ID: 595323
Sample Name: elBAfme5gQ
Cookbook: default.jbs
Time: 16:03:08
Date: 23/03/2022
Version: 34.0.0 Boulder Opal

Table of Contents

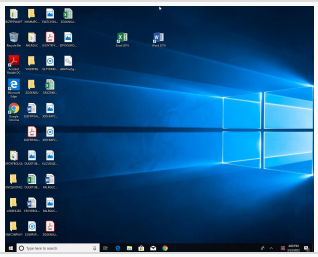
Windows Analysis Report

elBAfme5gQ

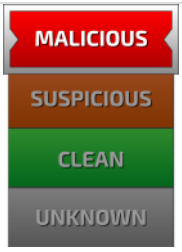
Overview

General Information

Sample Name:	elBAfme5gQ (renamed file extension from none to dll)
Analysis ID:	595323
MD5:	ca7c6f265e4bc0…
SHA1:	1720aadb4965df..
SHA256:	a8f566b8d2d9f9a.
Tags:	Dridex exe
Infos:	



Detection



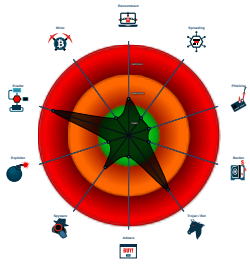
Dridex

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…
- Modifies the prolog of user mode fun…
- Queues an APC in another process …
- Sigma detected: Suspicious Call by…
- Machine Learning detection for drop…
- Uses Atom Bombing / ProGate to in…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 6828 cmdline: loaddll64.exe "C:\Users\user\Desktop\elBAfme5gQ.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 6836 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\elBAfme5gQ.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 6856 cmdline: rundll32.exe "C:\Users\user\Desktop\elBAfme5gQ.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6844 cmdline: rundll32.exe C:\Users\user\Desktop\elBAfme5gQ.dll,CreateXmlReader MD5: 73C519F050C20580F8A62C849D49215A)
    - explorer.exe (PID: 3968 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - PresentationSettings.exe (PID: 7040 cmdline: C:\Windows\system32\PresentationSettings.exe MD5: 76086DD04B6760277A2B897345A0B457)
      - PresentationSettings.exe (PID: 5432 cmdline: C:\Users\user\AppData\Local\A3MiXbeK\PresentationSettings.exe MD5: 76086DD04B6760277A2B897345A0B457)
      - DmNotificationBroker.exe (PID: 5352 cmdline: C:\Windows\system32\DmNotificationBroker.exe MD5: 1643D5735213BC89C0012F0E48253765)
      - DmNotificationBroker.exe (PID: 5876 cmdline: C:\Users\user\AppData\Local\WRsLe\DmNotificationBroker.exe MD5: 1643D5735213BC89C0012F0E48253765)
      - WFS.exe (PID: 4504 cmdline: C:\Windows\system32\WFS.exe MD5: CD6ACF3B997099B6CFB2417D3942F755)
      - WFS.exe (PID: 6212 cmdline: C:\Users\user\AppData\Local\daH0n9\WFS.exe MD5: CD6ACF3B997099B6CFB2417D3942F755)
      - DmNotificationBroker.exe (PID: 6008 cmdline: C:\Windows\system32\DmNotificationBroker.exe MD5: 1643D5735213BC89C0012F0E48253765)
      - DmNotificationBroker.exe (PID: 1804 cmdline: C:\Users\user\AppData\Local\pEcAZnNU3\DmNotificationBroker.exe MD5: 1643D5735213BC89C0012F0E48253765)
      - wusa.exe (PID: 6376 cmdline: C:\Windows\system32\wusa.exe MD5: 04CE745559916B99248F266BBF5F9ED9)
      - SystemSettingsRemoveDevice.exe (PID: 6408 cmdline: C:\Windows\system32\SystemSettingsRemoveDevice.exe MD5: 87AF711D6518C0CF91560D7C98301BBB)
  - rundll32.exe (PID: 6896 cmdline: rundll32.exe C:\Users\user\Desktop\elBAfme5gQ.dll,CreateXmlReaderInputWithEncodingCodePage MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6928 cmdline: rundll32.exe C:\Users\user\Desktop\elBAfme5gQ.dll,CreateXmlReaderInputWithEncodingName MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000015.00000002.455715001.00007FFC66921000.00000020.00000001.01000000.0000000C.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000002.00000002.382683427.00007FFC646C1000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
0000001F.00000002.529541082.00007FFC67881000.00000020.00000001.01000000.00000010.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000006.00000002.279312817.00007FFC646C1000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000003.00000002.265252224.00007FFC646C1000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	

Click to see the 4 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
18.2.PresentationSettings.exe.7ffc66970000.3.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
25.2.WFS.exe.7ffc66970000.3.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
2.2.rundll32.exe.7ffc646c0000.2.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
31.2.DmNotificationBroker.exe.7ffc67880000.3.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
5.2.rundll32.exe.7ffc646c0000.2.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	

Click to see the 4 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

Hooking and other Techniques for Hiding and Protection

Modifies the prolog of user mode functions (user mode inline hooks)

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)

