN.1138339		Download File
0.2.loaddll64.exe.1d745960000.0.unpack	100%	Avira	HEUR/AGEN.1202768		Download File
8.2.rundll32.exe.1bde0fe0000.1.unpack	100%	Avira	HEUR/AGEN.1202768		Download File
4.2.rundll32.exe.7ffc68290000.2.unpack	100%	Avira	HEUR/AGEN.1138339		Download File
3.2.rundll32.exe.7ffc68290000.2.unpack	100%	Avira	HEUR/AGEN.1138339		Download File
4.2.rundll32.exe.18772c80000.1.unpack	100%	Avira	HEUR/AGEN.1202768		Download File
27.2.cmstp.exe.16fcb7b0000.0.unpack	100%	Avira	HEUR/AGEN.1202768		Download File
6.2.rundll32.exe.14c9a260000.1.unpack	100%	Avira	HEUR/AGEN.1202768		Download File
35.2.sppsvc.exe.7ffc6e290000.3.unpack	100%	Avira	HEUR/AGEN.1138339		Download File
0.2.loaddll64.exe.7ffc68290000.2.unpack	100%	Avira	HEUR/AGEN.1138339		Download File
6.2.rundll32.exe.7ffc68290000.2.unpack	100%	Avira	HEUR/AGEN.1138339		Download File
15.2.SysResetErr.exe.7ffc67de0000.3.unpack	100%	Avira	HEUR/AGEN.1138339		Download File
3.2.rundll32.exe.267f4940000.1.unpack	100%	Avira	HEUR/AGEN.1202768		Download File
30.2.DWWIN.EXE.7ffc6e290000.3.unpack	100%	Avira	HEUR/AGEN.1138339		Download File
30.2.DWWIN.EXE.25593050000.0.unpack	100%	Avira	HEUR/AGEN.1202768		Download File
35.2.sppsvc.exe.2955f650000.0.unpack	100%	Avira	HEUR/AGEN.1202768		Download File
15.2.SysResetErr.exe.204e44f0000.0.unpack	100%	Avira	HEUR/AGEN.1202768		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
canonicalizer.ucsuri.tcs	unknown	unknown	false		unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	575240
Start date:	20.02.2022
Start time:	08:19:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	dry.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:	38
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
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@45/15@5/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 26.3% (good quality ratio 21.1%) • Quality average: 55.4% • Quality standard deviation: 35.4%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll

Warnings

- Connection to analysis system has been lost, crash info: Unknown
- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, login.live.com, ctldl.windowsupdate.com, settings-win.data.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where 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\0rPbJb\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:	A093BF3C40C880A80164F2CAA87DF76DCD854375C5216D761E60F3770DFA04F4B02EC0CA6313C32413AC99A3EBDC081CF915A7B468EE3CED80F9B1ECF4B498 04
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<.BL]..L]..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.....p&..(...p%.....&.....P.....text..... ..`.imrsiv.....rdata..... .....@..@.data.....@.. ..pdata.....@..@.didat.....@....rsrc...@.... .....@..@.reloc.....0.....@..B.....

C:\Users\user\AppData\Local\0rPbJb\UxTheme.dll

Process:	C:\Windows\explorer.exe

File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1376256
Entropy (8bit):	5.014670719687533
Encrypted:	false
SSDEEP:	12288:slORVEAueQmTmQKO2nMlqVaSEwzH7YxiCyJ86azEZy1f11pNx:gORVEVNmaDznMlqVNE27dJ8J2inNx
MD5:	119D43AEE03F7225BC2DCB9758976345
SHA1:	D319D9BF1C114A6B348E524FE493D629051EA78B
SHA-256:	B75A0694F4450FB2669A15039537A666D40FD592D75C0300F0A4262D86A86D8B
SHA-512:	C1A72C43D0866B8508AE5D0F3ECDF5DFF184A6862BC93E8BCDD569A650086051C7918186CEFF816503EE2566BE336793F7190C9D698FB543CC04307B4068F39
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...z.v^.....".....*.....@.....`.....x...x.....0..8.....0.....text..... ..`.rdata...._...0...`...0.....@..@.data....*.....0.....@....pdata..D.....@..@.rsrc.....@..@.reloc.....@..B .cwkw.....@..@.pbpwn..tQ.....`.....@..@.pem....

C:\Users\user\AppData\Local\DLKXiO\WMsgAPI.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1372160
Entropy (8bit):	5.013506443062603
Encrypted:	false
SSDEEP:	12288:alORVEAueQmTmQKO2nMlqVaSEwzH7YxiCyJ86azEZy1f11pNx:OORVEVNmaDznMlqVNE27dJ8J2inNx
MD5:	4E74BAB6EE3BFC6FA8A83FF4932E1B0B
SHA1:	6DAEBBD85383F6ED11734BF342DE98051BC66985
SHA-256:	10108D4E0584A0F4218094210008B0802CF79BF4325983A16E1E31CEA14A76AC
SHA-512:	BFA2EDB51E5CE6A59FBD7BA2C55E6985F77B3A63DC00ABA2436F689F934CD571E17A6C9A895F0CEAB0C96ED379151605D98A6D9D21B0ED545F38A5685B83E 48
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...z.v^.....".....*.....@.....`.....x...x.....0..8.....0.....text..... ..`.rdata...._...0...`...0.....@..@.data....*.....0.....@....pdata..D.....@..@.rsrc.....@..@.reloc.....@..B. cwkw.....@..@.pbpwn..tQ.....`.....@..@.pem....

C:\Users\user\AppData\Local\DLKXiO\consent.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	157080
Entropy (8bit):	5.924344092826888
Encrypted:	false
SSDEEP:	3072:4eana1Hze2vHL+u5F28BrciRXBis72z5B+o:Aa1TfD+u5F2wrTio2z2o
MD5:	74D31E4F51873160D91B1F80E0C472D0
SHA1:	35DEC0D1A12C6F1F7A460E3AE75E4D74D5BD815A
SHA-256:	113813A699063EBF391D436A4EFE0B6F95F81E12AF773FABE5511B5CA08E189C
SHA-512:	F026CBBDF3792A05091B3CC0A97F825D353BC5FF9AB7248F4544B81BA2F86FD28CEB04468D755715BB3BD220BB72781DC079423D912A56E3793AC1687AEE7E 5
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Y_GE.>)..>)..>)..F..Y>).rZ*..>).rZ-..>).rZ,..>).rZ(..>)..>(.9?).rZ'..>). rZ...>).rZ+..>).Rich.>).....PE..d...i.7.....".....H.....C.....@..... .....PP..\.....h....D...!.....0%..T..... .....(...(...HL.....text..... ..`.rdata...c.....d.....@..@.data...l.....h.....@....pdata..h.....j.....@..@.didat. .....x.....@...consent.b.....z.....@....rsrc.....|.....@..@.reloc.....B.....@..B..... .....

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

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1376256
Entropy (8bit):	5.00173504502067
Encrypted:	false
SSDEEP:	12288:4lORVEAueQmTmQKO2nMlqVaSEwzH7YxiCyJ86azEZy1f11pNx:8ORVEVNmaDznMlqVNE27dJ8J2inNx
MD5:	AF59F0A6E12F5BAED3D43F9834F4D94B
SHA1:	815BBF09917B4BBF81E82184227B5ECD0B8146BB
SHA-256:	F4A6912D5E559E145C0DC0E33079F856886AD1165BD7773DA037E9E760202232
SHA-512:	DDA08D082DF135515642046CCC337140AC9672296AE8882497E05C29481D41422DA46DA8513B8675320AF91AB33E46B4AAFC02B53EA60FD34A847130AEAFE6B
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...z.v^....."..... .....*.....@.....`.....x...x.....0..8.....0.....text..... .. ..... ..`.rdata..._...0...`...0.....@..@.data....*.....0.....@....pdata..D.....@..@.rsrc.....@..@.reloc.....@..B .cwkw.....@..@.pbpwn..tQ.....`.....@..@.pem....

