ID: 579430
Sample Name: dpnhupnp.dll
Cookbook: default.jbs
Time: 17:43:09
Date: 27/02/2022
Version: 34.0.0 Boulder Opal

Table of Contents

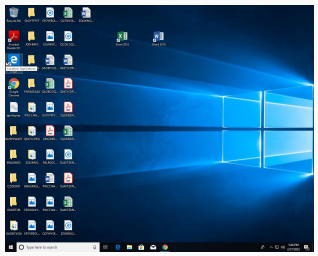
Windows Analysis Report

dpnhupnp.dll

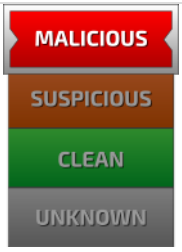
Overview

General Information

Sample Name:	dpnhupnp.dll
Analysis ID:	579430
MD5:	cf22fca6a1c8035..
SHA1:	85cae7532a2198..
SHA256:	3a52c4f27db221..
Tags:	dll dridex exe
Infos:	



Detection



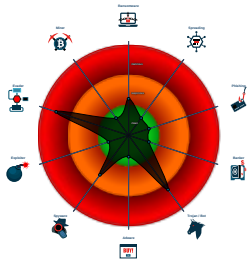
Dridex

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…
- 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 …
- Sigma detected: Suspicious Call by…
- Machine Learning detection for drop…
- Uses Atom Bombing / ProGate to in…
- Uses a Windows Living Off The Lan…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 4592 cmdline: loaddll64.exe "C:\Users\user\Desktop\dpnhupnp.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 4532 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\dpnhupnp.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 4356 cmdline: rundll32.exe "C:\Users\user\Desktop\dpnhupnp.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 2332 cmdline: rundll32.exe C:\Users\user\Desktop\dpnhupnp.dll,GetFileVersionInfoA MD5: 73C519F050C20580F8A62C849D49215A)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - DisplaySwitch.exe (PID: 2172 cmdline: C:\Windows\system32\DisplaySwitch.exe MD5: 97411B8A84E5980E509E500C3209E5C0)
      - DisplaySwitch.exe (PID: 1740 cmdline: C:\Users\user\AppData\Local\4xeLXaDKW\DisplaySwitch.exe MD5: 97411B8A84E5980E509E500C3209E5C0)
      - wusa.exe (PID: 5472 cmdline: C:\Windows\system32\wusa.exe MD5: 04CE745559916B99248F266BBF5F9ED9)
      - GamePanel.exe (PID: 4868 cmdline: C:\Windows\system32\GamePanel.exe MD5: 4EF330EFAE954723B1F2800C15FDA7EB)
      - GamePanel.exe (PID: 5712 cmdline: C:\Users\user\AppData\Local\uRSIQRt4\GamePanel.exe MD5: 4EF330EFAE954723B1F2800C15FDA7EB)
      - msdt.exe (PID: 4792 cmdline: C:\Windows\system32\msdt.exe MD5: 8BE43BAF1F37DA5AB31A53CA1C07EE0C)
      - msdt.exe (PID: 4796 cmdline: C:\Users\user\AppData\Local\1XXGC21\msdt.exe MD5: 8BE43BAF1F37DA5AB31A53CA1C07EE0C)
      - cmstp.exe (PID: 6272 cmdline: C:\Windows\system32\cmstp.exe MD5: 2A9828E0C405422D166E0141054A04B3)
      - cmstp.exe (PID: 6384 cmdline: C:\Users\user\AppData\Local\M4eXJF\cmstp.exe MD5: 2A9828E0C405422D166E0141054A04B3)
      - PresentationHost.exe (PID: 4516 cmdline: C:\Windows\system32\PresentationHost.exe MD5: E3053C73EA240F4C2F7971B3905A91CF)
      - PresentationHost.exe (PID: 2208 cmdline: C:\Users\user\AppData\Local\a6o\PresentationHost.exe MD5: E3053C73EA240F4C2F7971B3905A91CF)
      - cmstp.exe (PID: 2880 cmdline: C:\Windows\system32\cmstp.exe MD5: 2A9828E0C405422D166E0141054A04B3)
      - cmstp.exe (PID: 5004 cmdline: C:\Users\user\AppData\Local\96P3D\cmstp.exe MD5: 2A9828E0C405422D166E0141054A04B3)
  - rundll32.exe (PID: 5880 cmdline: rundll32.exe C:\Users\user\Desktop\dpnhupnp.dll,GetFileVersionInfoByHandle MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 7008 cmdline: rundll32.exe C:\Users\user\Desktop\dpnhupnp.dll,GetFileVersionInfoExA MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.278695271.00007FFC6F9E1000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000003.00000002.357902587.00007FFC6F9E1000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000018.00000002.424452492.00007FFC6F9E1000.00000020.00000001.01000000.0000000A.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000014.00000002.392236668.00007FFC6F9E1000.00000020.00000001.01000000.00000008.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000020.00000002.463842556.00007FFC6E2A1000.00000020.00000001.01000000.0000000C.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
Click to see the 6 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
35.2.cmstp.exe.7ffc7c2f0000.3.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
38.2.PresentationHost.exe.7ffc7c2f0000.3.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
3.2.rundll32.exe.7ffc6f9e0000.2.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
4.2.rundll32.exe.7ffc6f9e0000.2.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
20.2.DisplaySwitch.exe.7ffc6f9e0000.3.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
Click to see the 6 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

Benign windows process drops PE files

Changes memory attributes in foreign processes to executable or writable

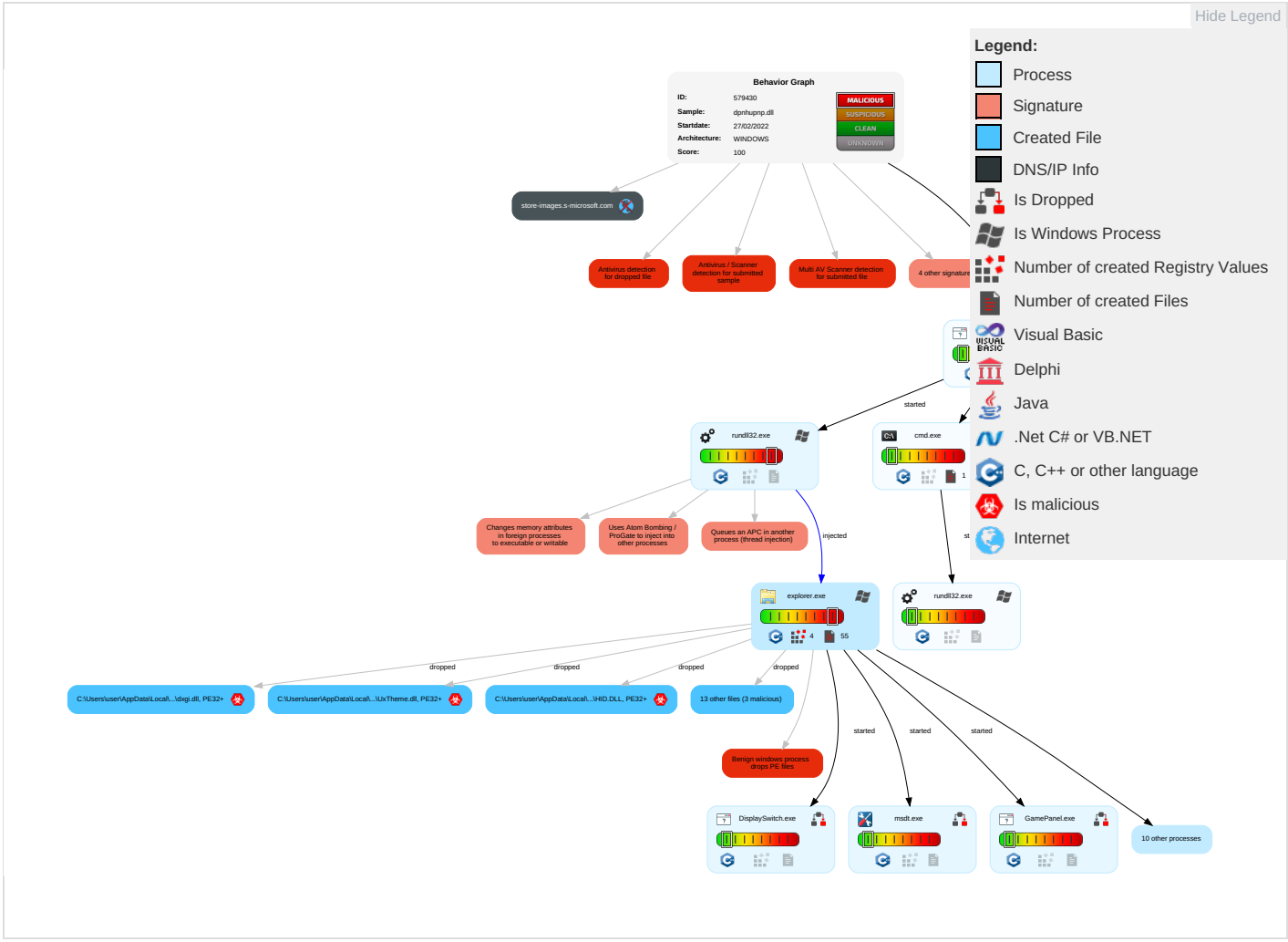
Queues an APC in another process (thread injection)

Uses Atom Bombing / ProGate to inject into other processes

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Native API	1 DLL Side-Loading	1 Exploitation for Privilege Escalation	1 Disable or Modify Tools	2 1 Input Capture	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Exploitation for Client Execution	1 Registry Run Keys / Startup Folder	1 DLL Side-Loading	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	2 1 Input Capture	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 Command and Scripting Interpreter	Logon Script (Windows)	3 1 3 Process Injection	3 Obfuscated Files or Information	Security Account Manager	1 File and Directory Discovery	SMB/Windows Admin Shares	1 Clipboard Data	Automated Exfiltration	1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 Registry Run Keys / Startup Folder	2 Software Packing	NTDS	2 4 System Information 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 Timestomp	LSA Secrets	3 1 Security Software 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	1 DLL Side-Loading	Cached Domain Credentials	1 Virtualization/Sandbox Evasion	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 Masquerading	DCSync	3 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Virtualization/Sandbox Evasion	Proc Filesystem	1 System Owner/User Discovery	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)	3 1 3 Process Injection	/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
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Rundll32	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