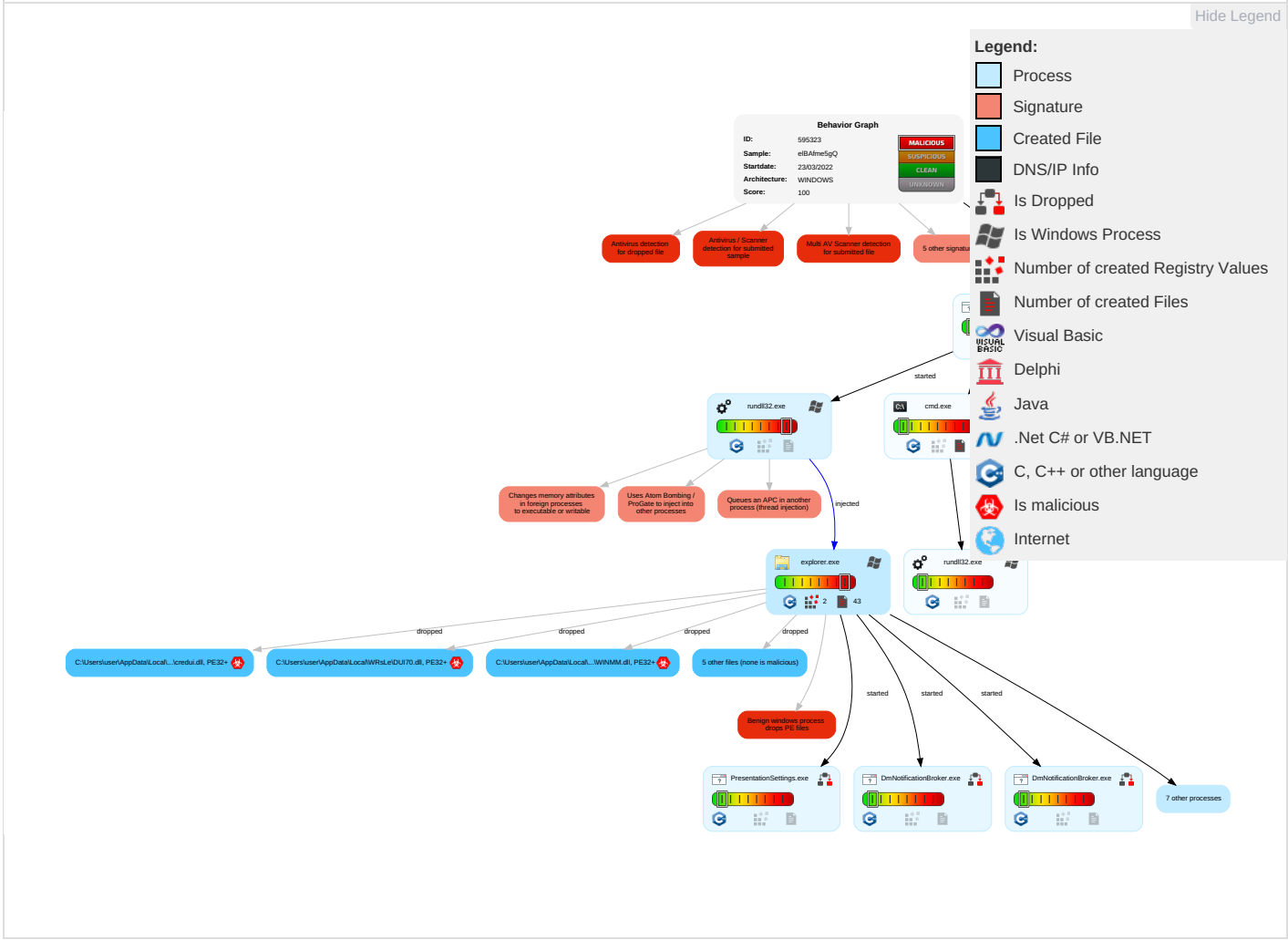
Uses Atom Bombing / ProGate to inject into other processes

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
1 Valid Accounts	2 Native API	1 DLL Side-Loading	1 DLL Side-Loading	1 Deobfuscate/Decode Files or Information	1 Credential API Hooking	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Exploitation for Client Execution	1 Valid Accounts	1 Valid Accounts	3 Obfuscated Files or Information	LSASS Memory	1 Account Discovery	Remote Desktop Protocol	1 Credential API Hooking	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)	1 Access Token Manipulation	2 Software Packing	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	At (Windows)	Logon Script (Mac)	3 1 2 Process Injection	1 Timestomp	NTDS	2 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 DLL Side-Loading	LSA Secrets	3 1 Security Software Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Rootkit	Cached Domain Credentials	1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Masquerading	DCSync	3 Process Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Valid Accounts	Proc Filesystem	1 Application Window Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Virtualization/Sandbox Evasion	/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 Access Token Manipulation	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	3 1 2 Process Injection	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Protocols			Service Stop

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	1 Rundll32	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS			Inhibit System Recovery