C:\Users\user\AppData\Local\GsjW\sppsvc.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	4527680
Entropy (8bit):	7.180545050051135
Encrypted:	false
SSDEEP:	49152:hzB335WOshFXigiF5l5mpb0+bOnBmB8XEsDfA+uLCKls0did8Pf6ZJ6t3Ovenev1:8X5iFrEpdAkZ6W3xYBP149K
MD5:	FEEC8055C5986182C717DD888000AEF6
SHA1:	7749D1C531D85C69047576B3BB3525E0B01A2942
SHA-256:	E09B7B1DE43A226842A4B8C591D712E51585BC7E8A39CFB8852CBF16D234C3A6
SHA-512:	822869C7506824537 70C66D7C6665CECCCB0BB27ECEB8E0A9202FE5C1942492359280057345 04AED79D80583CED2A2F203D4133A11E7F4A8D6160F21F7F3919F
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....-..C..C..C...@..C.....C...G...C...F..C...B...C..B...C...J...C...@..C .....C...A..C.Rich.C.....PE..d...A.Lc.....".....8.....P.....@.....CS P.....D.....4.E.....|.A.....D..+....B.4|...ZD.@....@D..n....?.T.. .....i:.(....h:.....8i:.....text...L.7.....7..... ..`?g_Encry.-....7.....7..... ..`?g_Encry|-... 8.....8..... ..`?g_Encry.....P8..0...<8..... ..`?g_Encry.-....8.....l8..... ..`.rdata.....8.....8.....@..@.data.....A.....A.....@....pdata..4|....B..~...BB.....@..@.rsrc....+....D..,....C.....@..@.reloc. ..n...@D..n....C.....@..B.....

C:\Users\user\AppData\Local\dfAZPUGwQ\WINSTA.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1380352
Entropy (8bit):	5.021595856508205
Encrypted:	false
SSDEEP:	12288:plORVEAueQmTmQKO2nMlqVaSEwzH7YxiCyJ86azEZy1f11pNx:vORVEVNmaDznMlqVNE27dJ8J2inNx
MD5:	1367EA1D2FB80856D934FC85D5BC1CA3
SHA1:	D32840D9585DC3912CBCDA2ED5B2CD1749EA6F90
SHA-256:	978D7EF5411593FD8A52C4E7139E13BB6F514AFE59D1CE3A51067E8D65959FB4
SHA-512:	B366F6120651CBC4E0F3AC585825D74710C01D3D7EE58F641201383DC2CA6FB6C68B9D06A3880F2FBF2170DD0B07CA8BFF860FC8283629A7B329DC077F2B2F1C
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...z.v^....."..... .....*.....@.....`.....m...x...x.....0..8.....0.....text..... .. ..... ..`.rdata..._...0...`...0.....@..@.data....*.....0.....@....pdata..D.....@..@.rsrc.....@..@.reloc.....@..B .cwkw.....@..@.pbpwn..tQ.....`.....@..@.pem....

C:\Users\user\AppData\Local\dfAZPUGwQ\consent.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	157080
Entropy (8bit):	5.924344092826888
Encrypted:	false
SSDEEP:	3072:4eana1Hze2vHL+u5F28BrciRXBis72z5B+o:Aa1TfD+u5F2wrTio2z2o
MD5:	74D31E4F51873160D91B1F80E0C472D0
SHA1:	35DEC0D1A12C6F1F7A460E3AE75E4D74D5BD815A
SHA-256:	113813A699063EBF391D436A4EFE0B6F95F81E12AF773FABE5511B5CA08E189C
SHA-512:	F026CBBDF3792A05091B3CC0A97F825D353BC5FF9AB7248F4544B81BA2F86FD28CEB04468D755715BB3BD220BB72781DC079423D912A56E3793AC1687AEE7E0 5
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Y_GE.>)..>)..>)..F..Y>).rZ*..>).rZ-..>).rZ,..>).rZ(..>)..>(.9?).rZ'..>). rZ...>).rZ+..>).Rich.>).....PE..d...i.7.....".....H.....C.....@..... .....PP..\.....h....D...!.....0%..T..... .....(...(...HL.....text..... ..`.rdata...c.....d.....@..@.data...l.....h.....@....pdata..h.....j.....@..@.didat. .....x.....@...consent.b.....z.....@....rsrc.....|.....@..@.reloc.....B.....@..B.....

C:\Users\user\AppData\Local\oudoiG\DWWIN.EXE

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	210944
Entropy (8bit):	6.120150246944804
Encrypted:	false
SSDEEP:	6144:JXatPVkbIwsNIUwrMWzp3jRiVbsBwnNCm:KacJNmYWzri9I8Y
MD5:	3C21F944D5FF44E45BC753919F6AE445
SHA1:	47D86DB63905203837FEDFF006C20E0717716160
SHA-256:	2952F67C8882C9B1FAF0425C2047613EA147EBE6BE610B174A627B760B5C59F3
SHA-512:	03965F1952AC90D43E579A9ACEC01290134949438C1525B3A3170DC998336C7F20F5650AE27BB428E6ED77810756438CB35D9CDD6B4FB4AF26A332EB8DC2397
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....I.%.(.v.(.v.(.v.PDv.(.v.L.w.(.v.L.w.(.v.(.v.).v.L.w.(.v.L.w.(.v.L.w.(.v .L(v.(.v.L.w.(.vRich.(.v.....PE..d... -.=.....".....F.....@.....@.....R....`..... .....p.....@.....(...0...T..... Ph..(...Pg.....xh..`...D.....text....E.....F..... ..`.rdata.....`.....J.....@..@.data..... .....@....pdata.....@.....@..@.did at..@...`.....&.....@....rsrc.....p.....(.....@..@.reloc..(.....4.....@..B.....

C:\Users\user\AppData\Local\oudoiG\VERSION.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1376256
Entropy (8bit):	5.002940406932
Encrypted:	false
SSDEEP:	12288:+lORVEAueQmTmQKO2nMlqVaSEwzH7YxiCyJ86azEZy1f11pNx:CORVEVNmaDznMlqVNE27dJ8J2inNx
MD5:	6A433E0692F93D6EA886128CA048DC76
SHA1:	C2583C249530B63023F3BFD1014B2E21FBFD210B
SHA-256:	7071CEB809E1259B9B7A9EE26059CFFB695597C2554A933DFF933571331CF22E
SHA-512:	520B41951D6E2459B34D69C1C81CFE420EF0D856A34A83573CE54C9F3F208D9AC9D941719C6DD1825E558601FFB8E497B532C79FFB37B118689C34AEC5D4C90
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...z.v^....." ....*.....@.....`.....+...x...x.....0..8.....0.....text..... .. ..... ..`.rdata...._...0...`...0.....@..@.data....*.....0.....@....pdata..D.....@..@.rsrc.....@..@.reloc.....@..B .cwkw.....@..@.pbpwn..tQ.....`.....@..@.pem....

C:\Users\user\AppData\Local\s8hTTPzEx\DUI70.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1658880
Entropy (8bit):	5.4487843616720495
Encrypted:	false
SSDEEP:	12288:llORVEAueQmTmQKO2nMlqVaSEwzH7YxiCyJ86azEZy1f11pNx7BK:bORVEVNmaDznMlqVNE27dJ8J2inNx7
MD5:	90CAFAE897080913A8CC42EDD70F1EDD
SHA1:	2CB8E96190567E28223890A7D64D00CEE9DCC202
SHA-256:	3050C8CB5530EF03B66A8D89CC9BE9B83060290FC7B1ADC266AA38E036C566EC
SHA-512:	3665BCE424F86F8CC3AB7E8E1C07A8CC65F5C78C445BB0CB89997A2C3B9190F57CD1489679EDCB312CF992D847D01E0208587A15E1DF9278EFA8E22B82677F6
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...z.v^....." .... *.....@.....P.....`.....dQ..x...x.....0..8.....0.....text..... .. ..... ..`.rdata...._...0...`...0.....@..@.data....*.....0.....@....pdata..D.....@..@.rsrc.....@..@.reloc.....@..B .cwkw.....@..@.pbpwn..tQ.....`.....@..@.pem....

