ID: 595303
Sample Name: AyBhhRZXPj
Cookbook: default.jbs
Time: 15:40:41
Date: 23/03/2022
Version: 34.0.0 Boulder Opal

Table of Contents

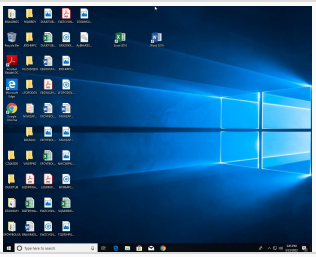
Windows Analysis Report

AyBhhRZXPj

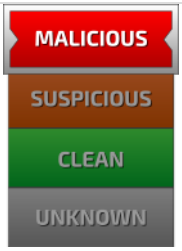
Overview

General Information

Sample Name:	AyBhhRZXPj (renamed file extension from none to dll)
Analysis ID:	595303
MD5:	518cc4a9888e76..
SHA1:	148d6f12f12a0ca..
SHA256:	57b0d95f62fc799..
Tags:	Dridex exe
Infos:	



Detection



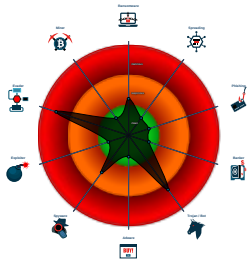
Dridex

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…
- Uses Atom Bombing / ProGate to in…
- Queries the volume information (nam…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 6608 cmdline: loaddll64.exe "C:\Users\user\Desktop\AyBhhRZXPj.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 6620 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\AyBhhRZXPj.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 6640 cmdline: rundll32.exe "C:\Users\user\Desktop\AyBhhRZXPj.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6632 cmdline: rundll32.exe C:\Users\user\Desktop\AyBhhRZXPj.dll,ApplyCompatResolutionQuirking MD5: 73C519F050C20580F8A62C849D49215A)
    - explorer.exe (PID: 3968 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - Magnify.exe (PID: 5372 cmdline: C:\Windows\system32\Magnify.exe MD5: F97BE20B374457236666607EE4BA7F7F)
      - FileHistory.exe (PID: 5788 cmdline: C:\Windows\system32\FileHistory.exe MD5: 989B5BDB2BEAC9F894BBC236F1B67967)
      - FileHistory.exe (PID: 7004 cmdline: C:\Users\user\AppData\Local\u70W8\FileHistory.exe MD5: 989B5BDB2BEAC9F894BBC236F1B67967)
      - RdpSa.exe (PID: 7028 cmdline: C:\Windows\system32\RdpSa.exe MD5: 0795B6F790F8E52D55F39E593E9C5BBA)
      - mspaint.exe (PID: 7064 cmdline: C:\Windows\system32\mspaint.exe MD5: 99F86A0D360FD9A3FCAD6B1E7D92A90C)
      - mspaint.exe (PID: 4576 cmdline: C:\Users\user\AppData\Local\NYpervHTp\mspaint.exe MD5: 99F86A0D360FD9A3FCAD6B1E7D92A90C)
      - mmc.exe (PID: 6244 cmdline: C:\Windows\system32\mmc.exe MD5: BA80301974CC8C4FB9F3F9DDB5905C30)
      - EaseOfAccessDialog.exe (PID: 6176 cmdline: C:\Windows\system32\EaseOfAccessDialog.exe MD5: F87F2E5EBF3FFBA39DF1621B5F8689B5)
      - unregmp2.exe (PID: 4948 cmdline: C:\Windows\system32\unregmp2.exe MD5: 9B517303C58CA8A450B97B0D71594CBB)
      - unregmp2.exe (PID: 4908 cmdline: C:\Users\user\AppData\Local\vVin\unregmp2.exe MD5: 9B517303C58CA8A450B97B0D71594CBB)
      - omadmclient.exe (PID: 6340 cmdline: C:\Windows\system32\omadmclient.exe MD5: AD7C6CD7A8EEC95808AA77C5D7987941)
      - omadmclient.exe (PID: 6392 cmdline: C:\Users\user\AppData\Local\iv505rrw\omadmclient.exe MD5: AD7C6CD7A8EEC95808AA77C5D7987941)
      - SystemPropertiesPerformance.exe (PID: 4040 cmdline: C:\Windows\system32\SystemPropertiesPerformance.exe MD5: F325976CDC0F7E9C680B51B35D24D23A)
      - eudcedit.exe (PID: 6164 cmdline: C:\Windows\system32\eudcedit.exe MD5: 0ED10F2F98B80FF9F95EED2B04CFA076)
      - GamePanel.exe (PID: 5244 cmdline: C:\Windows\system32\GamePanel.exe MD5: 4EF330EFAE954723B1F2800C15FDA7EB)
      - GamePanel.exe (PID: 5832 cmdline: C:\Users\user\AppData\Local\Odp\GamePanel.exe MD5: 4EF330EFAE954723B1F2800C15FDA7EB)
  - rundll32.exe (PID: 6724 cmdline: rundll32.exe C:\Users\user\Desktop\AyBhhRZXPj.dll,CompatString MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6868 cmdline: rundll32.exe C:\Users\user\Desktop\AyBhhRZXPj.dll,CompatValue MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.254650738.00007FFC670C1000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000000.00000002.274237724.00007FFC670C1000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000008.00000002.268092209.00007FFC670C1000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000023.00000002.497477137.00007FFC74C21000.00000020.00000001.01000000.00000010.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000005.00000002.260480210.00007FFC670C1000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	

Click to see the 5 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.rundll32.exe.7ffc670c0000.2.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
35.2.unregmp2.exe.7ffc74c20000.3.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
21.2.FileHistory.exe.7ffc74c20000.3.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
37.2.omadmclient.exe.7ffc74c20000.3.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
5.2.rundll32.exe.7ffc670c0000.2.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	

Click to see the 5 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

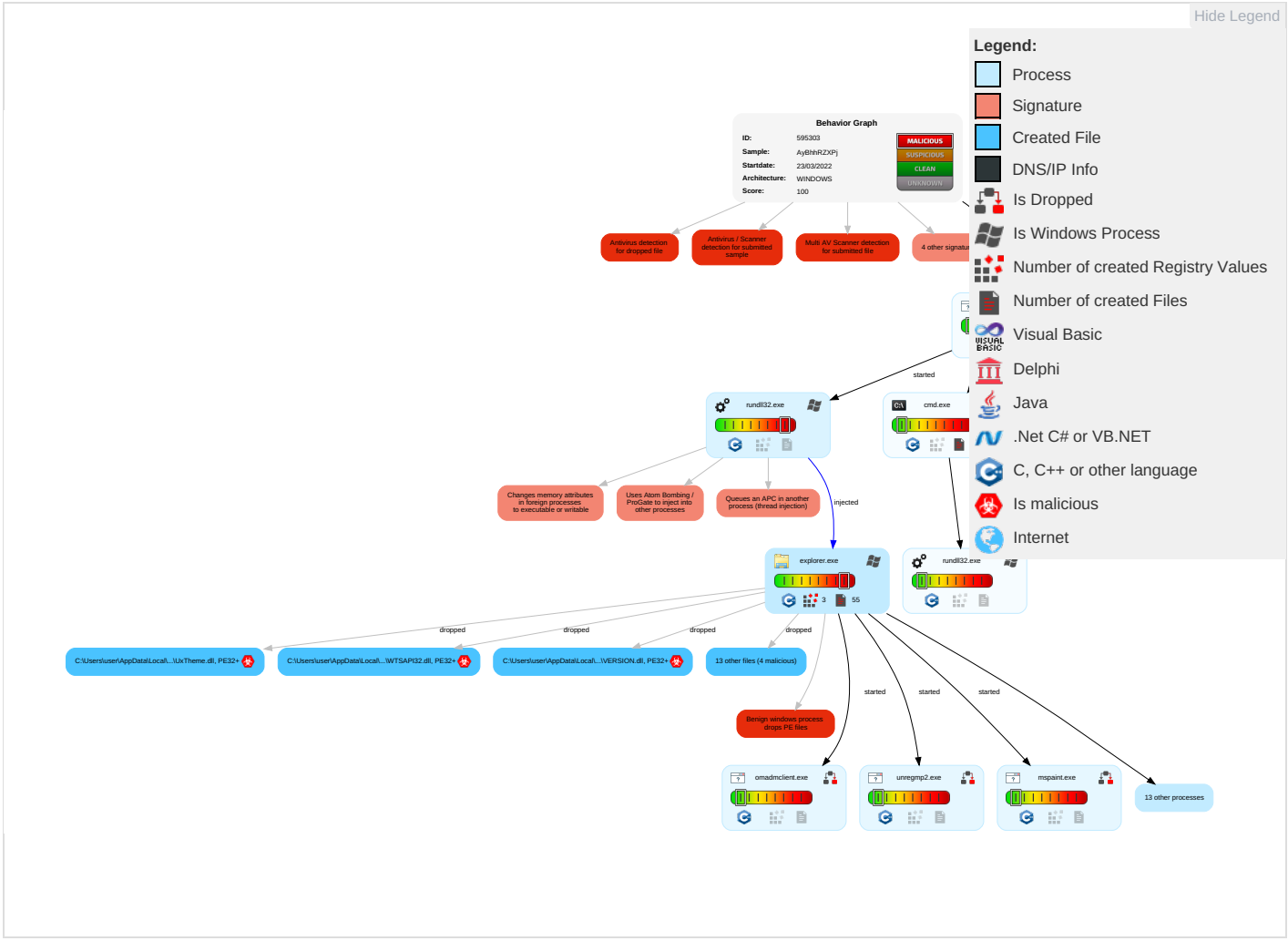
Queues an APC in another process (thread injection)