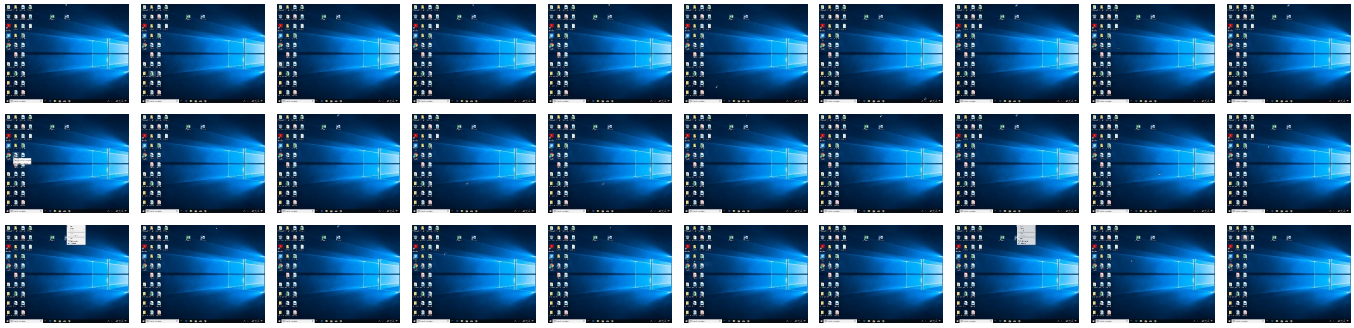
Behavior Graph

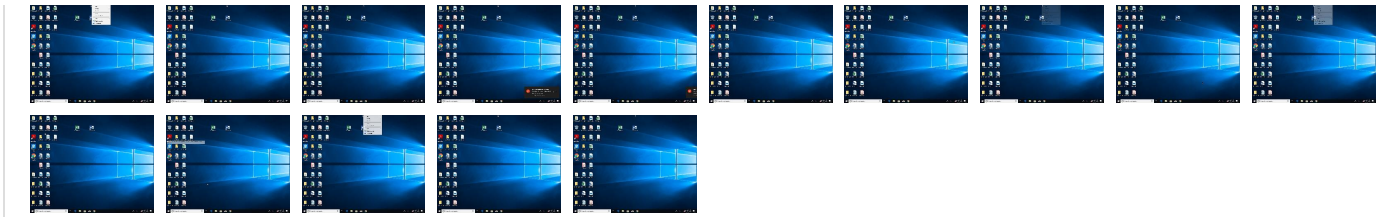


Screenshots

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
elBAfme5gQ.dll	63%	Virustotal		Browse
elBAfme5gQ.dll	66%	Metadefender		Browse
elBAfme5gQ.dll	88%	ReversingLabs	Win64.Trojan.Occamy	
elBAfme5gQ.dll	100%	Avira	TR/Crypt.XPACK.Gen7	
elBAfme5gQ.dll	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\WRsLe\DUI70.dll	100%	Avira	TR/Crypt.XPACK.Gen4	
C:\Users\user\AppData\Local\daH0n9\credui.dll	100%	Avira	TR/Crypt.XPACK.Gen7	
C:\Users\user\AppData\Local\WRsLe\DUI70.dll	100%	Avira	TR/Crypt.XPACK.Gen4	
C:\Users\user\AppData\Local\A3MiXbeK\WINMM.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\WRsLe\DUI70.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\daH0n9\credui.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\WRsLe\DUI70.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\A3MiXbeK\WINMM.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\A3MiXbeK\PresentationSettings.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\A3MiXbeK\PresentationSettings.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\A3MiXbeK\PresentationSettings.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
31.2.DmNotificationBroker.exe.25ea0a40000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
25.2.WFS.exe.20e998e0000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
6.2.rundll32.exe.20ea8c10000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
2.2.rundll32.exe.1e683d50000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
0.2.loaddll64.exe.1c6c38c0000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
5.2.rundll32.exe.18b9c500000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
18.2.PresentationSettings.exe.7ffc66970000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.rundll32.exe.1da43850000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
21.2.DmNotificationBroker.exe.1f554500000.1.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
25.2.WFS.exe.7ffc66970000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.rundll32.exe.7ffc646c0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.rundll32.exe.7ffc646c0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.2.PresentationSettings.exe.173c4f40000.0.unpack	100%	Avira	HEUR/AGEN.1215493		Download File
31.2.DmNotificationBroker.exe.7ffc67880000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
3.2.rundll32.exe.7ffc646c0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.7ffc646c0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.2.DmNotificationBroker.exe.7ffc66920000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.loaddll64.exe.7ffc646c0000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	595323
Start date and time:	2022-03-23 15:03:08 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	elBAfme5gQ (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:	35
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@31/9@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 25.6% (good quality ratio 16.8%) • Quality average: 44.6% • Quality standard deviation: 38.9%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, sls.update.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtEnumerateKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\A3MiXbeK\PresentationSettings.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	222208
Entropy (8bit):	6.618425906220987
Encrypted:	false
SSDEEP:	3072:dklO/b97taQPr5pT8as3lJwvkAarSvDZpFB+2xmh0QSoKKBlKxyAZEHA:Oo/b1txPlh8l+rUts2xmhfGKraEH
MD5:	76086DD04B6760277A2B897345A0B457
SHA1:	DC65093DB601FE7AA2F4C0C400D18F43DA92DCFA
SHA-256:	BF492302281E3CD4F023FB54E101D8C3BD00FFEAFF75B5D7FE0C1CA43F291A81
SHA-512:	6528C86BA0272274A907F8559DFD79C55D1A6BAF3A4545EF3F6CDC4C790CC9FBDB7A3A8A2E72D0ED39651975DF5967608111448D1351BDC659E8F0F5E8C724
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....._.">.q.>.q.>.q.F~q.>.q.Z.p.>.q.Z.p.>.q.Z.p.>.q.Z.p.>.q.>.q/> .q.Z.p.>.q.Z.q.>.q.Z.p.>.qRich.>.q.....PE..d... ..8.....".....J... ..... O.....@.....9....`..... .....x..... T.....a.....b.....text....H.....J..... ..`.rdata...]...`...^...N.....@..@.data...H.....@....pdata..x..... ..@..@.rsrc.....@..@.reloc.....b.....@..B.....

C:\Users\user\AppData\Local\A3MiXbeK\WINMM.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1429504

Entropy (8bit):	4.925425107744081
Encrypted:	false
SSDEEP:	12288:xZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuw:xZK6F7n5eRmDFJivohZFV
MD5:	37B80DA01055C6036ABE9D98E2EEF1B8
SHA1:	844CA9FADA6210A0CD67E24257B49D8BCF217DAA
SHA-256:	EC8D39D3F13C11B6C259591469742E56ACB4D72BE5E48E929B53F021BEB8F36E
SHA-512:	A3951AC7C775BA9358E84C3636E18D43B9E88553C5866E295FF25EB35A7067A7AEEE6B34FDCAB0277CC1531469845F77F28051F1B1260C02B0703DB3CCAED11F
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....X..Z.qb..qb..qb.a...jqb.s....qb.9...\qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb..(c..qb.;...,qb./..Tqb.....Zqb.....qb.z. ..Bqb.....nqb.....[qb.....qb.;...{qb.....qb..#...qb...f.oqb....hqb.z....qb.....:qb.;...tqb.Rich.qb.....PE..d.G...}^....." ....$.....@.....`.....h...$...<.....0..(.....text..... .. .....@..... ..`.rdata...o...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\WRsLe\DUI70.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1708032
Entropy (8bit):	5.373706741928563
Encrypted:	false
SSDEEP:	12288:xZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuwP3WN/0138:xZK6F7n5eRmDFJivohZFVPWNW
MD5:	ECEB1D6165AEE8F6644397DF9F126839
SHA1:	87D4E499BF3DFEC6E30A698CE3E05AC0E34DC7D8
SHA-256:	F5136D89F200A1FD6B7DA976CBBF1DB66661381EA8C044C4FB0C55239F4ED3FC
SHA-512:	102C7642D267A302EEF694F8156ABE5447140C950404FC01F261C6B317CD5ED784759120D52D2CB79BE14496EBB0EE00333F41FD31D6A6D6651417AE17648C2E
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....X..Z.qb..qb..qb.a...jqb.s....qb.9...\qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb..(c..qb.;...,qb./..Tqb.....Zqb.....qb.z. ..Bqb.....nqb.....[qb.....qb.;...{qb.....qb..#...qb...f.oqb....hqb.z....qb.....:qb.;...tqb.Rich.qb.....PE..d.G...}^....." ....$.....@.....`.....dQ..$...<.....0..(.....text..... .. .....@..... ..`.rdata...o...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\WRsLe\DmNotificationBroker.exe

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

C:\Users\user\AppData\Local\daH0n9\WFS.exe

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

Size (bytes):	930304
Entropy (8bit):	5.99262413442194
Encrypted:	false
SSDEEP:	12288:YVpcWBIX7oU/HEx5a/DTROFJTl7XjY5uUMUd1vLf1k+xt4vFe:spnBUoR5AfREllTjY5umjz1ivFe
MD5:	CD6ACF3B997099B6CFB2417D3942F755
SHA1:	7376A8000CB7B5CE0F5DA783BAF9F9C2C36F1670
SHA-256:	B699695F47AA8E8B70A21267BA1648B59B33BD677E29D334BC73EBB1A4B81F3E
SHA-512:	F301F0D87CB5FFFFB88AB0B86035DA7705DED1121107D2FDF7A9132F8DFBDEFFAFBE452E3BC7ACEAD1A0E368815127942B2E642B214EA83D90E97B015C766D E0
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....OR...3.,.3.,.3.,dW.-.3.,dW.-.3.,dW.-.3.,dW.-$3.,.3.,o7.,dW.-q3 .,dW.,.3.,dW.-.3.,Rich.3.,.....PE..d...d.D.....".....F.....@.....`..... .....`.....0...%.....@A.....`..D ..`@.. T.....Y..(... .....Y..8... W.....text...2..... ..`.rdata.....@..@.data..../..... .....@....pdata..@A.....B..... ..@..@.didat..... .....@....rsrc....%...0...&.....@..@.reloc..D ...`..".....@..B..... .....

