ID: 595305
Sample Name: GpUSRuIBHx
Cookbook: default.jbs
Time: 15:41:42
Date: 23/03/2022
Version: 34.0.0 Boulder Opal

Table of Contents

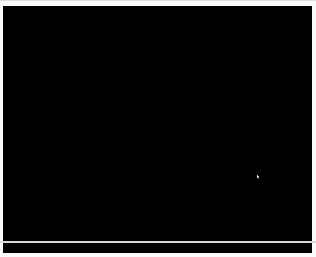
Windows Analysis Report

GpUSRuIBHx

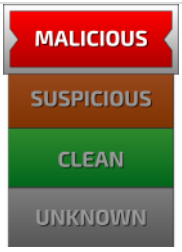
Overview

General Information

Sample Name:	GpUSRuIBHx (renamed file extension from none to dll)
Analysis ID:	595305
MD5:	288c35481252c1..
SHA1:	9c48ba2239b5ae..
SHA256:	cb793c295b0bcd..
Tags:	Dridex exe
Infos:	



Detection



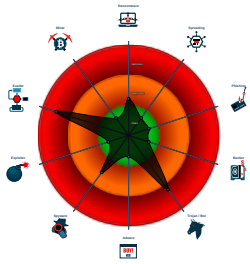
Dridex

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

Signatures

- Yara detected Dridex unpacked file
- Multi AV Scanner detection for subm…
- Benign windows process drops PE f…
- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Changes memory attributes in foreig…
- Machine Learning detection for sam…
- Queues an APC in another process …
- Sigma detected: Suspicious Call by…
- Machine Learning detection for drop…
- Contains functionality to automate e…
- Uses Atom Bombing / ProGate to in…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 852 cmdline: loaddll64.exe "C:\Users\user\Desktop\GpUSRuIBHx.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 6932 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\GpUSRuIBHx.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 7012 cmdline: rundll32.exe "C:\Users\user\Desktop\GpUSRuIBHx.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 7036 cmdline: rundll32.exe C:\Users\user\Desktop\GpUSRuIBHx.dll,??0VolumeFveStatus@@IEAA@XZ MD5: 73C519F050C20580F8A62C849D49215A)
    - explorer.exe (PID: 3808 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - BackgroundTransferHost.exe (PID: 5856 cmdline: "BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1 MD5: 02BA81746B929ECC9DB6665589B68335)
      - FileHistory.exe (PID: 5804 cmdline: C:\Windows\system32\FileHistory.exe MD5: 989B5BDB2BEAC9F894BBC236F1B67967)
      - FileHistory.exe (PID: 6388 cmdline: C:\Users\user\AppData\Local\6f22a\FileHistory.exe MD5: 989B5BDB2BEAC9F894BBC236F1B67967)
      - rdpinput.exe (PID: 6940 cmdline: C:\Windows\system32\rdpinput.exe MD5: 4403785D297C55D5DF26176B4F1A52C8)
      - rdpinput.exe (PID: 6992 cmdline: C:\Users\user\AppData\Local\Kyz7D\rdpinput.exe MD5: 4403785D297C55D5DF26176B4F1A52C8)
      - SndVol.exe (PID: 6428 cmdline: C:\Windows\system32\SndVol.exe MD5: CDD7C7DF2D0859AC3F4088423D11BD08)
      - SndVol.exe (PID: 6436 cmdline: C:\Users\user\AppData\Local\bTcR2e\SndVol.exe MD5: CDD7C7DF2D0859AC3F4088423D11BD08)
      - SnippingTool.exe (PID: 7052 cmdline: C:\Windows\system32\SnippingTool.exe MD5: 9012F9C6AC7F3F99ECDD37E24C9AC3BB)
      - SnippingTool.exe (PID: 5480 cmdline: C:\Users\user\AppData\Local\LoReH\SnippingTool.exe MD5: 9012F9C6AC7F3F99ECDD37E24C9AC3BB)
      - slui.exe (PID: 5012 cmdline: C:\Windows\system32\slui.exe MD5: 96A8EF9387619D17BB30B024DDF52BF3)
      - slui.exe (PID: 3852 cmdline: C:\Users\user\AppData\Local\2Yf2pw501\slui.exe MD5: 96A8EF9387619D17BB30B024DDF52BF3)
      - rdpinput.exe (PID: 4236 cmdline: C:\Windows\system32\rdpinput.exe MD5: 4403785D297C55D5DF26176B4F1A52C8)
      - rdpinput.exe (PID: 780 cmdline: C:\Users\user\AppData\Local\Fjrn\rdpinput.exe MD5: 4403785D297C55D5DF26176B4F1A52C8)
      - printfilterpipelinesvc.exe (PID: 5112 cmdline: C:\Windows\system32\printfilterpipelinesvc.exe MD5: 4164BD4D8E23C672E40D203E4B4A38A7)
      - printfilterpipelinesvc.exe (PID: 4752 cmdline: C:\Users\user\AppData\Local\2HophZ6P\printfilterpipelinesvc.exe MD5: 4164BD4D8E23C672E40D203E4B4A38A7)
      - Utilman.exe (PID: 1508 cmdline: C:\Windows\system32\Utilman.exe MD5: C91CCEF3884CFDE746B4BAEF5F1BC75C)
      - Utilman.exe (PID: 1332 cmdline: C:\Users\user\AppData\Local\D6R1uM\Utilman.exe MD5: C91CCEF3884CFDE746B4BAEF5F1BC75C)
      - phoneactivate.exe (PID: 2912 cmdline: C:\Windows\system32\phoneactivate.exe MD5: 09D1974A03068D4311F1CE94B765E817)
      - phoneactivate.exe (PID: 5856 cmdline: C:\Users\user\AppData\Local\op5PCy\phoneactivate.exe MD5: 09D1974A03068D4311F1CE94B765E817)
      - DmNotificationBroker.exe (PID: 6180 cmdline: C:\Windows\system32\DmNotificationBroker.exe MD5: 1643D5735213BC89C0012F0E48253765)
      - DmNotificationBroker.exe (PID: 6460 cmdline: C:\Users\user\AppData\Local\CSYG\DmNotificationBroker.exe MD5: 1643D5735213BC89C0012F0E48253765)
      - ProximityUxHost.exe (PID: 6936 cmdline: C:\Windows\system32\ProximityUxHost.exe MD5: E7F0E9B3779E54CD271959C600A2A531)
      - ProximityUxHost.exe (PID: 6560 cmdline: C:\Users\user\AppData\Local\oOQGGow\ProximityUxHost.exe MD5: E7F0E9B3779E54CD271959C600A2A531)
      - omadmclient.exe (PID: 244 cmdline: C:\Windows\system32\omadmclient.exe MD5: AD7C6CD7A8EEC95808AA77C5D7987941)
  - rundll32.exe (PID: 6764 cmdline: rundll32.exe C:\Users\user\Desktop\GpUSRuIBHx.dll,??0VolumeFveStatus@@QEAA@K_KJW4_FVE_WIPING_STATE@@@Z MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5872 cmdline: rundll32.exe C:\Users\user\Desktop\GpUSRuIBHx.dll,??4BuiVolume@@QEAAAEAV0@AEBV0@@Z MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000028.00000002.836674261.00007FF8CA681000.00000020.00000001.01000000.00000020.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000026.00000002.791054747.00007FF8CA681000.00000020.00000001.01000000.0000001E.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000016.00000002.541815176.00007FF8CA981000.00000020.00000001.01000000.0000000E.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
0000001C.00000002.616859661.00007FF8CA981000.00000020.00000001.01000000.00000013.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000003.00000002.352441583.00007FF8BA5D1000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	

Click to see the 11 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
22.2.SndVol.exe.7ff8ca980000.3.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
3.2.rundll32.exe.7ff8ba5d0000.2.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
28.2.slui.exe.7ff8ca980000.3.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
25.2.SnippingTool.exe.7ff8ca980000.3.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
18.2.FileHistory.exe.7ff8ca980000.3.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	

Click to see the 11 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

HIPS / PFW / Operating System Protection Evasion

Benign windows process drops PE files

Changes memory attributes in foreign processes to executable or writable

Queues an APC in another process (thread injection)

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

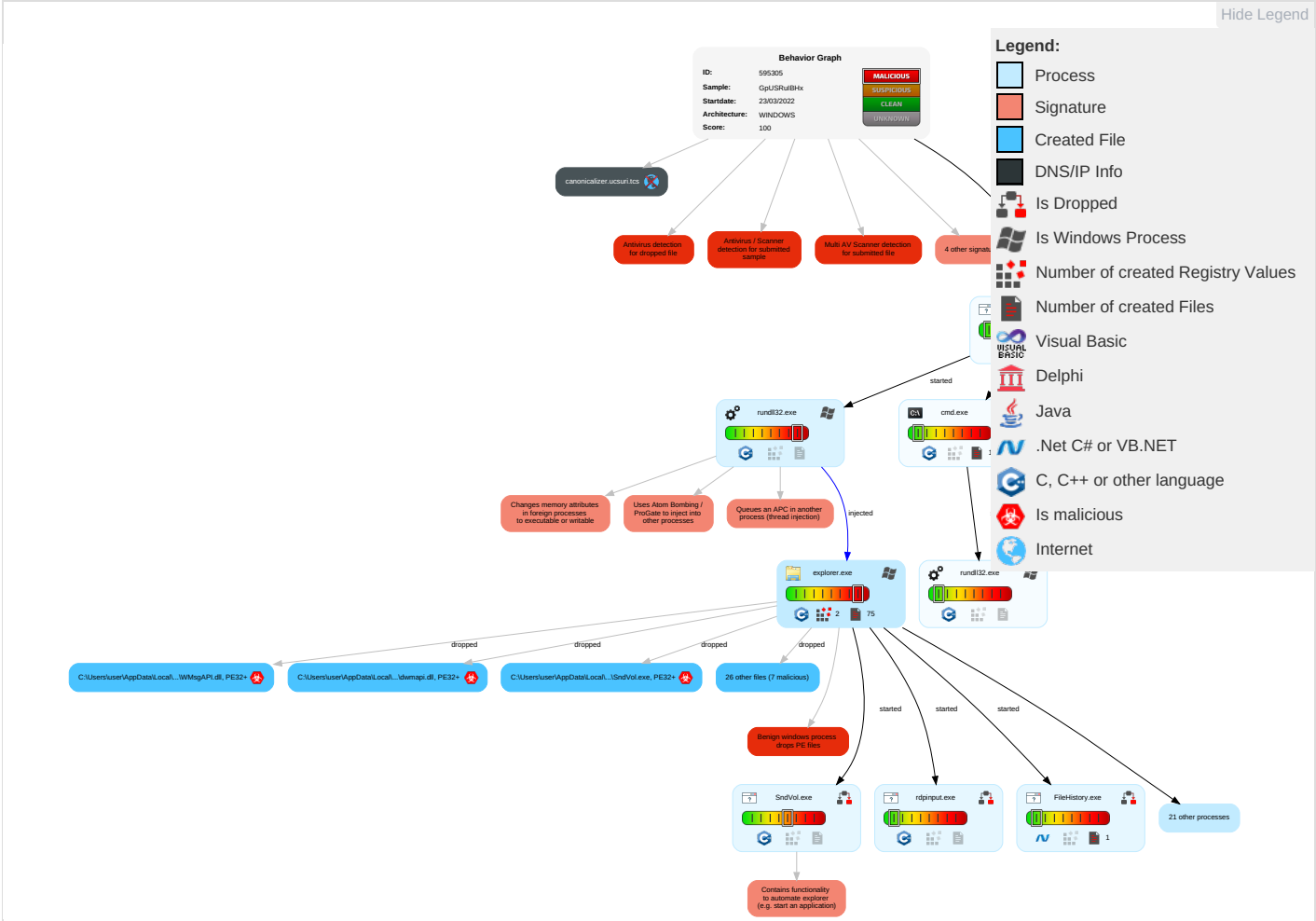
Uses Atom Bombing / ProGate to inject into other processes

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	1 Native API	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Exploitation for Client Execution	1 Windows Service	1 Windows Service	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	1 Clipboard Data	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 Service Execution	Logon Script (Windows)	3 1 2 Process Injection	3 Obfuscated Files or Information	Security Account Manager	1 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	2 Software Packing	NTDS	3 5 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	2 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	2 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 Application Window 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 2 Process Injection	/etc/passwd and /etc/shadow	1 System Owner/User Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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