Uses Atom Bombing / ProGate to inject into other processes

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Native API	1 DLL Side-Loading	1 DLL Side-Loading	1 1 Disable or Modify Tools	1 1 Input Capture	2 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Exploitation for Client Execution	1 Windows Service	1 Windows Service	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	1 1 Input Capture	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 Command and Scripting Interpreter	Logon Script (Windows)	3 1 2 Process Injection	2 Obfuscated Files or Information	Security Account Manager	1 File and Directory Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 Service Execution	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	1 Query Registry	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	2 1 Security Software Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Masquerading	DCSync	1 Virtualization/Sandbox Evasion	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	3 Process 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
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
AyBhhRZXPj.dll	70%	Virustotal		Browse
AyBhhRZXPj.dll	62%	Metadefender		Browse
AyBhhRZXPj.dll	88%	ReversingLabs	Win64.Trojan.Occamy	
AyBhhRZXPj.dll	100%	Avira	TR/Crypt.XPACK.Gen7	
AyBhhRZXPj.dll	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Odp\dwmapi.dll	100%	Avira	TR/Crypt.XPACK.Gen7	
C:\Users\user\AppData\Local\u70W8\UxTheme.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\NYpervHTp\MFC42u.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\iv505rrw\XmlLite.dll	100%	Avira	TR/Crypt.XPACK.Gen7	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\pkru2Wsoo\VERSION.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\pkru2Wsoo\VERSION.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\QpruqOk1\DUI70.dll	100%	Avira	TR/Crypt.XPACK.Gen4	
C:\Users\user\AppData\Local\rgsL2C4\WTSAPI32.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\Odp\dwmapi.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\u70W8\UxTheme.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\NYpervHTp\MFC42u.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\iv505rrw\XmlLite.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\pkru2Wsoo\VERSION.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\pkru2Wsoo\VERSION.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\QpruqOk1\DUI70.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\rgsL2C4\WTSAPI32.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\NYpervHTp\mspaint.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\NYpervHTp\mspaint.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\NYpervHTp\mspaint.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Odp\GamePanel.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Odp\GamePanel.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Odp\GamePanel.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\QpruqOk1\wlrmdr.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\QpruqOk1\wlrmdr.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
41.2.GamePanel.exe.2470ec10000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
21.2.FileHistory.exe.7ffc74c20000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.2.rundll32.exe.7ffc670c0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
35.2.unregmp2.exe.7ffc74c20000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
37.2.omadmclient.exe.7ffc74c20000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.2.FileHistory.exe.216cde30000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
5.2.rundll32.exe.7ffc670c0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
41.2.GamePanel.exe.7ffc678e0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.2.rundll32.exe.1ff796f0000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
25.2.mspaint.exe.7ffc74c10000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.rundll32.exe.7ffc670c0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.loaddll64.exe.228311a0000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
2.2.rundll32.exe.1b4136b0000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
0.2.loaddll64.exe.7ffc670c0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
25.2.mspaint.exe.214ad6f0000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
35.2.unregmp2.exe.292a12f0000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
5.2.rundll32.exe.2a99d010000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
3.2.rundll32.exe.1a65a440000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
3.2.rundll32.exe.7ffc670c0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
37.2.omadmclient.exe.2684a170000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File

Domains

No Antivirus matches

URLs

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

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://mixer.com/api/v1/oauth/xbl/login	GamePanel.exe	false		high
http://https://profile.xboxlive.com/users/me/profile/settings?settings=GameDisplayPicRaw	GamePanel.exe	false		high
http://https://aka.ms/imrx2o	GamePanel.exe	false		high
http://https://mixer.com/_latest/assets/emoticons/%ls.png	GamePanel.exe	false		high
http://https://mixer.com/api/v1/users/current	GamePanel.exe	false		high
http://https://mixer.com/_latest/assets/emoticons/%ls.pngtitleIdaumIdkgIldprocessNamenametypeIdmultimedia	GamePanel.exe, 00000029.00000000.542785985.00007FF76CAB7000.00000002.00000001.01000000.00000013.sdmp, GamePanel.exe, 00000029.00000002.566549316.00007FF76CAB7000.00000002.00000001.01000000.00000013.sdmp	false		high
http://https://mixer.com/api/v1/broadcasts/current	GamePanel.exe, GamePanel.exe, 00000029.00000000.542785985.00007FF76CAB7000.00000002.00000001.01000000.00000013.sdmp, GamePanel.exe, 00000029.00000002.566549316.00007FF76CAB7000.00000002.00000001.01000000.00000013.sdmp	false		high
http://https://mixer.com/%wsWindows.System.Launcher	GamePanel.exe, 00000029.00000000.542785985.00007FF76CAB7000.00000002.00000001.01000000.00000013.sdmp, GamePanel.exe, 00000029.00000002.566549316.00007FF76CAB7000.00000002.00000001.01000000.00000013.sdmp	false		high
http://https://aka.ms/v5do45	GamePanel.exe	false		high
http://https://mixer.com/api/v1/types/lookup%ws	GamePanel.exe	false		high
http://https://MediaData.XboxLive.com/broadcasts/Augmenthttps://MediaData.XboxLive.com/screenshots/Augmenth	GamePanel.exe, 00000029.00000000.542785985.00007FF76CAB7000.00000002.00000001.01000000.00000013.sdmp, GamePanel.exe, 00000029.00000002.566549316.00007FF76CAB7000.00000002.00000001.01000000.00000013.sdmp	false		high
http://https://aka.ms/wk9ocd	GamePanel.exe, GamePanel.exe, 00000029.00000000.542785985.00007FF76CAB7000.00000002.00000001.01000000.00000013.sdmp, GamePanel.exe, 00000029.00000002.566549316.00007FF76CAB7000.00000002.00000001.01000000.00000013.sdmp	false		high
http://https://MediaData.XboxLive.com/broadcasts/Augment	GamePanel.exe	false		high
http://https://aka.ms/imfx4k	GamePanel.exe	false		high
http://https://www.xboxlive.comMBI_SSLhttps://profile.xboxlive.com/users/me/profile/settings?settings=GameD	GamePanel.exe, 00000029.00000000.542785985.00007FF76CAB7000.00000002.00000001.01000000.00000013.sdmp, GamePanel.exe, 00000029.00000002.566549316.00007FF76CAB7000.00000002.00000001.01000000.00000013.sdmp	false	• Avira URL Cloud: safe	low
http://https://MediaData.XboxLive.com/gameclips/Augment	GamePanel.exe	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.xboxlive.com	GamePanel.exe	false		high
http://https://mixer.com/api/v1/channels/%d	GamePanel.exe	false		high
http://https://mixer.com/api/v1/types/lookup%wshttps://mixer.com/api/v1/channels/%wshttps://mixer.com/api/v	GamePanel.exe, 00000029.00000000.542785985.00007FF76CAB7000.00000002.00000001.01000000.00000013.sdmp, GamePanel.exe, 00000029.00000002.566549316.00007FF76CAB7000.00000002.00000001.01000000.00000013.sdmp	false		high
http://https://mixer.com/api/v1/channels/%ws	GamePanel.exe	false		high
http://https://mixer.com/api/v1/chats/%.0fhttps://mixer.com/api/v1/users/currentBEAM_IMAGEGamesGuide::BeamC	GamePanel.exe, 00000029.00000000.542785985.00007FF76CAB7000.00000002.00000001.01000000.00000013.sdmp, GamePanel.exe, 00000029.00000002.566549316.00007FF76CAB7000.00000002.00000001.01000000.00000013.sdmp	false		high
http://https://MediaData.XboxLive.com/screenshots/Augment	GamePanel.exe	false		high
http://https://mixer.com/api/v1/chats/%.0f	GamePanel.exe	false		high
http://https://aka.ms/ifg0es	GamePanel.exe	false		high
http://https://mixer.com/%ws	GamePanel.exe	false		high
http://https://aka.ms/w5ryqnhttps://aka.ms/imfx4kQUITTING	GamePanel.exe, 00000029.00000000.542785985.00007FF76CAB7000.00000002.00000001.01000000.00000013.sdmp, GamePanel.exe, 00000029.00000002.566549316.00007FF76CAB7000.00000002.00000001.01000000.00000013.sdmp	false		high
http://https://aka.ms/w5ryqn	GamePanel.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	595303
Start date and time:	2022-03-23 14:40:41 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 17m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	AyBhhRZXPj (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@49/18@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 23.6% (good quality ratio 16.4%) • Quality average: 43.9% • Quality standard deviation: 37%
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, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing behavior and disassembly 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\Microsoft\CLR_v4.0\UsageLogs\FileHistory.exe.log