C:\Users\user\AppData\Local\daH0n9\credui.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1425408
Entropy (8bit):	4.919681432675964
Encrypted:	false
SSDEEP:	12288:RZgJtlQepQn+NDo7nlYegQCLDF/B9wvj/cLvVZFuw:RZK6F7n5eRmDFJivohZFV
MD5:	FFCCCB5ECF191C6B30DC3F0C3D5C4238
SHA1:	8F3620F81C7A59A7B0C59AD20DCF82FF53F78996
SHA-256:	3F164C230BB5416C66713A3D03B5374C55EE85A1E3D97BB7663818AF719ABB87
SHA-512:	22523EA25E9927211ADC02123EEC2F86C5FB66A79F9C262D7EA3ABBE8A0C4A7FAACAB3FF0713033A1812D8465B32B352F2D73EA4839C4F0B23A615A8EE8289 D
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....X..Z.qb..qb..qb.a...jqb.s....qb.9...\qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb..(c..qb.;...,qb../..Tqb.....Zqb.....qb.z. ..Bqb.....nqb.....[qb.....qb.;...{qb.....qb..#...qb...f.oqb....hqb.z....qb.....:qb.;...tqb.Rich.qb.....PE..d.G...}^....." ....$.....@.....`.....$...<.....0..(.....text..... .. .....@..... ..`.rdata...o...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\pEcAZnNU3\DUI70.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1708032
Entropy (8bit):	5.373867229558349
Encrypted:	false
SSDEEP:	12288:YZgJtlQepQn+NDo7nlYegQCLDF/B9wvj/cLvVZFuw6aN/0138:YZK6F7n5eRmDFJivohZFVLNW
MD5:	F1ABEB8232250B108AC5E4BA8F9795CC
SHA1:	A7E6D97B7B192E2D570061DD416DB45D8DD5F9D6
SHA-256:	314A8F8EBF9905FFDEE0BD9BEBB3EA6D08AACC22305B3A7D518022D4B512042D
SHA-512:	6D4558AFABA5359438F67A7E416426E54CACF4D356D8911E0FBA6EAD47F2DF561B8092AAA1CFB154B0BD25F87BED44C467D8981D7CDF21C3BAF19E57878DD 6F
Malicious:	false
Preview:	MZ.....@.....X..Z.qb..qb..qb.a...jqb.s....qb.9...\qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb..(c..qb.;...,qb../..Tqb.....Zqb.....qb.z. ..Bqb.....nqb.....[qb.....qb.;...{qb.....qb..#...qb...f.oqb....hqb.z....qb.....:qb.;...tqb.Rich.qb.....PE..d.G...}^....." ....$.....@.....`.....dQ..$...<.....0..(.....text..... .. .....@..... ..`.rdata...o...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\pEcAZnNU3\DmNotificationBroker.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	32256
Entropy (8bit):	5.250876383836324

Encrypted:	false
SSDEEP:	768:ghunFhykO4aAvnsvpzte5+Ql0/iqmjjn:58kO4asshu+Q+/Ojjn
MD5:	1643D5735213BC89C0012F0E48253765
SHA1:	D076D701929F1F269D34C8FD7BD1BAB4DAF42A9D
SHA-256:	4176FA24D56BB870316D07BD7211BC8A797394F77DCC12B35FFEBAA0326525D2
SHA-512:	F0BD45FE66EDC6F615C0125C1AE81E657CA26544544769651AB0623DD3C724F96D9D78835EF6B1D15083D1BB9D501F6DC48487DDA5C361CAFA96022D5F33A4F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....j.?H..lH..lH..lAs.lT..l'o.mJ..l'o.m[..lH..l...l'o.mC..l'o.mA..l'o.mA..l 'ohll..l'o.ml..lRichH..l.....PE..d....."....*...V.....&.....@.....n3..... .....x..... .....Po..T... .....]..... .....^..p.....text....(.....*..... ..`.imrsiv.....@.....rdata..P8...P...:.....@..@.data...(.....h.....@. ...pdata.....j.....@..@.rsrc... .....n.....@..@.reloc.....z.....@..B..... ....

C:\Users\user\AppData\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):	7.333126465225537
Encrypted:	false
SSDEEP:	24:URrWQXgUcjg2eNTXpQutJeZwztuBZFRydqukcVq1b2t+Oq1pUWcgouzr4bhm2rf1:URkUc8PNDOZwJu9yqsw1bOwf7cbu/GH1
MD5:	05221058F2A6FC026C52AB5D3DF5A8ED
SHA1:	AA9A4864BFC81C855A884B05157129ACC36F6883
SHA-256:	094C4EB0EF4FB9F35A6E0BDF504E80C37FBDDA9736F587E1A0C60579D62F9610
SHA-512:	18CF3230240F1684C5F3BC524D8AB6CE11A274BC78C5FF4F048B25FECFCF3F69A8E4369F1E7E118023C89B964A8B43F58473D33F8150100F6F1A23DAFFD48003
Malicious:	false
Preview:	.....user.....RSA1.....z".n...5.....V#..pd).jS..&..d..../S.....1b....Xa~.].....G....w-X.Y3...m.D.jA..0q..>Y.....$.U"...&...I.5.....t...ya.C.E. .....z..O.....w...L.al....?E.....,...C.r.y.p.t.o.A.P.I. .P.r.i.v.a.t.e. .K.e.y....f..... .....s.+..#.h*u....R.=.e8.y..... ....;`.....H.....*qY`....O^.....`.....VB.:.....I.W..c D...=$...?.....V...D..$.4<.....AE..v]Z..Xz.:.L...'.d...9.....9..^...#..H.Y....o...@.k.#.z.VT.j?.7/Dp.. .U.[.i...m..J..?..I.,..Y..0..{;&..Lhow...>W..C..y..9h..t.Dh..!..U./..N.xK..<..... .....Xg..L..NB....P)Gh-z..t5>J.....J.7..j.E.2..L....(.N..$...e0.[."<.S..I...]z...M..4t.....C].....Z.s..v (.\:.....Z1$....I.6zm$)I."3..)..=X..T.<.....pKHD\....!....Hf.....>.(t.t..t..O.G.. .....74Xz.id.:l..1xu.7M.I.=9.v...Fs..~.U9'....6.%Bf..X..6....E....;..y..H.O..Z...~..l...tdQ.,.cta....|_.^.8t..''..=.y..a..ii....Wk!bT.9.'&..^...lq..5.....