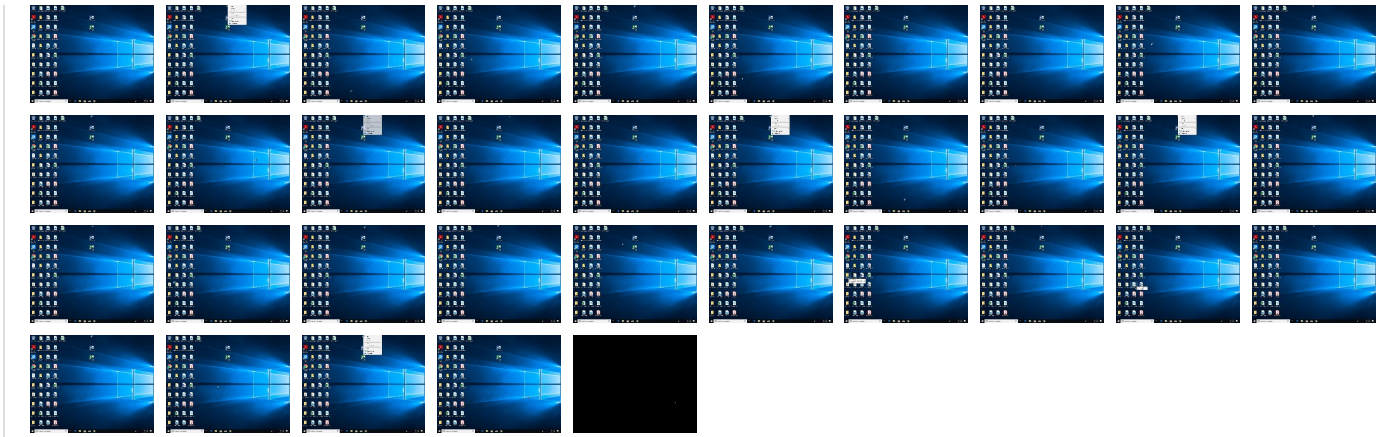
Behavior Graph

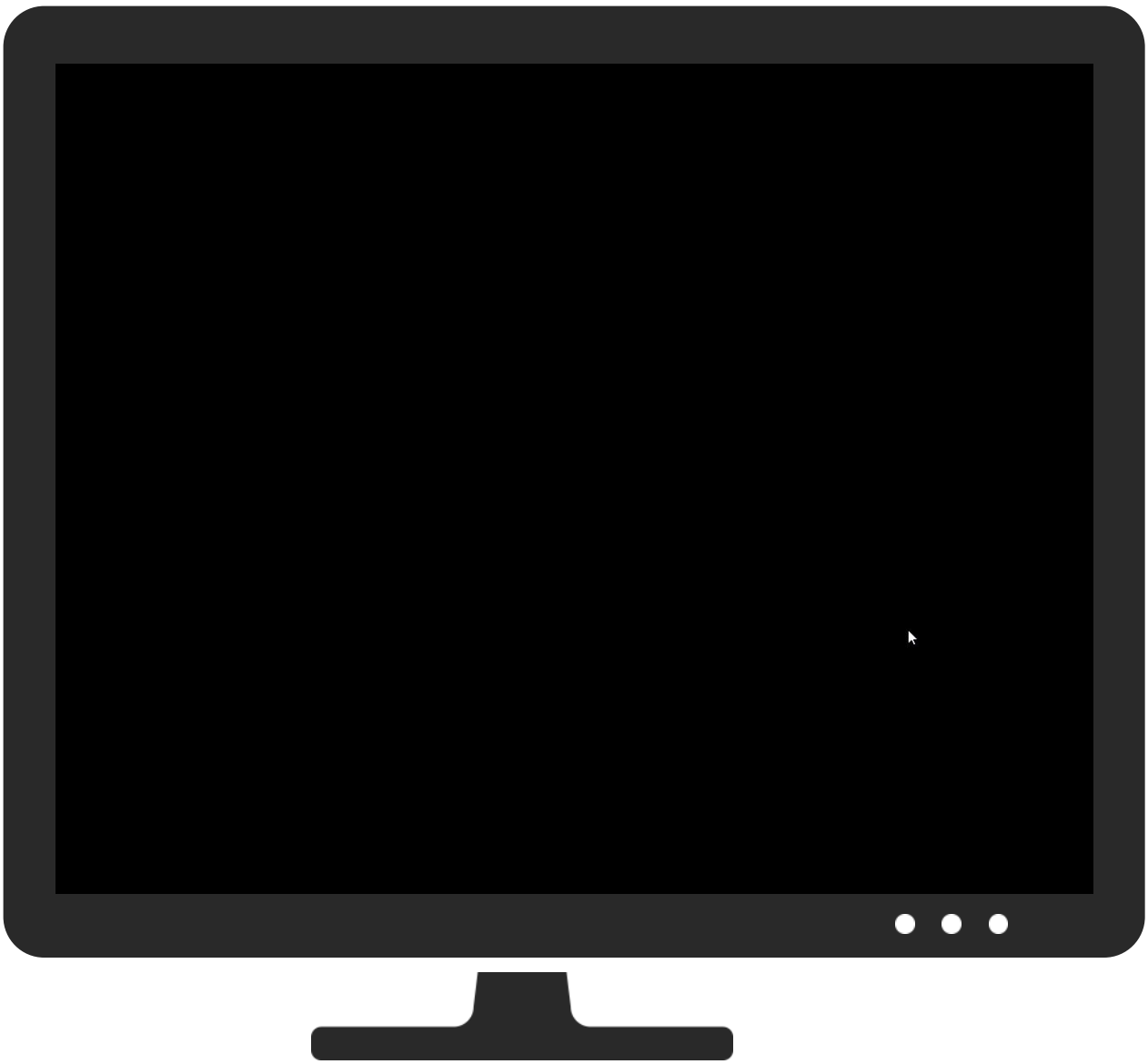


Screenshots

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
GpUSRuIBHx.dll	70%	Virustotal		Browse
GpUSRuIBHx.dll	63%	Metadefender		Browse
GpUSRuIBHx.dll	88%	ReversingLabs	Win64.Trojan.Occamy	

Source	Detection	Scanner	Label	Link
GpUSRuIBHx.dll	100%	Avira	TR/Crypt.XPACK.Gen7	
GpUSRuIBHx.dll	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\2Yf2pw501\WTSAPI32.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\bTcR2e\dwmapi.dll	100%	Avira	TR/Crypt.XPACK.Gen7	
C:\Users\user\AppData\Local\CSYG\DUI70.dll	100%	Avira	TR/Crypt.XPACK.Gen4	
C:\Users\user\AppData\Local\CSYG\DUI70.dll	100%	Avira	TR/Crypt.XPACK.Gen4	
C:\Users\user\AppData\Local\rDAhA\WMsgAPI.dll	100%	Avira	TR/Crypt.XPACK.Gen7	
C:\Users\user\AppData\Local\6f22a\UxTheme.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\2HophZ6P\XmlLite.dll	100%	Avira	TR/Crypt.XPACK.Gen7	
C:\Users\user\AppData\Local\2HophZ6P\XmlLite.dll	100%	Avira	TR/Crypt.XPACK.Gen7	
C:\Users\user\AppData\Local\D6R1uM\DUser.dll	100%	Avira	TR/Crypt.XPACK.Gen7	
C:\Users\user\AppData\Local\CSYG\DUI70.dll	100%	Avira	TR/Crypt.XPACK.Gen4	
C:\Users\user\AppData\Local\2Yf2pw501\WTSAPI32.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\Fjrn\WINSTA.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\6f22a\UxTheme.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\LoReH\OLEACC.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\LoReH\OLEACC.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\2Yf2pw501\WTSAPI32.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\bTcR2e\dwmapi.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\CSYG\DUI70.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\CSYG\DUI70.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\rDAhA\WMsgAPI.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\6f22a\UxTheme.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\2HophZ6P\XmlLite.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\2HophZ6P\XmlLite.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\D6R1uM\DUser.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\CSYG\DUI70.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\2Yf2pw501\WTSAPI32.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Fjrn\WINSTA.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\6f22a\UxTheme.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\LoReH\OLEACC.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\LoReH\OLEACC.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\2HophZ6P\printfilterpipelinesvc.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\2HophZ6P\printfilterpipelinesvc.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\2Yf2pw501\slui.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\2Yf2pw501\slui.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\6f22a\FileHistory.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\6f22a\FileHistory.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\CSYG\DmNotificationBroker.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\CSYG\DmNotificationBroker.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download

Source	Detection	Scanner	Label	Link	Download
18.2.FileHistory.exe.2d7d9c90000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
18.2.FileHistory.exe.7ff8ca980000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.loaddll64.exe.23665550000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
0.2.loaddll64.exe.7ff8ba5d0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
34.2.Utilman.exe.7ff8bb380000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.rundll32.exe.7ff8ba5d0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.2.rdpinput.exe.1edbea50000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
22.2.SndVol.exe.7ff8ca980000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
40.2.ProximityUxHost.exe.1b64bc90000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
28.2.slui.exe.7ff8ca980000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
25.2.SnippingTool.exe.7ff8ca980000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.rundll32.exe.7ff8ba5d0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.7ff8ba5d0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.rundll32.exe.1d069e40000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
22.2.SndVol.exe.1be81c30000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
5.2.rundll32.exe.1ed7c920000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
38.2.DmNotificationBroker.exe.140ded90000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
32.2.printfilterpipelinesvc.exe.1c1f8de0000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
36.2.phoneactivate.exe.209a5e50000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
30.2.rdpinput.exe.7ff8ca980000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.2.rdpinput.exe.7ff8ca980000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.rundll32.exe.1c8d5d60000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
30.2.rdpinput.exe.171ee190000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
38.2.DmNotificationBroker.exe.7ff8ca680000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
34.2.Utilman.exe.255917d0000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
32.2.printfilterpipelinesvc.exe.7ff8bb380000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.rundll32.exe.7ff8ba5d0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.21aaeee0000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
25.2.SnippingTool.exe.168c9480000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
40.2.ProximityUxHost.exe.7ff8ca680000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.2.slui.exe.21e04fe0000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
36.2.phoneactivate.exe.7ff8ca680000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ns.adobY	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dual-a-0001.a-msedge.net	204.79.197.200	true	false		high
canonicalizer.ucsuri.tcs	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://ns.adobY	explorer.exe, 00000004.00000000.41173605 8.00000000026D0000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 004.00000000.390915909.00000000026D0000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000004.00000000.355411214.000000 00026D0000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000004.0000 0000.439321830.00000000026D0000.00000004 .00000001.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	595305
Start date and time:	2022-03-23 14:41:42 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	GpUSRuIBHx (renamed file extension from none to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	41
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@64/31@1/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 32.6% (good quality ratio 23.9%) • Quality average: 49.1% • Quality standard deviation: 36.8%

HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.190.159.22, 20.190.159.1, 40.126.31.70, 20.190.159.70, 20.190.159.5, 40.126.31.64, 20.190.159.3, 40.126.31.68
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, www.bing.com, client.wns.windows.com, a-0001.a-afdentry.net.trafficmanager.net, login.live.com, www.tm.lg.prod.aadmsa.akadns.net, ctldl.windowsupdate.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, login.msa.msidentity.com, www.tm.a.prd.aadg.trafficmanager.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.
- Report size getting too big, too many NtProtectVirtualMemory 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\2HophZ6P\XmlLite.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1372160
Entropy (8bit):	5.066584957420403

Encrypted:	false
SSDEEP:	12288:LZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuw:LZK6F7n5eRmDFJivohZFV
MD5:	52E01AB79E9003A546318454EFB421FB
SHA1:	56598E165CCF95720EC6862BD5D850587F30902F
SHA-256:	39013B96E8FD7840563EC2C5EBD85401EC6E500E18634FCF3BF070A3917F36DF
SHA-512:	6F47B027A4E43CD0A5D5F5FCF0F2A946C12577AB607966C65B104DA9EDE992FF17AB9E020A0AB2FB7E9FFC51AAC5FEA04FBB3248EC9E2C617FE2C0A78F113EB7
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....X..Z.qb..qb..qb.a...jqb.s....qb.9...\qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb..(c..qb.;...,qb../..Tqb.....Zqb.....qb.z...Bqb.....nqb.....[qb.....qb.;...{qb.....qb..#...qb...f.oqb....hqb.z....qb.....:qb.;...tqb.Rich.qb.....PE..d.=...}^......" ....$.....@.....`.....$...<.....0..(.....text..... .....@..... ..`.rdata..Co...0...p...0...0.@Co.....@..@.data....;.....@.....@.;.....@....pdata..8.....@8.....@..@.rsrc.....@.....@..@.reloc..1.....@1.....@..B.vxl..... .....@.....@..@.qwubgr.$....0... ...0...0.@$.....@..@.eer....

C:\Users\user\AppData\Local\2HophZ6P\printfilterpipelinesvc.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	841728
Entropy (8bit):	6.098715724182093
Encrypted:	false
SSDEEP:	12288:JvOaQRxqg2DF9GOdw+UEx3OlRrd7p1dj6znesD0Xk++J:JvOaut2hf7r+lRZl6ak+
MD5:	4164BD4D8E23C672E40D203E4B4A38A7
SHA1:	7D7BC2BEB5B3669764EB0CA10E1C3E820413F8CA
SHA-256:	643F40ABCDA332944BBF92B4D2F846570A34B10BA0A0619B54F4FCF27AD116D0
SHA-512:	39969503FDF09107FD3B35F8A29CFB640B96E4A7DD257F9561F8BD34A22DC93B7246A424FC22D06EB1D7A01717CD05DCC3C5B00FB13F222F30D09D7F2EC31B4
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....'...F...F...F...>I..F..''...F..''...F..''...F...F...G..''.^F..''...F..''%..F..''...F..Rich.F.....PE..d...!.i....."....X.....b.....@.....`..... .....`/.....X....p...u.....h.....T.....(..... .....@.....text....W.....X..... ..`.rdata..>....p.....\.....@..@.data.....P.....8.....@....pdata...u...p...v...B.....@..@.rsrc...X..... .....@..@.reloc..h.....@..B..... .....

C:\Users\user\AppData\Local\2Yf2pw501\WTSAPI32.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1372160
Entropy (8bit):	5.076486334846654
Encrypted:	false
SSDEEP:	12288:eZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuw:eZK6F7n5eRmDFJivohZFV
MD5:	139E8C7A8F2D8A7AF205FA3F2C4D1EA7
SHA1:	D6E7B262E7E2ED200186875C5D5B123DC397BA80
SHA-256:	52B0ED5C7C71FC53DF99C24322B873C20F78444EAB0B6F093FA86CE1DCDF32D8
SHA-512:	0C66074A6149BBAEB9A10389D8A480B3FE57EB3F9F98514C080D048FFCE5FD4D9BB7C7842ACBB759267DC238CDD3F64D52802696081748EBE3B708998C8DB8E
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....X..Z.qb..qb..qb.a...jqb.s....qb.9...\qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb..(c..qb.;...,qb../..Tqb.....Zqb.....qb.z...Bqb.....nqb.....[qb.....qb.;...{qb.....qb..#...qb...f.oqb....hqb.z....qb.....:qb.;...tqb.Rich.qb.....PE..d.=...}^......" ....$.....@.....`.....$...<.....0..(.....text..... .....@..... ..`.rdata..Co...0...p...0...0.@Co.....@..@.data....;.....@.....@.;.....@....pdata..8.....@8.....@..@.rsrc.....@.....@..@.reloc..1.....@1.....@..B.vxl..... .....@.....@..@.qwubgr.$....0... ...0...0.@$.....@..@.eer....

C:\Users\user\AppData\Local\2Yf2pw501\slui.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	445952
Entropy (8bit):	6.661655128700218
Encrypted:	false
SSDEEP:	6144:q++gR8ZWU7WZ1rpvJw1DouE71kL3qY/W5R02qO7VKCyWQp:MgzKWZ1VJwEmDq3nyR
MD5:	96A8EF9387619D17BB30B024DDF52BF3
SHA1:	02DFA07143911500925C6298864477296F414AB0
SHA-256:	ECC41BB93E0E1EA63A1027D551BA0FCE503E53EF1BA2E70944FD7E7C7C9A9B8A
SHA-512:	01701BCFB3D3F09DF86CAF75ED76DC82A4B1480A284AB68FB4B7E4941466DB1ED23187B4D2E51B63C7526123EB4647FB5D155F31832E9ED7F4DBADF78F1F94EA
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....*...n.rMn.rMn.rMg..Mr.rM..qLm.rM..vLx.rM..wLj.rM..sL{.rMn.sM..rM..|Lv.rM...Mo.rM..pLo.rMRichn.rM.....PE..d...O.h{.....".....0.....@..... .....`..... .....-.....`.....T.....(.....text...&..... ..`.rdata.....@..@.data.....P.....*.....@....pdata.....`.....0.....@..@.rsrc.....J.....@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\6f22a\FileHistory.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	246784
Entropy (8bit):	6.054877934071265
Encrypted:	false
SSDEEP:	3072:5WQz0maAVV604aFUxzYuVD8o+otlxAGQW7A70TshCbdmyTVulAyXRON:5WZmxPZUxzYuVD8ortlxAGJKSuCbd
MD5:	989B5BDB2BEAC9F894BBC236F1B67967
SHA1:	7B964642FEE2D6508E66C615AA6CF7FD95D6196E
SHA-256:	FF1DE8A606FDB6A932E7A3E5EE5317A6483F08712DE93603C92C058E05A89C0C
SHA-512:	0360C9FE88743056FD25AC17F12087DAD026B033E590A93F394B00EB486A2F5E2331EDCCA9605AA7573D892FBA41557C9E0EE4FAC69FCA687D6B6F144E5E5249
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.s..k ..k ..k .hh!..k .^. ..k .ho!..k .hb!..k .hj!..k ..j #.k .hn!..k .h. ..k .hi!..k Rich..k .....PE..d.....".....t...X.....{.....@..... .....\....`..... .....0..... ..8.....$... ...T.....H.....text...{m.....n..... ..`.nep.....r..... ..`.rdata...i.....j...x.....@..@.data... .....@....pdata..8.... .....@..@..@.rsrc.....0.....@..@.reloc..$.....@..B.....