Process:	C:\Users\user\AppData\Local\u70W8\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\NYpervHTp\MFC42u.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1380352
Entropy (8bit):	5.14522678065983
Encrypted:	false
SSDEEP:	12288:3ZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuw8Ib:3ZK6F7n5eRmDFJivohZFV8W
MD5:	EF4106DB513D825B821B6BAE9E504D27
SHA1:	383AA64894D212196C899AF3F850C9B189E1EC60
SHA-256:	08AFB768749C8F06C7FB5CD2B0FA3DF90EBD19A30244E19840DC434B5C2435B6
SHA-512:	199F4A0F739DAE81B46CAF24D7ADD13CAAFBFEBA7A558C004220D2F6B669BF15732D415D323EDB08576E22A229CCBA8064AF83813C8F54BCA962E83DF2243E56
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.:...}^.....".....$.....@.....`.....l..$...<.....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\NYpervHTp\mspaint.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	6780928
Entropy (8bit):	6.184072371216434
Encrypted:	false
SSDEEP:	98304:ez2u7InCOgQwyRPM1mlawYL260GBGrGrGWAub7jPhivQ:ez6n/gQw4MllawYVb7jP8v
MD5:	99F86A0D360FD9A3FCAD6B1E7D92A90C
SHA1:	65F36247C0FFBB881947F68B352128C0C9CFCBE5
SHA-256:	D46519B76D09DFF8BC5C7B34A4E73AD8E7CF6E4C40BDAD6C769E34A099ECE017
SHA-512:	5071487AA218712FBA3A1FCEA6A810C3B27D26A145BC728315CA8078B6A88E51989038CAE4F5EE494B1FEE7515C6E86742D280D1A763B044BDBE7D2E360124A9
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;.....o.....W.....Rich.....PE..d.....S.....".....j...<^.....0.....@.....g....._h...`..... .....X.....p..`BY.....f.....g..*....,..T.....9..(... .....:.("......@.....text....i.....j..... ..`.rdata.....n.....@..@.data.....`...P...L.....@....pdata...f.....h.....@..@.didat..h....`.....@....rsrc...`BY..p...DY.....@..@.reloc...*....g..,...Lg.....@..B.....

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

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

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

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

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1355776
Entropy (8bit):	5.1221876396248325
Encrypted:	false
SSDEEP:	12288:zZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuw:zZK6F7n5eRmDFJivohZFV
MD5:	921B46AEA923BE300B1D6EF4E7C1CC5F
SHA1:	40CBBD90B7F456E05C533C1066DD2D8F5601FA90
SHA-256:	F7DCD2DCAF06B60C5DAEA5E89C60030F2571B662C2383FC876742E96F52B3C76
SHA-512:	22C21A6A7F802DBAB287513D47E8DBADFBAD215258D43D8A5F0B3292836B8EA58F1B0C94F3ACF3AACAEC6BEE87DCC68BCF269BE712B3A78C4F9099AFF9B0133D
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\QpruqOk1\DUI70.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1638400
Entropy (8bit):	5.548556004393981
Encrypted:	false
SSDEEP:	12288:6ZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuwujCTy+:6ZK6F7n5eRmDFJivohZFVujCG
MD5:	DB436F220DAA0C2AF20E59BCE6EEC8B5
SHA1:	26DB68E5B14525B216760A40C474477014543776
SHA-256:	4D70CB2101B735E522F8EB0B3DF0E11D1DCCBF3828AEA07B94D19ACFE9EC3AA6
SHA-512:	7F86D71ED7833493A82845BDE6C53CA0CD19F474891D8397FFC0AF7E3750402DBCFB66B2BA6B2D208D9518597439DB21C40C39EA8C52070667F9FC9756CE0F9
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.:...}^....." ....$.....@.....`.....dQ..$...<.....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\QpruqOk1\wlrmdr.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	65704

Entropy (8bit):	5.834154867756865
Encrypted:	false
SSDEEP:	1536:B14+6gGQ7ubZiQ+KytHlyObsvqr9PxDt8PcPs:QgGIu1iFtHJLu9ZDt8kU
MD5:	4849E997AF1274DD145672A2F9BC0827
SHA1:	D24E9C6079A20D1AED8C1C409C3FC8E1C63628F3
SHA-256:	B43FC043A61BDBCF290929666A62959C8AD2C8C121C7A3F36436D61BBD011C9D
SHA-512:	FB9227F0B758496DE1F1D7CEB3B7A5E847C6846ADD360754CFB900358A71422994C4904333AD51852DC169113ACE4FF3349520C816E7EE796E0FBE6106255AEF
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....$.....j.s... ... ... .s\ ... .o.!... .o.!... .o.!... .o.!... ... t.. .o.!... .o0 ... .o.!... Rich ... .PE..d....2....."....4.....:.....@.....@.....b.....P.....xg.....$...0.....y..T.....f..... .....g..x.....text....3.....4..... ..`.imrsiv.....P.....rdata..J2...`...4...8.....@..@.data...h.....l.....@....pdata.....n..... ..@..@.rsrc...xg.....h...r.....@..@.reloc.....0.....@..B..... .....

C:\Users\user\AppData\Local\iv505rrw\XmlLite.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1355776
Entropy (8bit):	5.1147607814329605
Encrypted:	false
SSDEEP:	12288:hZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuw:hZK6F7n5eRmDFJivohZFV
MD5:	44295A0E00ADDDD50261D8F890897B4D
SHA1:	856508331E1867C99519588A25DE434090D05FA5
SHA-256:	973CDBB17CDCE9C019AAE83347912CCE7955D1D8DB1B8DC80082B15EDC28206B
SHA-512:	B8A99ADEF9BFA3BB5D3D7BFEC9489405EF5D3381E4B7723CABB84113C6E073F2D96371ACE74988F7953FBF722121E0F78B89A9621D89A9C5D82BE2051CF5A3E
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\iv505rrw\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
Antivirus:	
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\pkru2Wsoo\PresentationHost.exe

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

Category:	dropped
Size (bytes):	259072
Entropy (8bit):	6.5074250085194665
Encrypted:	false
SSDEEP:	6144:8kfs4/kfxzJTbHfyH5KNXwy3Odjp19k5KNXf:fs4ixzJTbHmKVwy3OdLaKV
MD5:	E3053C73EA240F4C2F7971B3905A91CF
SHA1:	1848AD66BD55E5484616FB85E80BA58BE1D5BA4B
SHA-256:	0BACCDB2B5ACB7B3C2E9085655457532964CAFFF1AE250016CE1A80E839B820C
SHA-512:	167BCC3E2552286F7D985A65674DA2FF0D0AA6A7F0C4C3B43193943B606E0133C06EEB33656EFBB8B827AC9221FB1BA00A49ADCC2489BD4F38DF62A015806D 3
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3/.]|.]|.]|...|.]|...|..]|..^}.]|..Y}.]|.\|..]|..\}.]|..T}..]|..X}.]|..|.]|..._}.]|Rich.]|. .....PE..d..../.....".....&.....@.....0.....`..... .....p.,.....j.....l..... ..,....d..T.....#..... .....$.....text...o..... ..`.rdata.....@..@.data.....r.....@....pdata..l.....t.....@..@.rsrc....j.....l...~..... ...@..@.reloc.,.... .....@..B..... .....