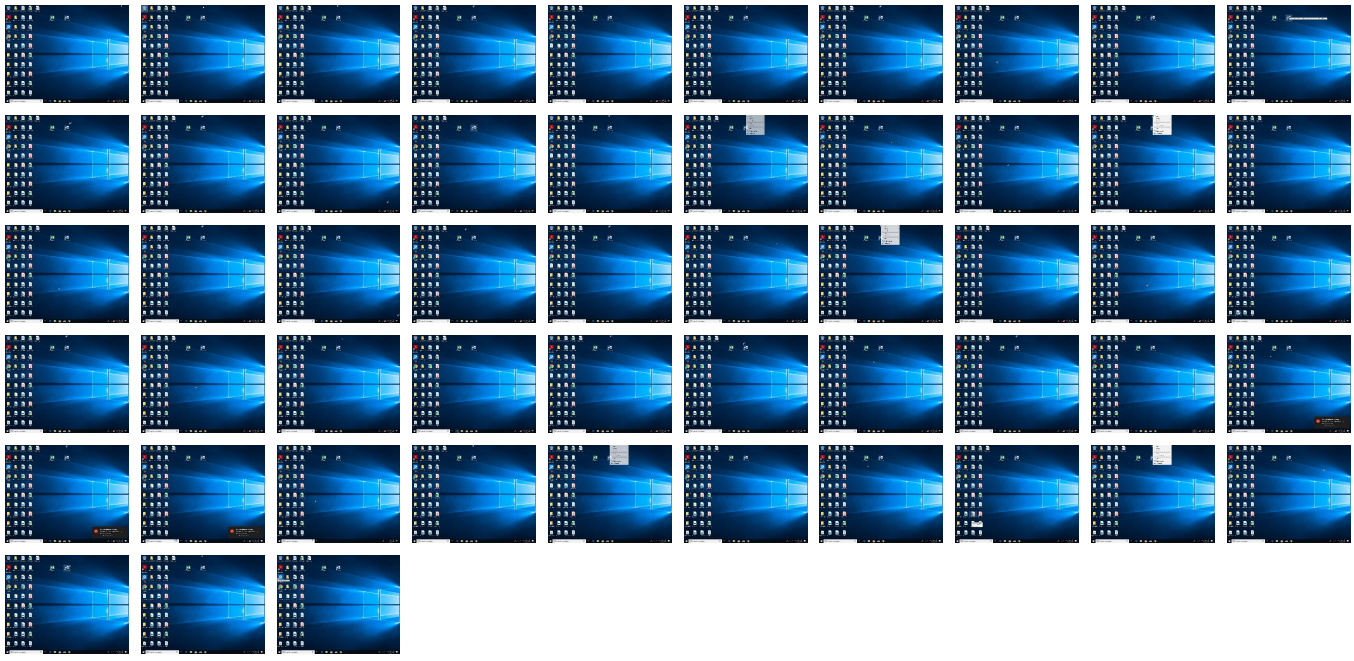
Behavior Graph



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
dpnhupnp.dll	66%	Virustotal		Browse
dpnhupnp.dll	63%	Metadefender		Browse
dpnhupnp.dll	84%	ReversingLabs	Win64.Infostealer.Dridex	
dpnhupnp.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
dpnhupnp.dll	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\4xeLXaDKW\WINSTA.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\WPx7QKO3\UxTheme.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\uRSIQRt4\dxgi.dll	100%	Avira	TR/Crypt.XPACK.Gen7	
C:\Users\user\AppData\Local\96P3D\VERSION.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\96P3D\VERSION.dll	100%	Avira	TR/Crypt.ZPACK.Gen	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\1XXGC21\DUI70.dll	100%	Avira	TR/Crypt.XPACK.Gen7	
C:\Users\user\AppData\Local\96P3D\VERSION.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\RiK2PNsRy\HID.DLL	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\4xeLXaDKW\WINSTA.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\WPx7QKO3\UxTheme.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\uRSIQRt4\dxgi.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\96P3D\VERSION.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\96P3D\VERSION.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\1XXGC21\DUI70.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\96P3D\VERSION.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\RiK2PNsRy\HID.DLL	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\1XXGC21\msdt.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\1XXGC21\msdt.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\4xeLXaDKW\DisplaySwitch.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\4xeLXaDKW\DisplaySwitch.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\96P3D\cmstp.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\96P3D\cmstp.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\M4eXJF\cmstp.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\M4eXJF\cmstp.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
38.2.PresentationHost.exe.7ffc7c2f0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.2.DisplaySwitch.exe.1b6db1c0000.0.unpack	100%	Avira	HEUR/AGEN.1202768		Download File
3.2.rundll32.exe.7ffc6f9e0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
40.2.cmstp.exe.1a4aa710000.0.unpack	100%	Avira	HEUR/AGEN.1202768		Download File
3.2.rundll32.exe.2717dff0000.0.unpack	100%	Avira	HEUR/AGEN.1202768		Download File
20.2.DisplaySwitch.exe.7ffc6f9e0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.rundll32.exe.7ffc6f9e0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.rundll32.exe.7ffc6f9e0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.2.GamePanel.exe.25bee100000.0.unpack	100%	Avira	HEUR/AGEN.1202768		Download File
14.2.rundll32.exe.20953580000.0.unpack	100%	Avira	HEUR/AGEN.1202768		Download File
38.2.PresentationHost.exe.1f1fd100000.1.unpack	100%	Avira	HEUR/AGEN.1202768		Download File
35.2.cmstp.exe.7ffc7c2f0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.2.GamePanel.exe.7ffc6f9e0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.rundll32.exe.258372f0000.0.unpack	100%	Avira	HEUR/AGEN.1202768		Download File
35.2.cmstp.exe.200c5250000.0.unpack	100%	Avira	HEUR/AGEN.1202768		Download File
32.2.msdt.exe.15126930000.0.unpack	100%	Avira	HEUR/AGEN.1202768		Download File
32.2.msdt.exe.7ffc6e2a0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.rundll32.exe.2ac821f0000.1.unpack	100%	Avira	HEUR/AGEN.1202768		Download File
14.2.rundll32.exe.7ffc6f9e0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.loaddll64.exe.7ffc6f9e0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
40.2.cmstp.exe.7ffc7c2f0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.loaddll64.exe.24c71410000.0.unpack	100%	Avira	HEUR/AGEN.1202768		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://schemas.mi	0%	URL Reputation	safe	
http://schemas.micr	0%	URL Reputation	safe	
http://https://www.xboxlive.comMBI_SSLhttps://profile.xboxlive.com/users/me/profile/settings?settings=GameD	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
store-images.s-microsoft.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://mixer.com/api/v1/oauth/xbl/login	GamePanel.exe	false		high
http://schemas.mi	explorer.exe, 00000006.00000000.31354711 2.000000000EE50000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 006.00000000.293192524.000000000EE50000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000006.00000000.326336701.000000 000EE50000.00000004.00000001.00020000.00 000000.sdmp	false	• URL Reputation: safe	unknown
http://https://profile.xboxlive.com/users/me/profile/settings?settings=GameDisplayPicRaw	GamePanel.exe	false		high
http://https://aka.ms/imrx2o	GamePanel.exe	false		high
http://https://mixer.com/_latest/assets/emoticons/%ls.png	GamePanel.exe	false		high
http://https://mixer.com/api/v1/users/current	GamePanel.exe	false		high
http://https://mixer.com/_latest/assets/emoticons/%ls.pngtitleIdaumIdkglIdprocessNamenametypeIdmultimedia	GamePanel.exe, 00000018.00000000.3986662 37.00007FF775557000.00000002.00000001.01 000000.00000009.sdmp, GamePanel.exe, 000 00018.00000002.423900656.00007FF77555700 0.00000002.00000001.01000000.00000009.sdmp, GamePanel.exe.6.dr	false		high
http://https://mixer.com/api/v1/broadcasts/current	GamePanel.exe, GamePanel.exe, 00000018.0 0000000.398666237.00007FF775557000.00000 002.00000001.01000000.00000009.sdmp, Gam ePanel.exe, 00000018.00000002.423900656. 00007FF775557000.00000002.00000001.01000 000.00000009.sdmp, GamePanel.exe.6.dr	false		high
http://https://mixer.com/%wsWindows.System.Launcher	GamePanel.exe, 00000018.00000000.3986662 37.00007FF775557000.00000002.00000001.01 000000.00000009.sdmp, GamePanel.exe, 000 00018.00000002.423900656.00007FF77555700 0.00000002.00000001.01000000.00000009.sdmp, GamePanel.exe.6.dr	false		high
http://https://aka.ms/v5do45	GamePanel.exe	false		high
http://https://mixer.com/api/v1/types/lookup%ws	GamePanel.exe	false		high
http://https://MediaData.XboxLive.com/broadcasts/Augmenthttps://MediaData.XboxLive.com/screenshots/Augmenth	GamePanel.exe, 00000018.00000000.3986662 37.00007FF775557000.00000002.00000001.01 000000.00000009.sdmp, GamePanel.exe, 000 00018.00000002.423900656.00007FF77555700 0.00000002.00000001.01000000.00000009.sdmp, GamePanel.exe.6.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://aka.ms/wk9ocd	GamePanel.exe, GamePanel.exe, 00000018.00000000.398666237.00007FF775557000.00000002.00000001.01000000.00000009.sdmp, GamePanel.exe, 00000018.00000002.423900656.00007FF775557000.00000002.00000001.01000000.00000009.sdmp, GamePanel.exe.6.dr	false		high
http://https://MediaData.XboxLive.com/broadcasts/Augment	GamePanel.exe	false		high
http://https://aka.ms/imfx4k	GamePanel.exe	false		high
http://schemas.micr	explorer.exe, 00000006.00000000.312547112.000000000EE50000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000006.00000000.293192524.000000000EE50000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000006.00000000.326336701.000000000EE50000.00000004.00000001.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.xboxlive.comMBI_SSLhttps://profile.xboxlive.com/users/me/profile/settings?settings=GameD	GamePanel.exe, 00000018.00000000.398666237.00007FF775557000.00000002.00000001.01000000.00000009.sdmp, GamePanel.exe, 00000018.00000002.423900656.00007FF775557000.00000002.00000001.01000000.00000009.sdmp, GamePanel.exe.6.dr	false	• Avira URL Cloud: safe	low
http://https://MediaData.XboxLive.com/gameclips/Augment	GamePanel.exe	false		high
http://https://www.xboxlive.com	GamePanel.exe	false		high
http://https://mixer.com/api/v1/channels/%d	GamePanel.exe	false		high
http://https://mixer.com/api/v1/types/lookup%wshttps://mixer.com/api/v1/channels/%wshttps://mixer.com/api/v	GamePanel.exe, 00000018.00000000.398666237.00007FF775557000.00000002.00000001.01000000.00000009.sdmp, GamePanel.exe, 00000018.00000002.423900656.00007FF775557000.00000002.00000001.01000000.00000009.sdmp, GamePanel.exe.6.dr	false		high
http://https://mixer.com/api/v1/channels/%ws	GamePanel.exe	false		high
http://https://mixer.com/api/v1/chats/%.0fhttps://mixer.com/api/v1/users/currentBEAM_IMAGEGamesGuide::BeamC	GamePanel.exe, 00000018.00000000.398666237.00007FF775557000.00000002.00000001.01000000.00000009.sdmp, GamePanel.exe, 00000018.00000002.423900656.00007FF775557000.00000002.00000001.01000000.00000009.sdmp, GamePanel.exe.6.dr	false		high
http://https://MediaData.XboxLive.com/screenshots/Augment	GamePanel.exe	false		high
http://https://mixer.com/api/v1/chats/%.0f	GamePanel.exe	false		high
http://https://aka.ms/ifg0es	GamePanel.exe	false		high
http://https://mixer.com/%ws	GamePanel.exe	false		high
http://https://aka.ms/w5ryqnhttps://aka.ms/imfx4kQUITTING	GamePanel.exe, 00000018.00000000.398666237.00007FF775557000.00000002.00000001.01000000.00000009.sdmp, GamePanel.exe, 00000018.00000002.423900656.00007FF775557000.00000002.00000001.01000000.00000009.sdmp, GamePanel.exe.6.dr	false		high
http://https://aka.ms/w5ryqn	GamePanel.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	579430
Start date:	27.02.2022
Start time:	17:43:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	dpnhupnp.dll
Cookbook file name:	default.jbs

Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	41
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@43/17@1/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 33.5% (good quality ratio 24.6%) • Quality average: 48.7% • Quality standard deviation: 37.9%
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 • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.35.236.56, 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code 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\1XXGC21\DUI70.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1351680
Entropy (8bit):	6.395884203288439
Encrypted:	false
SSDEEP:	12288:qZgJtlQepQn+NDo7nIgegQCLDF/B9wvj/cLvVZFuwg51:qZK6F7nVeRmDFJivohZFVO
MD5:	3CC9749FD256A9E45E0003772762292C
SHA1:	DF8B170A18069DE9B54BA7069424141A66F3E3E4
SHA-256:	7B82E724E1DF34A91E82DBF0185A62576737B491611375DA37153F2DE6220630
SHA-512:	F39551D6091C6EA61554A1535E334A4C4F2F0CD244B7765DDF89B7522541FCC1B7C64D7BD91F759ACCBC2AF1E9E870E735E65C75F487B42C577CACAA79D827 2
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.7...}^.....`.....`.....@..dQ..$...<.....0..(.....text..... .. ..`.rdata..Co...0...p...0.....@..@.data....;.....@.....@....pdata..8.....@..@.rsrc.....@..@.reloc..1.....@..B .vxl..... .....@..@.qwubgr.$....0... ...0.....@..@.eer....