C:\Users\user\AppData\Local\6f22a\UxTheme.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1372160
Entropy (8bit):	5.079592473637229
Encrypted:	false
SSDEEP:	12288:SZgJtlQepQn+NDo7nlYegQCLDF/B9wvj/cLvVZFuw:SZK6F7n5eRmDFJivohZFV
MD5:	B5F32E397CE86A9CB3EBFB3B6F366367
SHA1:	02D184436324DEEAE909FB30679C902949E0E1D3
SHA-256:	D5A5310463837F98DD9273746ED845CD2928B1FA3699B2BAE4FEF5F0CFDF0E2B
SHA-512:	ABB46329D4ED085D52A4C7ED6E590DC7CE95CF129A2D8C1F42827BBA8290EA94CD207E07CAC34363B592AB1B4BB58299A1FF74CD0D4EDF7145A6E4DF8BFCC5D
Malicious:	**true**

Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....X..Z.qb..qb..qb.a...jqb.s....qb.9...\qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb..(c..qb.;...,qb../..Tqb.....Zqb.....qb.z. ..Bqb.....nqb.....[qb.....qb.;...{qb.....qb..#...qb...f.oqb....hqb.z....qb.....:qb.;...tqb.Rich.qb.....PE..d.=...}^......" ....$.....@.....`.....$...<.....0..(.....text..... .. .....@..... ..`.rdata..Co...0...p...0...0.@Co.....@..@.data....;.....@.....@.;.....@....pdata..8.....@8.....@..@.rsrc.....@.....@..@.reloc..1..... .....@1.....@..B.vxl..... .....@.....@..@.qwubgr.$....0... ...0...0.@$.....@..@.eer....

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

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1654784
Entropy (8bit):	5.5068060987929055
Encrypted:	false
SSDEEP:	12288:3ZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuwW2bXt:3ZK6F7n5eRmDFJivohZFVvL
MD5:	CFBBAAFFD60DA5EAA23E4E2126D743A3
SHA1:	1EE71CE1791D2FB5E2DCD515A9D0258487EE6044
SHA-256:	3306757CEBBF8E9D6FB1C217CA621835CF67120EF37D9A56326427CFEA851F21
SHA-512:	76735C5D56F23705FF3D4E8FDEE2E11D82F59EDC0F03B7A0B93470C528D61BC31BF00F2813CF1748CCA03986BB8DE484A8EAD0E22509A6D0D349DAA9397E4BF4
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%
Reputation:	unknown
Preview:	MZ.....@.....X..Z.qb..qb..qb.a...jqb.s....qb.9...\qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb..(c..qb.;...,qb../..Tqb.....Zqb.....qb.z. ..Bqb.....nqb.....[qb.....qb.;...{qb.....qb..#...qb...f.oqb....hqb.z....qb.....:qb.;...tqb.Rich.qb.....PE..d.=...}^......" ....$.....@.....@.....`.....dQ..$...<.....0..(.....text..... .. .....@..... ..`.rdata..Co...0...p...0...0.@Co.....@..@.data....;.....@.....@.;.....@....pdata..8.....@8.....@..@.rsrc.....@.....@..@.reloc..1..... .....@1.....@..B.vxl..... .....@.....@..@.qwubgr.$....0... ...0...0.@$.....@..@.eer....

C:\Users\user\AppData\Local\CSYG\DmNotificationBroker.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	32256
Entropy (8bit):	5.250876383836324
Encrypted:	false
SSDEEP:	768:ghunFhykO4aAvnsvpzte5+Ql0/iqmjjn:58kO4asshu+Q+/Ojjn
MD5:	1643D5735213BC89C0012F0E48253765
SHA1:	D076D701929F1F269D34C8FD7BD1BAB4DAF42A9D
SHA-256:	4176FA24D56BB870316D07BD7211BC8A797394F77DCC12B35FFEBAA0326525D2
SHA-512:	F0BD45FE66EDC6F615C0125C1AE81E657CA26544544769651AB0623DD3C724F96D9D78835EF6B1D15083D1BB9D501F6DC48487DDA5C361CAFA96022D5F33A4F
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....j.?H..lH..lH..lAs.lT..l'o.mJ..l'o.m[..lH..l...l'o.mC..l'o.mA..l'o.mA..l 'ohll..l'o.ml..lRichH..l.....PE..d.....".....*...V.....&.....@.....n3..... .....x..... .....Po..T... .....].....^..p.....text....(.....*..... ..`.imrsiv.....@.....rdata..P8...P...:.....@..@.data...(.....h.....@. ...pdata.....j.....@..@.rsrc... .....n.....@..@.reloc.....z.....@..B.....

C:\Users\user\AppData\Local\D6R1uM\DUser.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1376256

Entropy (8bit):	5.074660007590237
Encrypted:	false
SSDEEP:	12288:IZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuw7:IZK6F7n5eRmDFJivohZFV7
MD5:	E53857E285A4C8CB1F38A2248A75D9B3
SHA1:	3AF95C6BF8F52ACA38C907D9D693FD587F4E015F
SHA-256:	51890BB945271DD1BB68E1369540EC20FE2CB545D9B89890F2C6B507A469991A
SHA-512:	7034AD6EFCB023220A61311AB4515D9BE2F5DBB08631CF247F81C397BE38A06E86F9841C0346FE87C21BFB83442A3E8227235B204FF7477DFD4F9D807EB596E7
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....X..Z.qb..qb..qb.a...jqb.s....qb.9...\qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb..(c..qb.;...,qb./..Tqb.....Zqb.....qb.z. ..Bqb.....nqb.....[qb.....qb.;...{qb.....qb..#...qb...f.oqb....hqb.z....qb.....:qb.;...tqb.Rich.qb.....PE..d.=...}^......" ....$.....@.....`.....$...<.....0..(.....text..... .. .....@..... ..`.rdata..Co...0...p...0...0.@Co.....@..@.data....;.....@.....@.;.....@....pdata..8.....@8.....@..@.rsrc.....@.....@..@.reloc..1..... .....@1.....@..B.vxl..... .....@.....@..@.qwubgr.$....0... ...0...0.@$.....@..@.eer....

C:\Users\user\AppData\Local\D6R1uM\Utilman.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	98304
Entropy (8bit):	5.996546491031358
Encrypted:	false
SSDEEP:	1536:3bo99g4+4G8mMM+nCA+o6UJMUHznV80KCt1p7Gx:LXH4GvNKAUHR80KCt/G
MD5:	C91CCEF3884CFDE746B4BAEF5F1BC75C
SHA1:	9A7E17BA64FE1842E904D4019D9BB9B005E61E55
SHA-256:	E6C9C88491EF6FB4B4DAFAC3276C8E2A3B2BC3C4D7825F4EAA3AC99E1801195B
SHA-512:	431754EC35871B2ED1F5E9FC621F24B6187720C0562D0ABDC9232A063DA1E8419A07CDC1740A3B433A80BA15FF25F0EAE0E5B331985A7B8ABC9CE8E73CBC210E
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....D.....@..@..@..8@..@o..A..@o..A..@o..A..@o..A..@..@4 .@o..A..@o.T@..@o..A..@Rich..@.....PE..d....0.....".....@.....R.....L.,.....x.....d...p ...T.....text..... ..`.imrsiv.....rdata...x.....z.....@..@.data.....P.....@.... pdata.....Z.....@..@.rsrc...x.....d.....@..@.reloc..d.....~.....@..B.....

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

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1376256
Entropy (8bit):	5.0860522102577175
Encrypted:	false
SSDEEP:	12288:OZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuw:OZK6F7n5eRmDFJivohZFV
MD5:	FBBA3564BA5F51259BE135DB99FAB04C
SHA1:	BA142953FF1896712641B3494996B9EA499FEFD8
SHA-256:	5D98C039970BBD9ED9C005F62E8CAF263AA0CAE097BE621E7465AE800987DDBD
SHA-512:	BB559FF0FD7266C2E83B6E39911CDF742C67257C17C75D757C50D9CC762B7B87727396B2B58E10749515849EF9D3BE96A6C1CC8EC75A447936B4485C2C9626E
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
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.=...}^......" ....$.....@.....`.....m...$...<.....0..(.....text..... .. .....@..... ..`.rdata..Co...0...p...0...0.@Co.....@..@.data....;.....@.....@.;.....@....pdata..8.....@8.....@..@.rsrc.....@.....@..@.reloc..1..... .....@1.....@..B.vxl..... .....@.....@..@.qwubgr.$....0... ...0...0.@$.....@..@.eer....

C:\Users\user\AppData\Local\Fjrn\rdpinput.exe

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

Category:	dropped
Size (bytes):	178688
Entropy (8bit):	6.278002754824444
Encrypted:	false
SSDEEP:	3072:8i0hLL+KEukKO40+enSqroxn2JIQLtBDYiBJD3cR4DJSpzrA:10d/O40+8Sqk4ZLnBt2tp/
MD5:	4403785D297C55D5DF26176B4F1A52C8
SHA1:	4889F6E0B3CF649C3A8778779D7CEA534B9174B2
SHA-256:	7B8ED6EB50068D4C1B8E51F6F2E3604E6C3B6BB42C6D81ADD4C3B023B6386FF6
SHA-512:	3BAFC7BAE2586F05F05125BF34299D556D46F519D718DAEF8007A0B45D40B0D3CD794A4C55B93CBC1BA2DF111346E6012DEEAD0539AEA91BE71E8ABC877E5 1F
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....i..s:..s:..s:..:..s:..p;..s:..w;..s:..v;..s:..r;..s:..r:..s:..z;..s:..:..s:..q ;..s:Rich..s:.....PE..d....9`..... ".....  #.....@.....&m....`..... .....p.....d.....T.....A. .....B.....text...s..... ..`.rdata..2n...0...p..."..... .....@..@.data.....@....pdata..d.....@..@.rsrc...p..... .....@..@.reloc.....@..B. .....

C:\Users\user\AppData\Local\G6gv6e\AtBroker.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	62976
Entropy (8bit):	5.750635515620841
Encrypted:	false
SSDEEP:	768:LqMH7HUyeCtu1URDrYxfxyLzkd0S2B3ZEI1yfdc9X1vV09SOI9HiEiOpF1QtNcEd:L3RtZkNxCk61BW6901I9HDF1QH8ST
MD5:	E2C775244B3951A401A9083DD742029A
SHA1:	B4DC87649038B7A4E86B5D6AEBAAD975ECE2F477
SHA-256:	80CC3FB17D8CBB4A68F27C607A8D1C0208CEE892F6D2A2E222E18B23D4E0FC76
SHA-512:	CCFABD50BF7F1F9D2DBF3D0F7FFC5A9C862F623472F9AE51A2F4EDB88EF06BCE23731A925405ACF5BF4BB466EA862413EA01B23177C710CA5FE97EA97E6B8 32C
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5`..q.b.q.b.q.b..ea.r.b..ef.d.b..eg.y.b..ec.b.b.q.c...b..ek.~.b..e..p.b. .e`.p.b.Richq.b.....PE..d...=..~..... ".....d.....@.....@.....`.....  .....  ..8.....0.....p...T..... p.....p...@.....text..... ..`.rdata..8B.....D.....@..@.data.....@....pdata.....@..@.rsrc...8.... ....@..@.reloc.....0.....@..B. .....

C:\Users\user\AppData\Local\G6gv6e\UxTheme.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1372160
Entropy (8bit):	5.079555555268202
Encrypted:	false
SSDEEP:	12288:sZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuw:sZK6F7n5eRmDFJivohZFV
MD5:	FEE466621F8AFBC6093E27846305DECE
SHA1:	449724149967C4D9E91A7751BF4EAD687BB9843D
SHA-256:	733A2C02B82BA8C993C216AB5CA6EAA3DF4620226A5BB54A85A140BF69E48AEF
SHA-512:	EBE75C5BF620374A50D51B0E3AEDDC0499E96404761470217183BB62CF8153F7BC3A71948F8BB225775FD8E8860FE0C89BAFC8E7BA52B2F3BA8C076C5E2F106 A
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....X..Z.qb..qb..qb.a...jqb.s....qb.9...\qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb..(c..qb.;...,qb../..Tqb.....Zqb.....qb.z. ..Bqb.....nqb.....[qb.....qb.;...{qb.....qb..#...qb...f.oqb....hqb.z....qb.....:qb.;...tqb.Rich.qb.....PE..d.=...}^..... " ....$.....@.....`.....$...<.....0..(.....text.....  .. .....@.....  ..`.rdata..Co...0...p...0...0.@Co.....@..@.data....;.....@.....@.;.....@....pdata..8.....@8.....@..@.rsrc.....@.....@..@.reloc..1..... .....@1.....@..B.vxl..... .....@.....@..@.qwubgr.$....0... ...0...0.@$.....@..@.eer....

C:\Users\user\AppData\Local\Kyz7D\WTSAPI32.dll

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

Category:	dropped
Size (bytes):	1372160
Entropy (8bit):	5.076527741249057
Encrypted:	false
SSDEEP:	12288:vZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuw:vZK6F7n5eRmDFJivohZFV
MD5:	4384579040D56FD57B803F7511EDBDE6
SHA1:	0ECBE10487CC3A4279AE4C67CEB1FDBC9AAE5767
SHA-256:	54AC63AA9C154D172CEBA33E5CB6FBCED2D130148F7BC2BF146464F6B3C995EE
SHA-512:	82527458FB44B510B1406527551D53C5A9EEECCAF7AC52C54CF890F7B2D84532ED235F6B7D8F24A48D939DB413D22F38062468E9CEE54C720BC1792D170D4DA F
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....X..Z.qb..qb..qb.a...jqb.s....qb.9...\qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb..(c..qb.;...,qb../..Tqb.....Zqb.....qb.z. ..Bqb.....nqb.....[qb.....qb.;...{qb.....qb..#...qb...f.oqb....hqb.z....qb.....:qb.;...tqb.Rich.qb.....PE..d.=...}^......" ....$.....@.....`.....$...<.....0..(.....text..... .. .....@..... ..`.rdata..Co...0...p...0...0.@Co.....@..@.data....;.....@.....@.;.....@....pdata..8.....@8.....@..@.rsrc.....@.....@..@.reloc..1..... .....@1.....@..B.vxl..... .....@.....@..@.qwubgr.$....0... ...0...0.@$.....@..@.eer....