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Entropy (8bit):	4.927389050456392
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:	elBAfme5gQ.dll
File size:	1421312
MD5:	ca7c6f265e4bc09e6d9d0b2b6234e8b3
SHA1:	1720aadb4965df64ee40d32957ee6080500639b2
SHA256:	a8f566b8d2d9f9a418211039cb76552d460f83195d519a89313a880ead9bd4a4
SHA512:	d7ab70fc544e2ab4354ad7dfc502eaf37f46e8c62bf7e74421b02cee78fe3cefbaf7347c4def1dc728649563fc6e61cb5463558c94fd5494ddf672145a347f3e
SSDEEP:	12288:6ZgJtlQepQn+NDo7nIYegQCLDF/B9wvj/cLvVZFuw:6ZK6F7n5eRmDFJivohZFV
File Content Preview:	MZ.....@.....X..Z.qb..qb..qb.a...jqb.s....qb.9...\qb.s...(qb.....qb..#.. qb../b..qb.....qb.....Hqb..(c./qb.r,f..qb.. (c..qb.;...,qb../..Tqb.....Zqb.....qb.z...Bqb.....nqb.....[qb.....qb.;...{qb.....qb

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

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

Entrypoint Preview
Instruction
dec eax
mov dword ptr [00070639h], ecx
dec eax
lea ecx, dword ptr [FFFFF2F2h]
dec esp
mov dword ptr [0007064Bh], eax
dec esp
mov dword ptr [00070654h], edi
dec esp
mov dword ptr [00070655h], esi
dec eax
xor eax, eax
dec eax
inc eax
dec eax
add ecx, eax
dec esp
mov dword ptr [00070655h], esp
dec eax
dec ecx
dec eax
mov dword ptr [00070653h], esi
dec eax
test eax, eax
je 00007FEBE0AD2DCDh
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 00007FEBE0AD2DACh
dec esp
mov dword ptr [000705FEh], ecx

Instruction
dec esp
mov dword ptr [0007060Fh], ebp
dec eax
mov dword ptr [000705D0h], edx
jmp ecx
dec eax
add edi, ecx
retn 0008h
ud2
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
push esi
dec eax
sub esp, 00000080h
dec eax
mov dword ptr [esp+78h], 58225FC8h
mov dword ptr [esp+60h], 2DFAE652h
mov al, byte ptr [esp+77h]
mov dl, al
add dl, FFFFFF85h
mov byte ptr [esp+77h], dl
mov word ptr [esp+5Eh], 3327h
dec esp
mov eax, dword ptr [esp+78h]
inc esp
mov ecx, dword ptr [esp+64h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x15a010	0x12e	.drmed
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	0x66fe7	0x67000	False	0.700320938258	data	7.87281050709	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xaa000	0x13ba7	0x14000	False	0.0782836914062	data	2.51707039551	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0xbe000	0x138	0x1000	False	0.061279296875	PEX Binary Archive	0.599172422844	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0xbf000	0x69e	0x1000	False	0.123291015625	data	1.07831823765	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc0000	0xf31	0x1000	False	0.416748046875	data	5.36145191459	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.vxl	0xc1000	0x14d4	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.qwubgr	0xc3000	0x1124	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.eer	0xc5000	0x1e66	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.xwwauf	0xc7000	0x9cd	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pkc	0xc8000	0x42a	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.npkda	0xc9000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vhs	0xca000	0x1af	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.iaywj	0xcb000	0x1455	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.nasi	0xcd000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.zhvprh	0xce000	0x6cd0	0x7000	False	0.00177873883929	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.yatdsp	0xd5000	0x543	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.njso	0xd6000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.lgliat	0xd8000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ntqjh	0xd9000	0xbf6	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.sucsek	0xda000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.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

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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.pvv	0xfc000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.lug	0xfd000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ski	0x143000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.japjd	0x144000	0x128f	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.mwtzml	0x146000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vgssf	0x147000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.gsroye	0x148000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vcmr	0x14a000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.kvjqnl	0x14b000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.zlu	0x14c000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.nrcvk	0x14d000	0x3fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pfz	0x14e000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.hxz	0x150000	0x1f2a	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.snjrs	0x152000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bffts	0x153000	0x128f	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.oqqo	0x155000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ancqi	0x156000	0x3fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.wnpyu	0x157000	0xd33	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.eflx	0x158000	0x3ba	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.mjql	0x159000	0x2da	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.drmed	0x15a000	0x13e	0x1000	False	0.046142578125	data	0.651345168	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
CreateXmlReader	1	0x14001f0f0
CreateXmlReaderInputWithEncodingCodePage	2	0x1400146c8
CreateXmlReaderInputWithEncodingName	3	0x1400251b8
CreateXmlWriter	4	0x140024134
CreateXmlWriterOutputWithEncodingCodePage	5	0x14003ab88
CreateXmlWriterOutputWithEncodingName	6	0x140039890

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

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
ZwSetEvent	INLINE	explorer.exe
RtlAllocateMemoryBlockLookaside	INLINE	explorer.exe
RtlAllocateMemoryZone	INLINE	explorer.exe
NtSetEvent	INLINE	explorer.exe

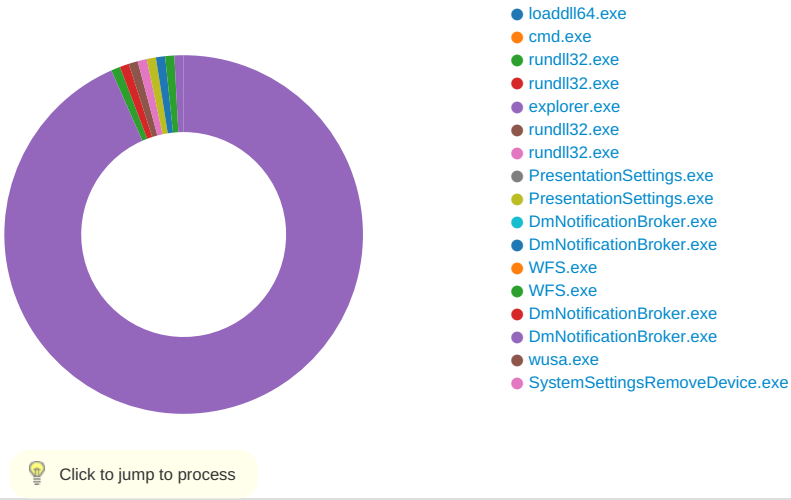
Processes

Process: explorer.exe, Module: ntdll.dll

Function Name	Hook Type	New Data
ZwSetEvent	INLINE	0xE9 0x9B 0xBB 0xB5 0x5E 0xEF
RtlAllocateMemoryBlockLookaside	INLINE	0x28 0x84 0x48 0x88 0x8D 0xD4
RtlAllocateMemoryZone	INLINE	0x5C 0xC2 0x24 0x43 0x38 0x84
NtSetEvent	INLINE	0xE9 0x9B 0xBB 0xB5 0x5E 0xEF

Statistics

Behavior



System Behavior

Analysis Process: loaddll64.exe PID: 6828, Parent PID: 5292

General

Target ID:	0
Start time:	16:05:13
Start date:	23/03/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\elBAfme5gQ.dll"
Imagebase:	0x7ff72c750000
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: 00000000.00000002.285761236.00007FFC646C1000.00000020.00000001.01000000.00000003.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: 6836, Parent PID: 6828

General

Target ID:	1
Start time:	16:05:14
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\elBAfme5gQ.dll",#1
Imagebase:	0x7ff753e60000
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: **6844**, Parent PID: **6828**