C:\Users\user\AppData\Local\pkru2Wsoo\VERSION.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1355776
Entropy (8bit):	5.115920691070016
Encrypted:	false
SSDEEP:	12288:vZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuw:vZK6F7n5eRmDFJivohZFV
MD5:	4F53DEE2F65AEDCF002B0D96E136EA3E
SHA1:	E6B72A1016718C24DF891B7A7A4A2B389E2E8F32
SHA-256:	68E5BFBFFA535A346A0203DB796A87168AB0D81619AC2E0B688E1120B6E71253
SHA-512:	401FAE3B8A52F7ED45078DB29E0D33B31878F7D78F8C9C23DD898121118A4BAD13A23313249648BC2A5ED468813CA1843610B9640C982E40832D34FBA9AC77A
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\rgsL2C4\BdeUISrv.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	52736
Entropy (8bit):	5.7946530792580475
Encrypted:	false
SSDEEP:	768:NS51B2sZMD1mYu/Lr7p0dHkf9abpWnGjTopPjZdWC2bNrHuOKAh/4J99j4ktPUww:J/Yn/Lr7qwYb7/oRjeJh2991t8Yte
MD5:	25D86BC656025F38D6E626B606F1D39D
SHA1:	673F32CCA79DC890ADA1E5A2CF6ECA3EF863629D
SHA-256:	202BEC0F63167ED57FCB55DB48C9830A5323D72C662D9A58B691D16CE4DB8C1E
SHA-512:	D4B4BC411B122499E611E1F9A45FD40EC2ABA23354F261D4668BF0578D30AEC5419568489261FC773ABBB350CC77C1E00F8E7C0B135A1FD4A9B6500825FA6E0 6
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3..hw.;w.;w.;~.";u.;...:t.;...`.;...:q.;...:d.;w.;.;...:.;..N;v.;...:v.;Richw.; .....PE..d...X....."....v...\.....0y.....@..... .....Db....`..... .....p.....x.....T..... .....text...At.....v..... ..`.rdata...3.....4...z.....@..@.data.....@....pdata.....@..@.rsrc.....@..@. reloc..x.....@..B..... .....

C:\Users\user\AppData\Local\rgsL2C4\WTSAPI32.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1355776
Entropy (8bit):	5.124725524561735
Encrypted:	false
SSDEEP:	12288:CZgJtlQepQn+NDo7nlYegQCLDF/B9wvj/cLvVZFuw:CZK6F7n5eRmDFJivohZFV
MD5:	50047C3C2FDDB29A6170BF9FB64D658F
SHA1:	E7FD6768FA2840B0AE0665705B1D17845E11D949
SHA-256:	B90283A2A83F8711C82411C783A2194C3F2A5C197021E3D3F8B7D1CCB185C763
SHA-512:	0AAE4C226EE7B4710993E52C36D042FB255B13D554A1068D008596E713F02E8EAB9631742322697F799CFF5C2854754C749DD96BE1590F3253E15C001E082722
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\u70W8\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+otIxAGQW7A70TshCbdmyTVulAyXRON:5WZmxPZUxzYuVD8ortIxAGJKSuCbd
MD5:	989B5BDB2BEAC9F894BBC236F1B67967
SHA1:	7B964642FEE2D6508E66C615AA6CF7FD95D6196E
SHA-256:	FF1DE8A606FDB6A932E7A3E5EE5317A6483F08712DE93603C92C058E05A89C0C
SHA-512:	0360C9FE88743056FD25AC17F12087DAD026B033E590A93F394B00EB486A2F5E2331EDCCA9605AA7573D892FBA41557C9E0EE4FAC69FCA687D6B6F144E5E5249
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....m.s..k ..k .hh!..k .^. ..k .ho!..k .hb!..k .hj!..k ..j #.k .hn!..k .h. ..k .h i!..k Rich..k .....PE..d.....".....t...X.....{.....@..... .....\.....`..... .....0..... ..8.....$... ...T..... .....H.....text...{m.....n..... ..`.nep.....r..... ..`.rdata...i.....j...x.....@..@.data... .....@....pdata..8.... ....@..@.rsrc.....0.....@..@.reloc..$.....@..B..... .....

C:\Users\user\AppData\Local\u70W8\UxTheme.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1355776
Entropy (8bit):	5.12781164219402
Encrypted:	false
SSDEEP:	12288:mZgJtlQepQn+NDo7nlYegQCLDF/B9wvj/cLvVZFuw:mZK6F7n5eRmDFJivohZFV
MD5:	76A91627D3EEA2BEF8EE5C34AACAE4CA
SHA1:	6588DF88F6E323D1A50D7072FD06FD988CF46813
SHA-256:	B39F61630D4E6D5480F9753656363D95BB70B013C9AD6744A04B0625EB7B406A
SHA-512:	9AA9E3F80148D341C6ED163F6B50692E8C06685492EF8F5E24796E15E139E0102F7BF0C190E6C6D02496E7896210FED17EF64068F2B8F04513D83E3633ABC2B8
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\vVin\VERSION.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1355776
Entropy (8bit):	5.115947255580537
Encrypted:	false
SSDEEP:	12288:pZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuw:pZK6F7n5eRmDFJivohZFV
MD5:	8E1EDE32BC38B1366D17603AD093B828
SHA1:	558B6C1219EF5E58A0386A13DF8C451BD0135BB3
SHA-256:	B0093BAA1CE69EF63A7CF2A8C59D6EF94FBDEE8C05AF26B04D6BB029205E2AF2
SHA-512:	0E4F519D25B16643540E0CB8053AAFB97EC938E93879B51AF92C7031D13E92A28AC2695D6AAB39E0C4468465B0FC885190E0F2A812C6BAED12E186C1EDABD0 D
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\vVin\unregmp2.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	254976
Entropy (8bit):	5.093220071075157
Encrypted:	false
SSDEEP:	3072:1t+/6BNqqNRhdutq4jCoNhdxtYEbvyIwYKO8/+9vAwk4OdamabJ9:3Bhhd+7QKb
MD5:	9B517303C58CA8A450B97B0D71594CBB
SHA1:	BE75E3F10E17400DA7C0FAF70BF16EE7D0AA93A8
SHA-256:	2A38BFC3813D7E845F455B31DF099C8A6E657EF4556BFF681315F86A883A3314
SHA-512:	6A47EC7800E1F1FCDBB44A018147CE4A87FF0F5B94597B182AAE4E8545D9B18FAAAA07379BA1086D8F7785F0F66C36E4B6C68FCF49130333B8A9DC3A9E9E08 E8
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....|.R.....y.....y.....y.....y.....w....y.....yf.....y.....Rich..... .....PE..d....Q&.....".....^.....@.....0.....A....`..... .....0.....T.....V..(....U.....V..... .....text...w..... ..`.rdata..4.....@..@.data....8.....&.....@....pdata..0.....@..@.rsrc.....@..@.relo c.....@..B..... .....

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\414045e2d09286d5db2581e0d955d358_d06ed635-68f6-4e9a-955c-4899f5f57b9a

Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	1450
Entropy (8bit):	7.361727904797889
Encrypted:	false
SSDEEP:	24:UKUUXqUcSodCyBlrAEKWs6/hAnL4XdQc2aBtHX:U7U6Uc625AnL4XdQcht3
MD5:	5F02ECE7D1EB5FADDDFDEBE2D3475E9A
SHA1:	4D62C892CCC31C9079E2F22D909AF2CB3AAD74C1
SHA-256:	B1C472B75EF62235374FF8CF1B83E53D52971FA9A755F7C60C9BBA2951133A3F
SHA-512:	1ED4B6120EE533D907084AE9999A257517EAFC30A8CE25F6E88EACB556D907A91B03FF5B2DC4F90F5F2A448913C25F80D100314EB1519F8EED9ECB21707E436 0
Malicious:	false
Reputation:	unknown
Preview:	.....user.....RSA1.....8.".Mc.j....3.....}...7.<..M..D9..Z..#x.>JFs.`.vJ..y9+.$...n(ck.G!IS.@.@k..}..Mb...^X.t..6.....L.E.q]/A..Z....<.W..... .....z..O.....w...L.aI....?E.....,...C.r.y.p.t.o.A.P.I. .P.r.i.v.a.t.e. .K.e.y....f..... ....A .U...c..e...2.>B....PE..#..... ...).GX.v.Y.X.8..@..EK.6.[h8.q.j\.).....#....d*i.Q..."n.!6'oj.. g..R.[..RS....&.G..H^(O..WP.....(...i0.1.=T.....8L.L]...o.*U.DA.....a.t..R..U*.Ob...@....8..V&1...6. ...2V.G.....4#=:NnN..;.H..Gz...F....@...w....I^V0q.r.%<.k#.1c..H.BR.....o.*E .L....<..X...S5.....RZv,q#=6..>.W.:.a.f.6\..6.....Dj&!B=..i..Hi.6.9~.Y6O...P.2.C..g.>.J....Z..o...,.vO$@..Y.GY..zd.Yuy..1...z..1U2..c.={...P&.VW..BL..x..m...^H.....".5.L.Y.. .D..]...\.}.Jhg..K...n.4%.t....w..g2..#2.4gI.2.Y.y.<l.8.... .?.C]...[...U..t..~7.....K..+.a.c.@.^_^;....I.w.d/9..Fi..9...+,.Blc.+..`..0HU.f.}.....?..8k1Y\{6l.I.#.1..f.`.?8A....r.x.m.o.