C:\Users\user\AppData\Local\Kyz7D\rdpinput.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	178688
Entropy (8bit):	6.278002754824444
Encrypted:	false
SSDEEP:	3072:8i0hLL+KEukKO40+enSqroxn2JlQLtBDYiBJD3cR4DJSpzrA:10d/O40+8Sqk4ZLnBt2tp/
MD5:	4403785D297C55D5DF26176B4F1A52C8
SHA1:	4889F6E0B3CF649C3A8778779D7CEA534B9174B2
SHA-256:	7B8ED6EB50068D4C1B8E51F6F2E3604E6C3B6BB42C6D81ADD4C3B023B6386FF6
SHA-512:	3BAFC7BAE2586F05F05125BF34299D556D46F519D718DAEF8007A0B45D40B0D3CD794A4C55B93CBC1BA2DF111346E6012DEEAD0539AEA91BE71E8ABC877E5 1F
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....i..s:..s:..s:..:..s:..p;..s:..w;..s:..v;..s:..r;..s:..r:..s:..z;..s:...:..s:..q ;..s:Rich..s:.....PE..d....9`....."..... #.....@.....&m...`..... .....p.....d.....T.....A. .....B.....text...s..... ..`.rdata..2n...0...p..."....@..@.data.....@....pdata..d.....@..@.rsrc...p..... .....@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\LoReH\OLEACC.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1372160
Entropy (8bit):	5.069764908705699
Encrypted:	false
SSDEEP:	12288:uZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuw:uZK6F7n5eRmDFJivohZFV
MD5:	488339CCCB8069AA1F4D361DC71CC57B
SHA1:	FAA4C69A7BCC7E7D9E51D4B43B07128AFDA14901
SHA-256:	DD75F8939D20001A6EA39B113EA82700B842FEBF17598BCB2F3B94681BA0200B
SHA-512:	004B508835CCAD846CF19F21C9EAB9F188E79A4F4D3C89171FFC40022D65CEE2721490B4E21177A8A72CE3D2611814CAF402212D473A7CBB7BE7414AEDAE7D 3
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....X..Z.qb..qb..qb.a...jqb.s....qb.9...\qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb..(c..qb.;...,qb../..Tqb.....Zqb.....qb.z. ..Bqb.....nqb.....[qb.....qb.;...{qb.....qb..#...qb...f.oqb....hqb.z....qb.....:qb.;...tqb.Rich.qb.....PE..d.=...}^......" ....$.....@.....`.....$...<.....0..(.....text..... .. .....@..... ..`.rdata..Co...0...p...0...0.@Co.....@..@.data....;.....@.....@.;.....@....pdata..8.....@8.....@..@.rsrc.....@.....@..@.reloc..1..... .....@1.....@..B.vxl..... .....@.....@..@.qwubgr.$....0... ...0...0.@$.....@..@.eer....

C:\Users\user\AppData\Local\LoReH\SnippingTool.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	3292160
Entropy (8bit):	4.311007815185121
Encrypted:	false
SSDEEP:	24576:+oNva52v20/OB1b1v+YMTvlcZbbAbn3ltpG:VNtv20/OB1hXulc10L4tp
MD5:	9012F9C6AC7F3F99ECDD37E24C9AC3BB
SHA1:	7B8268C1B847301C0B5372C2A76CCE326C74991E
SHA-256:	4E30A8C88C755944145F2BC6C935EE5107C56832772F2561229E20CEAB1D10D2
SHA-512:	B76D2BE02A22990E224DBC5AED9E5B701EAC52C1376529DE3E90B084CD6860B88D746CD61093E93FC932E12FBAF45B4CA342CC0D9C9DAE4EAFE05921D83A7397
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....$...w...w...w...w...v...w...v...w...v...w...v...w...w'..w...v...w ..mw...w..ow...w...v...wRich...w.....PE..d....i....."....v/.....0.....@.....2.....I.2...`..... .....P..(;...0.....2.|.. .`...T.....(.....text...9..... ..`.rdata.....@..@.data....0.....@....pdata.....0.....@.. @.rsrc...(;...P...<.....@..@.reloc..|.....2.....82.....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\FileHistory.exe.log	
Process:	C:\Users\user\AppData\Local\6f22a\FileHistory.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	42
Entropy (8bit):	4.0050635535766075
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUy:Q3La/xwQ
MD5:	84CFDB4B995B1DBF543B26B86C863ADC
SHA1:	D2F47764908BF30036CF8248B9FF5541E2711FA2
SHA-256:	D8988D672D6915B46946B28C06AD8066C50041F6152A91D37FFA5CF129CC146B
SHA-512:	485F0ED45E13F00A93762CBF15B4B8F996553BAA021152FAE5ABA051E3736BCD3CA8F4328F0E6D9E3E1F910C96C4A9AE055331123EE08E3C2CE3A99AC2E177CE
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..

C:\Users\user\AppData\Local\Ui9PsZ9\OLEACC.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1372160
Entropy (8bit):	5.0697307938945215
Encrypted:	false
SSDEEP:	12288:JZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuw:JZK6F7n5eRmDFJivohZFV
MD5:	66AAD5D9E18874517CFDF3554D87B2A2
SHA1:	A8753910F8CCA16980D08D7BAB32371C341576AF
SHA-256:	47DE30D9FA852851AF9462DDC79DADAA73F270EA429264EDC5159CCA2577DEB6
SHA-512:	BAFC276095729B1213B63A67484349359A3F1729CF1796C4C9EF33E128309BEE019C456C012E4EE8C42B6370AEF353E6AA45F76AD88D80A7EA44801F3AA71D65
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....X..Z.qb..qb..qb.a...jqb.s....qb.9...\qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb..(c..qb.;...,qb./..Tqb.....Zqb.....qb.z. ..Bqb.....nqb.....[qb.....qb.;...{qb.....qb..#...qb...f.oqb....hqb.z....qb.....:qb.;...tqb.Rich.qb.....PE..d.=...}^....." ....$.....@.....`.....$...<.....0..(.....text..... .. .....@..... ..`.rdata..Co...0...p...0...0.@Co.....@..@.data....;.....@.....@.;.....@....pdata..8.....@8.....@..@.rsrc.....@.....@..@.reloc..1..... .....@1.....@..B.vxl..... .....@.....@..@.qwubgr.$....0... ...0...0.@$.....@..@.eer....

C:\Users\user\AppData\Local\bTcR2e\SndVol.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows

Category:	dropped
Size (bytes):	259904
Entropy (8bit):	5.955701055747905
Encrypted:	false
SSDEEP:	3072:UfYIZJbRydnidilSnGvLqeD358rwW39nuyHjVozZcxSHfcBL1ljbEyB7Hbla+:Uf9JonidFnqLV358rNnJqcRcy10/
MD5:	CDD7C7DF2D0859AC3F4088423D11BD08
SHA1:	128789A2EA904F684B5DF2384BA6EEF4EB60FB8E
SHA-256:	D98DB8339EB1B93A7345EECAC2B7290FA7156E3E12B7632D876BD0FD1F31EC66
SHA-512:	A093BF3C40C880A80164F2CAA87DF76DCD854375C5216D761E60F3770DFA04F4B02EC0CA6313C32413AC99A3EBDC081CF915A7B468EE3CED80F9B1ECF4B498 04
Malicious:	**true**
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<.BL]..L]..L]..E%...]..#9..O]..#9..U]..#9..F]..#9..W]..L]...\..#9..o].. #9k.M]..#9..M]..RichL].....PE..d...wJSn....."....@.....@..... .....p.... ..@.....@+...0..... ..U..T.....p&..(...p%.....&.....P.....text..... ..`.imrsiv.....rdata..... .....@..@.data.....@.. ..pdata.....@..@.didat.....@....rsrc...@.... .....@..@.reloc.....0.....@..B.....

C:\Users\user\AppData\Local\bTcR2e\dwmapi.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1372160
Entropy (8bit):	5.073973927598516
Encrypted:	false
SSDEEP:	12288:LZgJtlQepQn+NDo7nlYegQCLDF/B9wvj/cLvVZFuw:LZK6F7n5eRmDFJivohZFV
MD5:	48C36CC6ADF7DE6F96D11BC1D2B68952
SHA1:	EA3B2200BA9760095E1472EF38DFB4170DBBC7B2
SHA-256:	D1800979A9F1D68E94B7F47B0087EDDDBEC124C109B09FEEA09EEE1F801D81F5
SHA-512:	5E2DF5ED5597527E22E33CEB72510DF41466E37C9055666D2F35EE1F2CB30250BA0F17C83E7B3E1AB814788B918C2329F9F2860580B14DF81A7B9CA2FCC3493
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....X..Z.qb..qb..qb.a...jqb.s....qb.9...\qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb..(c..qb.;...,qb../..Tqb.....Zqb.....qb.z. ..Bqb.....nqb.....[qb.....qb.;...{qb.....qb..#...qb...f.oqb....hqb.z....qb.....:qb.;...tqb.Rich.qb.....PE..d.=...}^....."..... .....$.....@.....`.....&...$...<.....0..(.....text..... .. .....@..... ..`.rdata..Co...0...p...0...0.@Co.....@..@.data....;.....@.....@.;.....@....pdata..8.....@8.....@..@.rsrc.....@.....@..@.reloc..1..... .....@1.....@..B.vxl..... .....@.....@..@.qwubgr.$....0... ...0...0.@$.....@..@.eer....

C:\Users\user\AppData\Local\l5T\XmlLite.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1372160
Entropy (8bit):	5.066584527926527
Encrypted:	false
SSDEEP:	12288:GZgJtlQepQn+NDo7nlYegQCLDF/B9wvj/cLvVZFuw:GZK6F7n5eRmDFJivohZFV
MD5:	2455197D114CD7C9932979153ED6B9DE
SHA1:	18D6D668DAACF859CC19CFD702238B1B082535BD
SHA-256:	91A1808AD24EE0A139492D1AC9F52195C19C070B82E3D4DFC016F32BF2C9B70A
SHA-512:	3AD994C1BF3055DDE2FF2217BE05A3B537102B3AB0C4CBEAD6B6782E8B2D37D4984F3ABAAC036B43C2BB2AE9F378E242D4C861CB9E0AF22FC9DD59E9C137F 9CA
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....X..Z.qb..qb..qb.a...jqb.s....qb.9...\qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb..(c..qb.;...,qb../..Tqb.....Zqb.....qb.z. ..Bqb.....nqb.....[qb.....qb.;...{qb.....qb..#...qb...f.oqb....hqb.z....qb.....:qb.;...tqb.Rich.qb.....PE..d.=...}^....."..... .....$.....@.....`.....$...<.....0..(.....text..... .. .....@..... ..`.rdata..Co...0...p...0...0.@Co.....@..@.data....;.....@.....@.;.....@....pdata..8.....@8.....@..@.rsrc.....@.....@..@.reloc..1..... .....@1.....@..B.vxl..... .....@.....@..@.qwubgr.$....0... ...0...0.@$.....@..@.eer....

C:\Users\user\AppData\Local\l5T\omadmclient.exe

Process:	C:\Windows\explorer.exe

File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	315904
Entropy (8bit):	6.1346795928867035
Encrypted:	false
SSDEEP:	6144:uwqIVaD9RkjUYNBDXEDBdcA1gBnbC03j0xjGKEgsQOQ25te8lG:XqIVaDrn6BD0NOA1gBnfj01QW
MD5:	AD7C6CD7A8EEC95808AA77C5D7987941
SHA1:	96985DDF5C2C30918F69CA4405D955BDD0C7E44E
SHA-256:	D7EED58A955ED6ADEF429FA78F82776BBC905C507E1ABE6D5CFCD5C8AC1B0AC9
SHA-512:	047EA8C542774045450B51BF367C75B4ED11E883553842BCACD9E6DFC4C27CDC8BE86A9BADFD5345DA068B4A881BC8522525BF9CEC72FEE1856E365E7CD205E
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....`2.K$S~.$S~.$S~.-+..nS~.K7}.'S~.K7z.1S~.$S...R~.K7..=S~.K7{.)S ~.K7w..S~.K7..%S~.K7|.%S~.Rich$S~.....PE..d...H..-.....".....d...x.....J.....@.....@.....`..... ....0.....T.....(.....8...8.....text....b.....d..... ..`.rdata..~4.....6...h.....@..@.data...l.....@....pdata... .....".. .....@..@.didat.....@....rsrc..... .....@..@.reloc.....0.....@..B..... .....

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

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1654784
Entropy (8bit):	5.50689551347506
Encrypted:	false
SSDEEP:	12288:UZgJtlQepQn+NDo7nlYegQCLDF/B9wvj/cLvVZFuwkt:UZK6F7n5eRmDFJivohZFVk
MD5:	8C330DCE7F7E0C1054A3AAFACF8FD93C
SHA1:	A543BE373A7875FA70B18151AE9937FD81C7B642
SHA-256:	E494E4EDD78008824CB90A18302CCD6347A3F2163B652F09D4326BA863308F73
SHA-512:	DE0851884D8ED3863B12DF1C53C0382B3E4B7C3D2BDDADF3A76791AE79DAEA28AD64544A3101A30C58CA367C3EECA260FFDFD5E2532B0E5781C87A36F79EC8F8
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....X..Z.qb..qb..qb.a...jqb.s....qb.9...\qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb..(c..qb.;...,qb./..Tqb.....Zqb.....qb.z. ..Bqb.....nqb.....[qb.....qb.;...{qb.....qb..#...qb...f.oqb....hqb.z....qb.....:qb.;...tqb.Rich.qb.....PE..d.=...}^....." ....$.....@.....@.....`.....dQ..$...<.....0..(.....text..... .. .....@..... ..`.rdata..Co...0...p...0...0.@Co.....@..@.data....;.....@.....@.;.....@....pdata..8.....@8.....@..@.rsrc.....@.....@..@.reloc..1..... .....@1.....@..B.vxl..... .....@.....@..@.qwubgr.$....0... ...0...0.@$.....@..@.eer....

C:\Users\user\AppData\Local\oOQGGow\ProximityUxHost.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	264480
Entropy (8bit):	6.478365286411354
Encrypted:	false
SSDEEP:	6144:xSt+s2GFGbqEuzhJONjx9UVuCuHpwqr/vt9r+ULJBaBpcIFz:xStzFGbGhoPgMHpwqrHthUB6IF
MD5:	E7F0E9B3779E54CD271959C600A2A531
SHA1:	8006E2D1AA91798E48D8BFDE1EBF94A2D6BA6C0A
SHA-256:	155CE33E0E145314FE9D8911BE69B8CBBD2AC09B7B6D98363F9BAA277C71954E
SHA-512:	E10C3FD9C5F34260323CEC9E8EEDF2290F40254F0FFDCA582DB57D113B32871793CDFFF03D55941EF5E79FA8141803AB353BA4938357A4555233F2D090045338
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B..B..B..K.`.&..-..A..-...U..-...K..-..U..B..t..-...]..-...C..-..C..RichB..... .....PE..d...;.*Q.....".....@..... .....&..... .....H.....T..... +.....Pa..T.....p3..(...p2.....3. .....text..... ..`.imrsiv.....rdata..... .....@..@.data...x.....@....pdata..T.....@..@. rsrc...H.....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\op5PCy\DUI70.dll

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

Category:	dropped
Size (bytes):	1654784
Entropy (8bit):	5.506636144897031
Encrypted:	false
SSDEEP:	12288:bZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuwlCat:bZK6F7n5eRmDFJivohZFVlD
MD5:	B21D0B4EEDE745E1C527C304BC803F8A
SHA1:	0EFFD1FC33D4C0B4972B8AD1D5A481B59F623D15
SHA-256:	5C4DF307C0D2E137852AE87435AF221D1365B1990A58FCEAAC73263EB08E27CD
SHA-512:	30235E5F81A1586F8D44D79F7D864669D608CE99342BB1A329E6BB3F3422CC6CBB7C5D74A2136B5374AC3FEE30C1F0283420EE0C5F9A1A258C1E5C2A27E897E F
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....X..Z.qb..qb..qb.a...jqb.s....qb.9...\qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb..(c..qb.;...,qb../..Tqb.....Zqb.....qb.z. ..Bqb.....nqb.....[qb.....qb.;...{qb.....qb..#...qb...f.oqb....hqb.z....qb.....:qb.;...tqb.Rich.qb.....PE..d.=...}^......" ....$.....@.....@.....`.....dQ..$...<.....0..(.....text..... .. .....@..... ..`.rdata..Co...0...p...0...0.@Co.....@..@.data....;.....@.....@.;.....@....pdata..8.....@8.....@..@.rsrc.....@.....@..@.reloc..1..... .....@1.....@..B.vxl..... .....@.....@..@.qwubgr.$....0... ...0...0.@$.....@..@.eer....