C:\Users\user\AppData\Local\s8hTTPzEx\SysResetErr.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	42392
Entropy (8bit):	5.943178981884173
Encrypted:	false
SSDEEP:	768:zYVfzVTBuXwMHhrdXbsxoXF8Q0no8pV1Pxo:CfuXXrdrXXD0no8xPxo
MD5:	6A3F2F3C36FE45A87E3BFA80B6D92E07
SHA1:	8C211767AD8393F9F184FC926FE3B8913F414289
SHA-256:	069608FF0FF5918681A80CF7603275DC6CD7D416A73D033D19962B0F0F1E1EAC
SHA-512:	A75669E0481901FC7CFCA55FBC7BD7FC0E8636767537017A41B1C720F34B5AD45AC75555D0AD246AC0DF670FDC31CBA1BEFD21D63E112AD427472DE3EA59CA6
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%7..aV..aV..aV..h.S.cV...2..cV...2..vV...2..kV...2..tV..aV...V...2..oV...2?.`V...2..`V..RichaV.....PE..d...v.+J.....".....6...X.....9.....@.....I..... .....!.....,...0t..T..... .....`d..(...`c.....d..`.....text...{4.....6..... ..`.imrsiv.....P.....rdata.....`...0...`.....@..@.data...h.....j.....@....pdata .....n.....@..@.rsrc.....t.....@..@.reloc..,.....@..B..... .....

C:\Users\user\AppData\Local\y1c6p\VERSION.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1376256
Entropy (8bit):	5.00289604284856
Encrypted:	false
SSDEEP:	12288:glORVEAueQmTmQKO2nMlqVaSEwzH7YxiCyJ86azEZy1f11pNx:UORVEVNmaDznMlqVNE27dJ8J2inNx
MD5:	9491BB6F5E9F7443CD95617BA713E9AF
SHA1:	E322CBCD1F7789DFF816E1398FCE97925AF34937
SHA-256:	23FA64118E9250A0F0D225A813E5895D0A2260B0D0E8188A54F0EC487BA28C9F
SHA-512:	9DB6159FF7F4834570F7E6CB5F5F25150C3C1834C859220C9ABA13D53499EDFEA9593DF0EAFA9C2D72D56EB24F62AFB4584F8491D2E1A5ECA654C103070CDE2
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.;...tqb.Rich.qb.....PE..d...z.v^....." ....*.....@.....`.....+...x...x.....0..8.....0.....text..... .. ..... ..`.rdata...._...0...`...0.....@..@.data....*.....0.....@....pdata..D.....@..@.rsrc.....@..@.reloc.....@..B .cwkw.....@..@.pbpwn..tQ.....`.....@..@.pem....

C:\Users\user\AppData\Local\y1c6p\cmstp.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows

Category:	dropped
Size (bytes):	92672
Entropy (8bit):	5.749238064237604
Encrypted:	false
SSDEEP:	1536:7olXq0f2yF9sDb/RjxgnvkmVUqAVnKUMjbWg+I/87BM/Z4j8Qi1Yv9V:0Izw/RooolWlk7BM/ZNQi1EV
MD5:	2A9828E0C405422D166E0141054A04B3
SHA1:	84AA48946D4F9A9DFE4C1AF6F96C44B643229A73
SHA-256:	94152FB98573FE31C0CE49D260D760DD173741D663414DE718A37AAC7E8EF11F
SHA-512:	B9B0472706C11D3AECDAB055D4CF319EDD50E8C97B7099D1DC7B768812E804975392E327A1E62301077AB92C1CA97E706628B07172892AB09753FBDD9A07277
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....I....X...X...X...Y...X...Y...X...Y...X...Y...X...XQ..X...Y...X...X...X ...Y...XRich...X.....PE..d....mg.....".....@.....`..... .....M.....p.....X....B..T..... .....H.....text..... ..`.rdata..".l.....n.....@..@.data.....`.....R.....@....pdata.....p.....T.....@..@.rsrc..... .....Z.....@..@.reloc..X.....h.....@..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):	7.3483724297376805
Encrypted:	false
SSDEEP:	24:U+zDBW7TtU5LZ0Ezzo0VOb2T82x+wgNK5tb9H9aV4++kKI77oZBZtxUxsw:UADgTtU70E7L82xZHH2z+kKI7qUxN
MD5:	86C68B8FD1449527DE2236FF9203D1A8
SHA1:	5678A470E16DE0815D29B463CD32B31FEEB97013
SHA-256:	A6F04F4EEFBE8055640DF7FD0EFCA410663F76AA9D746EC32A9BAF1A24F76BC0
SHA-512:	97DCBAA0FFF2F31CC55095891F6B02FDA48E2F8E50B4BFD79E0F60715BD6689F45AC48025BA4512F396ECBD4E3D816169C07E8E9364158135D17548E0BDB938B
Malicious:	false
Preview:	.....user.....RSA1.....m.....#....x.<K.6..Wt.KJ...{@{\.!....?...#..(Z.`.OPD":.A.`%./I....QI.p....?.|<A"$F8....v~.B.A....f.q....1...8..,K6..(O..... .....z..O.....C.^*.....,...C.r.y.p.t.o.A.P.I. .P.r.i.v.a.t.e. .K.e.y....f..... ...da...\|.y....[..nh.R...8.... E..... ...w.tC..()....'x..>... .....^..F.....\.E.Q.g....."..m.B.q. <\|...p..<..9....2X.j.u.0i...y.r.../...?O....J...w....p-P{.Y.au...`..._-f...d.n3BY...TS^....g.1.....N...c....W.....'.....B...g...IS.....9F.....O...z.m....(;^...\|....U.....;."..)..r%..".i....V...._.p..... ....=e..._.b.H.W.VN..D.9....S.....n.....=O}.N..).S..6.Wj.U..d.0...T^ fGy....n..R.....Z....z.Y$....Y(X..|.>..+dK,F.k..%4..@...E.~....(....v.A...9.....a..[...{Y...&.....:...wH._.3.3.3$YR-n.$aA.3.....G;..uT",d.....z...7mz.....ru.y...>....X.K..y.R.*^...>....u|&~Y8..*.x..bP.....I.....5.'.

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	5.013513255725167
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:	dry.dll
File size:	1372160
MD5:	4bec705de3584b911018c84f31659a17
SHA1:	b29ff37578ef950b702ec5db59161294c2e1a7b3
SHA256:	13aa6bed5b3a656b9c86cc2d397f765779f4a7dff49f73d58bd97e11423e0635
SHA512:	5841f5d288fa4496391fa008326d15ac9abc644c07bf970b20fd1ed2719d5ce01c457d84d17fc8025ff801d7aaec371ee2b6504cabab853d02fb6c1ad49ec423
SSDEEP:	12288:6lORVEAueQmTmQKO2nMlqVaSEwzH7YxiCyJ86azEZy1f11pNx:uORVEVNmaDznMlqVNE27dJ8J2inNx
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:	0x140042ad0
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:	0x5E76817A [Sat Mar 21 21:04:58 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:	a272733471032e2064bf69c66a9c775a

Entrypoint Preview

Instruction
dec eax
mov dword ptr [0006E699h], ecx
dec eax
lea ecx, dword ptr [FFFFEA62h]
dec esp
mov dword ptr [0006E6ABh], eax
dec esp
mov dword ptr [0006E6B4h], edi
dec esp
mov eax, esi
dec eax
mov dword ptr [0006E6B2h], eax
dec eax
mov eax, 00001204h
dec eax
add ecx, eax
dec esp
mov dword ptr [0006E6B1h], esp
dec eax
sub ecx, 00001204h
dec eax
mov dword ptr [0006E6ABh], esi
dec eax
test eax, eax
je 00007F28489BF6D0h
dec eax
mov eax, ecx
dec eax
mov dword ptr [0006E664h], esp
dec eax
mov dword ptr [0006E655h], ebp
dec eax
mov dword ptr [0006E69Eh], ebx
dec eax
mov dword ptr [0006E68Fh], edi