C:\Users\user\AppData\Local\1XXGC21\msdt.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1560576
Entropy (8bit):	6.10038070749878
Encrypted:	false
SSDEEP:	24576:tnPfp054tZwxDl6XH4qvIReK1odddGdBnyE0k26kVZnBm:VC4tAqNK7utRB
MD5:	8BE43BAF1F37DA5AB31A53CA1C07EE0C
SHA1:	F2C9EB38775B91C4DE45AA25CDDDB86F5F056BF5
SHA-256:	BD59B4362F8590C5009B28830FF11B339B37FF142FB873204368905A9C843A08
SHA-512:	B30BDD7C3B71D58140F642196D5E44ED4C8B11A35DB65D37414C49F7FE64DD0C63DDEE4A0FDF5E75BB0BEB69FE0AA1D609C252F05D5661E7DCD4B6A427415 1C7
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....+..eo..6o..6o..6...7m..6...7q..6...7@..6o..6...6...7\..6...7k..6..X6n..6 ...7n..6Richo..6.....PE..d...4.....".....b...r.....]..... @..... _.....`..... ..... ..P.....".....^..T..... .....text....`.....b..... ..`.rdata...^.....`...f.....@..@.data...p.....@....pdata..."....$.....@..@.rsrc...P.... .....@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\4xeLXaDKW\DisplaySwitch.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1930224
Entropy (8bit):	1.9511202288226894
Encrypted:	false
SSDEEP:	3072:LvyYYIF4cmwcTigBmZWRHLxgMNnVYvkkVp66oB4E7p6:LvyYBF4R/igoZWRryMNnqz3

MD5:	97411B8A84E5980E509E500C3209E5C0
SHA1:	23398F8DA469DEAF10C32773062A6A62B7B004B4
SHA-256:	2C968556FCAD7EBB9A866B21A9F3F3DFCD0CA490CAF8F6B2ECDB423B9D24D3EF
SHA-512:	1D5E598B51B37E8A92FA188A8D59C67B7522480B46AFB5D2033D4380A3C5A120D0DB2BE6FE62B636A23AD83F757B7A1803B77A0EA19DF3C51B9BD36B0F06CB6A
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... ..zd..)d..)d..)m.T)R..)...(g..)...(q..)...(c..)...(E..)d..)...)...({..)..8)e..)...(e..)Richd..).....PE..d....[~....."..... ....@.....`..... .....\.....(3.....d.....c...P..X.....T.....K..(....J. .....K..x.....text..... ..... ..`.imrsiv.....0.....rdata..6....@.....$.....@..@.data...(.....@....pdata..d..... .....@..@.rsrc...(3.....4.....@..@.reloc..X....P.....@..B..... .....

C:\Users\user\AppData\Local\4xeLXaDKW\WINSTA.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1073152
Entropy (8bit):	6.158853615581382
Encrypted:	false
SSDEEP:	12288:fZgJtlQepQn+NDo7nIgegQCLDF/B9wvj/cLvVZFuw:fZK6F7nVeRmDFJivohZFV
MD5:	B4329EA1517938DC6AAB87CBCFB1A3BF
SHA1:	64AFFCC0C5F83C296CAB67DB1E21DED763F8B2A9
SHA-256:	226C6EF8E18A396860447D0A5371663A6A24EF303DF337BCB43505C127CC8DFC
SHA-512:	B7F7F766D8F7A08D0141C041F6EA4675D17DBE8AD9DDECC5FDD98E8F2DD58427FAECEFA5A9F11E5D278FEDC789A35B79352294ACC423BD05E9BA763CC461A60
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.7...}^....." ....0.....$.....@.....`.....`.....@..m...$...<.....0..(.....text..... .. ..`.rdata..Co...0...p...0.....@..@.data...;.....@.....@....pdata..8.....@..@.rsrc.....@..@.reloc..1.....@..B .vxl..... .....@..@.qwubgr.$....0... ...0.....@..@.eer....

C:\Users\user\AppData\Local\96P3D\VERSION.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1069056
Entropy (8bit):	6.141902843002243
Encrypted:	false
SSDEEP:	12288:HZgJtlQepQn+NDo7nIgegQCLDF/B9wvj/cLvVZFuw:HZK6F7nVeRmDFJivohZFV
MD5:	7D34C94AEC52AB539CE9621C7ACBF5E7
SHA1:	90E2CE7C119C169CFEE312CF196EAC52C2E62079
SHA-256:	87B15D5897BA84E39B2D96E521FC0ADDE0966A1322808F3E79D36CA24B370951
SHA-512:	A7E45DB172222317FE9EEB735CEA34AC69E2B22DE08ECB7F8D1889AAC85B9FA03EFAE9C86EF0E2E847907A6C9D656F017DF215A646557A1F85CCAF7E95FF15E8
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....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.7...}^....." ....$.....@.....P.....`.....@..+...$...<.....0..(.....text..... .. ..... ..`.rdata..Co...0...p...0.....@..@.data...;.....@.....@....pdata..8.....@..@.rsrc.....@..@.reloc..1.....@..B .vxl..... .....@..@.qwubgr.$....0... ...0.....@..@.eer....

C:\Users\user\AppData\Local\96P3D\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:	1536:7oIXq0f2yF9sDb/RjxgnvkmVUqAVnKUMjbWg+I/87BM/Z4j8Qi1Yv9V:0Izw/RooolWIk7BM/ZNQi1EV
MD5:	2A9828E0C405422D166E0141054A04B3
SHA1:	84AA48946D4F9A9DFE4C1AF6F96C44B643229A73
SHA-256:	94152FB98573FE31C0CE49D260D760DD173741D663414DE718A37AAC7E8EF11F
SHA-512:	B9B0472706C11D3AECDAB055D4CF319EDD50E8C97B7099D1DC7B768812E804975392E327A1E62301077AB92C1CA97E706628B07172892AB09753FBDD9A07277
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
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\Local\M4eXJF\VERSION.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1069056
Entropy (8bit):	6.141896454346896
Encrypted:	false
SSDEEP:	12288:6ZgJtlQepQn+NDo7nIgegQCLDF/B9wvj/cLvVZFuw:6ZK6F7nVeRmDFJivohZFV
MD5:	28BA9C651ADD8C1F86960D3B39C833FA
SHA1:	60E90D2DF79CFC0672F07A5895C4A10F641C5369
SHA-256:	0556D99CCE10073214B4DB3C7D9AEF79C1B5F60F4F34EB47929689756D7C2964
SHA-512:	69A1362D037D52FD8D10FB1EE159FF54E9776A7C0F707D2886B5D510A82A1CC06F939DC5FC15CCAD0CA62447F8FE200FB8C0D11C48994F55466E46A526E52B3
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.7...}^.....'' ....$.....@.....P.....`.....@..+...$...<.....0..(.....text..... .. ..... ..`.rdata..Co...0...p...0.....@..@.data...;.....@.....@....pdata..8.....@..@.rsrc.....@..@.reloc..1.....@..B .vxl..... .....@..@.qwubgr.$....0... ...0.....@..@.eer....

C:\Users\user\AppData\Local\M4eXJF\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:	1536:7oIXq0f2yF9sDb/RjxgnvkmVUqAVnKUMjbWg+I/87BM/Z4j8Qi1Yv9V:0Izw/RooolWIk7BM/ZNQi1EV
MD5:	2A9828E0C405422D166E0141054A04B3
SHA1:	84AA48946D4F9A9DFE4C1AF6F96C44B643229A73
SHA-256:	94152FB98573FE31C0CE49D260D760DD173741D663414DE718A37AAC7E8EF11F
SHA-512:	B9B0472706C11D3AECDAB055D4CF319EDD50E8C97B7099D1DC7B768812E804975392E327A1E62301077AB92C1CA97E706628B07172892AB09753FBDD9A07277
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
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\Local\RiK2PNsRy\HID.DLL

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1069056
Entropy (8bit):	6.146958184893933

Encrypted:	false
SSDEEP:	12288:FZgJtlQepQn+NDo7nIgegQCLDF/B9wvj/cLvVZFuw:FZK6F7nVeRmDFJivohZFV
MD5:	EAD848991934B10FD663BB3E31D43D74
SHA1:	E544561E5A33491ADB5D7854E8FEB315262CE7BD
SHA-256:	411EB58C6A93FC5E0570D7641BC1E0989136349379DA4871E320D3715401A9E6
SHA-512:	3ABE5D6844119578BC9A683CEC740C6497DCB91794E7DACACB0AE3D12E30B3B1DDB3CE010B2D371DC25757A8CB22E2F928D0216EB81309B6713D2208EC44973
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.7...}^.....'' .... $.....@.....P.....`.....@.....$...<.....0..(.....text..... .. ..... ..`.rdata..Co...0...p...0.....@..@.data...;.....@.....@....pdata..8.....@..@.rsrc.....@..@.reloc..1.....@..B.vxl..... .....@..@.qwubgr.$....0... ...0.....@..@.eer....

C:\Users\user\AppData\Local\RiK2PNsRy\tabcal.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	5.705817452511626
Encrypted:	false
SSDEEP:	1536:Q77RYSqLmKbndnBRdv2RWUUTtj11VM0bJDrdfW2jbJK:QuxLmKbndDdv2WUczVMKrdfZbs
MD5:	F04F239BA5FED275E652372222D1BE00
SHA1:	883C7915ADD2B47D1012E52321D670A4A29ABB53
SHA-256:	CE81E5BFF4C0A646EFD86791DB938A7F5E148666F518990B156FE208F8454423
SHA-512:	61B80BC6E68057C425C624DC4FC8A551F60F6E4DA60A7F5A6D6520FE92E0B61D1B63B16DF70A5019C3F0AFFE8064CD072BBADC3C69E1DB8833E1E3ABA9C4529
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....d.. ... ...).`.>...O..."...O...2...O...&...O...7... ...$...O...)...O...!...O..!...Rich .....PE..d...r.T,....."..... .....@.....&....`..... .....0..@r.....|...p...T..... .....,.....text...J..... ..`.rdata..f4.....6.....@..@.data....!.....@....pdata.....@..@.didat..P.... ....@....rsrc...@r...0...t.....@..@.reloc..|.....B.....@..B..... .....

C:\Users\user\AppData\Local\WPx7QKO3\CloudNotifications.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	77072
Entropy (8bit):	6.115516882753233
Encrypted:	false
SSDEEP:	1536:PBw6bK5qGy2vbnG4bhimIHw28N6GgIpdNtgdNttP+O1K9dr3uhyZb3NnPg5:FbK522vDfnp28a+O1AdCoZxno5
MD5:	D9FF4C8DBC1682E0508322307CB89C0F
SHA1:	52FF480ABF6A6CE9BC32BD3B467C028C35849C6F
SHA-256:	E99A6238FDF53700DE8588E1C1128D52680C1DCAAD4E32B38EF2170395495D29
SHA-512:	C068F98855514994AA7CD66ED02E3FD05B7E81EAD714F83CC158B65AAC6DE12A1D324375C41FEC5C1B6A3F1D6D8639EBFF71D510A720148A33E645ED066DAF2C
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....=.....e.....Q.....Rich.....PE..d.....".....@.....p.....*..... .....p.....@.. .... ..L.....%...`.....P...T..... .....`.....text..... ..`.imrsiv.....rdata...W.....X.....@..@.data...x.....@....pdata..L.... .....@..@.didat.....0.....@....rsrc... ....@.....@..@.reloc.....`.....@..B..... .....

C:\Users\user\AppData\Local\WPx7QKO3\UxTheme.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1069056
Entropy (8bit):	6.155376692081572
Encrypted:	false
SSDEEP:	12288:7ZgJtlQepQn+NDo7nIgegQCLDF/B9wvj/cLvVZFuw:7ZK6F7nVeRmDFJivohZFV

MD5:	788F93041CC68AAF0D2981E3664C4513
SHA1:	C570BCFAD5BDBBFE27125E0B4D18CFFDFF193DCE
SHA-256:	CD4DED826CB26B1FE448CCC265AEDD60A17D3452BE8920008E49967651FDF953
SHA-512:	946E4D6B553DC66AF809AF36D46A8449ED30A4B94CEEAB5D41CFC7B548AECD65EF2BBC0346BDD6A3CE326FB76105BAD69C9498AE7F2B29D4AA241E153056EF3
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.7...}^......" ....$.....@.....P.....`.....@.....$...<.....0..(.....text..... .. ..... ..`.rdata..Co...0...p...0.....@..@.data...;.....@.....@....pdata..8.....@..@.rsrc.....@..@.reloc..1.....@..B .vxl..... .....@..@.qwubgr.$....0... ...0.....@..@.eer....