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	5.128940497635626
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:	AyBhhRZXPj.dll
File size:	1351680
MD5:	518cc4a9888e76bc1a916fd67a08a075
SHA1:	148d6f12f12a0cae195f36f4319839f6687b7144
SHA256:	57b0d95f62fc7999dd21b6a0aef4087ad855ccb2d28b99463ee6c88ddf037009
SHA512:	b14a3bcbfa68e5cf71ccfdd68ff5da696ca1e44073dbf6cd4d15dfab2a9ff29f56855c828ae7ac0dc346dfab93679f7d1ae52cb24ccc2976e6d4ba1fb5f6221e
SSDEEP:	12288:aZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuw:aZK6F7n5eRmDFJivohZFV
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

Instruction
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 00007F93DCE90D1Dh
dec eax
mov dword ptr [0007060Fh], esp
dec eax
mov dword ptr [00070600h], ebp
dec eax
mov dword ptr [00070649h], ebx
dec eax
mov dword ptr [0007063Ah], edi
dec eax
test eax, eax
je 00007F93DCE90CFCh
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]

Instruction
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	0x149010	0x2ca	.vje
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa9924	0x3c	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbf000	0x3d8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x1000	0x0	.text
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xc0000	0xefc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x43000	0x28	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.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
.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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.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
.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
.qqb	0x148000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vje	0x149000	0x2da	0x1000	False	0.119873046875	data	1.44574959876	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

DLL	Import
KERNEL32.dll	LoadLibraryA, HeapUnlock

Exports

Name	Ordinal	Address
ApplyCompatResolutionQuirking	1	0x14000c1b4
CompatString	2	0x140012180
CompatValue	3	0x140011544
CreateDXGIFactory	11	0x14002123c
CreateDXGIFactory1	12	0x14001b1e4
CreateDXGIFactory2	13	0x140023a64
DXGID3D10CreateDevice	14	0x14003a46c
DXGID3D10CreateLayeredDevice	15	0x14003ad28
DXGID3D10ETWRundown	16	0x140037ae0
DXGID3D10GetLayeredDeviceSize	17	0x140038fac
DXGID3D10RegisterLayers	18	0x140007b90
DXGIDeclareAdapterRemovalSupport	19	0x140022980
DXGIDumpJournal	4	0x1400072e4
DXGIGetDebugInterface1	20	0x1400323d0
DXGIReportAdapterConfiguration	21	0x140023758
DXGIRevertToSxS	5	0x1400170f8
PIXBeginCapture	6	0x14001cd84
PIXEndCapture	7	0x140003058
PIXGetCaptureState	8	0x140022ba4
SetAppCompatStringPointer	9	0x140019d84
UpdateHMDEmulationStatus	10	0x14003fb08

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

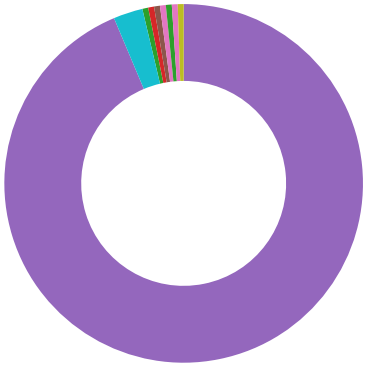
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Statistics

Behavior



- loaddll64.exe
- cmd.exe
- rundll32.exe
- rundll32.exe
- explorer.exe
- rundll32.exe
- rundll32.exe
- Magnify.exe
- FileHistory.exe
- FileHistory.exe
- RdpSa.exe
- mspaint.exe
- mspaint.exe
- mmc.exe
- EaseOfAccessDialog.exe
- unregmp2.exe
- unregmp2.exe
- omadmclient.exe
- omadmclient.exe
- SystemPropertiesPerformance.exe
- eudcedit.exe
- GamePanel.exe
- GamePanel.exe

Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: 6608, Parent PID: 1032

General

Target ID:	0
Start time:	15:41:44
Start date:	23/03/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\AyBhhRZXPj.dll"
Imagebase:	0x7ff7ac2b0000
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: 00000000.00000002.274237724.00007FFC670C1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6620, Parent PID: 6608

General

Target ID:	1
Start time:	15:41:45
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\AyBhhRZXPj.dll",#1

Imagebase:	0x7ff6f9620000
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: **6632**, Parent PID: **6608**

General

Target ID:	2
Start time:	15:41:45
Start date:	23/03/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\AyBhhRZXPj.dll,ApplyCompatResolutionQuirking
Imagebase:	0x7ff7d29d0000
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: 00000002.00000002.363013775.00007FFC670C1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\AyBhhRZXPj.dll	unknown	1351680	success or wait	1	7FFC6711F8D6	ReadFile

Analysis Process: rundll32.exe PID: **6640**, Parent PID: **6620**

General

Target ID:	3
Start time:	15:41:45
Start date:	23/03/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\AyBhhRZXPj.dll",#1
Imagebase:	0x7ff7d29d0000
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: 00000003.00000002.254650738.00007FFC670C1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\AyBhhRZXPj.dll	unknown	1351680	success or wait	1	7FFC6711F8D6	ReadFile

Analysis Process: explorer.exe PID: **3968**, Parent PID: **6632**

General

Target ID:	4
Start time:	15:41:48
Start date:	23/03/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6b8cf0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\AddIns\zs3	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\u70W8\	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\u70W8\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\u70W8\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\NYpervHTp\	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\NYpervHTp\MFC42u.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\NYpervHTp\mspaint.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\vVin\	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\vVin\VERSION.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\vVin\unregmp2.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\iv505rrw\	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\iv505rrw\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\iv505rrw\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\Odp\	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\Odp\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\Odp\GamePanel.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\pkru2Wsoo\	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\pkru2Wsoo\VERSION.dll	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\pkru2Wsoo\PresentationHost.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\rgsL2C4\	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\rgsL2C4\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\rgsL2C4\BdeUISrv.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\QpruqOk1\	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\QpruqOk1\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\QpruqOk1\wlrmdr.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\u70W8\FileHistory.exe	success or wait	1	14005FB70	DeleteFileW

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\u70W8\UxTheme.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\NYpervHTp\MFC42u.dll	cannot delete	28	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\NYpervHTp\mspaint.exe	cannot delete	28	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\NYpervHTp\MFC42u.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\NYpervHTp\mspaint.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\vVin\unregmp2.exe	cannot delete	23	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\vVin\VERSION.dll	cannot delete	24	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\vVin\unregmp2.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\vVin\VERSION.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\iv505rrw\omadmclient.exe	cannot delete	8	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\iv505rrw\XmlLite.dll	cannot delete	8	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\iv505rrw\omadmclient.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\iv505rrw\XmlLite.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\Odp\dwmapi.dll	cannot delete	9	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\Odp\GamePanel.exe	cannot delete	9	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\Odp\dwmapi.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\Odp\GamePanel.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\pkru2Wsoo\PresentationHost.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\pkru2Wsoo\VERSION.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\rgsL2C4\BdeUISrv.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\rgsL2C4\WTSAPI32.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\u70W8\UxTheme.dll	0	1355776	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\u70W8\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\NYpervHTp\MFC42u.dll	0	1380352	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 58 10 0c 5a 1c 71 62 09 1c 71 62 09 1c 71 62 09 61 08 fd 09 6a 71 62 09 73 07 fd 09 18 71 62 09 39 06 fd 09 5c 71 62 09 73 07 fd 09 28 71 62 09 fd 15 fd 09 0b 71 62 09 11 23 fd 09 20 71 62 09 fd 2f 62 08 07 71 62 09 15 09 fd 09 09 71 62 09 07 fd fd 09 48 71 62 09 fd 28 63 08 2f 71 62 09 72 2c 66 08 0b 71 62 09 fd 28 63 08 10 71 62 09 3b fd fd 09 2c 71 62 09 fd 2f fd 09 54 71 62 09 fd fd fd 09 5a 71 62 09 fd fd fd 09 1e 71 62 09 7a fd fd 09 42 71 62 09 fd fd fd 09 6e 71 62 09 fd 15 fd 09 5b 71 62 09 9d fd 09 1b 71 62 09 3b fd 0c 09 7b 71 62 09 1f 09 fd 09 7f 71 62	MZ@XZqbqbqbajqbsqb9\qbs(qbqb#qb/bqbqbHqb(c/qbr,fqb(cqb;,qb/TqbZqbqbzBqbnqb[qbqb;{qbqb	success or wait	1	14005F160	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\NYpervHTp\mspaint.exe	0	6780928	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 8a fd fd fd 4d fd fd 4d fd fd 44 fd 3b 7d fd fd fd fd 0e fd fd fd fd fd 16 fd fd fd fd fd 3d fd fd fd fd fd 10 fd fd 4d fd fd fd 6f fd fd fd fd fd fd 09 fd fd fd fd fd 57 4c fd fd fd fd fd 0c fd fd fd 52 69 63 68 fd fd fd fd 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 07 00 fd fd 53 fd 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$;oWRichPEdS"	success or wait	1	14005F160	WriteFile
C:\Users\user\AppData\Local\vVin\VERSION.dll	0	1355776	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\vVin\unregmp2.exe	0	254976	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 7c fd 52 fd 1d fd 01 fd 1d fd 01 fd 1d fd 01 fd 79 fd 00 fd 1d fd 01 fd 79 fd 00 fd 1d fd 01 fd 79 fd 00 fd 1d fd 01 fd 79 fd 00 fd 1d fd 01 fd 1d fd 01 77 1d fd 01 fd 79 fd 00 fd 1d fd 01 fd 79 66 01 fd 1d fd 01 fd 79 fd 00 fd 1d fd 01 52 69 63 68 fd 1d fd 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06 00 16 51 26 fd 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$|RyyyywyyfyRichPEdQ&"	success or wait	1	14005F160	WriteFile
C:\Users\user\AppData\Local\iv505rrw\XmlLite.dll	0	1355776	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\iv505rrw\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 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\Odp\dwmapi.dll	0	1355776	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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\Odp\GamePanel.exe	0	1292288	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 54 01 75 72 10 60 1b 21 10 60 1b 21 10 60 1b 21 19 18 fd 21 50 60 1b 21 7f 04 1f 20 00 60 1b 21 7f 04 18 20 13 60 1b 21 7f 04 1e 20 34 60 1b 21 7f 04 1a 20 39 60 1b 21 10 60 1a 21 64 65 1b 21 7f 04 12 20 fd 60 1b 21 7f 04 fd 21 12 60 1b 21 7f 04 fd 21 11 60 1b 21 7f 04 19 20 11 60 1b 21 52 69 63 68 10 60 1b 21 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 08 00 fd 8e 1b 00 00 00	MZ@!L!This program cannot be run in DOS mode.$Tur`!`!`!!P`! `! `! 4`! 9`!`!de! `!!`!!`! `! Rich`!PEd	success or wait	1	14005F160	WriteFile
C:\Users\user\AppData\Local\pkru2Wsoo\VERSION.dll	0	1355776	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