Instruction
dec eax
test eax, eax
je 00007F28489BF6ACh
dec esp
mov dword ptr [0006E653h], ecx
dec esp
mov dword ptr [0006E664h], ebp
dec eax
mov dword ptr [0006E625h], edx
jmp eax
dec eax
add edi, ecx
retn 0008h
ud2
int3
int3
int3
push esi
dec eax
sub esp, 70h
dec eax
lea eax, dword ptr [FFFF9F34h]
dec eax
mov edx, dword ptr [esp+60h]
dec ecx
mov eax, edx
dec ecx
and eax, 7C240CB9h
dec esp
mov dword ptr [esp+60h], eax
dec eax
mov dword ptr [esp+50h], 0B39C477h
dec ecx
mov eax, edx
dec ecx
xor eax, FFFFFFFFh
dec esp
mov dword ptr [esp+60h], eax
mov word ptr [eax+eax+00h], 0000h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0xa8dd7	0x12e	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa8578	0x78	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbd000	0x3d8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x1000	0x0	.text
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xbe000	0xdfc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x430b0	0x38	.rdata
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	
IMAGE_DIRECTORY_ENTRY_IAT	0x43000	0xa8	.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	0x41ebf	0x42000	False	0.781523733428	data	7.76153125253	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x43000	0x65f05	0x66000	False	0.697476256127	data	7.85586414334	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa9000	0x12a18	0x13000	False	0.0770841899671	data	2.46325796792	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0xbc000	0x144	0x1000	False	0.062744140625	data	0.615463451963	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0xbd000	0x7af	0x1000	False	0.117919921875	data	1.08794585954	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xbe000	0xdfc	0x1000	False	0.39990234375	data	5.20528905542	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.cwkw	0xbf000	0xbf6	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pbpwn	0xc0000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pem	0x106000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vpd	0x107000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ianurq	0x109000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xbd0a0	0x2dc	data	English	United States
RT_MANIFEST	0xbd380	0x56	ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
SHLWAPI.dll	ChrCmpIW, UrlIsOpaqueW
GDI32.dll	GetPolyFillMode, CreateBitmapIndirect
USER32.dll	WaitForInputIdle, GetFocus, GetParent, LookupIconIdFromDirectoryEx
ADVAPI32.dll	GetServiceDisplayNameW
KERNEL32.dll	HeapUnlock, TerminateJobObject, DeleteTimerQueue, GetNamedPipeServerProcessId, GetConsoleFontSize, GetFileInformationByHandle, GetThreadLocale

Exports

Name	Ordinal	Address
CreateXmlReader	1	0x140034b28
CreateXmlReaderInputWithEncodingCodePage	2	0x140005f28
CreateXmlReaderInputWithEncodingName	3	0x1400203d0
CreateXmlWriter	4	0x140037b74
CreateXmlWriterOutputWithEncodingCodePage	5	0x140015b64
CreateXmlWriterOutputWithEncodingName	6	0x14001f778

Version Infos

Description	Data
LegalCopyright	Copyright 2005-2007 Mark Russinovich
InternalName	streams
FileVersion	1.56
CompanyName	Sysinternals
ProductName	Sysinternals Streams
ProductVersion	1.56
FileDescription	streams
OriginalFilename	streams.exe
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/20/22-08:22:03.280642	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.1	192.168.2.3

UDP Packets

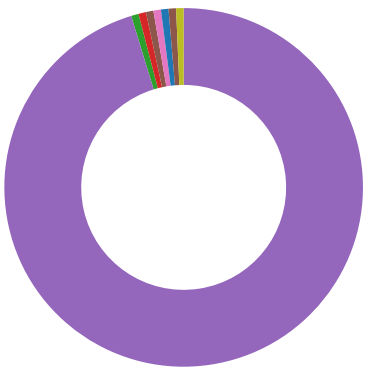
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 20, 2022 08:22:56.190840960 CET	56176	53	192.168.2.3	8.8.8.8
Feb 20, 2022 08:22:57.182591915 CET	56176	53	192.168.2.3	8.8.8.8
Feb 20, 2022 08:22:58.182760000 CET	56176	53	192.168.2.3	8.8.8.8
Feb 20, 2022 08:23:00.198551893 CET	56176	53	192.168.2.3	8.8.8.8
Feb 20, 2022 08:23:04.214570999 CET	56176	53	192.168.2.3	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 20, 2022 08:22:56.190840960 CET	192.168.2.3	8.8.8.8	0x95f5	Standard query (0)	canonicalizer.ucsuri.tcs	A (IP address)	IN (0x0001)
Feb 20, 2022 08:22:57.182591915 CET	192.168.2.3	8.8.8.8	0x95f5	Standard query (0)	canonicalizer.ucsuri.tcs	A (IP address)	IN (0x0001)
Feb 20, 2022 08:22:58.182760000 CET	192.168.2.3	8.8.8.8	0x95f5	Standard query (0)	canonicalizer.ucsuri.tcs	A (IP address)	IN (0x0001)
Feb 20, 2022 08:23:00.198551893 CET	192.168.2.3	8.8.8.8	0x95f5	Standard query (0)	canonicalizer.ucsuri.tcs	A (IP address)	IN (0x0001)
Feb 20, 2022 08:23:04.214570999 CET	192.168.2.3	8.8.8.8	0x95f5	Standard query (0)	canonicalizer.ucsuri.tcs	A (IP address)	IN (0x0001)

Statistics

Behavior



SndVol.exe

Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: **6572**, Parent PID: **5416**

General

Target ID:	0
Start time:	08:20:05
Start date:	20/02/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\dry.dll"
Imagebase:	0x7ff7d9bf0000
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: 00000000.00000002.311387870.00007FFC68291000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: crime_win64_dridex_bot_hook, Description: Detects latest Dridex bot hook, Source: 00000000.00000002.311387870.00007FFC68291000.00000020.00000001.01000000.00000003.sdmp, Author: @VK_Intel
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: **6612**, Parent PID: **6572**

General

Target ID:	1
Start time:	08:20:05
Start date:	20/02/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\dry.dll",#1
Imagebase:	0x7ff6b94e0000
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: **5792**, Parent PID: **6572**

General

Target ID:	3
Start time:	08:20:05
Start date:	20/02/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\dry.dll,CreateXmlReader
Imagebase:	0x7ff694030000
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: 00000003.00000002.366937086.00007FFC68291000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: crime_win64_dridex_bot_hook, Description: Detects latest Dridex bot hook, Source: 00000003.00000002.366937086.00007FFC68291000.00000020.00000001.01000000.00000003.sdmp, Author: @VK_Intel
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\dry.dll	unknown	1372160	success or wait	1	7FFC682EE7A6	ReadFile

Analysis Process: rundll32.exe PID: **4484**, Parent PID: **6612**

General

Target ID:	4
Start time:	08:20:06
Start date:	20/02/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\dry.dll",#1
Imagebase:	0x7ff694030000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000004.00000002.289927845.00007FFC68291000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: crime_win64_dridex_bot_hook, Description: Detects latest Dridex bot hook, Source: 00000004.00000002.289927845.00007FFC68291000.00000020.00000001.01000000.00000003.sdmp, Author: @VK_Intel
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\dry.dll	unknown	1372160	success or wait	1	7FFC682EE7A6	ReadFile