C:\Users\user\AppData\Local\a6o\PresentationHost.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	259072
Entropy (8bit):	6.5074250085194665
Encrypted:	false
SSDEEP:	6144:8kfs4/kfxzJTbHfyH5KNXwy3Odjp19k5KNXf:fs4ixzJTbHmKVwy3OdLaKV
MD5:	E3053C73EA240F4C2F7971B3905A91CF
SHA1:	1848AD66BD55E5484616FB85E80BA58BE1D5BA4B
SHA-256:	0BACCDB2B5ACB7B3C2E9085655457532964CAFFF1AE250016CE1A80E839B820C
SHA-512:	167BCC3E2552286F7D985A65674DA2FF0D0AA6A7F0C4C3B43193943B606E0133C06EEB33656EFBB8B827AC9221FB1BA00A49ADCC2489BD4F38DF62A015806DB3
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3/.]|.]|.]|...|.]|...|..]|..^}.]|..Y}.]|.\|..]|..\}.]|..T}..]|..X}.]|..|.]|..._}.]|Rich.]|. .....PE..d..../.....".....&.....@.....0.....`..... .....p..,.....j.....l..... .,....d..T.....#..... .....$.....text...o..... ..`.rdata.....@..@.data.....r.....@....pdata..l.....t.....@..@.rsrc...j.....l...~..... ...@..@.reloc..,.... .....@..B..... .....

C:\Users\user\AppData\Local\a6o\VERSION.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1069056
Entropy (8bit):	6.141888354644453
Encrypted:	false
SSDEEP:	12288:+ZgJtlQepQn+NDo7nIgegQCLDF/B9wvj/cLvVZFuw:+ZK6F7nVeRmDFJivohZFV
MD5:	D4D5B95886C89B810B29F8FF8818337B
SHA1:	7CDAC1ACF63AEEB8E21F7B60789EB18D38322771
SHA-256:	1C9BFFF102C998B55137C47A7B541741D341F5BE2C1758A82E06B7537396B3DD
SHA-512:	885439E76F4995FB9F4553B867AA8BB4789ED9AE8B76CB34161F9FB17A559324C620088C7C3C3DA770E4FCDB3F385DA8D7C59E2A606A59634B8FA80D14D53EAB
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.7...}^......" ....$.....@.....P.....`.....@..+...$...<.....0..(.....text..... .. ..... ..`.rdata..Co...0...p...0.....@..@.data...;.....@.....@....pdata..8.....@..@.rsrc.....@..@.reloc..1.....@..B .vxl..... .....@..@.qwubgr.$....0... ...0.....@..@.eer....

C:\Users\user\AppData\Local\uRSIQRt4\GamePanel.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1292288
Entropy (8bit):	6.159394598062476
Encrypted:	false
SSDEEP:	24576:tg6uRV8QrFa8Zdntp/LEz2INhgITVXTvlHQroF:tgJVbFaqtpDEznyQVjvZQroF
MD5:	4EF330EFAE954723B1F2800C15FDA7EB
SHA1:	3E152C0B10E107926D6A213C882C161D80B836C9

SHA-256:	0494166D4AE6BB7925E4F57BB6DFAC629C95AE9E03DFC925F8232893236BD982
SHA-512:	C122CD7A245EF6A6A7B7DECAB6500BDC11E4C57B8E35F8462CC0615E44E54071E6BF79B69BB8519470ACBAF0D2E62ABC45C38CBF0606261792EDB4A84790EC61
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....T.ur.`.!.`.!.`.!...!P`.!... .`.!... .`.!... 4`.!... 9`.!.`.!de.!... .`.!...!.`.!...!.`.!... .`.!Rich.`.!.....PE..d.....".....H.....0.....@.....@..... .....u.....`.....:..p...T.....@..(...pp... .....8@..H... ...@.....text....F.....H..... .`.imrsiv.....`.....rdata.....p.....L.....@..@.data.....@....pdata..`.....~..... .....@..@.didat.....p.....@....rsrc....u.....v.....@..@.reloc...:.....<...|.....@..B..... .....

C:\Users\user\AppData\Local\uRSIQRt4\dxgi.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1069056
Entropy (8bit):	6.142847456522913
Encrypted:	false
SSDEEP:	12288:TZgJtlQepQn+NDo7nIgegQCLDF/B9wvj/cLvVZFuw:TZK6F7nVeRmDFJivohZFV
MD5:	7F99325FD34A10C1AD7942EC2C79D921
SHA1:	672047B806244B31EF978C237F5C248580CEDCCB
SHA-256:	DADA800E9EF0A9ED81DF2CC3FE254A261E7D6B246082A596CEC98EF52FE786D6
SHA-512:	67A1CEFC2FADD32E5A59C3E03ABE5217083736FECBAA0F07888BF2A55328F0563EBAA39B93580CEEA25BAA2073D18BA2B33A5A846333CA5C8092FDB220E9B412
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.7...}^....."..... .....$.....@.....P.....`.....@.....$...<.....0..(.....text.....  .....  ..`.rdata..Co...0...p...0.....@..@.data...;.....@.....@....pdata..8.....@..@.rsrc.....@..@.reloc..1.....@..B .vxl..... .....@..@.qwubgr.$....0... ...0.....@..@.eer....

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):	7.319876797981463
Encrypted:	false
SSDEEP:	24:UHzfK1Iv8tUyNY46eYIi9voySd5cKrM7RSzIpwAgTUL8LSeeBweiiJVEWybp0VgP:UT2K+Uxe8NVSbrwSzqwxCe2wcEWc92A
MD5:	85E52B4A28FEE63F46413C9EB25206D5
SHA1:	0140AAD8B9AD754C5D35200991F581514E5C2314
SHA-256:	4956E2A4D0F745E7B325478B6E5E5F6C345D9BB422AF69E386E854043EA4D289
SHA-512:	D990279BCAE61753CAFA3CCE11527F8A90F7756F7A1777E4B11B95BF211053CDA6394E13776AD14704EFB790CD0D4B3D0E58CFEA6E7B51B30B38BC6E9FE27635
Malicious:	false
Preview:	.....user.....RSA1.....T|.uo9.?R(....NHQ.n.H.I....O..0...r..%0...s.2ETw...$.....i..$-.[..;...E].ea...M&O..+u,h..n.T.B..w..z...I....X..y..Sr|. .....z..O.....L.M.5.t.xY.....,...C.r.y.p.t.o.A.P.I. .P.r.i.v.a.t.e. .K.e.y....f..... ....eU.S...K..X.-.Jv....B.s....U..... ...,.u.>.....*A.W..~.+U.....:nm=.;...j...^x..... SU...D.....6.vK..+Ej...0..~Yj..j....s.Q }#.r.....L.q.u...H.Nd.?...R.....Z&...q.Z.B5.e..w.|,.)#...'.....7e....@...+..-q.'...5"..B~.....2.Eqy23...(;.....3....yj..-.....\...A.`3..2..=..Tg..C~ .3....h..=.....L.lb.g".k.....cY....q2.2..3.(.....C.+....`.'J....1.~..f/T....u8K....g.!..^P?[m..z..E.d.....Kc..6.pC.m....X..(..H..lm.@.K.py&Ss.Y...M..h..h.....67.`...5.,%..b.....L\...2.z. $...C."../:E.F4../....i...@.*kS.....s..S.2...B..$q/.....f?..I...iT.}.<..G7..6..k.gH.h.]y.....T!..k5..<.p.r@.....t.....-.d.....hZk

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	6.159361029232143
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:	dpnhupnp.dll
File size:	1064960
MD5:	cf22fca6a1c8035cb38867787f16be21
SHA1:	85cae7532a21983295a2c0aad5889e8dbd024c9f
SHA256:	3a52c4f27db221ed975af3d38ac4b9060203b9c6fb3532cdc61b969e21ca666c
SHA512:	0a1e9e8f6d149d6cada2b29257087819a7a09ebf47f31e31c03b0cd26241f487a695faa9d23ce509b413f2585be426e310b8308818445ad039328293bd17cd4c
SSDEEP:	12288:JZgJtlQepQn+NDo7nIgegQCLDF/B9wvj/cLvVZFuw:JZK6F7nVeRmDFJivohZFV
File Content Preview:	MZ.....@.....X..Z.qb..qb..qb.a...jqb.s....qb.9...\qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb.. (c..qb.;...,qb../..Tqb.....Zqb.....qb.z...Bqb.....nqb.....[qb.....qb.;...{qb.....qb

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x1400424b0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x140000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x5E7D9D05 [Fri Mar 27 06:28:21 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	4a2e61e1749a0183eccaadb9c4ef6ec2

Entrypoint Preview

Instruction
dec eax
mov dword ptr [00070639h], ecx
dec eax
lea ecx, dword ptr [FFFFF2F2h]
dec esp
mov dword ptr [0007064Bh], eax
dec esp
mov dword ptr [00070654h], edi
dec esp
mov dword ptr [00070655h], esi
dec eax
xor eax, eax
dec eax
inc eax
dec eax
add ecx, eax
dec esp
mov dword ptr [00070655h], esp
dec eax
dec ecx
dec eax

Instruction
mov dword ptr [00070653h], esi
dec eax
test eax, eax
je 00007F54089D45BDh
dec eax
mov dword ptr [0007060Fh], esp
dec eax
mov dword ptr [00070600h], ebp
dec eax
mov dword ptr [00070649h], ebx
dec eax
mov dword ptr [0007063Ah], edi
dec eax
test eax, eax
je 00007F54089D459Ch
dec esp
mov dword ptr [000705FEh], ecx
dec esp
mov dword ptr [0007060Fh], ebp
dec eax
mov dword ptr [000705D0h], edx
jmp ecx
dec eax
add edi, ecx
retn 0008h
ud2
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push esi
dec eax
sub esp, 00000080h
dec eax
mov dword ptr [esp+78h], 58225FC8h
mov dword ptr [esp+60h], 2DFAE652h
mov al, byte ptr [esp+77h]
mov dl, al
add dl, FFFFFF85h
mov byte ptr [esp+77h], dl
mov word ptr [esp+5Eh], 3327h
dec esp
mov eax, dword ptr [esp+78h]
inc esp
mov ecx, dword ptr [esp+64h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x103010	0x22b	.rqfw

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa9924	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbf000	0x3d8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x1000	0x0	.text
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc0000	0xefc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x43000	0x28	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x418cc	0x42000	False	0.781412760417	data	7.78392111205	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x43000	0x66f43	0x67000	False	0.700313827367	data	7.87278268617	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xaa000	0x13ba7	0x14000	False	0.0782836914062	data	2.51707039551	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0xbe000	0x138	0x1000	False	0.061279296875	PEX Binary Archive	0.599172422844	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0xbf000	0x69e	0x1000	False	0.123291015625	data	1.07831823765	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc0000	0xf31	0x1000	False	0.416748046875	data	5.36145191459	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.vxl	0xc1000	0x14d4	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.qwubgr	0xc3000	0x1124	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.eer	0xc5000	0x1e66	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.xwwauf	0xc7000	0x9cd	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pkc	0xc8000	0x42a	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.npkda	0xc9000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vhs	0xca000	0x1af	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.iaywj	0xcb000	0x1455	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.nasi	0xcd000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.zhvprh	0xce000	0x6cd0	0x7000	False	0.00177873883929	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.yatdsp	0xd5000	0x543	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.njso	0xd6000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.lgliat	0xd8000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ntqjh	0xd9000	0xbf6	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.sucsek	0xda000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.qsxjui	0xdb000	0x9cd	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.twctcm	0xdc000	0x1124	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.nms	0xde000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ogj	0xdf000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vrkgb	0xe1000	0x706	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.gikfw	0xe2000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ktl	0xe3000	0x9cd	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.crcn	0xe4000	0x5a7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.wtfr	0xe5000	0x1ee	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.hep	0xe6000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ywg	0xe7000	0xd33	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.sqsp	0xe8000	0x2da	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tkyonf	0xe9000	0x1f2a	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.lmr	0xeb000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.nmvll	0xec000	0x1f2a	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.uvboq	0xee000	0x389	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pck	0xef000	0x3ba	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.cui	0xf0000	0x128f	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bjpf	0xf2000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tdsza	0xf3000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.ljyns	0xf4000	0x128f	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.uvvcd	0xf6000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.dhcna	0xf7000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ntjkji	0xf8000	0x3ba	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.copgfj	0xf9000	0x1f2a	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.zmu	0xfb000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.nqzul	0xfc000	0x3ba	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.qgbg	0xfd000	0x389	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.obih	0xfe000	0x543	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.igwjz	0xff000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.mkzlg	0x100000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ovmzdw	0x101000	0x1e66	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rqfw	0x103000	0x23b	0x1000	False	0.07958984375	data	1.11634042299	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