General

Target ID:	2
Start time:	16:05:14
Start date:	23/03/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\elBAfme5gQ.dll,CreateXmlReader
Imagebase:	0x7ff73c5c0000
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: 00000002.00000002.382683427.00007FFC646C1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\elBAfme5gQ.dll	unknown	1421312	success or wait	1	7FFC6471F8D6	ReadFile

Analysis Process: rundll32.exe PID: **6856**, Parent PID: **6836**

General

Target ID:	3
Start time:	16:05:14
Start date:	23/03/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\elBAfme5gQ.dll",#1
Imagebase:	0x7ff73c5c0000
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: 00000003.00000002.265252224.00007FFC646C1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\elBAfme5gQ.dll	unknown	1421312	success or wait	1	7FFC6471F8D6	ReadFile

Analysis Process: explorer.exe PID: **3968**, Parent PID: **6844**

General

Target ID:	4
Start time:	16:05:17
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\Crypto\RSA\yY6	read data or list directory | synchronize	device | compressed	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005F2F5	CreateDirectoryW
C:\Users\user\AppData\Local\A3MiXbeK\	read data or list directory | synchronize	device | compressed	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005F2F5	CreateDirectoryW
C:\Users\user\AppData\Local\A3MiXbeK\WINMM.dll	read attributes | synchronize | generic read | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\A3MiXbeK\PresentationSettings.exe	read attributes | synchronize | generic read | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\WRsLe\	read data or list directory | synchronize	device | compressed	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005F2F5	CreateDirectoryW
C:\Users\user\AppData\Local\WRsLe\DUI70.dll	read attributes | synchronize | generic read | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\WRsLe\DmNotificationBroker.exe	read attributes | synchronize | generic read | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\daH0n9\	read data or list directory | synchronize	device | compressed	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005F2F5	CreateDirectoryW
C:\Users\user\AppData\Local\daH0n9\credui.dll	read attributes | synchronize | generic read | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\daH0n9\WFS.exe	read attributes | synchronize | generic read | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\pEcAZnNU3\	read data or list directory | synchronize	device | compressed	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	14005F2F5	CreateDirectoryW
C:\Users\user\AppData\Local\pEcAZnNU3\DUI70.dll	read attributes | synchronize | generic read | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW
C:\Users\user\AppData\Local\pEcAZnNU3\DmNotificationBroker.exe	read attributes | synchronize | generic read | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	14005F6CE	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\A3MiXbeK\PresentationSettings.exe	cannot delete	7	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\A3MiXbeK\WINMM.dll	cannot delete	7	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\A3MiXbeK\PresentationSettings.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\A3MiXbeK\WINMM.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\WRsLe\DmNotificationBroker.exe	cannot delete	10	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\WRsLe\DUI70.dll	cannot delete	10	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\WRsLe\DmNotificationBroker.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\WRsLe\DUI70.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\daH0n9\credui.dll	cannot delete	16	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\daH0n9\WFS.exe	cannot delete	16	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\daH0n9\credui.dll	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\daH0n9\WFS.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\pEcAZnNU3\DmNotificationBroker.exe	cannot delete	9	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\pEcAZnNU3\DUI70.dll	cannot delete	9	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\pEcAZnNU3\DmNotificationBroker.exe	success or wait	1	14005FB70	DeleteFileW
C:\Users\user\AppData\Local\pEcAZnNU3\DUI70.dll	success or wait	1	14005FB70	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\A3MiXbeK\WINMM.dll	0	1429504	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
C:\Users\user\AppData\Local\A3MiXbeK\PresentationSettings.exe	0	222208	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 5f fd 22 fd 3e fd 71 fd 3e fd 71 fd 3e fd 71 fd 46 7e 71 fd 3e fd 71 fd 5a fd 70 fd 3e fd 71 fd 5a fd 70 fd 3e fd 71 fd 5a fd 70 fd 3e fd 71 fd 5a fd 70 fd 3e fd 71 fd 3e fd 71 2f 3e fd 71 fd 5a fd 70 fd 3e fd 71 fd 5a 12 71 fd 3e fd 71 fd 5a fd 70 fd 3e fd 71 52 69 63 68 fd 3e fd 71 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 06 00 20 fd fd 38 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$_">q>q>qF~q>qZp>qZp>qZp>qZp>q>q/>qZp>qZq>qZp >qRich>qPEd 8"	success or wait	1	14005F160	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\WRsLe\DUI70.dll	0	1708032	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
C:\Users\user\AppData\Local\WRsLe\DmNotificationBroker.exe	0	32256	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 0c 6a fd 3f 48 0b fd 6c 48 0b fd 6c 48 0b fd 6c 41 73 04 6c 54 0b fd 6c 27 6f fd 6d 4a 0b fd 6c 27 6f fd 6d 5b 0b fd 6c 48 0b fd 6c 16 0b fd 6c 27 6f fd 6d 43 0b fd 6c 27 6f fd 6d 41 0b fd 6c 27 6f fd 6d 41 0b fd 6c 27 6f 68 6c 49 0b fd 6c 27 6f fd 6d 49 0b fd 6c 52 69 63 68 48 0b fd 6c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 07	MZ@!L!This program cannot be run in DOS mode.$j?HlHlHlAslTl'omJl'om[lHll'omCl'omAl'omAl'ohlIl'omIlRichHlPEd	success or wait	1	14005F160	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\daH0n9\credui.dll	0	1425408	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
C:\Users\user\AppData\Local\daH0n9\WFS.exe	0	930304	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 4f 52 fd 7f 0b 33 fd 2c 0b 33 fd 2c 0b 33 fd 2c 64 57 fd 2d 08 33 fd 2c 64 57 fd 2d 10 33 fd 2c 64 57 fd 2d 04 33 fd 2c 64 57 fd 2d 24 33 fd 2c 0b 33 fd 2c 6f 37 fd 2c 64 57 fd 2d 71 33 fd 2c 64 57 06 2c 0a 33 fd 2c 64 57 fd 2d 0a 33 fd 2c 52 69 63 68 0b 33 fd 2c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 07 00 64 fd 44 fd 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$OR3,3,3,dW-3,dW-3,dW-3,dW-$3,3,o7,dW-q3,dW,3,dW-3,Rich3,PEddD"	success or wait	1	14005F160	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\pEcAZnNU3\DUI70.dll	0	1708032	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 58 10 0c 5a 1c 71 62 09 1c 71 62 09 1c 71 62 09 61 08 fd 09 6a 71 62 09 73 07 fd 09 18 71 62 09 39 06 fd 09 5c 71 62 09 73 07 fd 09 28 71 62 09 fd 15 fd 09 0b 71 62 09 11 23 fd 09 20 71 62 09 fd 2f 62 08 07 71 62 09 15 09 fd 09 09 71 62 09 07 fd fd 09 48 71 62 09 fd 28 63 08 2f 71 62 09 72 2c 66 08 0b 71 62 09 fd 28 63 08 10 71 62 09 3b fd fd 09 2c 71 62 09 fd 2f fd 09 54 71 62 09 fd fd fd 09 5a 71 62 09 fd fd fd 09 1e 71 62 09 7a fd fd 09 42 71 62 09 fd fd fd 09 6e 71 62 09 fd 15 fd 09 5b 71 62 09 9d fd 09 1b 71 62 09 3b fd 0c 09 7b 71 62 09 1f 09 fd 09 7f 71 62	MZ@XZqbqbqbajqbsqb9\qbs(qbqb# qb/bqbqbHqb(c/qbr,fqb(c qb;,qb/ TqbZqbqbzBqbnqb[qbqb; {qbqb	success or wait	1	14005F160	WriteFile