C:\Users\user\AppData\Local\op5PCy\phoneactivate.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	107504
Entropy (8bit):	6.536585324272613
Encrypted:	false
SSDEEP:	1536:UhKYFAVrKO6PcIgpCaYov3ZKCZwaG70Ur/61cVtat/gLaoU0Sj09P0e:dmlPcNphvo0mtV1La8Lse
MD5:	09D1974A03068D4311F1CE94B765E817
SHA1:	7DD683571E4DCCAF181A5271BBCF15B3BC9D0155
SHA-256:	5D4F713CFC98E7148B67D063193D93BFE29F8329705A03690590633FADE32EE5
SHA-512:	07FD0700C8368485BEC91847C4B9721B059FEDB678C603A57FBD5DABCF110C80B0BD1D114384D4334F0412F3F4FD93C839A1B17F3A9F02C25CD59216692A8A0
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....i.....O.....Rich..... ....PE..d.....^....."..... `.....@.....;;..... .....0.....p.. J...`.....~...%.....`"..T.....(..... .....text..... ..`.imrsiv.....rdata...I.....J.....@..@.data...8....P.....$.....@....pdata.....`.....&.....@..@.rsrc... J.. .p...L...0.....@..@.reloc.....|.....@..B.....

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

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1372160
Entropy (8bit):	5.066183661537441
Encrypted:	false
SSDEEP:	12288:lZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuw:lZK6F7n5eRmDFJivohZFV
MD5:	B92B9B63E4AB54171E00DEE18C499D86
SHA1:	570ADD4C1D784036CB1F6260448D6F3DE4B4F76F
SHA-256:	9F42BA0E8B9707A120985207030E554233EF0F221F2859DA5C88D9D88D41FEBB
SHA-512:	F9D89B45E834154B3AEDCEA23EBEEC5E632F3815C1F314C90B69D23AB4A9E3A7DB7D6231D0BB5F0648397049C7A2273F8625549F45562E7E8BB8B2CE9DE134 C
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....X..Z.qb..qb..qb.a...jqb.s....qb.9...\qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb..(c..qb.;...,qb../..Tqb.....Zqb.....qb.z. ..Bqb.....nqb.....[qb.....qb.;...{qb.....qb..#...qb...f.oqb....hqb.z....qb.....:qb.;...tqb.Rich.qb.....PE..d.=...}^......" ....$.....@.....`.....$...<.....0..(.....text..... .. .....@..... ..`.rdata..Co...0...p...0...0.@Co.....@..@.data....;.....@.....@.;.....@....pdata..8.....@8.....@..@.rsrc.....@.....@..@.reloc..1..... .....@1.....@..B.vxl..... .....@.....@..@.qwubgr.$....0... ...0...0.@$.....@..@.eer....

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

Process:	C:\Windows\explorer.exe

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

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\eb42b1a5c308fc11edf1ddbdd25c8486_d06ed635-68f6-4e9a-955c-4899f5f57b9a

Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	1454
Entropy (8bit):	7.36525526598561
Encrypted:	false
SSDEEP:	24:wk5hikT2UP04Kv5qEpIKAeWI8tTBe8NpXvTyCacF1wAS8i8bz98ryrHF1wskGl:w3kT2UP0pUEmKY/xyOMAS8i8bh8GrHFd
MD5:	7134EEA4FE32F1314E23325499370847
SHA1:	5C9520DBFCFD0322D7D23AB1D92B2F5400289E27
SHA-256:	A88E4C07558257D2D4AFE6DCF9FCA843A8B496508F8A785896A55A1EEAB52A2B
SHA-512:	8B50069FEC5CA60731AB1E221120A5B74320206D9DE5B705A7936501EFFAC01752C96D0C607B2AFF1F4FD780F9749F7850BED0D7B37F518852A2E3935C60776C
Malicious:	false
Reputation:	unknown
Preview:	.....user.....RSA1.....1.....M.....E.....q+..?w.N..'6...>(L.....k.....v.S..}.w.9,0.&@..a.Cp....-?.....b...a."....._..j...,...1.6.].9.<W}{. ....z..O.....bn.C..~P..y7....,..C.r.y.p.t.o.A.P.I. .P.r.i.v.a.t.e. .K.e.y....f..... .....E.x...`.mU.I...]....o(.[..... .....t.#M6X.=)..Cz..3..(U;..D.,.....S/...5._s.:..V..,+..%\....a.%). .....X.H..^S..y...~.]a.+H..."..R.my].4o_....b.ibx..}...L..."^_.PcQ.F..*...).....^#Y...\...j?!zW..rVw>....X818b#..Rv0.J...T.3.....z....UB.k.b.h.d...m1.v.S)...H.!...?..W].5.!>9.G..#.....&. <e...9.fAg....0,....,S2.....`.R]....m.%...:N.:....E.j6.w...M~..?.S..(....f.h.{..(.(..q..z|.....{...|:3.~.....R.&...O>A...L...]h.x..~..7Hmd!..~E..2..%K.g....t.K...!ht...(.....k...~..r..."..p.*..'.[.....b]w.J.....z.u...<.6.y.Ls....Xy...:P%.....{.lE.3.z^..N.UZ.t,./.m..-...F.M..t3.....w.5.F.0.....=a.....\t....mS...m...n...

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	5.088563317300119
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:	GpUSRuIBHx.dll
File size:	1368064
MD5:	288c35481252c1212cbb764c490c2ad8
SHA1:	9c48ba2239b5ae5675d0eb6b92cf0a37884403fd
SHA256:	cb793c295b0bcd3baec5546b7176cdfdf10b0a9291d958c72eb85551825d22d6
SHA512:	8a3b343ad8819f09f94868b19ab6f94a6fdf852f3c5183a371cd323a57af0b7fb9d5249516044e8f59721e6220ecd43338b6990c56cb0006840842cb923be112
SSDEEP:	12288:pZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuw:pZK6F7n5eRmDFJivohZFV
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
mov dword ptr [00070653h], esi
dec eax
test eax, eax
je 00007F4CC8D5BFFDh
dec eax
mov dword ptr [0007060Fh], esp
dec eax
mov dword ptr [00070600h], ebp
dec eax
mov dword ptr [00070649h], ebx
dec eax

Instruction
mov dword ptr [0007063Ah], edi
dec eax
test eax, eax
je 00007F4CC8D5BFDCh
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	0x14d010	0x886	.adsxi
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa9924	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbf000	0x3d8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x1000	0x0	.text
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc0000	0xefc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	

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

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x418cc	0x42000	False	0.781412760417	data	7.78392111205	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x43000	0x66f43	0x67000	False	0.700320938258	data	7.87281050709	IMAGE_SCN_CNT_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
.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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.qsxjui	0xdb000	0x9cd	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_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
.gzb	0xe9000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.fatlss	0xea000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.plqa	0xeb000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vzt	0xec000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.dsbyd	0xed000	0x1e66	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.cdelc	0xef000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.qkhkj	0xf0000	0x5a7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.mnzegr	0xf1000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.krw	0xf2000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.jvsmn	0xf3000	0x389	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bygpq	0xf4000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.kzdbu	0xf6000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.mwxorn	0xf7000	0x3fe	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
.raf	0xf8000	0x389	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.zcyw	0xf9000	0x2da	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.zeczh	0xfa000	0x128f	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pvv	0xfc000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.lug	0xfd000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ski	0x143000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.japjd	0x144000	0x128f	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.mwtzml	0x146000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vgssf	0x147000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.gsroye	0x148000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vcmr	0x14a000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.kvjqnl	0x14b000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ikzlp	0x14c000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.adsxi	0x14d000	0x896	0x1000	False	0.211181640625	data	3.76807441258	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
??0VolumeFveStatus@@IEAA@XZ	1	0x14000279c
??0VolumeFveStatus@@QEAA@K_KJW4_FVE_WIPING_STATE@@@Z	2	0x14003536c
??4BuiVolume@@QEAAAEAV0@AEBV0@@Z	3	0x1400326c8
??4VolumeFveStatus@@QEAAAEAV0@$$QEAV0@@Z	4	0x14003eb90
??4VolumeFveStatus@@QEAAAEAV0@AEBV0@@Z	5	0x140042688
?FailedDryRun@VolumeFveStatus@@QEBA_NXZ	6	0x14002e2f4
?GetExtendedFlags@VolumeFveStatus@@QEBA_KXZ	7	0x14001886c
?GetLastConvertStatus@VolumeFveStatus@@QEBAJXZ	8	0x1400131ac
?GetStatusFlags@VolumeFveStatus@@QEBAKXZ	9	0x14002279c
?HasExternalKey@VolumeFveStatus@@QEBA_NXZ	10	0x140004da8
?HasPBKDF2RecoveryPassword@VolumeFveStatus@@QEBA_NXZ	11	0x14001bab4
?HasPassphraseProtector@VolumeFveStatus@@QEBA_NXZ	12	0x140002c38

Name	Ordinal	Address
?HasPinProtector@VolumeFveStatus@@QEBA_NXZ	13	0x140013d50
?HasRecoveryData@VolumeFveStatus@@QEBA_NXZ	14	0x14000ab2c
?HasRecoveryPassword@VolumeFveStatus@@QEBA_NXZ	15	0x14003fff4
?HasSmartCardProtector@VolumeFveStatus@@QEBA_NXZ	16	0x14003af44
?HasStartupKeyProtector@VolumeFveStatus@@QEBA_NXZ	17	0x140031fe4
?HasTpmProtector@VolumeFveStatus@@QEBA_NXZ	18	0x140003984
?IsConverting@VolumeFveStatus@@QEBA_NXZ	19	0x140006b8c
?IsCsvMetadataVolume@VolumeFveStatus@@QEBA_NXZ	20	0x1400395bc
?IsDEAutoProvisioned@VolumeFveStatus@@QEBA_NXZ	21	0x14003fa38
?IsDecrypted@VolumeFveStatus@@QEBA_NXZ	22	0x140016024
?IsDecrypting@VolumeFveStatus@@QEBA_NXZ	23	0x14003e0b0
?IsDisabled@VolumeFveStatus@@QEBA_NXZ	24	0x1400088e8
?IsEDriveVolume@VolumeFveStatus@@QEBA_NXZ	25	0x14000cdac
?IsEncrypted@VolumeFveStatus@@QEBA_NXZ	26	0x1400393d0
?IsEncrypting@VolumeFveStatus@@QEBA_NXZ	27	0x140018384
?IsLocked@VolumeFveStatus@@QEBA_NXZ	28	0x140042060
?IsOn@VolumeFveStatus@@QEBA_NXZ	29	0x140023538
?IsOsCriticalVolume@VolumeFveStatus@@QEBA_NXZ	30	0x14000412c
?IsOsVolume@VolumeFveStatus@@QEBA_NXZ	31	0x1400212c4
?IsPartiallyConverted@VolumeFveStatus@@QEBA_NXZ	32	0x14003ab20
?IsPaused@VolumeFveStatus@@QEBA_NXZ	33	0x140036390
?IsPreProvisioned@VolumeFveStatus@@QEBA_NXZ	34	0x140040cd4
?IsRoamingDevice@VolumeFveStatus@@QEBA_NXZ	35	0x14001bf04
?IsSecure@VolumeFveStatus@@QEBA_NXZ	36	0x1400041b0
?IsUnknownFveVersion@VolumeFveStatus@@QEBA_NXZ	37	0x14003239c
?IsWiping@VolumeFveStatus@@QEBA_NXZ	38	0x140020f68
?NO_DRIVE_LETTER@BuiVolume@@2IB	39	0x14003905c
?NeedsRestart@VolumeFveStatus@@QEBA_NXZ	40	0x140009f9c
FveuiWizard	41	0x140039d64
FveuipClearFveWizOnStartup	42	0x14002bf34

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
Mar 23, 2022 15:47:01.145245075 CET	53907	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 23, 2022 15:47:01.164192915 CET	53	53907	8.8.8.8	192.168.2.7

DNS Queries

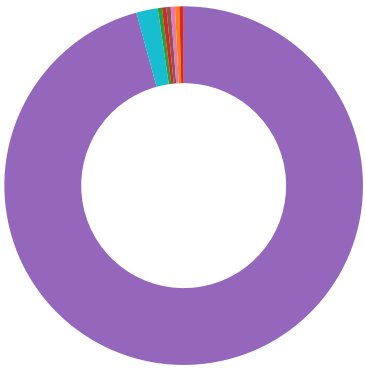
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Mar 23, 2022 15:47:01.145245075 CET	192.168.2.7	8.8.8.8	0xa82	Standard query (0)	canonicalizer.ucsuri.tcs	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Mar 23, 2022 15:47:00.687875986 CET	8.8.8.8	192.168.2.7	0x41b3	No error (0)	www-bing-com.dual-a-0001.a-msedge.net	dual-a-0001.a-msedge.net		CNAME (Canonical name)	IN (0x0001)
Mar 23, 2022 15:47:00.687875986 CET	8.8.8.8	192.168.2.7	0x41b3	No error (0)	dual-a-0001.a-msedge.net		204.79.197.200	A (IP address)	IN (0x0001)
Mar 23, 2022 15:47:00.687875986 CET	8.8.8.8	192.168.2.7	0x41b3	No error (0)	dual-a-0001.a-msedge.net		13.107.21.200	A (IP address)	IN (0x0001)
Mar 23, 2022 15:47:00.713713884 CET	8.8.8.8	192.168.2.7	0x7827	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Mar 23, 2022 15:47:01.164192915 CET	8.8.8.8	192.168.2.7	0xa82	Name error (3)	canonicalizer.ucsuri.tcs	none	none	A (IP address)	IN (0x0001)

Statistics

Behavior



- loaddll64.exe
- cmd.exe
- rundll32.exe
- rundll32.exe
- explorer.exe
- rundll32.exe
- rundll32.exe
- BackgroundTransferHost.exe
- FileHistory.exe
- FileHistory.exe
- rdpinput.exe
- rdpinput.exe
- SndVol.exe
- SndVol.exe
- SnippingTool.exe
- SnippingTool.exe
- slui.exe
- slui.exe
- rdpinput.exe
- rdpinput.exe
- printfilterpipelinesvc.exe
- printfilterpipelinesvc.exe
- Utilman.exe
- Utilman.exe
- phoneactivate.exe
- phoneactivate.exe
- DmNotificationBroker.exe
- DmNotificationBroker.exe
- ProximityUxHost.exe
- ProximityUxHost.exe
- omadmclient.exe

Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: 852, Parent PID: 5640

General

Target ID:	0
Start time:	15:42:50
Start date:	23/03/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\GpUSRuIBHx.dll"
Imagebase:	0x7ff63d400000
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: 00000000.00000002.372939527.00007FF8BA5D1000.00000020.00000001.01000000.00000003.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: **6932**, Parent PID: **852**

General

Target ID:	1
Start time:	15:42:51
Start date:	23/03/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\GpUSRuIBHx.dll",#1
Imagebase:	0x7ff6a6590000
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: **7036**, Parent PID: **852**

General

Target ID:	2
Start time:	15:42:51
Start date:	23/03/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\GpUSRuIBHx.dll,??0VolumeFveStatus@@IEAA@XZ
Imagebase:	0x7ff7c5d30000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000002.00000002.470593131.00007FF8BA5D1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\GpUSRuIBHx.dll	unknown	1368064	success or wait	1	7FF8BA62F8D6	ReadFile

Analysis Process: rundll32.exe PID: 7012, Parent PID: 6932

General

Target ID:	3
Start time:	15:42:52
Start date:	23/03/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\GpUSRuIBHx.dll",#1
Imagebase:	0x7ff7c5d30000
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: 00000003.00000002.352441583.00007FF8BA5D1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\GpUSRuIBHx.dll	unknown	1368064	success or wait	1	7FF8BA62F8D6	ReadFile