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

Imports

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

Exports

Name	Ordinal	Address
GetFileVersionInfoA	1	0x14000f7e4
GetFileVersionInfoByHandle	2	0x140002ba4
GetFileVersionInfoExA	3	0x14000d900
GetFileVersionInfoExW	4	0x14001482c
GetFileVersionInfoSizeA	5	0x14003fdcc
GetFileVersionInfoSizeExA	6	0x14002b8cc
GetFileVersionInfoSizeExW	7	0x14001c354
GetFileVersionInfoSizeW	8	0x140029090
GetFileVersionInfoW	9	0x14000ba2c
VerFindFileA	10	0x140033224
VerFindFileW	11	0x140035218
VerInstallFileA	12	0x140015484
VerInstallFileW	13	0x1400206e8
VerLanguageNameA	14	0x140029e8c
VerLanguageNameW	15	0x14003d800

Name	Ordinal	Address
VerQueryValueA	16	0x140010250
VerQueryValueW	17	0x1400314a0

Version Infos

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

Possible Origin

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

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 27, 2022 17:43:53.441113949 CET	60784	53	192.168.2.3	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 27, 2022 17:43:53.441113949 CET	192.168.2.3	8.8.8.8	0xe615	Standard query (0)	store-images.s-microsoft.com	A (IP address)	IN (0x0001)

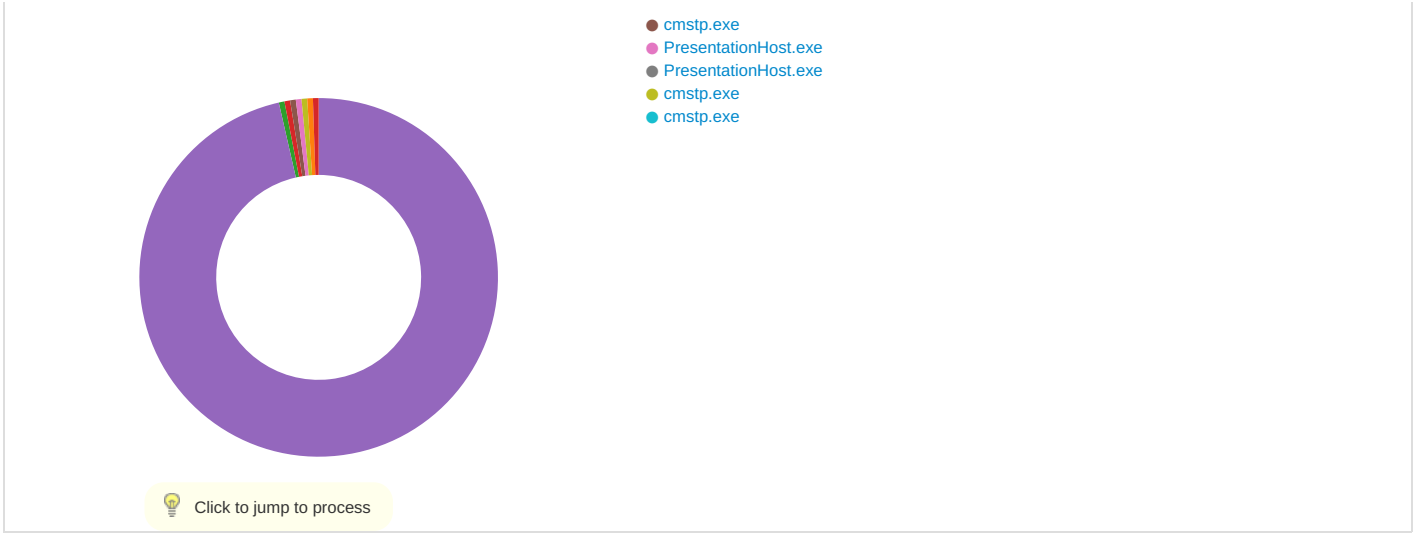
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 27, 2022 17:43:53.470438004 CET	8.8.8.8	192.168.2.3	0xe615	No error (0)	store-images.s-microsoft.com	store-images.s-microsoft.com-c.edgekey.net		CNAME (Canonical name)	IN (0x0001)

Statistics

Behavior

- loaddll64.exe
- cmd.exe
- rundll32.exe
- rundll32.exe
- explorer.exe
- rundll32.exe
- rundll32.exe
- DisplaySwitch.exe
- DisplaySwitch.exe
- wusa.exe
- GamePanel.exe
- GamePanel.exe
- msdt.exe
- msdt.exe
- cmstp.exe



System Behavior

Analysis Process: loaddll64.exe PID: 4592, Parent PID: 1296

General

Target ID:	0
Start time:	17:43:58
Start date:	27/02/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\dpnhupnp.dll"
Imagebase:	0x7ff7cf9b0000
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: 00000000.00000002.298715660.00007FFC6F9E1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 4532, Parent PID: 4592

General

Target ID:	1
Start time:	17:43:59
Start date:	27/02/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\dpnhupnp.dll",#1
Imagebase:	0x7ff74a650000
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: **2332**, Parent PID: **4592**

General

Target ID:	3
Start time:	17:43:59
Start date:	27/02/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\dpnhupnp.dll,GetFileVersionInfoA
Imagebase:	0x7ff6f85c0000
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: 00000003.00000002.357902587.00007FFC6F9E1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\dpnhupnp.dll	unknown	1064960	success or wait	1	7FFC6FA3F8D6	ReadFile

Analysis Process: rundll32.exe PID: **4356**, Parent PID: **4532**

General

Target ID:	4
Start time:	17:43:59
Start date:	27/02/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\dpnhupnp.dll",#1
Imagebase:	0x7ff6f85c0000
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: 00000004.00000002.278695271.00007FFC6F9E1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\dpnhupnp.dll	unknown	1064960	success or wait	1	7FFC6FA3F8D6	ReadFile