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\pkru2Wsoo\PresentationHost.exe</td><td>0</td><td>259072</td><td>4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 33 2f fd 5d 7c fd 5d 7c fd 5d 7c fd fd fd 7c fd 5d 7c fd fd fd 7c fd fd 5d 7c fd fd 5e 7d fd 5d 7c fd fd 59 7d fd 5d 7c fd 5c 7c 07 fd 5d 7c fd fd 5c 7d fd 5d 7c fd fd 54 7d fd fd 5d 7c fd fd 58 7d fd 5d 7c fd a2 7c fd 5d 7c fd fd 5f 7d fd 5d 7c 52 69 63 68 fd 5d 7c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td><td>MZ@!L!This program cannot be run in DOS mode.$3/]|]|]|||]|||]| ^}]|Y}]|\|]|\}]|T}]|X}]|||]|_}] |Rich]|</td><td>success or wait</td><td>1</td><td>14005F160</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\rgsL2C4\WTSAPI32.dll</td><td>0</td><td>1355776</td><td>4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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</td><td>MZ@XZqbqbqbajqbsqb9\ qbs(qbqb# qb/bqbqbHqb(c/qbr,fqb(c qb;,qb/ TqbZqbqbzBqbnqb[qbqb; {qbqb</td><td>success or wait</td><td>1</td><td>14005F160</td><td>WriteFile</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\rgsL2C4\BdeUISrv.exe	0	52736	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 33 fd fd 68 77 b1 3b 77 b1 3b 77 b1 3b 7e fd 22 3b 75 b1 3b 18 fd fd 3a 74 b1 3b 18 fd fd 3a 60 b1 3b 18 fd fd 3a 71 b1 3b 18 fd fd 3a 64 b1 3b 77 b0 3b fd b1 3b 18 fd fd 3a 7f b1 3b 18 fd 4e 3b 76 b1 3b 18 fd fd 3a 76 b1 3b 52 69 63 68 77 b1 3b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06 00 58 04 17 1f 00 00 00	MZ@!L!This program cannot be run in DOS mode.$3hw;w;w;~";u;:t;:`;:q;:d;w;;:;N;v;:v;Richw;PEdX	success or wait	1	14005F160	WriteFile
C:\Users\user\AppData\Local\QpruqOk1\DUI70.dll	0	1638400	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\QpruqOk1\wlrmdr.exe	0	65704	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 6a fd 73 fd 0b fd 20 fd 0b fd 20 fd 0b fd 20 fd 73 5c 20 fd 0b fd 20 fd 6f fd 21 fd 0b fd 20 fd 6f fd 21 fd 0b fd 20 fd 6f fd 21 fd 0b fd 20 fd 6f fd 21 fd 0b fd 20 fd 0b fd 20 74 0b fd 20 fd 6f fd 21 fd 0b fd 20 fd 6f 30 20 fd 0b fd 20 fd 6f fd 21 fd 0b fd 20 52 69 63 68 fd 0b fd 20 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 07 00 fd 32 fd fd 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$js s\ o! o! o! o! t o! o0 o! Rich PEd2"	success or wait	1	14005F160	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\Magnify.exe	unknown	809472	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\conhost.exe	unknown	625664	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\stordiag.exe	unknown	77312	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\cofire.exe	unknown	23552	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\RuntimeBroker.exe	unknown	99272	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\rwinsta.exe	unknown	22528	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\TieringEngineService.exe	unknown	303616	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\runonce.exe	unknown	57856	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\RdpSa.exe	unknown	43008	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\certreq.exe	unknown	517120	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\manage-bde.exe	unknown	215552	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\mspaint.exe	unknown	6780928	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\mfc42u.dll	unknown	1454592	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\desktopimgdownldr.exe	unknown	74752	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\mmc.exe	unknown	1859584	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\bcdedit.exe	unknown	461824	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\WpcMon.exe	unknown	1155016	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\msfeedssync.exe	unknown	15360	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\doskey.exe	unknown	18944	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\EaseOfAccessDialog.exe	unknown	304640	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\tsdiscon.exe	unknown	23552	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\ROUTE.EXE	unknown	23552	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\appidcertstorecheck.exe	unknown	19456	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\help.exe	unknown	11776	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\fsutil.exe	unknown	177664	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\LegacyNetUXHost.exe	unknown	200192	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\nbtstat.exe	unknown	20992	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\poqexec.exe	unknown	141312	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\dllhst3g.exe	unknown	12288	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\AppVClient.exe	unknown	826776	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\PkgMgr.exe	unknown	207872	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\hvix64.exe	unknown	1174432	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\ofdeploy.exe	unknown	84992	success or wait	1	14005F8D6	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\MultiDigiMon.exe	unknown	53760	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\iscsicpl.exe	unknown	122368	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\unregmp2.exe	unknown	254976	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\version.dll	unknown	30568	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\SgrmBroker.exe	unknown	163336	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\ApproveChildRequest.exe	unknown	231424	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\PING.EXE	unknown	21504	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\lsass.exe	unknown	57976	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\omadmclient.exe	unknown	315904	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\xmllite.dll	unknown	227840	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\SystemPropertiesPerformance.exe	unknown	83968	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\fc.exe	unknown	24576	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\winlogon.exe	unknown	677376	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\driverquery.exe	unknown	81920	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\RemotePosWorker.exe	unknown	12800	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\smartscreen.exe	unknown	2548224	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\timeout.exe	unknown	30720	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\eudcedit.exe	unknown	353280	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\GamePanel.exe	unknown	1292288	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\dwmapi.dll	unknown	146840	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\WSCollect.exe	unknown	93696	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\repair-bde.exe	unknown	126976	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\NETSTAT.EXE	unknown	37888	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\ARP.EXE	unknown	25600	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\appidpolicyconverter.exe	unknown	160256	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\logoff.exe	unknown	22528	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\appidtel.exe	unknown	25088	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\PresentationHost.exe	unknown	259072	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\RelPost.exe	unknown	156160	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\wininit.exe	unknown	366792	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\fsquirt.exe	unknown	141824	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\UevAppMonitor.exe	unknown	