Analysis Process: explorer.exe PID: **3352**, Parent PID: **5792**

General

Target ID:	5

Start time:	08:20:07
Start date:	20/02/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff720ea0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\UserData\ZkpzbsG7v	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005E1C5	CreateDirectoryW
C:\Users\user\AppData\Local\DLKXiO\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005E1C5	CreateDirectoryW
C:\Users\user\AppData\Local\DLKXiO\WMsgAPI.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005E59E	CreateFileW
C:\Users\user\AppData\Local\DLKXiO\consent.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005E59E	CreateFileW
C:\Users\user\AppData\Local\s8hTTPzEx\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005E1C5	CreateDirectoryW
C:\Users\user\AppData\Local\s8hTTPzEx\DUI70.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005E59E	CreateFileW
C:\Users\user\AppData\Local\s8hTTPzEx\SysResetErr.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005E59E	CreateFileW
C:\Users\user\AppData\Local\dfAZPUGwQ\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005E1C5	CreateDirectoryW
C:\Users\user\AppData\Local\dfAZPUGwQ\WINSTA.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005E59E	CreateFileW
C:\Users\user\AppData\Local\dfAZPUGwQ\consent.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005E59E	CreateFileW
C:\Users\user\AppData\Local\y1c6p\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005E1C5	CreateDirectoryW
C:\Users\user\AppData\Local\y1c6p\VERSION.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005E59E	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\y1c6p\cmstp.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005E59E	CreateFileW
C:\Users\user\AppData\Local\oudoiG\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005E1C5	CreateDirectoryW
C:\Users\user\AppData\Local\oudoiG\VERSION.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005E59E	CreateFileW
C:\Users\user\AppData\Local\oudoiG\DWWIN.EXE	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005E59E	CreateFileW
C:\Users\user\AppData\Local\GsjW\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005E1C5	CreateDirectoryW
C:\Users\user\AppData\Local\GsjW\XmlLite.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005E59E	CreateFileW
C:\Users\user\AppData\Local\GsjW\sppsvc.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005E59E	CreateFileW
C:\Users\user\AppData\Local\0rPbJb\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005E1C5	CreateDirectoryW
C:\Users\user\AppData\Local\0rPbJb\UxTheme.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005E59E	CreateFileW
C:\Users\user\AppData\Local\0rPbJb\SndVol.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005E59E	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DLKXiO\consent.exe	success or wait	1	14005EA40	DeleteFileW
C:\Users\user\AppData\Local\DLKXiO\WMsgAPI.dll	success or wait	1	14005EA40	DeleteFileW
C:\Users\user\AppData\Local\s8hTTPzEx\DUI70.dll	cannot delete	8	14005EA40	DeleteFileW
C:\Users\user\AppData\Local\s8hTTPzEx\SysResetErr.exe	cannot delete	8	14005EA40	DeleteFileW
C:\Users\user\AppData\Local\s8hTTPzEx\DUI70.dll	success or wait	1	14005EA40	DeleteFileW
C:\Users\user\AppData\Local\s8hTTPzEx\SysResetErr.exe	success or wait	1	14005EA40	DeleteFileW
C:\Users\user\AppData\Local\dfAZPUGwQ\consent.exe	success or wait	1	14005EA40	DeleteFileW
C:\Users\user\AppData\Local\dfAZPUGwQ\WINSTA.dll	success or wait	1	14005EA40	DeleteFileW
C:\Users\user\AppData\Local\y1c6p\cmstp.exe	cannot delete	5	14005EA40	DeleteFileW
C:\Users\user\AppData\Local\y1c6p\VERSION.dll	cannot delete	5	14005EA40	DeleteFileW
C:\Users\user\AppData\Local\y1c6p\cmstp.exe	success or wait	1	14005EA40	DeleteFileW
C:\Users\user\AppData\Local\y1c6p\VERSION.dll	success or wait	1	14005EA40	DeleteFileW
C:\Users\user\AppData\Local\oudoiG\DWWIN.EXE	cannot delete	7	14005EA40	DeleteFileW
C:\Users\user\AppData\Local\oudoiG\VERSION.dll	cannot delete	7	14005EA40	DeleteFileW
C:\Users\user\AppData\Local\oudoiG\DWWIN.EXE	success or wait	1	14005EA40	DeleteFileW
C:\Users\user\AppData\Local\oudoiG\VERSION.dll	success or wait	1	14005EA40	DeleteFileW
unknown	cannot delete	9	14005EA40	DeleteFileW
unknown	cannot delete	9	14005EA40	DeleteFileW
unknown	success or wait	1	14005EA40	DeleteFileW
unknown	success or wait	1	14005EA40	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\DLKXiO\WMsgAPI.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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	14005E030	WriteFile
C:\Users\user\AppData\Local\DLKXiO\consent.exe	0	157080	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 59 5f 47 45 1d 3e 29 16 1d 3e 29 16 1d 3e 29 16 14 46 fd 16 59 3e 29 16 72 5a 2a 17 1e 3e 29 16 72 5a 2d 17 05 3e 29 16 72 5a 2c 17 15 3e 29 16 72 5a 28 17 0a 3e 29 16 1d 3e 28 16 39 3f 29 16 72 5a 27 17 10 3e 29 16 72 5a fd 16 1c 3e 29 16 72 5a 2b 17 1c 3e 29 16 52 69 63 68 1d 3e 29 16 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 08 00 69 fd 37 00 00 00	MZ@!L!This program cannot be run in DOS mode.$Y_GE>)>)>)FY>) rZ*>)rZ->)rZ,>)rZ(>)> (9?)rZ'>) rZ>)rZ+>)Rich>)PEdi7	success or wait	1	14005E030	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\s8hTTPzEx\DUI70.dll	0	1658880	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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(cqb;,qb/TqbZqbqbzBqbnqb[qbqb;{qbqb	success or wait	1	14005E030	WriteFile
C:\Users\user\AppData\Local\s8hTTPzEx\SysResetErr.exe	0	42392	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 25 37 fd fd 61 56 fd fd 61 56 fd fd 61 56 fd fd 68 2e 53 fd 63 56 fd fd 0e 32 fd fd 63 56 fd fd 0e 32 fd fd 76 56 fd fd 0e 32 fd fd 6b 56 fd fd 0e 32 fd fd 74 56 fd fd 61 56 fd fd fd 56 fd fd 0e 32 fd fd 6f 56 fd fd 0e 32 3f fd 60 56 fd fd 0e 32 fd fd 60 56 fd fd 52 69 63 68 61 56 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 07 00 76 fd 2b 4a 00 00 00	MZ@!L!This program cannot be run in DOS mode.$%7aVaVaVh.ScV2cV2vV2kV2tVaVV2oV2?`V2`VRichaVPEdv+J	success or wait	1	14005E030	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\dfAZPUGwQ\WINSTA.dll	0	1380352	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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(cqb;,qb/TqbZqbqbzBqbnqb[qbqb;{qbqb	success or wait	1	14005E030	WriteFile
C:\Users\user\AppData\Local\dfAZPUGwQ\consent.exe	0	157080	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 59 5f 47 45 1d 3e 29 16 1d 3e 29 16 1d 3e 29 16 14 46 fd 16 59 3e 29 16 72 5a 2a 17 1e 3e 29 16 72 5a 2d 17 05 3e 29 16 72 5a 2c 17 15 3e 29 16 72 5a 28 17 0a 3e 29 16 1d 3e 28 16 39 3f 29 16 72 5a 27 17 10 3e 29 16 72 5a fd 16 1c 3e 29 16 72 5a 2b 17 1c 3e 29 16 52 69 63 68 1d 3e 29 16 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 08 00 69 fd 37 00 00 00	MZ@!L!This program cannot be run in DOS mode.$Y_GE>)>)>)FY>)rZ*>)rZ->)rZ,>)rZ(>)>(9?)rZ'>)rZ>)rZ+>)Rich>)PEdi7	success or wait	1	14005E030	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\y1c6p\VERSION.dll	0	1376256	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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(cqb;,qb/ TqbZqbqbzBqbnqb[qbqb;{qbqb	success or wait	1	14005E030	WriteFile
C:\Users\user\AppData\Local\y1c6p\cmstp.exe	0	92672	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 fd fd 6c 0b fd fd 02 58 fd fd 02 58 fd fd 02 58 fd fd 07 59 fd fd 02 58 fd fd 01 59 fd fd 02 58 fd fd 06 59 fd fd 02 58 fd fd 03 59 fd fd 02 58 fd fd 03 58 51 fd 02 58 fd fd 0b 59 fd fd 02 58 fd fd fd 58 fd fd 02 58 fd fd 00 59 fd fd 02 58 52 69 63 68 fd fd 02 58 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06 00 1b 6d 67 fd 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$lXXXYXYXYXYXXQ XYXXXYXRichXPEdmg"	success or wait	1	14005E030	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\oudoiG\VERSION.dll	0	1376256	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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(cqb;,qb/ TqbZqbqbzBqbnqb[qbqb;{qbqb	success or wait	1	14005E030	WriteFile