Analysis Process: explorer.exe PID: 3808, Parent PID: 7036

General

Target ID:	4
Start time:	15:42:54
Start date:	23/03/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff631f70000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\AccountPictures\OpCJf	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\6f22a\	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\6f22a\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\6f22a\FileHistory.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\Kyz7D\	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\Kyz7D\WTSAPI32.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\Kyz7D\rdpinput.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\bTcR2e\	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\bTcR2e\dwmapi.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\bTcR2e\SndVol.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\LoReH\	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\LoReH\OLEACC.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\LoReH\SnippingTool.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\2Yf2pw501\	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\2Yf2pw501\WTSAPI32.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\2Yf2pw501\slui.exe	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\Fjrn\	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\Fjrn\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\Fjrn\rdpinput.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\2HophZ6P\	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\2HophZ6P\XmlLite.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\2HophZ6P\printfilterpipelinesvc.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\D6R1uM\	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\D6R1uM\DUser.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\D6R1uM\Utilman.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\op5PCy\	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\op5PCy\DUI70.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\op5PCy\phoneactivate.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\CSYG\	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\CSYG\DUI70.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\CSYG\DmNotificationBroker.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\oOQGGow\	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\oOQGGow\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\oO QGGow\ProximityUxHost.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\l5T\	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\l5T\XmlLite.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\l5T\omadmclient.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\G6gv6e\	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\G6gv6e\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\G6gv6e\AtBroker.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\rDAhA\	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\rDAhA\WMsgAPI.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\rDAhA\consent.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\Ui9PsZ9\	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\Ui9PsZ9\OLEACC.dll	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\6f22a\FileHistory.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\6f22a\UxTheme.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\Kyz7D\rdpinput.exe	cannot delete	5	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\Kyz7D\WTSAPI32.dll	cannot delete	5	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\Kyz7D\rdpinput.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\Kyz7D\WTSAPI32.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\bTcR2e\dwmapi.dll	cannot delete	7	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\bTcR2e\SndVol.exe	cannot delete	7	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\bTcR2e\dwmapi.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\bTcR2e\SndVol.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\LoReH\OLEACC.dll	cannot delete	29	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\LoReH\SnippingTool.exe	cannot delete	28	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\LoReH\OLEACC.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\LoReH\SnippingTool.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\2Yf2pw501\slui.exe	cannot delete	14	14005FB70	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\2Yf2pw501\WTSAPI32.dll	cannot delete	13	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\2Yf2pw501\slui.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\2Yf2pw501\WTSAPI32.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\Fjrn\rdpinput.exe	cannot delete	6	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\Fjrn\WINSTA.dll	cannot delete	6	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\Fjrn\rdpinput.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\Fjrn\WINSTA.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\2HophZ6P\printfilterpipelinesvc.exe	cannot delete	8	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\2HophZ6P\XmlLite.dll	cannot delete	8	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\2HophZ6P\printfilterpipelinesvc.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\2HophZ6P\XmlLite.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\D6R1uM\DUser.dll	cannot delete	5	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\D6R1uM\Utilman.exe	cannot delete	5	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\D6R1uM\DUser.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\D6R1uM\Utilman.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\op5PCy\DUI70.dll	cannot delete	14	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\op5PCy\phoneactivate.exe	cannot delete	14	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\op5PCy\DUI70.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\op5PCy\phoneactivate.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\CSYG\DmNotificationBroker.exe	cannot delete	16	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\CSYG\DUI70.dll	cannot delete	16	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\CSYG\DmNotificationBroker.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\CSYG\DUI70.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\oOQGGow\DUI70.dll	cannot delete	17	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\oOQGGow\ProximityUxHost.exe	cannot delete	17	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\oOQGGow\DUI70.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\oOQGGow\ProximityUxHost.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\l5T\omadmclient.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\l5T\XmlLite.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\G6gv6e\AtBroker.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\G6gv6e\UxTheme.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\rDAhA\consent.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\rDAhA\WMsgAPI.dll	success or wait	1	14005FB70	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\6f22a\UxTheme.dll	0	1372160	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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\6f22a\FileHistory.exe	0	246784	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 6d 05 73 fd 0c 6b 20 fd 0c 6b 20 fd 0c 6b 20 fd 68 68 21 fd 0c 6b 20 fd 5e fd 20 fd 0c 6b 20 fd 68 6f 21 fd 0c 6b 20 fd 68 62 21 fd 0c 6b 20 fd 68 6a 21 fd 0c 6b 20 fd 0c 6a 20 23 0c 6b 20 fd 68 6e 21 fd 0c 6b 20 fd 68 fd 20 fd 0c 6b 20 fd 68 69 21 fd 0c 6b 20 52 69 63 68 fd 0c 6b 20 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 07 00 fd fd fd fd 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$msk k k hh!k ^ k ho!k hb!k hj!k j #k hn!k h k hi!k Richk PEd"	success or wait	1	14005F160	WriteFile
C:\Users\user\AppData\Local\Kyz7D\WTSAPI32.dll	0	1372160	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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\Kyz7D\rdpinput.exe	0	178688	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 1d 69 fd fd 73 3a fd fd 73 3a fd fd 73 3a ff fd 3a fd fd 73 3a fd fd 70 3b fd fd 73 3a fd fd 77 3b fd fd 73 3a fd fd 76 3b fd fd 73 3a fd fd 72 3b fd fd 73 3a fd fd 72 3a 17 fd 73 3a fd fd 7a 3b fd fd 73 3a fd fd fd 3a fd fd 73 3a fd fd 71 3b fd fd 73 3a 52 69 63 68 fd fd 73 3a 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06 00 fd 39 60 fd 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$is:s:s::s:p;s: w;s:v;s:r;s:r:s:z;s::s:q;s:Richs:PEd9`"	success or wait	1	14005F160	WriteFile
C:\Users\user\AppData\Local\bTcR2e\dwmapi.dll	0	1372160	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 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\bTcR2e\SndVol.exe	0	259904	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 08 3c fd 42 4c 5d fd 11 4c 5d fd 11 4c 5d fd 11 45 25 07 11 08 5d fd 11 23 39 fd 10 4f 5d fd 11 23 39 fd 10 55 5d fd 11 23 39 fd 10 46 5d fd 11 23 39 fd 10 57 5d fd 11 4c 5d fd 11 fd 5c fd 11 23 39 fd 10 6f 5d fd 11 23 39 6b 11 4d 5d fd 11 23 39 fd 10 4d 5d fd 11 52 69 63 68 4c 5d fd 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 08	MZ@!L!This program cannot be run in DOS mode.$<BL]L]L]E%]#9O]#9U]#9F]#9W]L]\#9o]#9kM]#9M]RichL]PEd	success or wait	1	14005F160	WriteFile
C:\Users\user\AppData\Local\LoReH\OLEACC.dll	0	1372160	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 58 10 0c 5a 1c 71 62 09 1c 71 62 09 1c 71 62 09 61 08 fd 09 6a 71 62 09 73 07 fd 09 18 71 62 09 39 06 fd 09 5c 71 62 09 73 07 fd 09 28 71 62 09 fd 15 fd 09 0b 71 62 09 11 23 fd 09 20 71 62 09 fd 2f 62 08 07 71 62 09 15 09 fd 09 09 71 62 09 07 fd fd 09 48 71 62 09 fd 28 63 08 2f 71 62 09 72 2c 66 08 0b 71 62 09 fd 28 63 08 10 71 62 09 3b fd fd 09 2c 71 62 09 fd 2f fd 09 54 71 62 09 fd fd fd 09 5a 71 62 09 fd fd fd 09 1e 71 62 09 7a fd fd 09 42 71 62 09 fd fd fd 09 6e 71 62 09 fd 15 fd 09 5b 71 62 09 9d fd 09 1b 71 62 09 3b fd 0c 09 7b 71 62 09 1f 09 fd 09 7f 71 62	MZ@XZqbqbqbajqbsqb9\qbs(qbqb#qb/bqbqbHqb(c/qbr,fqb(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\LoReH\SnippingTool.exe	0	3292160	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 fd 24 fd fd fd 77 fd fd fd 77 fd fd fd 77 fd fd 03 77 fd fd fd 77 fd fd fd 76 fd fd fd 77 fd fd fd 76 fd fd fd 77 fd fd fd 76 fd fd fd 77 fd fd fd 76 fd fd fd 77 fd fd fd 77 27 fd fd 77 fd fd fd 76 fd fd fd 77 fd fd 6d 77 fd fd fd 77 fd fd 6f 77 fd fd fd 77 fd fd fd 76 fd fd fd 77 52 69 63 68 fd fd fd 77 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06	MZ@!L!This program cannot be run in DOS mode.$$wwwwwvwvwvwvw w'wvwmwwowwvwRichwPEd	success or wait	1	14005F160	WriteFile
C:\Users\user\AppData\Local\2Yf2pw501\WTSAPI32.dll	0	1372160	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 58 10 0c 5a 1c 71 62 09 1c 71 62 09 1c 71 62 09 61 08 fd 09 6a 71 62 09 73 07 fd 09 18 71 62 09 39 06 fd 09 5c 71 62 09 73 07 fd 09 28 71 62 09 fd 15 fd 09 0b 71 62 09 11 23 fd 09 20 71 62 09 fd 2f 62 08 07 71 62 09 15 09 fd 09 09 71 62 09 07 fd fd 09 48 71 62 09 fd 28 63 08 2f 71 62 09 72 2c 66 08 0b 71 62 09 fd 28 63 08 10 71 62 09 3b fd fd 09 2c 71 62 09 fd 2f fd 09 54 71 62 09 fd fd fd 09 5a 71 62 09 fd fd fd 09 1e 71 62 09 7a fd fd 09 42 71 62 09 fd fd fd 09 6e 71 62 09 fd 15 fd 09 5b 71 62 09 9d fd 09 1b 71 62 09 3b fd 0c 09 7b 71 62 09 1f 09 fd 09 7f 71 62	MZ@XZqbqbqbajqbsqb9\qbs(qbqb# qb/bqbqbHqb(c/qbr,fqb(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\2Yf2pw501\slui.exe	0	445952	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 2a fd 1c 1e 6e fd 72 4d 6e fd 72 4d 6e fd 72 4d 67 fd fd 4d 72 fd 72 4d 01 fd 71 4c 6d fd 72 4d 01 fd 76 4c 78 fd 72 4d 01 fd 77 4c 6a fd 72 4d 01 fd 73 4c 7b fd 72 4d 6e fd 73 4d fd fd 72 4d 01 fd 7c 4c 76 fd 72 4d 01 fd fd 4d 6f fd 72 4d 01 fd 70 4c 6f fd 72 4d 52 69 63 68 6e fd 72 4d 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06	MZ@!L!This program cannot be run in DOS mode.$*nrMnrMnrMgMrrMqLmrMvLxrMwLjrMsL{rMnsMrM|LvrMMorMpLorMRichnrMPEd	success or wait	1	14005F160	WriteFile
C:\Users\user\AppData\Local\Fjrn\WINSTA.dll	0	1376256	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 58 10 0c 5a 1c 71 62 09 1c 71 62 09 1c 71 62 09 61 08 fd 09 6a 71 62 09 73 07 fd 09 18 71 62 09 39 06 fd 09 5c 71 62 09 73 07 fd 09 28 71 62 09 fd 15 fd 09 0b 71 62 09 11 23 fd 09 20 71 62 09 fd 2f 62 08 07 71 62 09 15 09 fd 09 09 71 62 09 07 fd fd 09 48 71 62 09 fd 28 63 08 2f 71 62 09 72 2c 66 08 0b 71 62 09 fd 28 63 08 10 71 62 09 3b fd fd 09 2c 71 62 09 fd 2f fd 09 54 71 62 09 fd fd fd 09 5a 71 62 09 fd fd fd 09 1e 71 62 09 7a fd fd 09 42 71 62 09 fd fd fd 09 6e 71 62 09 fd 15 fd 09 5b 71 62 09 9d fd 09 1b 71 62 09 3b fd 0c 09 7b 71 62 09 1f 09 fd 09 7f 71 62	MZ@XZqbqbqbajqbsqb9\qbs(qbqb#qb/bqbqbHqb(c/qbr,fqb(cqb;,qb/TqbZqbqbzBqbnqb[qbqb;{qbqb	success or wait	1	14005F160	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Fjrn\rdpinput.exe	0	178688	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 1d 69 fd fd 73 3a fd 73 3a fd fd 73 3a ff fd 3a fd fd 73 3a fd fd 70 3b fd fd 73 3a fd fd 77 3b fd fd 73 3a fd fd 76 3b fd fd 73 3a fd fd 72 3b fd fd 73 3a fd fd 72 3a 17 fd 73 3a fd fd 7a 3b fd fd 73 3a fd fd fd 3a fd fd 73 3a fd fd 71 3b fd fd 73 3a 52 69 63 68 fd fd 73 3a 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06 00 fd 39 60 fd 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$is:s:s::s:p;s:w;s:v;s:r;s:r:s:z;s::s:q;s:Richs:PEd9`"	success or wait	1	14005F160	WriteFile
C:\Users\user\AppData\Local\2HophZ6P\XmlLite.dll	0	1372160	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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\2HophZ6P\printfilterpipelinesvc.exe	0	841728	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 27 fd fd fd 46 fd fd fd 46 fd fd fd 46 fd fd fd 3e 49 fd fd 46 fd b5 22 fd fd fd 46 fd b5 22 fd fd fd 46 fd b5 22 fd fd fd 46 fd fd fd 46 fd fd fd 47 fd b5 22 fd fd 5e 46 fd b5 22 fd fd fd 46 fd b5 22 25 fd fd 46 fd b5 22 fd fd fd 46 fd fd 52 69 63 68 fd 46 fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06 00 21 fd 69 fd 00 00 00	MZ@!L!This program cannot be run in DOS mode.$'FFF>IF"F"FF G"^F"F"%F"FRichFPEd!i	success or wait	1	14005F160	WriteFile
C:\Users\user\AppData\Local\D6R1uM\DUser.dll	0	1376256	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 58 10 0c 5a 1c 71 62 09 1c 71 62 09 1c 71 62 09 61 08 fd 09 6a 71 62 09 73 07 fd 09 18 71 62 09 39 06 fd 09 5c 71 62 09 73 07 fd 09 28 71 62 09 fd 15 fd 09 0b 71 62 09 11 23 fd 09 20 71 62 09 fd 2f 62 08 07 71 62 09 15 09 fd 09 09 71 62 09 07 fd fd 09 48 71 62 09 fd 28 63 08 2f 71 62 09 72 2c 66 08 0b 71 62 09 fd 28 63 08 10 71 62 09 3b fd fd 09 2c 71 62 09 fd 2f fd 09 54 71 62 09 fd fd fd 09 5a 71 62 09 fd fd fd 09 1e 71 62 09 7a fd fd 09 42 71 62 09 fd fd fd 09 6e 71 62 09 fd 15 fd 09 5b 71 62 09 9d fd 09 1b 71 62 09 3b fd 0c 09 7b 71 62 09 1f 09 fd 09 7f 71 62	MZ@XZqbqbqbajqbsqb9\qbs(qbqb# qb/bqbqbHqb(c/qbr,fqb(cqb;,qb/ TqbZqbqbzBqbnqb[qbqb;{qbqb	success or wait	1	14005F160	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\D6R1uM\Utilman.exe	0	98304	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 44 fd fd 13 00 fd 40 00 fd 40 00 fd 40 09 fd 38 40 04 fd 40 6f fd fd 41 03 fd 40 6f fd fd 41 17 fd 40 6f fd fd 41 0d fd 40 6f fd fd 41 1b fd 40 00 fd 40 34 fd 40 6f fd fd 41 14 fd 40 6f fd 54 40 01 fd 40 6f fd fd 41 01 fd 40 52 69 63 68 00 fd 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 07 00 1c 30 fd 00 00 00	MZ@!L!This program cannot be run in DOS mode.$D@@@8@@oA @oA@o A@oA@@4@oA@oT@ @oA@Rich@PEd0	success or wait	1	14005F160	WriteFile
C:\Users\user\AppData\Local\op5PCy\DUI70.dll	0	1654784	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\op5PCy\phoneactivate.exe	0	107504	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 69 fd fd fd 07 fd 07 fd 07 fd fd fd 07 fd fd fd 04 fd 07 fd fd fd 03 fd 07 fd fd fd 02 fd 07 fd fd fd 06 fd 07 fd 06 fd 4f fd 07 fd fd fd 0e fd 07 fd fd fd fd fd 07 fd fd fd 05 fd 07 fd 52 69 63 68 fd fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 07	MZ@!L!This program cannot be run in DOS mode.$iORichPEd	success or wait	1	14005F160	WriteFile
C:\Users\user\AppData\Local\CSYG\DUI70.dll	0	1654784	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\CSYG\DmNotificationBroker.exe	0	32256	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 0c 6a fd 3f 48 0b fd 6c 48 0b fd 6c 48 0b fd 6c 41 73 04 6c 54 0b fd 6c 27 6f fd 6d 4a 0b fd 6c 27 6f fd 6d 5b 0b fd 6c 48 0b fd 6c 16 0b fd 6c 27 6f fd 6d 43 0b fd 6c 27 6f fd 6d 41 0b fd 6c 27 6f fd 6d 41 0b fd 6c 27 6f 68 6c 49 0b fd 6c 27 6f fd 6d 49 0b fd 6c 52 69 63 68 48 0b fd 6c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 07	MZ@!L!This program cannot be run in DOS mode.$j?HlHlHlAslTl'omJl'om[lHll'omCl'omAl'omAl'ohlIl'omIlRichHlPEd	success or wait	1	14005F160	WriteFile
C:\Users\user\AppData\Local\oOQGGow\DUI70.dll	0	1654784	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\oOQGGow\ProximityUxHost.exe	0	264480	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 06 fd fd fd 42 fd fd 42 fd fd 42 fd fd 4b fd 60 fd 26 fd fd 2d fd fd 41 fd fd 2d fd fd fd 55 fd fd 2d fd fd fd 4b fd fd 2d fd fd 55 fd fd 42 fd fd 74 fd fd 2d fd fd fd 5d fd fd 2d fd 0c fd 43 fd fd 2d fd fd 43 fd fd 52 69 63 68 42 fd fd 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 07 00 3b fd 2a 51 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$BBBK`&-A-U-K-UBt-]-C-CRichBPEd;*Q"	success or wait	1	14005F160	WriteFile
C:\Users\user\AppData\Local\l5T\XmlLite.dll	0	1372160	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 58 10 0c 5a 1c 71 62 09 1c 71 62 09 1c 71 62 09 61 08 fd 09 6a 71 62 09 73 07 fd 09 18 71 62 09 39 06 fd 09 5c 71 62 09 73 07 fd 09 28 71 62 09 fd 15 fd 09 0b 71 62 09 11 23 fd 09 20 71 62 09 fd 2f 62 08 07 71 62 09 15 09 fd 09 09 71 62 09 07 fd fd 09 48 71 62 09 fd 28 63 08 2f 71 62 09 72 2c 66 08 0b 71 62 09 fd 28 63 08 10 71 62 09 3b fd fd 09 2c 71 62 09 fd 2f fd 09 54 71 62 09 fd fd fd 09 5a 71 62 09 fd fd fd 09 1e 71 62 09 7a fd fd 09 42 71 62 09 fd fd fd 09 6e 71 62 09 fd 15 fd 09 5b 71 62 09 9d fd 09 1b 71 62 09 3b fd 0c 09 7b 71 62 09 1f 09 fd 09 7f 71 62	MZ@XZqbqbqbajqbsqb9\qbs(qbqb# qb/bqbqbHqb(c/qbr,fqb(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\l5T\omadmclient.exe	0	315904	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 60 32 10 4b 24 53 7e 18 24 53 7e 18 24 53 7e 18 2d 2b fd 18 6e 53 7e 18 4b 37 7d 19 27 53 7e 18 4b 37 7a 19 31 53 7e 18 24 53 7f 18 fd 52 7e 18 4b 37 7f 19 3d 53 7e 18 4b 37 7b 19 29 53 7e 18 4b 37 77 19 12 53 7e 18 4b 37 fd 18 25 53 7e 18 4b 37 7c 19 25 53 7e 18 52 69 63 68 24 53 7e 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 07	MZ@!L!This program cannot be run in DOS mode.$`2K$S~$S~$S~-+nS~K7}'S~K7z1S~$SR~K7=S~K7{)S~K7wS~K7%S~K7\|%S~Rich$S~PEd	success or wait	1	14005F160	WriteFile
C:\Users\user\AppData\Local\G6gv6e\UxTheme.dll	0	1372160	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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\G6gv6e\AtBroker.exe	0	62976	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 35 60 0c fd 71 01 62 fd 71 01 62 fd 71 01 62 fd 1e 65 61 fd 72 01 62 fd 1e 65 66 fd 64 01 62 fd 1e 65 67 fd 79 01 62 fd 1e 65 63 fd 62 01 62 fd 71 01 63 fd fd 01 62 fd 1e 65 6b fd 7e 01 62 fd 1e 65 fd fd 70 01 62 fd 1e 65 60 fd 70 01 62 fd 52 69 63 68 71 01 62 fd 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06 00 3d 1a fd 7e 00 00 00 00 00 00 00 00 fd 00 22 00 0b 02 0e 0c 00 fd 00	MZ@!L!This program cannot be run in DOS mode.$5`qbqbqbearbefdbegybecbbqcbek~bepbe`pbRichqbPEd=~"	success or wait	1	14005F160	WriteFile
C:\Users\user\AppData\Local\rDAhA\WMsgAPI.dll	0	1372160	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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\rDAhA\consent.exe	0	157080	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 59 5f 47 45 1d 3e 29 16 1d 3e 29 16 1d 3e 29 16 14 46 fd 16 59 3e 29 16 72 5a 2a 17 1e 3e 29 16 72 5a 2d 17 05 3e 29 16 72 5a 2c 17 15 3e 29 16 72 5a 28 17 0a 3e 29 16 1d 3e 28 16 39 3f 29 16 72 5a 27 17 10 3e 29 16 72 5a fd 16 1c 3e 29 16 72 5a 2b 17 1c 3e 29 16 52 69 63 68 1d 3e 29 16 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 08 00 69 fd 37 00 00 00	MZ@!L!This program cannot be run in DOS mode.$Y_GE>)>)>)FY>) rZ*>)rZ->)rZ,>)rZ(>)> (9?)rZ'>) rZ>)rZ+>)Rich>)PEdi7	success or wait	1	14005F160	WriteFile
C:\Users\user\AppData\Local\Ui9PsZ9\OLEACC.dll	0	1372160	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 58 10 0c 5a 1c 71 62 09 1c 71 62 09 1c 71 62 09 61 08 fd 09 6a 71 62 09 73 07 fd 09 18 71 62 09 39 06 fd 09 5c 71 62 09 73 07 fd 09 28 71 62 09 fd 15 fd 09 0b 71 62 09 11 23 fd 09 20 71 62 09 fd 2f 62 08 07 71 62 09 15 09 fd 09 09 71 62 09 07 fd fd 09 48 71 62 09 fd 28 63 08 2f 71 62 09 72 2c 66 08 0b 71 62 09 fd 28 63 08 10 71 62 09 3b fd fd 09 2c 71 62 09 fd 2f fd 09 54 71 62 09 fd fd fd 09 5a 71 62 09 fd fd fd 09 1e 71 62 09 7a fd fd 09 42 71 62 09 fd fd fd 09 6e 71 62 09 fd 15 fd 09 5b 71 62 09 9d fd 09 1b 71 62 09 3b fd 0c 09 7b 71 62 09 1f 09 fd 09 7f 71 62	MZ@XZqbqbqbajqbsqb9\ qbs(qbqb# qb/bqbqbHqb(c/qbr,fqb(c qb;,qb/ TqbZqbqbzBqbnqb[qbqb; {qbqb	success or wait	1	14005F160	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\manage-bde.exe	unknown	215552	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\BackgroundTransferHost.exe	unknown	36864	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\comp.exe	unknown	25088	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\immersivetpmvscmgrsvr.exe	unknown	142848	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\FileHistory.exe	unknown	246784	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\uxtheme.dll	unknown	599040	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\MBR2GPT.EXE	unknown	808960	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\OpenWith.exe	unknown	111120	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\rdpinput.exe	unknown	178688	success or wait	6	14005F8D6	ReadFile
C:\Windows\System32\wtsapi32.dll	unknown	64168	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\ReAgentc.exe	unknown	40448	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\SndVol.exe	unknown	259904	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\dwmapi.dll	unknown	146840	success or wait	1	14005F8D6	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\wuapihost.exe	unknown	10752	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\ntprint.exe	unknown	64000	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\rekeywiz.exe	unknown	120320	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\msdtc.exe	unknown	148480	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\mtstocom.exe	unknown	134144	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\RmClient.exe	unknown	17408	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\SnippingTool.exe	unknown	3292160	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\oleacc.dll	unknown	416768	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\UevTemplateConfigItemGenerator.exe	unknown	11776	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\diskpart.exe	unknown	154624	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\slui.exe	unknown	445952	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\dsregcmd.exe	unknown	704512	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\winsta.dll	unknown	332712	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\pwlauncher.exe	unknown	35328	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\sihost.exe	unknown	79360	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\SecEdit.exe	unknown	39936	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\powercfg.exe	unknown	94720	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\bootim.exe	unknown	25088	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\cofire.exe	unknown	23552	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\DpiScaling.exe	unknown	79360	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\alg.exe	unknown	91136	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\browser_broker.exe	unknown	43424	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\tcblaunch.exe	unknown	567176	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\printfilterpipelinesvc.exe	unknown	841728	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\xmllite.dll	unknown	227840	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\upnpcont.exe	unknown	39936	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\audiodg.exe	unknown	594128	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\NetHost.exe	unknown	10752	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\setupugc.exe	unknown	127488	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\systray.exe	unknown	10752	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\DeviceEject.exe	unknown	29696	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\prproc.exe	unknown	20728	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\spaceman.exe	unknown	35328	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\Utilman.exe	unknown	98304	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\duser.dll	unknown	578048	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\MdmDiagnosticsTool.exe	unknown	45568	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\wininit.exe	unknown	366792	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\omadmprc.exe	unknown	61952	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\conhost.exe	unknown	625664	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\phoneactivate.exe	unknown	107504	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\dui70.dll	unknown	1719808	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\ApplicationFrameHost.exe	unknown	69800	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\gpscript.exe	unknown	44544	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\CloudExperienceHostBroker.exe	unknown	75680	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\WpcTok.exe	unknown	274944	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\fodhelper.exe	unknown	46080	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\PackagedCWALauncher.exe	unknown	38400	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\rundll32.exe	unknown	69632	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\TSWbPrxy.exe	unknown	67584	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\DmNotificationBroker.exe	unknown	32256	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\mavinject.exe	unknown	183704	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\MSchedExe.exe	unknown	82944	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\ApproveChildRequest.exe	unknown	231424	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\repair-bde.exe	unknown	126976	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\UsoClient.exe	unknown	40960	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\DTUHandler.exe	unknown	116632	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\coredpussvr.exe	unknown	72192	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\ProximityUxHost.exe	unknown	264480	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\WWAHost.exe	unknown	930720	success or wait	1	14005F8D6	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\MDEServer.exe	unknown	456704	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\omadmclient.exe	unknown	315904	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\Microsoft.Uev.SyncController.exe	unknown	83456	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\regsvr32.exe	unknown	24064	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\mountvol.exe	unknown	17920	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\AtBroker.exe	unknown	62976	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\msiexec.exe	unknown	66048	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\winresume.exe	unknown	983008	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\sdbinst.exe	unknown	23552	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\RdpSaProxy.exe	unknown	27648	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\consent.exe	unknown	157080	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\wmsgapi.dll	unknown	18944	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\userinit.exe	unknown	32256	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\fsquirt.exe	unknown	141824	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\DeviceCredentialDeployment.exe	unknown	78336	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\Narrator.exe	unknown	349696	success or wait	2	14005F8D6	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{90E9AF86-66B0-3FAA-46C7-F205C1A19B58}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{90E9AF86-66B0-3FAA-46C7-F205C1A19B58}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{D42C02B8-7179-E06E-1356-7C9523E5CADA}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{D42C02B8-7179-E06E-1356-7C9523E5CADA}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{66F06FCD-523A-FF61-95B5-096CB3E44F3D}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{66F06FCD-523A-FF61-95B5-096CB3E44F3D}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{14AF6E52-AC2D-2BF7-1D37-EA081F79ABCC}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{14AF6E52-AC2D-2BF7-1D37-EA081F79ABCC}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{E565D85A-2C3B-E4D5-2469-C57A832EC41A}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{E565D85A-2C3B-E4D5-2469-C57A832EC41A}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{A2D170A2-C2B0-5D7D-DDCE-B62119CFE208}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{A2D170A2-C2B0-5D7D-DDCE-B62119CFE208}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{25BCDD8A-F0D8-9827-C247-ACF58A27E145}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{25BCDD8A-F0D8-9827-C247-ACF58A27E145}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{CF6E9F48-CAE2-5E64-E5B2-B9B8857D789B}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{CF6E9F48-CAE2-5E64-E5B2-B9B8857D789B}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{6A1B2CFF-DF0A-DDFE-1814-C4D249758C13}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{6A1B2CFF-DF0A-DDFE-1814-C4D249758C13}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{8E4DF133-7A8B-89EE-7E44-816CA0D8F00A}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{8E4DF133-7A8B-89EE-7E44-816CA0D8F00A}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{B5E86DC6-7D25-853D-C9AB-57085AAEA3AC}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{B5E86DC6-7D25-853D-C9AB-57085AAEA3AC}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{653463C5-36C3-44D2-30C0-C7631CD04B9B}	success or wait	1	14006340A	RegCreateKeyExW