C:\Users\user\AppData\Local\pEcAZnNU3\DmNotificationBroker.exe	0	32256	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 0c 6a fd 3f 48 0b fd 6c 48 0b fd 6c 48 0b fd 6c 41 73 04 6c 54 0b fd 6c 27 6f fd 6d 4a 0b fd 6c 27 6f fd 6d 5b 0b fd 6c 48 0b fd 6c 16 0b fd 6c 27 6f fd 6d 43 0b fd 6c 27 6f fd 6d 41 0b fd 6c 27 6f fd 6d 41 0b fd 6c 27 6f 68 6c 49 0b fd 6c 27 6f fd 6d 49 0b fd 6c 52 69 63 68 48 0b fd 6c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 07	MZ@!L!This program cannot be run in DOS mode.$j?HlHlHlAslTl' omJl'om[lHll'omCl'omAl'omAl'ohlIl'omIlRichHlPEd	success or wait	1	14005F160	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\secinit.exe	unknown	10240	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\PATHPING.EXE	unknown	19456	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\rdpsign.exe	unknown	86016	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\msg.exe	unknown	26112	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\licensingdiag.exe	unknown	223744	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\RmClient.exe	unknown	17408	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\RelPost.exe	unknown	156160	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\colorcpl.exe	unknown	87552	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\hvix64.exe	unknown	1174432	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\autoconv.exe	unknown	932352	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\winver.exe	unknown	58880	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\PerceptionSimulationDevice.exe	unknown	63904	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\prevhost.exe	unknown	28160	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\DsmUserTask.exe	unknown	29696	success or wait	1	14005F8D6	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\chgusr.exe	unknown	21504	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\comp.exe	unknown	25088	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\ResetEngine.exe	unknown	11264	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\mmgaserver.exe	unknown	1637376	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\PresentationSettings.exe	unknown	222208	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\winmm.dll	unknown	123584	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\LaunchWinApp.exe	unknown	41984	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\GameBarPresenceWriter.exe	unknown	297984	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\change.exe	unknown	17408	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\AppVShNotify.exe	unknown	231320	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\extrac32.exe	unknown	33792	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\DmNotificationBroker.exe	unknown	32256	success or wait	6	14005F8D6	ReadFile
C:\Windows\System32\dui70.dll	unknown	1719808	success or wait	2	14005F8D6	ReadFile
C:\Windows\System32\attrib.exe	unknown	21504	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\UIMgrBroker.exe	unknown	35840	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\backgroundTaskHost.exe	unknown	19352	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\WFS.exe	unknown	930304	success or wait	3	14005F8D6	ReadFile
C:\Windows\System32\credui.dll	unknown	48640	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\cmd.exe	unknown	273920	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\cmmon32.exe	unknown	42496	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\fhmanagew.exe	unknown	139264	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\dfrgui.exe	unknown	575488	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\wusa.exe	unknown	308736	success or wait	1	14005F8D6	ReadFile
C:\Windows\System32\SystemSettingsRemoveDevice.exe	unknown	39304	success or wait	2	14005F8D6	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{E537B88F-291B-2050-AFBD-F973D43CF92D}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{E537B88F-291B-2050-AFBD-F973D43CF92D}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{8EED0859-8BE8-044E-4A8A-EA0F9DBC337E}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{8EED0859-8BE8-044E-4A8A-EA0F9DBC337E}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{BF256B32-1283-5C9F-7335-13DB405FDB38}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{BF256B32-1283-5C9F-7335-13DB405FDB38}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{00752DF3-4E3C-A91F-492E-AB3DEE638AD1}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{00752DF3-4E3C-A91F-492E-AB3DEE638AD1}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{F868B419-AFC8-8C68-5BAA-D7734B26D2F5}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{F868B419-AFC8-8C68-5BAA-D7734B26D2F5}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{4D810CF1-6BF3-5761-34CE-8AB56C5CCB0B}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{4D810CF1-6BF3-5761-34CE-8AB56C5CCB0B}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{B66A219A-4DE5-1654-893E-12FA75860040}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{B66A219A-4DE5-1654-893E-12FA75860040}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{794FACB7-966E-A756-EDA5-35F790B3BBB8}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{794FACB7-966E-A756-EDA5-35F790B3BBB8}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{11EB41D4-9441-012C-D8E5-9DDE1EC51626}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{11EB41D4-9441-012C-D8E5-9DDE1EC51626}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{7044809E-6728-983F-51A4-E429A04CC373}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{7044809E-6728-983F-51A4-E429A04CC373}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{CC67E16B-D7A7-A849-FCD2-573E3EF5AE60}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{CC67E16B-D7A7-A849-FCD2-573E3EF5AE60}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{04DCD223-B4EA-4FEC-DBB5-BACED119C6DC}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{04DCD223-B4EA-4FEC-DBB5-BACED119C6DC}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{AC559538-A99C-3C85-1438-7DE5DB84EFA4}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{AC559538-A99C-3C85-1438-7DE5DB84EFA4}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{4A8EF815-DE6D-88D8-C16D-3A0B92345024}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{4A8EF815-DE6D-88D8-C16D-3A0B92345024}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{3DAC9352-EF2F-02E3-87C9-4F9B6EF10F9C}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{3DAC9352-EF2F-02E3-87C9-4F9B6EF10F9C}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{2A30A142-7AB1-3124-4200-37586C56EC34}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{2A30A142-7AB1-3124-4200-37586C56EC34}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{5297939A-4BE1-51FB-4958-6C5CF60475A5}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{5297939A-4BE1-51FB-4958-6C5CF60475A5}\ShellFolder	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{0DAE4A20-BD7E-F557-1FD9-C1D671193B02}	success or wait	1	14006340A	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{0DAE4A20-BD7E-F557-1FD9-C1D671193B02}\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\{CC67E16B-D7A7-A849-FCD2-573E3EF5AE60}\ShellFolder	{D2484701-257A-0A3D-D692-7BEB29F73749}	binary	C5 B8 57 21 E0 F6 6A 3E B0 5C DD 50 49 59 BA B9 5B AF 7D 2B DC 2A 37 E0 83 70 20 EB BE 89 D6 92 F8 66 C4 C0 51 56 EE 76 96 D2 00 90 3E 6B 19 DF F4 B4 D3 99 5A 5F 24 3C 4C 98 6F EF 2D 45 DC 19 31 DE C0 E4 39 1B 6F	success or wait	1	140062470	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{11EB41D4-9441-012C-D8E5-9DDE1EC51626}\ShellFolder	{534E41FE-102F-FB71-3892-BE6C2F00A428}	binary	C1 03 01 39 E2 10 74 AC C7 79 AE 8E 49 E4 2F 23 4A 56 F9 0B EC F5 CE 24 E2 59 36 43 58 E5 5A 9E 69 43 84 80 38 C6 31 07 E6 40 05 23 4B 7C 60 1E 7A AC CB F5 65 EB 02 32 A6 2D AF 84 16 D8 B6 18 8B AC 9A FD 94 2C 90 A7 35 6A 96 DC B1 82 84 3A 90 C3 B8 32 3D B2 A7 40 CC 1A B8 AD	success or wait	1	140062470	RegSetValueExA