C:\Users\user\AppData\Local\oudoiG\DWWIN.EXE	0	210944	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 fd 49 fd 25 fd 28 fd 76 fd 28 fd 76 fd 28 fd 76 fd 50 44 76 fd 28 fd 76 fd 4c fd 77 fd 28 fd 76 fd 4c fd 77 fd 28 fd 76 fd 28 fd 76 00 29 fd 76 fd 4c fd 77 fd 28 fd 76 fd 4c fd 77 fd 28 fd 76 fd 4c fd 77 fd 28 fd 76 fd 4c 28 76 fd 28 fd 76 fd 4c fd 77 fd 28 fd 76 52 69 63 68 fd 28 fd 76 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 07 00 20 2d fd 3d 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$I%(v(v(vPDv(vLw(vLw(v(v)vLw(vLw(vLw(vL(v(vLw(vRich(vPEd -="	success or wait	1	14005E030	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\GsjW\XmlLite.dll	0	1376256	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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(cqb;,qb/ TqbZqbqbzBqbnqb[qbqb;{qbqb	success or wait	1	14005E030	WriteFile
C:\Users\user\AppData\Local\GsjW\sppsvc.exe	0	4527680	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 fd fd 2d fd fd 43 fd fd 43 fd fd 43 fd fd fd 40 fd fd 43 fd fd fd fd fd fd fd 43 fd fd fd 47 fd fd fd 43 fd fd fd 46 fd fd 43 fd fd fd fd 42 fd fd fd 43 fd fd 42 fd fd fd 43 fd fd fd 4a fd 0d fd 43 fd fd fd 40 fd fd 43 fd fd fd fd fd 43 fd fd fd 41 fd fd 43 fd 52 69 63 68 fd 43 fd 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 0a 00 41 fd 4c 63 00 00 00	MZ@!L!This program cannot be run in DOS mode.$- CCC@CCGCFCBCBCJC@CCACRichCPEdALc	success or wait	1	14005E030	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\0rPbJb\UxTheme.dll	0	1376256	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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(cqb;,qb/TqbZqbqbzBqbnqb[qbqb;{qbqb	success or wait	1	14005E030	WriteFile
C:\Users\user\AppData\Local\0rPbJb\SndVol.exe	0	259904	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 08 3c fd 42 4c 5d fd 11 4c 5d fd 11 4c 5d fd 11 45 25 07 11 08 5d fd 11 23 39 fd 10 4f 5d fd 11 23 39 fd 10 55 5d fd 11 23 39 fd 10 46 5d fd 11 23 39 fd 10 57 5d fd 11 4c 5d fd 11 fd 5c fd 11 23 39 fd 10 6f 5d fd 11 23 39 6b 11 4d 5d fd 11 23 39 fd 10 4d 5d fd 11 52 69 63 68 4c 5d fd 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 08	MZ@!L!This program cannot be run in DOS mode.$<BL]L]L]E%]#9O]#9U]#9F]#9W]L]\#9o]#9kM]#9M]RichL]PEd	success or wait	1	14005E030	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\TieringEngineService.exe	unknown	303616	success or wait	1	14005E7A6	ReadFile
C:\Windows\System32\cipher.exe	unknown	46080	success or wait	1	14005E7A6	ReadFile
C:\Windows\System32\msfeedssync.exe	unknown	15360	success or wait	1	14005E7A6	ReadFile
C:\Windows\System32\setspn.exe	unknown	29184	success or wait	1	14005E7A6	ReadFile
C:\Windows\System32\SystemUWPLauncher.exe	unknown	75264	success or wait	1	14005E7A6	ReadFile
C:\Windows\System32\RpcPing.exe	unknown	30208	success or wait	1	14005E7A6	ReadFile
C:\Windows\System32\UevTemplateBaselineGenerator.exe	unknown	13824	success or wait	1	14005E7A6	ReadFile
C:\Windows\System32\consent.exe	unknown	157080	success or wait	4	14005E7A6	ReadFile
C:\Windows\System32\wmsgapi.dll	unknown	18944	success or wait	1	14005E7A6	ReadFile
C:\Windows\System32\sort.exe	unknown	27136	success or wait	1	14005E7A6	ReadFile
C:\Windows\System32\xbgmsvc.exe	unknown	59512	success or wait	1	14005E7A6	ReadFile
C:\Windows\System32\fixmapi.exe	unknown	20992	success or wait	1	14005E7A6	ReadFile
C:\Windows\System32\browserexport.exe	unknown	342528	success or wait	1	14005E7A6	ReadFile
C:\Windows\System32\UsoClient.exe	unknown	40960	success or wait	1	14005E7A6	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\chkdsk.exe	unknown	25088	success or wait	1	14005E7A6	ReadFile
C:\Windows\System32\SysResetErr.exe	unknown	42392	success or wait	3	14005E7A6	ReadFile
C:\Windows\System32\dui70.dll	unknown	1719808	success or wait	1	14005E7A6	ReadFile
C:\Windows\System32\dwm.exe	unknown	62464	success or wait	1	14005E7A6	ReadFile
C:\Windows\System32\appidcertstorecheck.exe	unknown	19456	success or wait	1	14005E7A6	ReadFile
C:\Windows\System32\ARP.EXE	unknown	25600	success or wait	1	14005E7A6	ReadFile
C:\Windows\System32\winsta.dll	unknown	332712	success or wait	1	14005E7A6	ReadFile
C:\Windows\System32\bthudtask.exe	unknown	40448	success or wait	1	14005E7A6	ReadFile
C:\Windows\System32\wsmprovhost.exe	unknown	37888	success or wait	1	14005E7A6	ReadFile
C:\Windows\System32\fontdrvhost.exe	unknown	790304	success or wait	1	14005E7A6	ReadFile
C:\Windows\System32\fsquirt.exe	unknown	141824	success or wait	1	14005E7A6	ReadFile
C:\Windows\System32\SystemSettingsBroker.exe	unknown	213392	success or wait	1	14005E7A6	ReadFile
C:\Windows\System32\subst.exe	unknown	16384	success or wait	1	14005E7A6	ReadFile
C:\Windows\System32\logagent.exe	unknown	101376	success or wait	1	14005E7A6	ReadFile
C:\Windows\System32\PnPUnattend.exe	unknown	59392	success or wait	2	14005E7A6	ReadFile
C:\Windows\System32\MDMAgent.exe	unknown	109056	success or wait	1	14005E7A6	ReadFile
C:\Windows\System32\rdpshell.exe	unknown	463872	success or wait	2	14005E7A6	ReadFile
C:\Windows\System32\PATHPING.EXE	unknown	19456	success or wait	1	14005E7A6	ReadFile
C:\Windows\System32\bootsect.exe	unknown	107416	success or wait	1	14005E7A6	ReadFile
C:\Windows\System32\cmstp.exe	unknown	92672	success or wait	2	14005E7A6	ReadFile
C:\Windows\System32\version.dll	unknown	30568	success or wait	2	14005E7A6	ReadFile
C:\Windows\System32\RMActivate_ssp_isv.exe	unknown	493568	success or wait	1	14005E7A6	ReadFile
C:\Windows\System32\SystemPropertiesComputerName.exe	unknown	83968	success or wait	2	14005E7A6	ReadFile
C:\Windows\System32\DWWIN.EXE	unknown	210944	success or wait	3	14005E7A6	ReadFile
C:\Windows\System32\Microsoft.Uev.CscUnpinTool.exe	unknown	406528	success or wait	1	14005E7A6	ReadFile
C:\Windows\System32\provlaunch.exe	unknown	60416	success or wait	1	14005E7A6	ReadFile
C:\Windows\System32\SystemPropertiesDataExecutionPrevention.exe	unknown	83968	success or wait	2	14005E7A6	ReadFile
C:\Windows\System32\dmclient.exe	unknown	102400	success or wait	2	14005E7A6	ReadFile
C:\Windows\System32\odbcconf.exe	unknown	25600	success or wait	1	14005E7A6	ReadFile
C:\Windows\System32\sppsvc.exe	unknown	4527680	success or wait	3	14005E7A6	ReadFile
C:\Windows\System32\xmllite.dll	unknown	227840	success or wait	1	14005E7A6	ReadFile
unknown	unknown	259904	success or wait	3	14005E7A6	ReadFile
unknown	unknown	599040	success or wait	1	14005E7A6	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{E5F98B9A-1953-0F82-61FE-67CA0984C627}	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{E5F98B9A-1953-0F82-61FE-67CA0984C627}\ShellFolder	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{F8BC10AE-6BB8-FDD3-5392-C1292E999831}	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{F8BC10AE-6BB8-FDD3-5392-C1292E999831}\ShellFolder	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{45BC36BF-5FCB-D5AA-9795-0FA88B3494FD}	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{45BC36BF-5FCB-D5AA-9795-0FA88B3494FD}\ShellFolder	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{35F2DED5-C2D7-DCFA-4D49-652CED3398F1}	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{35F2DED5-C2D7-DCFA-4D49-652CED3398F1}\ShellFolder	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{F665C9EF-AB6D-9070-F365-E3C99F877B6E}	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{F665C9EF-AB6D-9070-F365-E3C99F877B6E}\ShellFolder	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{E789C7A5-D5E0-6E43-8F71-FF8F1EDF9105}	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{E789C7A5-D5E0-6E43-8F71-FF8F1EDF9105}\ShellFolder	success or wait	1	1400622EA	RegCreateKeyExW