Analysis Process: explorer.exe PID: **3352**, Parent PID: **2332**

General

Target ID:	6
Start time:	17:44:01
Start date:	27/02/2022
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\Windows\Start Menu\Programs\Maintenance\RkRLYOhG1	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005F2F5	CreateDirectoryW
C:\Users\user\AppData\Local\4xeLXaDKW\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005F2F5	CreateDirectoryW
C:\Users\user\AppData\Local\4xeLXaDKW\WINSTA.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\4x eLXaDKW\DisplaySwitch.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\uRSIQRt4\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005F2F5	CreateDirectoryW
C:\Users\user\AppData\Local\uRSIQRt4\dxgi.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\uRSIQRt4\GamePanel.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\1XXGC21\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005F2F5	CreateDirectoryW
C:\Users\user\AppData\Local\1XXGC21\DUI70.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\1XXGC21\msdt.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\M4eXJF\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005F2F5	CreateDirectoryW
C:\Users\user\AppData\Local\M4eXJF\VERSION.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\M4eXJF\cmstp.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\a6o\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005F2F5	CreateDirectoryW
C:\Users\user\AppData\Local\a6o\VERSION.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\a6o\PresentationHost.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\96P3D\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005F2F5	CreateDirectoryW
C:\Users\user\AppData\Local\96P3D\VERSION.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\96P3D\cmstp.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\WPx7QKO3\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005F2F5	CreateDirectoryW
C:\Users\user\AppData\Local\WPx7QKO3\UxTheme.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\WPx7QKO3\CloudNotifications.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\RiK2PNsRy\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005F2F5	CreateDirectoryW
C:\Users\user\AppData\Local\RiK2PNsRy\HID.DLL	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\RiK2PNsRy\tabcal.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\4xeLXaDKW\DisplaySwitch.exe	cannot delete	9	14005FB70	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\4xeLXaDKW\WINSTA.dll	cannot delete	9	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\4xeLXaDKW\DisplaySwitch.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\4xeLXaDKW\WINSTA.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\uRSIQRt4\dxgi.dll	cannot delete	11	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\uRSIQRt4\GamePanel.exe	cannot delete	11	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\uRSIQRt4\dxgi.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\uRSIQRt4\GamePanel.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\1XXGC21\DUI70.dll	cannot delete	11	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\1XXGC21\msdt.exe	cannot delete	11	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\1XXGC21\DUI70.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\1XXGC21\msdt.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\M4eXJF\cmstp.exe	cannot delete	6	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\M4eXJF\VERSION.dll	cannot delete	6	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\M4eXJF\cmstp.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\M4eXJF\VERSION.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\a6o\PresentationHost.exe	cannot delete	5	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\a6o\VERSION.dll	cannot delete	5	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\a6o\PresentationHost.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\a6o\VERSION.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\96P3D\cmstp.exe	cannot delete	4	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\96P3D\VERSION.dll	cannot delete	4	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\96P3D\cmstp.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\96P3D\VERSION.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\WPx7QKO3\CloudNotifications.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\WPx7QKO3\UxTheme.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\RiK2PNsRy\HID.DLL	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\RiK2PNsRy\tabcal.exe	success or wait	1	14005FB70	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\4xeLXaDKW\WINSTA.dll	0	1073152	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	14005F160	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\4xeLXaDKW\DisplaySwitch.exe	0	1930224	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 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 20 fd fd 7a 64 fd fd 29 64 fd fd 29 64 fd fd 29 6d fd 54 29 52 fd fd 29 0b fd fd 28 67 fd fd 29 0b fd fd 28 71 fd fd 29 0b fd fd 28 63 fd fd 29 0b fd fd 28 45 fd fd 29 64 fd fd 29 fd fd fd 29 0b fd fd 28 7b fd fd 29 0b fd 38 29 65 fd fd 29 0b fd fd 28 65 fd fd 29 52 69 63 68 64 fd fd 29 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 07 00 fd 5b 7e 01 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$ zd)d)d)mT)R)(g)(q)(c)(E)d))({)8)e)(e)Richd)PEd[~"	success or wait	1	14005F160	WriteFile
C:\Users\user\AppData\Local\uRSIQRt4\dxgi.dll	0	1069056	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 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	14005F160	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\uRSIQRt4\GamePanel.exe	0	1292288	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 54 01 75 72 10 60 1b 21 10 60 1b 21 10 60 1b 21 19 18 fd 21 50 60 1b 21 7f 04 1f 20 00 60 1b 21 7f 04 18 20 13 60 1b 21 7f 04 1e 20 34 60 1b 21 7f 04 1a 20 39 60 1b 21 10 60 1a 21 64 65 1b 21 7f 04 12 20 fd 60 1b 21 7f 04 fd 21 12 60 1b 21 7f 04 fd 21 11 60 1b 21 7f 04 19 20 11 60 1b 21 52 69 63 68 10 60 1b 21 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 08 00 fd 8e 1b 00 00 00	MZ@!L!This program cannot be run in DOS mode.$Tur`!`!`!!P`! `! `! 4`! 9`!`!de! `!!`!!`! `! Rich`!PEd	success or wait	1	14005F160	WriteFile
C:\Users\user\AppData\Local\1XXGC21\DUI70.dll	0	1351680	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	14005F160	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\1XXGC21\msdt.exe	0	1560576	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 2b fd fd 65 6f fd fd 36 6f fd fd 36 6f fd fd 36 00 fd fd 37 6d fd fd 36 00 fd fd 37 71 fd fd 36 00 fd fd 37 40 fd fd 36 6f fd fd 36 fd fd fd 36 00 fd fd 37 5c fd fd 36 00 fd fd 37 6b fd fd 36 00 fd 58 36 6e fd fd 36 00 fd fd 37 6e fd fd 36 52 69 63 68 6f fd fd 36 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06 00 34 02 fd fd 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$+eo6o6o67m67q67@6o667\67k6X6n67n6Richo6PEd4"	success or wait	1	14005F160	WriteFile
C:\Users\user\AppData\Local\M4eXJF\VERSION.dll	0	1069056	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	14005F160	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\M4eXJF\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 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	14005F160	WriteFile
C:\Users\user\AppData\Local\a6o\VERSION.dll	0	1069056	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	14005F160	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\a6o\PresentationHost.exe	0	259072	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 01 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 33 2f fd 5d 7c fd 5d 7c fd 5d 7c fd fd fd 7c fd 5d 7c fd fd fd 7c fd fd 5d 7c fd fd 5e 7d fd 5d 7c fd fd 59 7d fd 5d 7c fd 5c 7c 07 fd 5d 7c fd fd 5c 7d fd 5d 7c fd fd 54 7d fd fd 5d 7c fd fd 58 7d fd 5d 7c fd a2 7c fd 5d 7c fd fd 5f 7d fd 5d 7c 52 69 63 68 fd 5d 7c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$3/]|]|]||]||]| ^}]|Y}]|\\]|\\}]|T}]|X}]||]|_}] |Rich]|	success or wait	1	14005F160	WriteFile
C:\Users\user\AppData\Local\96P3D\VERSION.dll	0	1069056	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	14005F160	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\96P3D\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 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	14005F160	WriteFile
C:\Users\user\AppData\Local\WPx7QKO3\UxTheme.dll	0	1069056	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	14005F160	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\WPx7QKO3\CloudNotifications.exe	0	77072	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 ff fd fd fd fd fd fd fd fd fd fd fd fd 3d fd fd fd fd fd fd 2d fd fd fd fd fd fd 2a fd fd fd fd fd fd 2b fd fd fd fd fd fd 2f fd fd fd fd fd fd fd fd fd 65 fd fd fd fd 27 fd fd fd fd fd fd fd 51 fd fd fd fd fd fd 2c fd fd fd fd fd 52 69 63 68 fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 08 00 16 fd 0b fd 00 00 00	MZ@!L!This program cannot be run in DOS mode.$=eQRichPEd	success or wait	1	14005F160	WriteFile
C:\Users\user\AppData\Local\RiK2PNsRy\HID.DLL	0	1069056	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	14005F160	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\RiK2PNsRy\tabcal.exe	0	82944	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 64 5d fd 20 fd fd fd 20 fd fd fd 20 fd fd fd 29 fd 60 fd 3e fd fd fd 4f fd fd fd 22 fd fd fd 4f fd fd fd 32 fd fd fd 4f fd fd fd 26 fd fd fd 4f fd fd fd 37 fd fd fd 20 fd fd fd 24 fd fd fd 4f fd fd fd 29 fd fd fd 4f fd 0c fd 21 fd fd fd 4f fd fd fd 21 fd fd fd 52 69 63 68 20 fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 07 00 72 fd 54 2c 00 00 00	MZ@!L!This program cannot be run in DOS mode.$d)`>O"O2O&O7 $O)O!O!Rich PEdrT,	success or wait	1	14005F160	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\efsui.exe	unknown	14336	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\DisplaySwitch.exe	unknown	1930224	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\winsta.dll	unknown	332712	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\wusa.exe	unknown	308736	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\GamePanel.exe	unknown	1292288	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\dxgi.dll	unknown	749024	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\securekernel.exe	unknown	604064	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\cliconfg.exe	unknown	30720	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\logman.exe	unknown	114176	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\RemotePosWorker.exe	unknown	12800	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\cofire.exe	unknown	23552	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\openfiles.exe	unknown	71680	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\7za.exe	unknown	289792	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\AuthHost.exe	unknown	139016	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\BdeHdCfg.exe	unknown	132608	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\msdt.exe	unknown	1560576	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\dui70.dll	unknown	1719808	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\wkspbroker.exe	unknown	271752	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\LanguageComponentsInstallerComHandler.exe	unknown	50688	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\cmstp.exe	unknown	92672	success or wait	6	14005F8D6	ReadFile
C:\Windows\System32\version.dll	unknown	30568	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\qwinsta.exe	unknown	28672	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\winrshost.exe	unknown	28160	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\PresentationHost.exe	unknown	259072	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\control.exe	unknown	117760	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\rasautou.exe	unknown	17920	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\PnPUnattend.exe	unknown	59392	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\xbgmsvc.exe	unknown	59512	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\certutil.exe	unknown	1557504	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\autoconv.exe	unknown	932352	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\LegacyNetUXHost.exe	unknown	200192	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\WUDFCompanionHost.exe	unknown	153528	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\mshta.exe	unknown	14848	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\regedt32.exe	unknown	11776	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\backgroundTaskHost.exe	unknown	19352	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\icsunattend.exe	unknown	17408	success or wait	1	14005F8D6	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\unarchiver.exe	unknown	10752	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\tar.exe	unknown	50176	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\MdSched.exe	unknown	91648	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\AppVClient.exe	unknown	826776	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\reg.exe	unknown	72704	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\logagent.exe	unknown	101376	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\DmOmaCpMo.exe	unknown	33280	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\iscsicpl.exe	unknown	122368	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\proquota.exe	unknown	33792	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\sort.exe	unknown	27136	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\ipconfig.exe	unknown	34304	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\tpmvscmgr.exe	unknown	105472	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\appidpolicyconverter.exe	unknown	160256	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\CloudNotifications.exe	unknown	77072	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\uxtheme.dll	unknown	599040	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\findstr.exe	unknown	34304	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\setspn.exe	unknown	29184	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\wecutil.exe	unknown	104448	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\LockAppHost.exe	unknown	88408	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\MultiDigiMon.exe	unknown	53760	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\DpiScaling.exe	unknown	79360	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\dmcfghost.exe	unknown	38400	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\netiougc.exe	unknown	29696	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\taskkill.exe	unknown	94720	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\repair-bde.exe	unknown	126976	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\cscript.exe	unknown	164352	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\pwlauncher.exe	unknown	35328	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\hvsievaluator.exe	unknown	124824	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\rasphone.exe	unknown	34304	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\Taskmgr.exe	unknown	1326952	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\poqexec.exe	unknown	141312	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\convertvhd.exe	unknown	209920	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\setx.exe	unknown	55296	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\relog.exe	unknown	43008	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\LocationNotificationWindows.exe	unknown	66048	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\PrintIsolationHost.exe	unknown	76288	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\RMActivate_isv.exe	unknown	597504	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\klist.exe	unknown	37376	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\EduPrintProv.exe	unknown	95232	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\MuiUnattend.exe	unknown	100352	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\tabcal.exe	unknown	82944	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\hid.dll	unknown	34816	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\DiskSnapshot.exe	unknown	91136	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\AtBroker.exe	unknown	62976	success or wait	1	14005F8D6	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{3590B5FE-00A4-E004-AD8F-0BDD685FC0B4}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{3590B5FE-00A4-E004-AD8F-0BDD685FC0B4}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{7987EB03-4175-48A9-6C3C-32D9ECEDB8E2}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{7987EB03-4175-48A9-6C3C-32D9ECEDB8E2}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{1E945B24-CF9D-2794-1752-9E04142F6969}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{1E945B24-CF9D-2794-1752-9E04142F6969}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{BD43B94C-BAC2-5EBF-E645-DEB45DC3A5CB}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{BD43B94C-BAC2-5EBF-E645-DEB45DC3A5CB}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{D35FDE86-D09C-AC74-9C4F-A1BAC7DBDE82}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{D35FDE86-D09C-AC74-9C4F-A1BAC7DBDE82}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{1A2A7A4B-1B31-BC76-DEB7-38E3D2E58C97}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{1A2A7A4B-1B31-BC76-DEB7-38E3D2E58C97}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{15D8B29A-9209-8100-8220-1FE8DB3EB636}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{15D8B29A-9209-8100-8220-1FE8DB3EB636}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{973F6FBC-CC07-A008-5AF9-9FE0E22365F5}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{973F6FBC-CC07-A008-5AF9-9FE0E22365F5}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{68465133-398A-8433-7923-2F5B3670B20D}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{68465133-398A-8433-7923-2F5B3670B20D}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{185C7A05-ABA1-0277-B026-F8B2FE85DDCE}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{185C7A05-ABA1-0277-B026-F8B2FE85DDCE}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{9F9E9D35-2B91-CEBE-3106-8CB23F631603}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{9F9E9D35-2B91-CEBE-3106-8CB23F631603}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{6C87BABA-EF4C-D846-E6FF-7ED409B04688}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{6C87BABA-EF4C-D846-E6FF-7ED409B04688}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{F0D62550-2624-F785-54B4-5E21E03BCDAB}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{F0D62550-2624-F785-54B4-5E21E03BCDAB}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{8D4D8287-C027-7636-CF2F-321286AAC3BF}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{8D4D8287-C027-7636-CF2F-321286AAC3BF}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{38E8CFF9-ABD1-2215-FDC3-BCBF3342086C}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{38E8CFF9-ABD1-2215-FDC3-BCBF3342086C}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{08F441E3-E48C-1109-2135-D95E5CF8D843}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{08F441E3-E48C-1109-2135-D95E5CF8D843}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{B552FE19-73FC-8E2A-9FAA-F468729D6772}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{B552FE19-73FC-8E2A-9FAA-F468729D6772}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{EDDB4C75-B656-DA6D-9182-1CFF1FD2B012}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{EDDB4C75-B656-DA6D-9182-1CFF1FD2B012}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{9F9E9D35-2B91-CEBE-3106-8CB23F631603}\ShellFolder	{B67C9B69-79EE-EFBB-1D56-DA6CC8C52089}	binary	EB 4C 10 BA 88 F8 F7 7A 48 12 43 DA DF AE 0D 9C 23 A3 70 DB A4 42 32 10 E4 C7 E7 69 ED 64 4C 86 33 06 69 7F FE 4D 94 7B BE A2 3F C1 E0 E7 E4 54 3C 5A 70 03 0F 7E 34 B6 AF 10 27 07 23 CA 3D 3D D7 1A 30 58 E1 19 DB	success or wait	1	140062470	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{68465133-398A-8433-7923-2F5B3670B20D}\ShellFolder	{BE94D293-3B8F-89D6-1DCA-8E8CA9EDEB0F}	binary	B5 6A FE CD AF 2E 5D 8F C5 F4 96 45 4B 38 5F 74 FA 16 AA 5A 1C A7 CA 3B EF 50 6F C3 71 CD D9 11 A7 E3 47 6C AA 8B 8E 66 61 3F 60 37 D1 40 17 79 14 0B 7C DB CB 8E DE C6 74 28 ED 54 02 1F 9F 90 40 16 57 BD 6C B0 AD 06 80 01 91 23 03 49 36 9A 9F 88 07 1F 69 08 A4 87 F5 D7 E2 30	success or wait	1	140062470	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{9F9E9D35-2B91-CEBE-3106-8CB23F631603}\ShellFolder	{09CCCB12-23D0-9A45-31B3-8960A66DBE17}	binary	DB 54 89 FD 91 9C 47 0E A0 BC 5B 29 D4 8E C5 38 6C 31 99 69 03 DA FB 64 C8 92 E4 1D E5 CA 2D BA FC D8 73 2C 7E D0 B4 37 DE D7 A7 CC 16 EB 10 67 E0 F1 89 69 54 85 9B 03 8C C7 51 DB 71 A7 9D 45 4E 88 E0 29 96 84 A2 82 61 92 30 45 ED 37 19 1F AC 4C D7 04 94 8C 16 B0 62 BE AC 28 C2 DA 91 38 2C 24 21 B6 F2 93 82 8C 4D E1 3B E3 88 66 BF 5C E3 8B C4 7F 2E 10 92 BE DA C8 F9 05 15 C1 5B 59 A9 13 09 E6 FF 68 9E 27 A4 98 06 56 85 93 42 47 DE CD FF 69 84 1E A9 9E FE 57 4D AA 74 E4 6A C3 06 A9 DA 71 07 61 1F FB 11 BB D5 F3 58 60 62 A7 3B E0 DD 72 15 86 E8 BF BB DD 16 76 6E 99 9A 3B C5 09 AB 46 85 63 C1 B3 C7 CC 18 8A 5E 43 FA CC D2 65 4F 09 38 A9 41 4E 96 FC AC 36 29 E1 B5 0D 1F 04 D4 F3 35 DE 0B B8 DF 1D 26 76 44 91 07 9E B2 B2 88 F8 FD F3 4A 78 21 26 7B 4D 86 7D 0C 14 F5 6F EF F6 C3 FF D2 ED 9E 0F 56 7C 6D FD 4A 3D 43 D5 D1 B7 E6 B9 F7 37 C3 63 75 F6 4E CA 86 E9 75 57 41 A9 AE 59 62 81 0F BB 54 95 F1 BC 4B DF 95 9F 20 A9 89 63 32 4C A0 77 26 0B F9 D9 B2 B4 ED 67 DC 1F 71 3A E1 BF 08 71 EA A4 F4 00 6F 3C 56 FE 88 9D 63 27 3E AB EF 34 B1 43 0B 69 AB F8 4A 99 71 4A 51 33 A2 8A AF 5D 39 D0 6A 83 84 F0 A7 8A B6 A2 F5 65 C4 A7 9E F8 AE 78 99 C2 60 0C 82 95 CE 03 7E 04 7B 16 ED A7 38 27 92 43 94 A3 25 D9 9B 2E BE 0A E2 28 38 9A BA 31 26 A0 7B 2A 9B 07 5F AA EB AC AF 99 B2 27 2A 23 DD B5 05 3C 32 9B 00 40 F5 90 69 07 26 C0 D0 05 29 A3 6C 51 8D D2 27 0E 53 51 28 CF 91 B7 9A BC 0F 34 65 F9 D5 99 31 49 F9 7E 0A 93 AA 87 37 2F 00 7A 45 1A 93 32 2F 7C 84 2D 0F D3 C3 9D 07 73 31 BB 06 7E 70 12 F7 E6 8A D9 FF C4 3B 84 5E 2C 28 55 7D AD A0 9A 40 19 45 02 D2 6A EB C3 7B B8 7D 8F A1 E2 E5 10 22 87 DC ED 6D EB 41 C3 3A 0F 89 80 6B EB 38 24 E8 C9 C6 FD B2 22 89 21 DD D0 C5 69 F3 8C FF 12 28 3A E8 6F AE EA 52 0D EC 5E C8 AA 14 52 78 AF FB 25 62 09 D1 33 C9 7F CD 33 C6 0B 86 24 5E 87 3C A4 13 43 26 30 AF AE E3 D7 9D 10 8C 6B 4D 51 5F 15 DE F3 93 2E 69 F2 8C 01 DF 78 8E 77 D7 EE 1F C4 00 4F B3 E9 B0 63 DA C6 71 19 EC 98 79 6B 92 7B 19 B9 52 19 4F 65 EB C9 7C A2 CE F9 05 CF C4 A4 1C CE 73 66 FE A8 3A EA 49 B4 03 6D 03 39 EC 7C 91 42 45 09 41 73 83 7F 9E D0 D3 93 49 E0 9A 8F 13 49 41 A2 AD D9 CA 9A E5 0A 7A F6 D8 50 AE 8D 76 FD 8B 3F 9F 34 45 37 1B 9A DD 3F 07 FD D2 F5 47 42 5E 0C 93 A8 17 B1 AA 9D 1D F9 C0 13 B8 66 FD FC A7 3D 20 2B 23 9B 6B 1B 5A 17 F7 2A CD AE A9 92 15 D8 6A FA 57 F7 A2 51 85 DC 8E 14 31 7B B6 F2 B2 05 78 AD 46 92 D2 C7 0C 2C 39 82 55 A9 FD 73 35 C2 BA 08 DE 9B 05 79 C5 FA F6 6F DE 1A DA 80 0C D7 DD AD A1 F9 F6 6A 6C 91 93 6F 19 81 51 FB D3 06 C9 41 04 F9 08 A4 AB 77 71 D2 4C 36 14 3B C0 15 58 8F 9F D7 C5 95 7E 8D 83 C2 14 16 F1 1B F3 16 EC D1 20 8A AA F6 27 AA E0 83 65 96 44 94 5C 2C 6B CD EE 63 2C 4F 27 A2 5B A5 35 83 9B 20 3E B8 E3 7D	success or wait	1	140062470	RegSetValueExA