55808	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\Windows.Media.BackgroundPlayback.exe	unknown	13312	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\gpresult.exe	unknown	223744	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\Locator.exe	unknown	10752	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\TokenBrokerCookies.exe	unknown	35840	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\BdeUISrv.exe	unknown	52736	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\wtsapi32.dll	unknown	64168	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\wlrmdr.exe	unknown	65704	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\dui70.dll	unknown	1719808	success or wait	1	14005F8D6	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{802DDF06-6025-3BD2-F896-3C205FCD1EC7}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{802DDF06-6025-3BD2-F896-3C205FCD1EC7}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{D9582133-FF48-7013-149D-ED87E8282F8A}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{D9582133-FF48-7013-149D-ED87E8282F8A}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{D98DC529-4B78-7307-BE65-230891702D0A}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{D98DC529-4B78-7307-BE65-230891702D0A}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{46907487-CFCD-DBA6-B28C-3810265CED21}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{46907487-CFCD-DBA6-B28C-3810265CED21}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{C287B9D2-E94D-FB6C-92E8-3B0EF539530C}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{C287B9D2-E94D-FB6C-92E8-3B0EF539530C}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{4A22E64C-2598-A755-401C-068E732D1CBE}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{4A22E64C-2598-A755-401C-068E732D1CBE}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{5733E236-6D8A-F105-4A7D-AB5AE249E022}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{5733E236-6D8A-F105-4A7D-AB5AE249E022}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{E16DF49E-43EE-031D-4526-EDED08B1E1E5}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{E16DF49E-43EE-031D-4526-EDED08B1E1E5}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{47AC49B4-2121-44C1-EAE3-4A5A38373266}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{47AC49B4-2121-44C1-EAE3-4A5A38373266}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{D3191B1C-5B17-33BE-0F45-E3DBA88DC04A}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{D3191B1C-5B17-33BE-0F45-E3DBA88DC04A}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{9FD17AD2-4476-6EFA-85DD-64A219A9B327}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{9FD17AD2-4476-6EFA-85DD-64A219A9B327}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{CD820C45-4324-D67B-1CA3-F89E36260981}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{CD820C45-4324-D67B-1CA3-F89E36260981}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{3203410A-B623-A7FA-B445-C009DC160025}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{3203410A-B623-A7FA-B445-C009DC160025}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{E0F17046-48DB-539D-AE87-1BEA72B227D4}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{E0F17046-48DB-539D-AE87-1BEA72B227D4}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{F3ADE953-82CC-999D-BFE2-2D5B69DDB55A}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{F3ADE953-82CC-999D-BFE2-2D5B69DDB55A}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{30F5808E-1B7D-D18A-C378-38317669F19A}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{30F5808E-1B7D-D18A-C378-38317669F19A}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{008F97C0-B9F0-C866-C03D-73F7A8209342}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{008F97C0-B9F0-C866-C03D-73F7A8209342}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{68EC2E73-13CA-FB9E-0AFA-7AF858648477}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{68EC2E73-13CA-FB9E-0AFA-7AF858648477}\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\{9FD17AD2-4476-6EFA-85DD-64A219A9B327}\ShellFolder	{273654A8-119A-17FA-2CC1-E06223FC8158}	binary	EA 11 C6 3C 5B 7A 0F D5 B6 B2 1A DC B0 25 3A 31 57 DA 4F 7D 63 D7 05 FE BD 4C 35 4F 47 C8 B2 C5 A0 A0 0C FD E8 B7 7F D4 ED 7D FB 35 DD 5D 59 E7 23 C0 2B B1 57 1B 48 D1 AC 2F 46 83 25 EC 7C 88 F7 FA E9 DB FA CA 95	success or wait	1	140062470	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{47AC49B4-2121-44C1-EAE3-4A5A38373266}\ShellFolder	{E92D68C9-22FD-E16A-BA37-C29721A58877}	binary	CA F5 8A F1 34 4A A4 23 2D 68 BD CD A6 A7 B1 4B 2C F9 78 8C FC 3C F6 5E BF AB 84 84 84 53 0B 35 93 37 E4 BA 51 8A 57 F3 B9 45 D9 A0 7C AE EB 3E 7C 5B FA 98 B3 44 FF 67 02 C5 B7 ED 7B 52 73 5A 5B 46 4D 59 9C 39 11 73 35 25 75 9D 66 23 F3 F1 20 5B F0 BA 40 2D 8C 4A C0 3A C9 60	success or wait	1	140062470	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{9FD17AD2-4476-6EFA-85DD-64A219A9B327}\ShellFolder	{8DCB5582-68AF-CC6F-DEBB-E4825D47012C}	binary	F6 EC 35 CD F2 93 CE A3 A1 5A CC B4 A0 80 4E A0 DA 8E 58 1C 38 F3 44 09 0F 28 FF FC 36 85 D7 A3 E1 48 2F C2 AF 69 AB D9 92 A2 8E 83 AF 89 19 A3 AA 93 6D A5 C5 49 99 70 20 94 7E 8C FE 03 E2 E2 E8 71 AA 31 D0 4F FC B3 AE C0 83 BD E3 B2 BC 19 9D 90 32 07 8F CB F4 B9 D4 24 E8 68 CF AB B0 E7 56 0B D0 21 43 39 8C C3 DC A3 F7 F0 9C 63 CF 80 0E BB 11 9B D4 36 E9 CD 8A 7C 6E A7 3F 64 55 F4 37 F6 48 94 09 1C 46 43 E4 9A 62 77 AA 4A 2D 87 87 99 6C 02 A3 67 61 82 7E 58 1E AD 02 02 F9 98 7C E8 F4 FA D1 B5 41 EE F5 F2 AC 08 30 2C A8 6C 74 BB 9A 13 3C 38 D1 EC 3C 11 34 7C E8 C8 B5 BC 95 11 9D 38 DE 0E 76 4D 3B E7 8E C0 BA 06 71 CE 83 E1 87 22 F9 10 40 72 10 BD 6C C4 6A 83 13 DE 12 B2 D3 9E 3B E2 6B 48 98 D7 02 1D 9D 4E F3 0D 78 2D CD 53 BB 21 2E 4D 1B 14 7E 92 98 34 62 F7 2A CF 77 0F 7A 08 64 8E 58 BA B1 F3 D6 B9 51 EE 3A E1 C8 55 9D 06 DE 31 AC 3A F8 BB EB 22 F2 34 21 CE 08 AB C4 73 2B 30 83 90 68 1D 25 0F F9 D0 EF 48 F2 B9 DD 44 02 9B 23 A3 66 FA 16 E4 40 51 3C 7C 9C B5 DA 2A 76 05 C9 21 70 DA 3D 21 16 DC 5C 11 1B E6 07 4B 67 B5 69 B6 38 AB 5E A7 9D E3 07 8D D8 3E D6 7F BA 9B CD E2 49 38 2D 84 B8 F2 DC 86 2B 9F C7 F6 C2 7F 94 41 75 32 A9 66 48 D3 ED 36 7D 34 2A CF 00 FB E5 8A 82 F8 29 CE 7B C3 A1 8A 8B 62 78 9D DB 61 E6 22 68 D4 FA 46 AF DA 3F 85 BC AA 2E 31 4F 71 2E F1 28 27 E7 81 9E 21 9F 5D 42 0E 9E E9 DB 0D 91 3F 2D DC 90 9E 9F 7D 94 7B 28 68 6D 33 48 4A 6A E2 48 08 E8 66 11 CE 43 0C 7E 89 EB DF 56 57 1D FC BB 68 D5 24 C4 BD 73 7D 99 8E 47 6A A6 95 3B 7F 8F FB 81 61 5E 18 08 A3 7B 78 53 86 3F 44 8B 41 33 D2 32 DE E7 20 F8 BD B6 BD 0D C5 55 19 0F 35 F9 A9 D0 14 2F 71 AA 00 F7 A9 22 7D 74 37 39 40 6A F7 C6 24 3B BA 3A B0 D3 58 4D 07 EF E0 DC B6 9E 11 E2 06 E2 05 B5 65 AE B9 DB FA 81 BD EC ED 9D CE 88 CB 63 91 D8 B1 CC 49 4B 7D 4C 12 29 FB 86 49 CC 30 9E 91 39 A2 16 D6 9C A9 45 1C D0 20 FB 72 69 7F A9 78 98 02 C5 5A 0C 92 D3 D7 A8 77 2B 1D 04 82 B4 C6 9D 3A 02 9B C6 F0 CB E6 A2 27 77 86 6E 4F 7B F9 FC D6 00 A5 95 25 A7 A9 B0 23 6E 42 B6 C5 7B DF FE CD 57 A1 7C C1 13 2E BE 31 CC 73 F2 60 71 04 86 0E 25 C6 59 BC B6 48 02 28 0F 32 03 C4 41 BB 34 FF 8B 33 AA 02 67 FA A9 2F 76 BD CC 44 9D 30 DC C9 4A CA E3 A6 7F 4C BC C1 FA 02 F0 55 73 AC 6E 18 F1 FC 6D FE 83 00 DC 8E 51 E6 10 9D 77 C5 A7 8E 6F D7 96 0C D3 D3 57 FE 5E 30 B0 12 B8 4C 9F 23 2F 46 81 C3 FD 28 D2 10 71 A8 5B 88 E0 4B 2C 67 7B F4 9F F9 97 A2 7C A9 7C 7F ED 78 59 90 FF E4 4B 93 31 E6 98 6B 48 E2 C0 BB C3 4D 3E B4 F2 C5 3A EE 16 4B 1E 28 53 FA DB D7 DF 45 85 82 A5 2F 42 71 84 C9 8F C9 94 C1 AD A0 8D DB 6F 1D EB EB B1 FC 70 97 0C 9F D8 17 54 41 22 B8 79 8B 39 4F A3 E9 81 33 66 52 73 02 7B 0F 0D 8E 7E 7B BF ED 5D FE F5 B9 9B FF 04 E0 8E 22 6F 3B 28 B2 02 68 EF E4 C3 53 A9 E2 85 6C A2 75	success or wait	1	140062470	RegSetValueExA