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{CEA58F1C-A97D-1919-11B2-C391DF3F788B}	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{CEA58F1C-A97D-1919-11B2-C391DF3F788B}\ShellFolder	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{863D8378-0246-471A-F9BE-12228B49B479}	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{863D8378-0246-471A-F9BE-12228B49B479}\ShellFolder	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{921DFF8E-2AAA-ADC5-03F3-FC4C9EC46A65}	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{921DFF8E-2AAA-ADC5-03F3-FC4C9EC46A65}\ShellFolder	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{881EC5AE-98FD-739B-72CE-6ED21BD79C2A}	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{881EC5AE-98FD-739B-72CE-6ED21BD79C2A}\ShellFolder	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{4EDF7252-E4F3-A7F5-5EAC-EE8685C8C2AA}	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{4EDF7252-E4F3-A7F5-5EAC-EE8685C8C2AA}\ShellFolder	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{64BDA516-D47D-7F0D-2467-407E19DB9C57}	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{64BDA516-D47D-7F0D-2467-407E19DB9C57}\ShellFolder	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{D94FC15A-8E82-173C-8CDE-EF67E5F3A970}	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{D94FC15A-8E82-173C-8CDE-EF67E5F3A970}\ShellFolder	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{E96777C5-586E-4375-01B1-1041681B87B6}	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{E96777C5-586E-4375-01B1-1041681B87B6}\ShellFolder	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{4E8BE1BE-4FA3-5B59-D2AC-5B90B2ECC67B}	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{4E8BE1BE-4FA3-5B59-D2AC-5B90B2ECC67B}\ShellFolder	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{9FF0D2C1-4805-90C9-CB4B-8A6C0837F903}	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{9FF0D2C1-4805-90C9-CB4B-8A6C0837F903}\ShellFolder	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{62212A6D-CCE8-B224-2FA6-E6A31FA52EA0}	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{62212A6D-CCE8-B224-2FA6-E6A31FA52EA0}\ShellFolder	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{13FAFB04-4521-EEBD-AFE1-8E4EF26B6020}	success or wait	1	1400622EA	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{13FAFB04-4521-EEBD-AFE1-8E4EF26B6020}\ShellFolder	success or wait	1	1400622EA	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{4EDF7252-E4F3-A7F5-5EAC-EE8685C8C2AA}\ShellFolder	{95A1E1F9-2A88-42FD-5517-DAA93D9F5106}	binary	59 D6 28 8D 8D D9 0C 0B 7F 2E AE 0C 6B 10 CF BC 9A 35 E5 5D B3 0F CE AF 6F 2E BB 0F D8 3A 9C 03 38 6C 09 D4 88 0E 45 B9 1A E1 D5 19 5A B4 24 2C B2 C2 65 A0 63 75 A0 D3 C5 2B 2C 6F 45 54 52 BD A2 D1 2F F2 96 CC 47	success or wait	1	140061350	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{921DFF8E-2AAA-ADC5-03F3-FC4C9EC46A65}\ShellFolder	{D7B8C5EA-741F-4D18-3958-DCE798BC7184}	binary	E0 D4 A5 92 D8 C9 02 25 CB BB DA EF 44 C2 66 C4 2C A8 D7 D9 C6 A8 AC 36 AA 76 0F F7 27 DF 98 D0 32 3C A5 3A 36 88 28 A1 67 D8 80 A7 AC 49 9F 2D AD 4D A9 1A 8C 09 C3 0E C7 7D C6 87 BB 59 DF 6D 03 68 13 FF C6 69 F0 9B 3C 60 EE 45 30 C4 7F E2 0F 0B 64 47 33 E9 20 CD 2C 6B 12 CD	success or wait	1	140061350	RegSetValueExA

Analysis Process: rundll32.exe PID: 568, Parent PID: 6572

General	
Target ID:	6
Start time:	08:20:09
Start date:	20/02/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\dry.dll,CreateXmlReaderInputWithEncodingCodePage
Imagebase:	0x7ff694030000
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: 00000006.00000002.296790826.00007FFC68291000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: crime_win64_dridex_bot_hook, Description: Detects latest Dridex bot hook, Source: 00000006.00000002.296790826.00007FFC68291000.00000020.00000001.01000000.00000003.sdmp, Author: @VK_Intel
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\dry.dll	unknown	1372160	success or wait	1	7FFC682EE7A6	ReadFile

Analysis Process: rundll32.exe PID: **5456**, Parent PID: **6572**

General	
Target ID:	8
Start time:	08:20:12
Start date:	20/02/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\dry.dll,CreateXmlReaderInputWithEncodingName
Imagebase:	0x7ff694030000
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: 00000008.00000002.305054509.00007FFC68291000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: crime_win64_dridex_bot_hook, Description: Detects latest Dridex bot hook, Source: 00000008.00000002.305054509.00007FFC68291000.00000020.00000001.01000000.00000003.sdmp, Author: @VK_Intel
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\dry.dll	unknown	1372160	success or wait	1	7FFC682EE7A6	ReadFile

Analysis Process: consent.exe PID: **4904**, Parent PID: **3352**

General	
Target ID:	12
Start time:	08:20:45
Start date:	20/02/2022
Path:	C:\Windows\System32\consent.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\consent.exe
Imagebase:	0x7ff6b4af0000
File size:	157080 bytes
MD5 hash:	74D31E4F51873160D91B1F80E0C472D0
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: consent.exe PID: **3576**, Parent PID: **3352**

General

Target ID:	13
Start time:	08:20:46
Start date:	20/02/2022
Path:	C:\Users\user\AppData\Local\DLKXiO\consent.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\DLKXiO\consent.exe
Imagebase:	0x7ff679f90000
File size:	157080 bytes
MD5 hash:	74D31E4F51873160D91B1F80E0C472D0
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

Analysis Process: SysResetErr.exe PID: **4676**, Parent PID: **3352**

General

Target ID:	14
Start time:	08:20:47
Start date:	20/02/2022
Path:	C:\Windows\System32\SysResetErr.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SysResetErr.exe
Imagebase:	0x7ff67d350000
File size:	42392 bytes
MD5 hash:	6A3F2F3C36FE45A87E3BFA80B6D92E07
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: SysResetErr.exe PID: **2064**, Parent PID: **3352**