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			74 00 E9 4E 36 19 2D 4C B4 B5 45 A3 DA 70 14 B1 4A 77 44 16 97 A0 13 57 6D E1 63 89 9F C6 39 64 1D 0B 26 68 5D 5E 9C D0 11 82 AE 11 C4 EB 33 59 97 AF B5 16 33 01 F5 A5 A2 2D 67 E6 D0 48 8F BB 45 B1 70 CC 03 C7 56 A8 4D 16 08 CF 57 89 A8 09 36 89 97 2D 3B E0 55 81 D3 B3 18 62 52 2C 36 96 08 4B 30 23 1B FE 7F 63 17 5B F6 B0 E8 4E F2 86 88 A0 D0 2E 41 81 DA 89 6D 8A 0B 0E EC 72 F9 F1 05 27 49 97 5B C4 E4 99 6A F5 1E E5 3D 89 FB 2E AB 14 19 2F 0B C8 A4 0D D5 04 C8 FD 86 71 92 77 6B B4 5D C1 E1 51 84 D2 63 13 18 7B 71 FA 25 73 C6 69 55 A9 FD 43 5C B6 0C 4C 12 AC 43 B1 F9 CE EF 13 C6 D5 61 3A E4 0D 7C 17 3E 67 71 FF E9 1D DD 6D CF FE 6A 28 85 62 58 FE 46 2A 98 13 C9 64 11 D2 82 2A B1 A4 EE 51 50 62 6B E8 1F 1E CF 83 D7 B1 3E 08 6B E2 1B 67 43 F5 87 FD 6C CF D3 83 D8 F1 A5 30 5B DE 23 22 09 EF 26 B4 C7 7E 61 EE EF 7E C2 A4 78 57 00 CC 58 30 05 EA FC 35 16 DF 4F 41 56 1F 27 5B 5C 7D 84 D4 EC 5F 7B 67 08 0A 04 F7 C9 ED 74 64 E9 6A CE 7B F8 E7 27 A1 14 F7 33 A4 23 BB 51 00 8C 0B B3 01 0D 2C B0 65 8B 44 52 C1 69 95 81 9F 9A E7 80 6F FF 86 E3 41 38 8F AB 71 03 67 D4 3A 81 73 95 77 B6 34 A3 E8 BF D2 E4 38 52 C7 63 31 93 B0 9A 90 AF 13 78 B3 5E 11 E3 58 43 FE 83 5B A9 93 7D ED 37 BE EC D5 B2 02 86 54 B5 2C 45 97 8F 2D A1 3E CD C7 16 28 E1 9E BE F2 1B 19 76 C5 0C BD 23 E3 CB D9 5F DB C5 CF 08 9C 3F 1A 52 9C 58 D0 A8 5C 27 1D E2 FB 0A 0D 09 70 79 BA F1 7C 6B ED 1E DD E1 B4 70 85 95 E4 34 93 EC 2E 4E 82 21 AE 97 DC 57 DE CD 5C D6 F2 DA 5B 71 7A 9C 20 CF FF 0D 4E 99 F7 F2 F1 48 EA E7 1C 57 99 D8 4B 14 59 AA 53 79 A7 CC AD 70 0B C4 9F 20 45 5A FE E2 6E CF 85 EC A7 C9 37 95 AD 29 FD E0 74 7B EC EC 17 07 0E 72 31 B0 83 F3 51 40 5A D0 DC 94 C9 BF B3 71 86 4E CC 38 BC 1F 57 5C 03 E7 49 6F 8D DD 02 41 17 57 F8 ED 77 39 9F 29 BD F4 6D 5C 06 9E 19 80 57 86 F6 17 B0 8A 82 08 F7 DB 96 6A AE 21 16 02 A0 A4 24 41 C3 F6 75 F0 C5 E8 D0 BE FB 1C 49 8A 30 F2 19 EA DE DE FB 30 FD CE A6 46 14 88 79 74 77 D2 42 8B D2 92 02 51 18 F4 F4 9B B6 A5 21 37 62 6E D8 D0 91 60 45 2D 72 8D B3 64 69 C0 87 E8 DF F6 E1 9C 11 F5 EF 21 DF 86 D8 A0 36 D3 BB 9B E3 55 EF 6A BE 59 23 C3 9D 38 73 64 B2 20 1D FC B6 F1 BA 24 CE FD DB 55 4A 92 20 7A 8F 8A 68 AF 31 A2 23 F5 BC 5C BF D9 EC C5 1F 52 7F CC 64 B4 B3 9D 27 7B 81 37 BA 16 29 91 F1 E0 60 BB A9 F9 E0 10 C2 F6 54 AC 66 90 1A 72 4C B8 CF 46 A6 61 D1 D7 1C F7 9D 3A 6E 29 CA 73 0B 1C 1A 08 BE E6 B5 CD 85 19 58 AD 60 AE F1 84 64 FE 23 1C 89 70 A3 DD 2D C6 4F 87 32 C8 7D 51 39 C7 D2 73 24 7E 57 60 A2 78 65 EE 22 B5 0B EE F4 DA F4 FF A6 E1 19 0D 75 39 A0 F2 E8 AF E1 38 04 F5 3E 8D 6F 27 43 DC 3C 1C A5 00 EC AE 05 F0 85 BA D0 21 65 99 78 12 6A 65 96 B5 BB DC DC F6 75 7A E0 72 03 74 C5 43 77 B0 E3 0B B8 23 0E 9C 33 EC 81 73 3D E2 9C C4 DA 23 23 3A 67 80 8B 46 EA 2A CB 50 3D 04 C5 79 D0 F6 AD A9 88 FE B0 18 C7 E1 4F CA 4C 55 9C D0 B6 F8 76 D1 A1 2A D3 81 87 F0 40 3C 12 13 19 C9 DE FE F9 4E 13 CE 46 D7 4D C0 99 FB 8E 2F 1F 18 45 13 CF F5 BE D5 0A 94 B2 0D 1A FB 5C CE A0 F0 C7 19 B1 3D 0E 55 A7 95 53 4C 08 16 04 FD				
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{9E56D35-2B91	{00000000-0000-0000-0000-000000000000}	binary	4A 69 DB BA 36 D0 15 E4 2A 71 66 FD 00 8A F8 90 AB 51 42 24 3C 1F E5 66 17 E7 56 5C 62 AD D4 2B DB	success or wait	1	140062470	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
Explorer\CLSID\{9F9E9D35-2B91-0000000} 6E2E-3106- 8CB23F631603}\ShellFolder			96 B5 CC BD DF C1 FA 12 EC DD 1F A5 74 C3 30 9E 92 EE C0 D2 AF 5B 14 E1 8D D7 12 A8 DF 9F B4 2C B9 B8 51 0B 10 FA DE F8 1D B5 34 75 ED 76 A1 BF CC C2 B2 42 FE 1E 8F BF 1A 6C B7 45 6A 3A 68 DD 7C E7 92 4B 7A 92 C6 F0 3C 4F FF A7 8E 2A E8 52 D9 45 7E A6 71 01 CE 6D F5 CF C0 B6 EE 88 B1 17 12 32 E0 6D 4F 34 25 1C 9F 28 5A 0F EF 65 CE 5C 6D 65 E6 3B 86 38 03 49 8A B3 1E F4 5C F5 00 F7 AF 42 87 C3 C4 A2 A0 52 38 6C 2D F7 A8 F5 93 07 8B 04 3A F2 23 17 1B C0 66 3A 69 0A 44 13 8C F5 21 94 0E E3 C8 6C 1B 58 F6 95 43 B7 8A 57 29 68 A7 C3 ED 79 6A 9B F6 03 71 9B 29 DA C0 A6 ED 46 D5 0B 48 5A 97 5D 4B 58 64 21 FF 9C 43 03 A0 EA AC BB EE 14 0C 9C BC C4 6C A9 FC 8E 1D B0 B7 6C 0E B3 27 C0 C4 D3 80 30 43 87 11 98 8E B2 D2 8F 69 96 FE 24 94 12 B5 E1 C9 83 4E 3B 89 27 EC 9E 48 F2 05 F9 88 47 8D A2 97 8D 05 63 12 26 63 F8 DD 0D 8D 68 1C 29 C3 1B 1C CE 09 CB 35 03 62 02 0A E7 D9 7F E9 FD 62 2B 8E 31 00 C8 99 98 85 86 DF B3 6B AD FD F8 53 39 B8 75 AB C5 03 A4 90 9B 1C 1E 6A 16 21 F7 81 15 23 09 1E 40 9C 12 1D 9A 2C 53 C4 C3 C0 8B 4B 64 40 E7 D3 74 DC 37 CD 42 D7 7B 2C 14 04 41 5D 6B 37 5D CD C9 DE B7 75 BB 02 51 FB E4 1F C9 EB 0C 76 DB 3B 9E 05 B1 D4 78 F0 35 83 C4 F7 9E CF 93 B3 44 6A 75 EB F5 4E 70 06 9F B5 86 3E 29 04 E7 6C 3A BA 15 67 13 04 93 DE F4 CA EC FC C6 21 60 AD 42 97 21 23 AC 9F DC E9 06 11 E8 04 E5 60 B6 65 01 DC 2A 46 56 F0 1F 44 6B CA 26 20 52 A9 14 2F F7 48 32 B4 63 96 C6 F8 08 71 69 5E 8E 13 AA B4 05 37 B7 C7 73 56 3D 6B DF 36 34 F1 1E 64 B1 DE 01 D1 99 4C A3 3B A1 97 7D 92 DD 2E 29 56 07 C2 EC 7A AC 89 01 F3 AB 9B 5B 49 CE 25 54 C1 A0 3A BA F4 7C 66 7F 5D 63 A4 39 55 25 09 C2 3C 8F C5 D9 56 22 20 98 A1 35 B5 FA 41 6B 18 7B E9 94 77 A8 74 0B 8D D5 2E E7 97 D8 51 0F 1D 58 7D 77 0C 81 2C F6 91 E0 FF 46 7E 40 71 B1 09 72 8A 86 8F 5D EB F3 04 19 A1 45 ED A3 8B 71 33 46 36 D4 30 70 D4 1B 7D 01 93 89 A9 48 BE 18 86 08 4E 1D 1C 49 53 5F 53 3B 1F A6 78 C1 49 18 E9 13 6C D6 5B DB 10 27 D4 AB E8 69 C1 AC 03 9C 33 27 9A CF B7 59 4F 8A 2A C5 9F E9 55 32 47 4F 11 FE B0 2B A4 A1 EC 65 3C 86 99 02 2C EB 5D 79 6B 78 B9 37 C0 33 15 0C A6 C6 83 45 F6 E7 E1 8C 7B DC 49 EE 4E 5E E7 81 92 28 6D 82 88 03 53 E2 37 79 C5 75 6C D9 24 D0 9E C2 FB D5 ED E7 5F E2 EE 41 E6 C8 A7 E0 B4 32 FD F1 75 B8 7D 16 80 B5 A5 C7 CF F7 85 E4 19 00 73 99 3E DA 0F EF DF 97 DD 62 90 75 9B E1 3B D1 40 74 8B 7D F4 DE B6 F9 4D 22 44 4F 5E B1 55 11 5C CB 4C D3 F4 EB B6 51 2C D5 AF 40 6D 42 75 66 D2 71 D9 27 B6 D5 92 3B A2 C5 ED 34 A9 10 AE 06 E8 91 FB 32 8E A0 27 8A 07 E9 C1 07 61 13 BB 6D AB A5 71 7E 76 D0 84 6A CC 10 F6 69 DC 20 62 1C 40 D7 01 96 25 1B 53 8A 3D 5B 6F 2B B4 10 86 D4 A2 69 62 B4 12 ED 43 9D B1 31 1A 2F 75 F3 85 25 52 2C D9 E7 EF F0 82 7F 4C BE 27 CC 9C CF 5A 7F F3 58 BC 46 19 0D E6 78 0A 93 E6 AB A3 90 95 B6 A1 2E 5C BA 52 F5 47 93 18 2B 5D FB 1D 09 9C DC 86 A1 89 C9 01 4C E0 DF B4 A3 7C B1 31 53 AD 1E 14 9B 42 22 37 5D 5A B2 AA 30 74 76 91 FA 95 C4 DE 53 0F 9B 4C 43 DC 6C 48 C5 DE 0F 13 5B A5 20 22 59 45 8E 80 56 73 6D 5C F5 C8 DE 11 E5 4E C1 90 5D 15 D0 A7 44 DF F0 C3 69 C8 5C 66 B1 9E 57 9C CF DC BB E6 51 2A 52 B6 C9 CD D6 95 27 AC 91 ED 54 99 A6 3F				