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

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

Analysis Process: rundll32.exe PID: 6724, Parent PID: 6608

General

Target ID:	5
Start time:	15:41:49
Start date:	23/03/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\AyBhhRZXPj.dll,CompatString
Imagebase:	0x7ff7d29d0000
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: 00000005.00000002.260480210.00007FFC670C1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\AyBhhRZXPj.dll	unknown	1351680	success or wait	1	7FFC6711F8D6	ReadFile

Analysis Process: rundll32.exe PID: 6868, Parent PID: 6608

General

Target ID:	8
Start time:	15:41:52
Start date:	23/03/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\AyBhhRZXPj.dll,CompatValue
Imagebase:	0x7ff7d29d0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000008.00000002.268092209.00007FFC670C1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\AyBhhRZXPj.dll	unknown	1351680	success or wait	1	7FFC6711F8D6	ReadFile

Analysis Process: Magnify.exe PID: 5372, Parent PID: 3968

General

Target ID:	19
Start time:	15:42:42
Start date:	23/03/2022
Path:	C:\Windows\System32\Magnify.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\Magnify.exe
Imagebase:	0x7ff7f33c0000
File size:	809472 bytes
MD5 hash:	F97BE20B3744572366666607EE4BA7F7F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: FileHistory.exe PID: **5788**, Parent PID: **3968**

General

Target ID:	20
Start time:	15:42:43
Start date:	23/03/2022
Path:	C:\Windows\System32\FileHistory.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\FileHistory.exe
Imagebase:	0x7ff6d53b0000
File size:	246784 bytes
MD5 hash:	989B5BDB2BEAC9F894BBC236F1B67967
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: FileHistory.exe PID: **7004**, Parent PID: **3968**

General

Target ID:	21
Start time:	15:42:44
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\u70W8\FileHistory.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\u70W8\FileHistory.exe
Imagebase:	0x7ff6811e0000
File size:	246784 bytes
MD5 hash:	989B5BDB2BEAC9F894BBC236F1B67967
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000015.00000002.383767376.00007FFC74C21000.00000020.00000001.01000000.0000000A.sdmp, Author: Joe Security

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	7FFC634586ED	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	7FFC63458769	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	7FFC62EBB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFC62EBB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFC62F912E7	ReadFile

Analysis Process: RdpSa.exe PID: **7028**, Parent PID: **3968**

General	
Target ID:	23
Start time:	15:42:48
Start date:	23/03/2022
Path:	C:\Windows\System32\RdpSa.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\RdpSa.exe
Imagebase:	0x7ff683750000
File size:	43008 bytes
MD5 hash:	0795B6F790F8E52D55F39E593E9C5BBA
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: mspaint.exe PID: **7064**, Parent PID: **3968**

General	
Target ID:	24
Start time:	15:42:49
Start date:	23/03/2022
Path:	C:\Windows\System32\mspaint.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\mspaint.exe
Imagebase:	0x7ff77f500000
File size:	6780928 bytes
MD5 hash:	99F86A0D360FD9A3FCAD6B1E7D92A90C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: mspaint.exe PID: **4576**, Parent PID: **3968**

General	
Target ID:	25
Start time:	15:43:04
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\NYpervHTp\mspaint.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\NYpervHTp\mspaint.exe
Imagebase:	0x7ff6efae0000
File size:	6780928 bytes
MD5 hash:	99F86A0D360FD9A3FCAD6B1E7D92A90C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000019.00000002.457997826.00007FFC74C11000.00000020.00000001.01000000.0000000E.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\NYpervHTp\MFC42u.dll	unknown	1380352	success or wait	1	7FFC74C6F8D6	ReadFile

Analysis Process: mmc.exe PID: 6244, Parent PID: 3968

General

Target ID:	32
Start time:	15:43:23
Start date:	23/03/2022
Path:	C:\Windows\System32\mmc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\mmc.exe
Imagebase:	0x7ff617390000
File size:	1859584 bytes
MD5 hash:	BA80301974CC8C4FB9F3F9DDB5905C30
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: EaseOfAccessDialog.exe PID: 6176, Parent PID: 3968

General

Target ID:	33
Start time:	15:43:23
Start date:	23/03/2022
Path:	C:\Windows\System32\EaseOfAccessDialog.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\EaseOfAccessDialog.exe
Imagebase:	0x7ff6664e0000
File size:	304640 bytes
MD5 hash:	F87F2E5EBF3FFBA39DF1621B5F8689B5
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: unregmp2.exe PID: 4948, Parent PID: 3968

General

Target ID:	34
Start time:	15:43:24
Start date:	23/03/2022
Path:	C:\Windows\System32\unregmp2.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\unregmp2.exe
Imagebase:	0x7ff69f7d0000
File size:	254976 bytes
MD5 hash:	9B517303C58CA8A450B97B0D71594CBB
Has elevated privileges:	false

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

Analysis Process: unregmp2.exe PID: **4908**, Parent PID: **3968**

General

Target ID:	35
Start time:	15:43:25
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\vVin\unregmp2.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\vVin\unregmp2.exe
Imagebase:	0x7ff672540000
File size:	254976 bytes
MD5 hash:	9B517303C58CA8A450B97B0D71594CBB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000023.00000002.497477137.00007FFC74C21000.00000020.00000001.01000000.00000010.sdmp, Author: Joe Security

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\vVin\VERSION.dll	unknown	1355776	success or wait	1	7FFC74C7F8D6	ReadFile

Analysis Process: omadmclient.exe PID: **6340**, Parent PID: **3968**

General

Target ID:	36
Start time:	15:43:41
Start date:	23/03/2022
Path:	C:\Windows\System32\omadmclient.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\omadmclient.exe
Imagebase:	0x7ff7bc730000
File size:	315904 bytes
MD5 hash:	AD7C6CD7A8EEC95808AA77C5D7987941
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: omadmclient.exe PID: **6392**, Parent PID: **3968**

General

Target ID:	37
Start time:	15:43:43
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\iv505rrw\omadmclient.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\iv505rrw\omadmclient.exe
Imagebase:	0x7ff6bfa30000
File size:	315904 bytes
MD5 hash:	AD7C6CD7A8EEC95808AA77C5D7987941
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000025.00000002.528095549.00007FFC74C21000.00000020.00000001.01000000.00000012.sdmp, Author: Joe Security

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\iv505rrw\XmlLite.dll	unknown	1355776	success or wait	1	7FFC74C7F8D6	ReadFile

Analysis Process: SystemPropertiesPerformance.exe PID: **4040**, Parent PID: **3968**

General

Target ID:	38
Start time:	15:43:56
Start date:	23/03/2022
Path:	C:\Windows\System32\SystemPropertiesPerformance.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SystemPropertiesPerformance.exe
Imagebase:	0x7ff71c990000
File size:	83968 bytes
MD5 hash:	F325976CDC0F7E9C680B51B35D24D23A
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: eudcedit.exe PID: **6164**, Parent PID: **3968**

General

Target ID:	39
Start time:	15:43:58
Start date:	23/03/2022
Path:	C:\Windows\System32\eudcedit.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\eudcedit.exe
Imagebase:	0x7ff7f4400000
File size:	353280 bytes
MD5 hash:	0ED10F2F98B80FF9F95EED2B04CFA076
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: GamePanel.exe PID: **5244**, Parent PID: **3968**

General

Target ID:	40
Start time:	15:44:00
Start date:	23/03/2022
Path:	C:\Windows\System32\GamePanel.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\GamePanel.exe
Imagebase:	0x7ff7b7e60000
File size:	1292288 bytes
MD5 hash:	4EF330EFAE954723B1F2800C15FDA7EB
Has elevated privileges:	false

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

Analysis Process: GamePanel.exe PID: **5832**, Parent PID: **3968**

General

Target ID:	41
Start time:	15:44:01
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\Odp\GamePanel.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Odp\GamePanel.exe
Imagebase:	0x7ff76ca00000
File size:	1292288 bytes
MD5 hash:	4EF330EFAE954723B1F2800C15FDA7EB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000029.00000002.566763440.00007FFC678E1000.00000020.00000001.01000000.00000014.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

Disassembly

No disassembly