General

Target ID:	15
Start time:	08:20:52
Start date:	20/02/2022
Path:	C:\Users\user\AppData\Local\s8hTTPzEx\SysResetErr.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\s8hTTPzEx\SysResetErr.exe
Imagebase:	0x7ff67a420000

File size:	42392 bytes
MD5 hash:	6A3F2F3C36FE45A87E3BFA80B6D92E07
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: 0000000F.00000002.410915340.00007FFC67DE1000.00000020.00000001.01000000.00000009.sdmp, Author: Joe Security • Rule: crime_win64_dridex_bot_hook, Description: Detects latest Dridex bot hook, Source: 0000000F.00000002.410915340.00007FFC67DE1000.00000020.00000001.01000000.00000009.sdmp, Author: @VK_Intel
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\s8hTTPzEx\DUI70.dll	unknown	1658880	success or wait	1	7FFC67E3E7A6	ReadFile

Analysis Process: consent.exe PID: **6440**, Parent PID: **3352**

General

Target ID:	19
Start time:	08:21:04
Start date:	20/02/2022
Path:	C:\Windows\System32\consent.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\consent.exe
Imagebase:	0x7ff6b4af0000
File size:	157080 bytes
MD5 hash:	74D31E4F51873160D91B1F80E0C472D0
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: consent.exe PID: **4740**, Parent PID: **3352**

General

Target ID:	23
Start time:	08:21:06
Start date:	20/02/2022
Path:	C:\Users\user\AppData\Local\dfAZPUGwQ\consent.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\dfAZPUGwQ\consent.exe
Imagebase:	0x7ff60d120000
File size:	157080 bytes
MD5 hash:	74D31E4F51873160D91B1F80E0C472D0
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

Analysis Process: rdpshell.exe PID: **6520**, Parent PID: **3352**

General

Target ID:	24

Start time:	08:21:07
Start date:	20/02/2022
Path:	C:\Windows\System32\rdpshell.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\rdpshell.exe
Imagebase:	0x7ff7f9220000
File size:	463872 bytes
MD5 hash:	4994A0ADA359924026FE631E54FC7A5D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmstp.exe PID: **4628**, Parent PID: **3352**

General

Target ID:	25
Start time:	08:21:07
Start date:	20/02/2022
Path:	C:\Windows\System32\cmstp.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmstp.exe
Imagebase:	0x7ff67f360000
File size:	92672 bytes
MD5 hash:	2A9828E0C405422D166E0141054A04B3
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmstp.exe PID: **6000**, Parent PID: **3352**

General

Target ID:	27
Start time:	08:21:10
Start date:	20/02/2022
Path:	C:\Users\user\AppData\Local\y1c6p\cmstp.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\y1c6p\cmstp.exe
Imagebase:	0x7ff768f80000
File size:	92672 bytes
MD5 hash:	2A9828E0C405422D166E0141054A04B3
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: 0000001B.00000002.448574954.00007FFC6E291000.00000020.00000001.01000000.0000000C.sdmp, Author: Joe Security • Rule: crime_win64_dridex_bot_hook, Description: Detects latest Dridex bot hook, Source: 0000001B.00000002.448574954.00007FFC6E291000.00000020.00000001.01000000.0000000C.sdmp, Author: @VK_Intel

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\y1c6p\VERSION.dll	unknown	1376256	success or wait	1	7FFC6E2EE7A6	ReadFile

Analysis Process: SystemPropertiesComputerName.exe PID: **5732**, Parent PID: **3352**

General

Target ID:	28
Start time:	08:21:21
Start date:	20/02/2022
Path:	C:\Windows\System32\SystemPropertiesComputerName.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SystemPropertiesComputerName.exe
Imagebase:	0x7ff649f80000
File size:	83968 bytes
MD5 hash:	BEE134E1F23AFD3AE58191D265BB9070
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: DWWIN.EXE PID: **5392**, Parent PID: **3352**

General

Target ID:	29
Start time:	08:21:22
Start date:	20/02/2022
Path:	C:\Windows\System32\DWWIN.EXE
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\DWWIN.EXE
Imagebase:	0x7ff7bd670000
File size:	210944 bytes
MD5 hash:	3C21F944D5FF44E45BC753919F6AE445
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: DWWIN.EXE PID: **4336**, Parent PID: **3352**

General

Target ID:	30
Start time:	08:21:23
Start date:	20/02/2022
Path:	C:\Users\user\AppData\Local\oudoiG\DWWIN.EXE
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\oudoiG\DWWIN.EXE
Imagebase:	0x7ff7eae80000
File size:	210944 bytes
MD5 hash:	3C21F944D5FF44E45BC753919F6AE445
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: 0000001E.00000002.477365919.00007FFC6E291000.00000020.00000001.01000000.0000000E.sdmp, Author: Joe Security • Rule: crime_win64_dridex_bot_hook, Description: Detects latest Dridex bot hook, Source: 0000001E.00000002.477365919.00007FFC6E291000.00000020.00000001.01000000.0000000E.sdmp, Author: @VK_Intel

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\oudoiG\VERSION.dll	unknown	1376256	success or wait	1	7FFC6E2EE7A6	ReadFile

Analysis Process: SystemPropertiesDataExecutionPrevention.exe PID: **4940**, Parent PID: **3352**

General	
Target ID:	32
Start time:	08:21:35
Start date:	20/02/2022
Path:	C:\Windows\System32\SystemPropertiesDataExecutionPrevention.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SystemPropertiesDataExecutionPrevention.exe
Imagebase:	0x7ff74d1b0000
File size:	83968 bytes
MD5 hash:	1A34577AEDE83993615D7F2E37024D4D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: sppsvc.exe PID: **5788**, Parent PID: **3352**

General	
Target ID:	33
Start time:	08:21:36
Start date:	20/02/2022
Path:	C:\Windows\System32\sppsvc.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\sppsvc.exe
Imagebase:	
File size:	4527680 bytes
MD5 hash:	FEEC8055C5986182C717DD888000AEF6
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: sppsvc.exe PID: **5012**, Parent PID: **3352**

General	
Target ID:	35
Start time:	08:21:39
Start date:	20/02/2022
Path:	C:\Users\user\AppData\Local\GsjW\sppsvc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\GsjW\sppsvc.exe
Imagebase:	0x7ff6a21c0000
File size:	4527680 bytes
MD5 hash:	FEEC8055C5986182C717DD888000AEF6
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: 00000023.00000002.514434351.00007FFC6E291000.00000020.00000001.01000000.00000010.sdmp, Author: Joe Security • Rule: crime_win64_dridex_bot_hook, Description: Detects latest Dridex bot hook, Source: 00000023.00000002.514434351.00007FFC6E291000.00000020.00000001.01000000.00000010.sdmp, Author: @VK_Intel
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: SndVol.exe PID: **3156**, Parent PID: **3352**

General	
Target ID:	36
Start time:	08:21:52

Start date:	20/02/2022
Path:	C:\Windows\System32\SndVol.exe
Wow64 process (32bit):	
Commandline:	C:\Windows\system32\SndVol.exe
Imagebase:	
File size:	259904 bytes
MD5 hash:	CDD7C7DF2D0859AC3F4088423D11BD08
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language

Analysis Process: SndVol.exe PID: **5664**, Parent PID: **3352**

General

Target ID:	37
Start time:	08:21:53
Start date:	20/02/2022
Path:	C:\Users\user\AppData\Local\0rPbJb\SndVol.exe
Wow64 process (32bit):	
Commandline:	C:\Users\user\AppData\Local\0rPbJb\SndVol.exe
Imagebase:	
File size:	259904 bytes
MD5 hash:	CDD7C7DF2D0859AC3F4088423D11BD08
Has elevated privileges:	
Has administrator privileges:	
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

Disassembly

No disassembly