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

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

Analysis Process: rundll32.exe PID: **5880**, Parent PID: **4592**

General

Target ID:	9
Start time:	17:44:02
Start date:	27/02/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\dpnhupnp.dll,GetFileVersionInfoByHandle

Imagebase:	0x7ff6f85c0000
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: 00000009.00000002.285131581.00007FFC6F9E1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\dpnhupnp.dll	unknown	1064960	success or wait	1	7FFC6FA3F8D6	ReadFile

Analysis Process: rundll32.exe PID: **7008**, Parent PID: **4592**

General

Target ID:	14
Start time:	17:44:06
Start date:	27/02/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\dpnhupnp.dll,GetFileVersionInfoExA
Imagebase:	0x7ff6f85c0000
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: 0000000E.00000002.293533164.00007FFC6F9E1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\dpnhupnp.dll	unknown	1064960	success or wait	1	7FFC6FA3F8D6	ReadFile

Analysis Process: DisplaySwitch.exe PID: **2172**, Parent PID: **3352**

General

Target ID:	18
Start time:	17:44:39
Start date:	27/02/2022
Path:	C:\Windows\System32\DisplaySwitch.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\DisplaySwitch.exe
Imagebase:	0x7ff7df870000
File size:	1930224 bytes
MD5 hash:	97411B8A84E5980E509E500C3209E5C0
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: DisplaySwitch.exe PID: **1740**, Parent PID: **3352**

General

Target ID:	20
Start time:	17:44:41
Start date:	27/02/2022
Path:	C:\Users\user\AppData\Local\4xeLXaDKW\DisplaySwitch.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\4xeLXaDKW\DisplaySwitch.exe
Imagebase:	0x7ff701bc0000
File size:	1930224 bytes
MD5 hash:	97411B8A84E5980E509E500C3209E5C0
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000014.00000002.392236668.00007FFC6F9E1000.00000020.00000001.01000000.00000008.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\4xeLXaDKW\WINSTA.dll	unknown	1073152	success or wait	1	7FFC6FA3F8D6	ReadFile

Analysis Process: wusa.exe PID: **5472**, Parent PID: **3352**

General

Target ID:	21
Start time:	17:44:54
Start date:	27/02/2022
Path:	C:\Windows\System32\wusa.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wusa.exe
Imagebase:	0x7ff75cc10000
File size:	308736 bytes
MD5 hash:	04CE745559916B99248F266BBF5F9ED9
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: GamePanel.exe PID: **4868**, Parent PID: **3352**

General

Target ID:	22
Start time:	17:44:54
Start date:	27/02/2022
Path:	C:\Windows\System32\GamePanel.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\GamePanel.exe
Imagebase:	0x7ff707610000
File size:	1292288 bytes
MD5 hash:	4EF330EFAE954723B1F2800C15FDA7EB
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: GamePanel.exe PID: **5712**, Parent PID: **3352**

General

Target ID:	24
Start time:	17:44:56
Start date:	27/02/2022
Path:	C:\Users\user\AppData\Local\uRSIQRt4\GamePanel.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\uRSIQRt4\GamePanel.exe
Imagebase:	0x7ff7754a0000
File size:	1292288 bytes
MD5 hash:	4EF330EFAE954723B1F2800C15FDA7EB
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: 00000018.00000002.424452492.00007FFC6F9E1000.00000020.00000001.01000000.0000000A.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\uRSIQRt4\dxgi.dll	unknown	1069056	success or wait	1	7FFC6FA3F8D6	ReadFile

Analysis Process: msdt.exe PID: **4792**, Parent PID: **3352**

General

Target ID:	31
Start time:	17:45:09
Start date:	27/02/2022
Path:	C:\Windows\System32\msdt.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msdt.exe
Imagebase:	0x7ff7021e0000
File size:	1560576 bytes
MD5 hash:	8BE43BAF1F37DA5AB31A53CA1C07EE0C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: msdt.exe PID: **4796**, Parent PID: **3352**

General

Target ID:	32
Start time:	17:45:15
Start date:	27/02/2022
Path:	C:\Users\user\AppData\Local\1XXGC21\msdt.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\1XXGC21\msdt.exe
Imagebase:	0x7ff7299c0000
File size:	1560576 bytes

MD5 hash:	8BE43BAF1F37DA5AB31A53CA1C07EE0C
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: 00000020.00000002.463842556.00007FFC6E2A1000.00000020.00000001.01000000.0000000C.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\1XXGC21\DUI70.dll	unknown	1351680	success or wait	1	7FFC6E2FF8D6	ReadFile

Analysis Process: cmstp.exe PID: 6272, Parent PID: 3352

General

Target ID:	34
Start time:	17:45:27
Start date:	27/02/2022
Path:	C:\Windows\System32\cmstp.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmstp.exe
Imagebase:	0x7ff792300000
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: 6384, Parent PID: 3352

General

Target ID:	35
Start time:	17:45:29
Start date:	27/02/2022
Path:	C:\Users\user\AppData\Local\M4eXJF\cmstp.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\M4eXJF\cmstp.exe
Imagebase:	0x7ff7de0b0000
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: 00000023.00000002.491431291.00007FFC7C2F1000.00000020.00000001.01000000.0000000E.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: PresentationHost.exe PID: 4516, Parent PID: 3352

General

Target ID:	37
Start time:	17:45:40
Start date:	27/02/2022

Path:	C:\Windows\System32\PresentationHost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\PresentationHost.exe
Imagebase:	0x7ff77cd10000
File size:	259072 bytes
MD5 hash:	E3053C73EA240F4C2F7971B3905A91CF
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: PresentationHost.exe PID: **2208**, Parent PID: **3352**

General

Target ID:	38
Start time:	17:45:41
Start date:	27/02/2022
Path:	C:\Users\user\AppData\Local\a6o\PresentationHost.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\a6o\PresentationHost.exe
Imagebase:	0x7ff76ed90000
File size:	259072 bytes
MD5 hash:	E3053C73EA240F4C2F7971B3905A91CF
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000026.00000002.520892941.00007FFC7C2F1000.00000020.00000001.01000000.00000010.sdmp, Author: Joe Security

Analysis Process: cmstp.exe PID: **2880**, Parent PID: **3352**

General

Target ID:	39
Start time:	17:45:54
Start date:	27/02/2022
Path:	C:\Windows\System32\cmstp.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmstp.exe
Imagebase:	0x7ff792300000
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: **5004**, Parent PID: **3352**

General

Target ID:	40
Start time:	17:45:55
Start date:	27/02/2022
Path:	C:\Users\user\AppData\Local\96P3D\cmstp.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\96P3D\cmstp.exe
Imagebase:	0x7ff72be30000
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: 00000028.00000002.548047896.00007FFC7C2F1000.00000020.00000001.01000000.00000012.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

Disassembly

No disassembly