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{653463C5-36C3-44D2-30C0-C7631CD04B9B}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{D6C83671-8689-DEA2-30F3-C4A27D7ECBA9}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{D6C83671-8689-DEA2-30F3-C4A27D7ECBA9}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{14C8E79E-F05D-7C78-7C3F-73EA921FA94D}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{14C8E79E-F05D-7C78-7C3F-73EA921FA94D}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{376AE45E-2278-8533-6726-F515F2703B7A}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{376AE45E-2278-8533-6726-F515F2703B7A}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{662BB791-C9E0-B813-177C-DCC2427CE5B0}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{662BB791-C9E0-B813-177C-DCC2427CE5B0}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{155244D4-2DEE-46B9-B42E-730A37C70F4D}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{155244D4-2DEE-46B9-B42E-730A37C70F4D}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{77C1EBF9-E18D-8DC0-733B-D523A8B74BA0}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{77C1EBF9-E18D-8DC0-733B-D523A8B74BA0}\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\{B5E86DC6-7D25-853D-C9AB-57085AAEA3AC}\ShellFolder	{6E8BA082-695C-D220-9A43-DF8C51CF6D08}	binary	8C 04 E9 3B 8F 3D 2F 73 3E 54 BD 33 0B 5C 03 78 62 09 26 95 07 D8 96 01 2B FF 68 02 CB CA 8C A5 EC 76 70 80 AC DF B6 51 C9 32 A0 08 75 CA 0A A7 96 DE 44 FF 5C CA 87 9F 96 00 27 59 11 33 C6 E5 83 6D DB 51 85 75 BD	success or wait	1	140062470	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{6A1B2CFF-DF0A-DDFE-1814-C4D249758C13}\ShellFolder	{1B4A2E68-D005-D2EC-2E80-7BAF5DCEC35F}	binary	9C 01 61 1F 39 46 47 A1 1D FD 96 7C BB 33 B6 60 E8 B6 7D 45 51 92 C4 5F 30 7E 06 2E 0A DC 94 E9 59 9E 66 41 84 D0 C7 C3 B1 FB BE D8 50 97 5A 71 0F 3B 9C EA 2E 0B E1 2B A8 2F A6 2C 23 78 24 D0 6B F4 C4 D5 6B F5 04 B0 F7 3E D9 73 2B A3 A1 84 25 29 7C 92 B4 7B A6 93 49 31 61 E2	success or wait	1	140062470	RegSetValueExA

Analysis Process: rundll32.exe PID: **6764**, Parent PID: **852**

General

Target ID:	5
Start time:	15:42:55
Start date:	23/03/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\GpUSRuIBHx.dll,??0VolumeFveStatus@@QEAA@K_KJW4_FVE_WIPING_STATE@@@Z
Imagebase:	0x7ff7c5d30000
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: 00000005.00000002.358622486.00007FF8BA5D1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\GpUSRuIBHx.dll	unknown	1368064	success or wait	1	7FF8BA62F8D6	ReadFile

Analysis Process: rundll32.exe PID: **5872**, Parent PID: **852**

General

Target ID:	6
Start time:	15:42:59
Start date:	23/03/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\GpUSRuIBHx.dll,??4BuiVolume@@QEAAAEAV0@AEBV0@@Z
Imagebase:	0x7ff7c5d30000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000006.00000002.366331885.00007FF8BA5D1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\GpUSRuIBHx.dll	unknown	1368064	success or wait	1	7FF8BA62F8D6	ReadFile

Analysis Process: BackgroundTransferHost.exe PID: **5856**, Parent PID: **796**

General

Target ID:	14
Start time:	15:43:34
Start date:	23/03/2022
Path:	C:\Windows\System32\BackgroundTransferHost.exe
Wow64 process (32bit):	false
Commandline:	"BackgroundTransferHost.exe" -ServerName:BackgroundTransferHost.1
Imagebase:	0x7ff7e4fa0000
File size:	36864 bytes
MD5 hash:	02BA81746B929ECC9DB6665589B68335
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
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	Completion	Count	Source Address	Symbol

Analysis Process: FileHistory.exe PID: **5804**, Parent PID: **3808**

General	
Target ID:	17
Start time:	15:43:51
Start date:	23/03/2022
Path:	C:\Windows\System32\FileHistory.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\FileHistory.exe
Imagebase:	0x7ff693090000
File size:	246784 bytes
MD5 hash:	989B5BDB2BEAC9F894BBC236F1B67967
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: FileHistory.exe PID: **6388**, Parent PID: **3808**

General	
Target ID:	18
Start time:	15:43:53
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\6f22a\FileHistory.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\6f22a\FileHistory.exe
Imagebase:	0x7ff6d0a30000
File size:	246784 bytes
MD5 hash:	989B5BDB2BEAC9F894BBC236F1B67967
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000012.00000002.484522001.00007FF8CA981000.00000020.00000001.01000000.00000008.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\FileHistory.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF8B8CA86ED	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\FileHistory.exe.log	0	42	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a	1,"fusion","GAC",01,"WinRT","NotApp",1	success or wait	1	7FF8B8CA8769	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FF8B870B9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FF8B870B9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FF8B87E12E7	ReadFile

Analysis Process: rdpinput.exe PID: **6940**, Parent PID: **3808**

General	
Target ID:	19
Start time:	15:43:56
Start date:	23/03/2022
Path:	C:\Windows\System32\rdpinput.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\rdpinput.exe
Imagebase:	0x7ff7e8070000
File size:	178688 bytes
MD5 hash:	4403785D297C55D5DF26176B4F1A52C8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rdpinput.exe PID: **6992**, Parent PID: **3808**

General	
Target ID:	20
Start time:	15:43:57
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\Kyz7D\rdpinput.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Kyz7D\rdpinput.exe
Imagebase:	0x7ff7bada0000
File size:	178688 bytes
MD5 hash:	4403785D297C55D5DF26176B4F1A52C8
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: 00000014.00000002.512496248.00007FF8CA981000.00000020.00000001.01000000.0000000C.sdmp, Author: Joe Security

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Kyz7D\WTSAPI32.dll	unknown	1372160	success or wait	1	7FF8CA9DF8D6	ReadFile

Analysis Process: SndVol.exe PID: **6428**, Parent PID: **3808**

General	
Target ID:	21
Start time:	15:44:09
Start date:	23/03/2022
Path:	C:\Windows\System32\SndVol.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SndVol.exe
Imagebase:	0x7ff7678e0000
File size:	259904 bytes
MD5 hash:	CDD7C7DF2D0859AC3F4088423D11BD08
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: SndVol.exe PID: **6436**, Parent PID: **3808**

General	
Target ID:	22
Start time:	15:44:11
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\bTcR2e\SndVol.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\bTcR2e\SndVol.exe
Imagebase:	0x7ff6c1bb0000
File size:	259904 bytes
MD5 hash:	CDD7C7DF2D0859AC3F4088423D11BD08
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: 00000016.00000002.541815176.00007FF8CA981000.00000020.00000001.01000000.0000000E.sdmp, Author: Joe Security

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\bTcR2e\dwmapi.dll	unknown	1372160	success or wait	1	7FF8CA9DF8D6	ReadFile

Analysis Process: SnippingTool.exe PID: **7052**, Parent PID: **3808**

General	
Target ID:	24
Start time:	15:44:23
Start date:	23/03/2022
Path:	C:\Windows\System32\SnippingTool.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SnippingTool.exe
Imagebase:	0x7ff61af50000
File size:	3292160 bytes
MD5 hash:	9012F9C6AC7F3F99ECDD37E24C9AC3BB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: SnippingTool.exe PID: **5480**, Parent PID: **3808**

General	
Target ID:	25
Start time:	15:44:24
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\LoReH\SnippingTool.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\LoReH\SnippingTool.exe
Imagebase:	0x7ff70c3f0000
File size:	3292160 bytes
MD5 hash:	9012F9C6AC7F3F99ECDD37E24C9AC3BB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000019.00000002.581334481.00007FF8CA981000.00000020.00000001.01000000.00000010.sdmp, Author: Joe Security

Analysis Process: slui.exe PID: **5012**, Parent PID: **3808**

General	
Target ID:	27
Start time:	15:44:41
Start date:	23/03/2022
Path:	C:\Windows\System32\slui.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\slui.exe
Imagebase:	0x7ff71ca20000
File size:	445952 bytes
MD5 hash:	96A8EF9387619D17BB30B024DDF52BF3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: slui.exe PID: **3852**, Parent PID: **3808**

General	
Target ID:	28
Start time:	15:44:43
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\2Yf2pw501\slui.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\2Yf2pw501\slui.exe
Imagebase:	0x7ff6a3f20000
File size:	445952 bytes
MD5 hash:	96A8EF9387619D17BB30B024DDF52BF3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000001C.00000002.616859661.00007FF8CA981000.00000020.00000001.01000000.00000013.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: rdpinput.exe PID: **4236**, Parent PID: **3808**

General	
Target ID:	29
Start time:	15:44:58
Start date:	23/03/2022
Path:	C:\Windows\System32\rdpinput.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\rdpinput.exe
Imagebase:	0x7ff7dae40000
File size:	178688 bytes
MD5 hash:	4403785D297C55D5DF26176B4F1A52C8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rdpinput.exe PID: **780**, Parent PID: **3808**

General	
Target ID:	30

Start time:	15:45:00
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\Fjrn\rdpinput.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Fjrn\rdpinput.exe
Imagebase:	0x7ff64db80000
File size:	178688 bytes
MD5 hash:	4403785D297C55D5DF26176B4F1A52C8
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: 0000001E.00000002.646421042.00007FF8CA981000.00000020.00000001.01000000.00000015.sdmp, Author: Joe Security

Analysis Process: printfilterpipelinesvc.exe PID: **5112**, Parent PID: **3808**

General

Target ID:	31
Start time:	15:45:11
Start date:	23/03/2022
Path:	C:\Windows\System32\printfilterpipelinesvc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\printfilterpipelinesvc.exe
Imagebase:	0x7ff6fba90000
File size:	841728 bytes
MD5 hash:	4164BD4D8E23C672E40D203E4B4A38A7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: printfilterpipelinesvc.exe PID: **4752**, Parent PID: **3808**

General

Target ID:	32
Start time:	15:45:13
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\2HophZ6P\printfilterpipelinesvc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\2HophZ6P\printfilterpipelinesvc.exe
Imagebase:	0x7ff6b4120000
File size:	841728 bytes
MD5 hash:	4164BD4D8E23C672E40D203E4B4A38A7
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: 00000020.00000002.678112483.00007FF8BB381000.00000020.00000001.01000000.00000017.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: Utilman.exe PID: **1508**, Parent PID: **3808**

General

Target ID:	33
Start time:	15:45:26
Start date:	23/03/2022
Path:	C:\Windows\System32\Utilman.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\Utilman.exe
Imagebase:	0x7ff6a6470000
File size:	98304 bytes
MD5 hash:	C91CCEF3884CFDE746B4BAEF5F1BC75C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: Utilman.exe PID: **1332**, Parent PID: **3808**

General	
Target ID:	34
Start time:	15:45:28
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\D6R1uM\Utilman.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\D6R1uM\Utilman.exe
Imagebase:	0x7ff7c58b0000
File size:	98304 bytes
MD5 hash:	C91CCEF3884CFDE746B4BAEF5F1BC75C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000022.00000002.705952583.00007FF8BB381000.00000020.00000001.01000000.00000019.sdmp, Author: Joe Security

Analysis Process: phoneactivate.exe PID: **2912**, Parent PID: **3808**

General	
Target ID:	35
Start time:	15:45:39
Start date:	23/03/2022
Path:	C:\Windows\System32\phoneactivate.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\phoneactivate.exe
Imagebase:	0x7ff730a10000
File size:	107504 bytes
MD5 hash:	09D1974A03068D4311F1CE94B765E817
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: phoneactivate.exe PID: **5856**, Parent PID: **3808**

General	
Target ID:	36
Start time:	15:45:44
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\op5PCy\phoneactivate.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\op5PCy\phoneactivate.exe
Imagebase:	0x7ff7f2eb0000
File size:	107504 bytes
MD5 hash:	09D1974A03068D4311F1CE94B765E817
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: 00000024.00000002.746490737.00007FF8CA681000.00000020.00000001.01000000.0000001B.sdmp, Author: Joe Security

Analysis Process: DmNotificationBroker.exe PID: **6180**, Parent PID: **3808**

General

Target ID:	37
Start time:	15:45:58
Start date:	23/03/2022
Path:	C:\Windows\System32\DmNotificationBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\DmNotificationBroker.exe
Imagebase:	0x7ff7f1a50000
File size:	32256 bytes
MD5 hash:	1643D5735213BC89C0012F0E48253765
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: DmNotificationBroker.exe PID: **6460**, Parent PID: **3808**

General

Target ID:	38
Start time:	15:46:04
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\CSYG\DmNotificationBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\CSYG\DmNotificationBroker.exe
Imagebase:	0x7ff7bfef0000
File size:	32256 bytes
MD5 hash:	1643D5735213BC89C0012F0E48253765
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000026.00000002.791054747.00007FF8CA681000.00000020.00000001.01000000.0000001E.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: ProximityUxHost.exe PID: **6936**, Parent PID: **3808**

General

Target ID:	39
Start time:	15:46:19
Start date:	23/03/2022
Path:	C:\Windows\System32\ProximityUxHost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\ProximityUxHost.exe
Imagebase:	0x7ff68fe50000
File size:	264480 bytes
MD5 hash:	E7F0E9B3779E54CD271959C600A2A531
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ProximityUxHost.exe PID: **6560**, Parent PID: **3808**

General	
Target ID:	40
Start time:	15:46:25
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\oOQGGow\ProximityUxHost.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\oOQGGow\ProximityUxHost.exe
Imagebase:	0x7ff777300000
File size:	264480 bytes
MD5 hash:	E7F0E9B3779E54CD271959C600A2A531
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000028.00000002.836674261.00007FF8CA681000.00000020.00000001.01000000.00000020.sdmp, Author: Joe Security

Analysis Process: omadmclient.exe PID: **244**, Parent PID: **3808**

General	
Target ID:	41
Start time:	15:46:40
Start date:	23/03/2022
Path:	C:\Windows\System32\omadmclient.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\omadmclient.exe
Imagebase:	0x7ff6e6700000
File size:	315904 bytes
MD5 hash:	AD7C6CD7A8EEC95808AA77C5D7987941
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

No disassembly