Analysis Process: rundll32.exe PID: **6896**, Parent PID: **6828**

General

Target ID:	5
Start time:	16:05:18
Start date:	23/03/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\elBAfme5gQ.dll,CreateXmlReaderInputWithEncodingCodePage
Imagebase:	0x7ff73c5c0000
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: 00000005.00000002.271180425.00007FFC646C1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\elBAfme5gQ.dll	unknown	1421312	success or wait	1	7FFC6471F8D6	ReadFile

Analysis Process: rundll32.exe PID: **6928**, Parent PID: **6828**

General

Target ID:	6
Start time:	16:05:21
Start date:	23/03/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\elBAfme5gQ.dll,CreateXmlReaderInputWithEncodingName
Imagebase:	0x7ff73c5c0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000006.00000002.279312817.00007FFC646C1000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\elBAfme5gQ.dll	unknown	1421312	success or wait	1	7FFC6471F8D6	ReadFile

Analysis Process: PresentationSettings.exe PID: **7040**, Parent PID: **3968**

General

Target ID:	17
Start time:	16:06:14
Start date:	23/03/2022
Path:	C:\Windows\System32\PresentationSettings.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\PresentationSettings.exe
Imagebase:	0x7ff603330000
File size:	222208 bytes
MD5 hash:	76086DD04B6760277A2B897345A0B457
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: PresentationSettings.exe PID: **5432**, Parent PID: **3968**

General	
Target ID:	18
Start time:	16:06:16
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\A3MiXbeK\PresentationSettings.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\A3MiXbeK\PresentationSettings.exe
Imagebase:	0x7ff7b4450000
File size:	222208 bytes
MD5 hash:	76086DD04B6760277A2B897345A0B457
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: 00000012.00000002.417833376.00007FFC66971000.00000020.00000001.01000000.0000000A.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities						
File Read						
File Path	**Offset**	**Length**	**Completion**	**Count**	**Source Address**	**Symbol**
C:\Users\user\AppData\Local\A3MiXbeK\WINMM.dll	unknown	1429504	success or wait	1	7FFC669CF8D6	ReadFile

Analysis Process: DmNotificationBroker.exe PID: **5352**, Parent PID: **3968**

General	
Target ID:	19
Start time:	16:06:28
Start date:	23/03/2022
Path:	C:\Windows\System32\DmNotificationBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\DmNotificationBroker.exe
Imagebase:	0x7ff698c80000
File size:	32256 bytes
MD5 hash:	1643D5735213BC89C0012F0E48253765
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

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

General	
Target ID:	21
Start time:	16:06:34
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\WRsLe\DmNotificationBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\WRsLe\DmNotificationBroker.exe
Imagebase:	0x7ff793f60000
File size:	32256 bytes
MD5 hash:	1643D5735213BC89C0012F0E48253765
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: 00000015.00000002.455715001.00007FFC66921000.00000020.00000001.01000000.0000000C.sdmp, Author: Joe Security

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\WRsLe\DUI70.dll	unknown	1708032	success or wait	1	7FFC6697F8D6	ReadFile

Analysis Process: WFS.exe PID: **4504**, Parent PID: **3968**

General

Target ID:	24
Start time:	16:06:45
Start date:	23/03/2022
Path:	C:\Windows\System32\WFS.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WFS.exe
Imagebase:	0x7ff66bd70000
File size:	930304 bytes
MD5 hash:	CD6ACF3B997099B6CFB2417D3942F755
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: WFS.exe PID: **6212**, Parent PID: **3968**

General

Target ID:	25
Start time:	16:06:47
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\daH0n9\WFS.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\daH0n9\WFS.exe
Imagebase:	0x7ff7e06f0000
File size:	930304 bytes
MD5 hash:	CD6ACF3B997099B6CFB2417D3942F755
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: 00000019.00000002.489503728.00007FFC66971000.00000020.00000001.01000000.0000000E.sdmp, Author: Joe Security

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\daH0n9\credui.dll	unknown	1425408	success or wait	1	7FFC669CF8D6	ReadFile

Analysis Process: DmNotificationBroker.exe PID: **6008**, Parent PID: **3968**

General

Target ID:	30
Start time:	16:07:01
Start date:	23/03/2022
Path:	C:\Windows\System32\DmNotificationBroker.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\DmNotificationBroker.exe
Imagebase:	0x7ff698c80000
File size:	32256 bytes
MD5 hash:	1643D5735213BC89C0012F0E48253765
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: DmNotificationBroker.exe PID: **1804**, Parent PID: **3968**

General

Target ID:	31
Start time:	16:07:07
Start date:	23/03/2022
Path:	C:\Users\user\AppData\Local\pEcAZnNU3\DmNotificationBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\pEcAZnNU3\DmNotificationBroker.exe
Imagebase:	0x7ff6dc630000
File size:	32256 bytes
MD5 hash:	1643D5735213BC89C0012F0E48253765
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: 0000001F.00000002.529541082.00007FFC67881000.00000020.00000001.01000000.00000010.sdmp, Author: Joe Security

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\pEcAZnNU3\DUI70.dll	unknown	1708032	success or wait	1	7FFC678DF8D6	ReadFile

Analysis Process: wusa.exe PID: **6376**, Parent PID: **3968**

General

Target ID:	32
Start time:	16:07:20
Start date:	23/03/2022
Path:	C:\Windows\System32\wusa.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wusa.exe
Imagebase:	0x7ff7378d0000
File size:	308736 bytes
MD5 hash:	04CE745559916B99248F266BBF5F9ED9
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: SystemSettingsRemoveDevice.exe PID: **6408**, Parent PID: **3968**

General

Target ID:	33
Start time:	16:07:21
Start date:	23/03/2022
Path:	C:\Windows\System32\SystemSettingsRemoveDevice.exe
Wow64 process (32bit):	true

Commandline:	C:\Windows\system32\SystemSettingsRemoveDevice.exe
Imagebase:	0xe00000
File size:	39304 bytes
MD5 hash:	87AF711D6518C0CF91560D7C98301BBB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Disassembly

No disassembly