ID: 492860
Sample Name: CiEceGPoOR
Cookbook: default.jbs
Time: 03:54:34
Date: 29/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Windows Analysis Report CiEceGPoOR

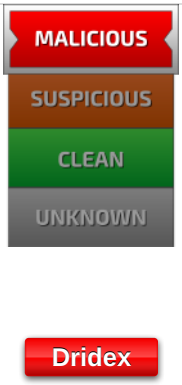
Overview

General Information

Sample Name:	CiEceGPoOR (renamed file extension from none to dll)
Analysis ID:	492860
MD5:	2ab698a4e76087..
SHA1:	300f4d7d2f462da..
SHA256:	3e814c52ab5198..
Tags:	Dridex exe
Infos:	

Most interesting Screenshot:

Detection

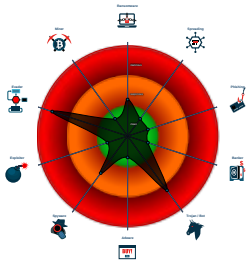


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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 samp…
- Queues an APC in another process …
- Machine Learning detection for dropp…
- Windows Update Standalone Installe…
- Contains functionality to prevent loc…
- Uses Atom Bombing / ProGate to in…

Classification



- **System is w10x64**
- loaddll64.exe (PID: 4956 cmdline: loaddll64.exe 'C:\Users\user\Desktop\CiEceGPoOR.dll' MD5: E0CC9D126C39A9D2FA1CAD5027EBBD18)
  - cmd.exe (PID: 4916 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\CiEceGPoOR.dll',#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 4756 cmdline: rundll32.exe 'C:\Users\user\Desktop\CiEceGPoOR.dll',#1 MD5: 73C519F050C20580F8A62C849D49215A)
      - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - BdeUISrv.exe (PID: 7060 cmdline: C:\Windows\system32\BdeUISrv.exe MD5: 25D86BC656025F38D6E626B606F1D39D)
        - BdeUISrv.exe (PID: 7076 cmdline: C:\Users\user\AppData\Local\f49B\BdeUISrv.exe MD5: 25D86BC656025F38D6E626B606F1D39D)
        - WMPDMC.exe (PID: 496 cmdline: C:\Windows\system32\WMPDMC.exe MD5: 4085FDA375E50214142BD740559F5835)
        - WMPDMC.exe (PID: 476 cmdline: C:\Users\user\AppData\Local\WMp\WMPDMC.exe MD5: 4085FDA375E50214142BD740559F5835)
        - LockScreenContentServer.exe (PID: 3620 cmdline: C:\Windows\system32\LockScreenContentServer.exe MD5: 45E51238434FAF543D66E17EF3783413)
        - LockScreenContentServer.exe (PID: 5012 cmdline: C:\Users\user\AppData\Local\ukxAYmxLA\LockScreenContentServer.exe MD5: 45E51238434FAF543D66E17EF3783413)
        - mspaint.exe (PID: 6932 cmdline: C:\Windows\system32\mspaint.exe MD5: 99F86A0D360FD9A3FCAD6B1E7D92A90C)
        - mspaint.exe (PID: 6940 cmdline: C:\Users\user\AppData\Local\vbVu\mspaint.exe MD5: 99F86A0D360FD9A3FCAD6B1E7D92A90C)
        - SystemPropertiesRemote.exe (PID: 5680 cmdline: C:\Windows\system32\SystemPropertiesRemote.exe MD5: 70E55B55A17F1D1C4047CC678EB936F0)
        - SystemPropertiesRemote.exe (PID: 5868 cmdline: C:\Users\user\AppData\Local\pjo7Mc7ll\SystemPropertiesRemote.exe MD5: 70E55B55A17F1D1C4047CC678EB936F0)
        - AgentService.exe (PID: 6040 cmdline: C:\Windows\system32\AgentService.exe MD5: F7E36C20DB953DFF4FDDB817904C0E48)
        - AgentService.exe (PID: 6064 cmdline: C:\Users\user\AppData\Local\Z7wAQ0\AgentService.exe MD5: F7E36C20DB953DFF4FDDB817904C0E48)
        - wusa.exe (PID: 4368 cmdline: C:\Windows\system32\wusa.exe MD5: 04CE745559916B99248F266BBF5F9ED9)
        - wusa.exe (PID: 4720 cmdline: C:\Users\user\AppData\Local\igQ\wusa.exe MD5: 04CE745559916B99248F266BBF5F9ED9)
  - rundll32.exe (PID: 3228 cmdline: rundll32.exe C:\Users\user\Desktop\CiEceGPoOR.dll,??0?$PatternProvider@VExpandCollapseProvider@DirectUI@@UIExpandCollapseProvider@@$00@DirectUI@@QEAA@XZ MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 2964 cmdline: rundll32.exe C:\Users\user\Desktop\CiEceGPoOR.dll,??0?$PatternProvider@VGridItemProvider@DirectUI@@UIGridItemProvider@@$01@DirectUI@@QEAA@XZ MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5228 cmdline: rundll32.exe C:\Users\user\Desktop\CiEceGPoOR.dll,??0?$PatternProvider@VGridProvider@DirectUI@@UIGridProvider@@$02@DirectUI@@QEAA@XZ MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.339185192.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000027.00000002.541829732.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000020.00000002.455241434.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000000.00000002.274495775.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000023.00000002.481917685.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
Click to see the 7 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

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

Persistence and Installation Behavior:

Windows Update Standalone Installer command line found (may be used to bypass UAC)

HIPS / PFW / Operating System Protection Evasion:

Benign windows process drops PE files

Changes memory attributes in foreign processes to executable or writable

Queues an APC in another process (thread injection)

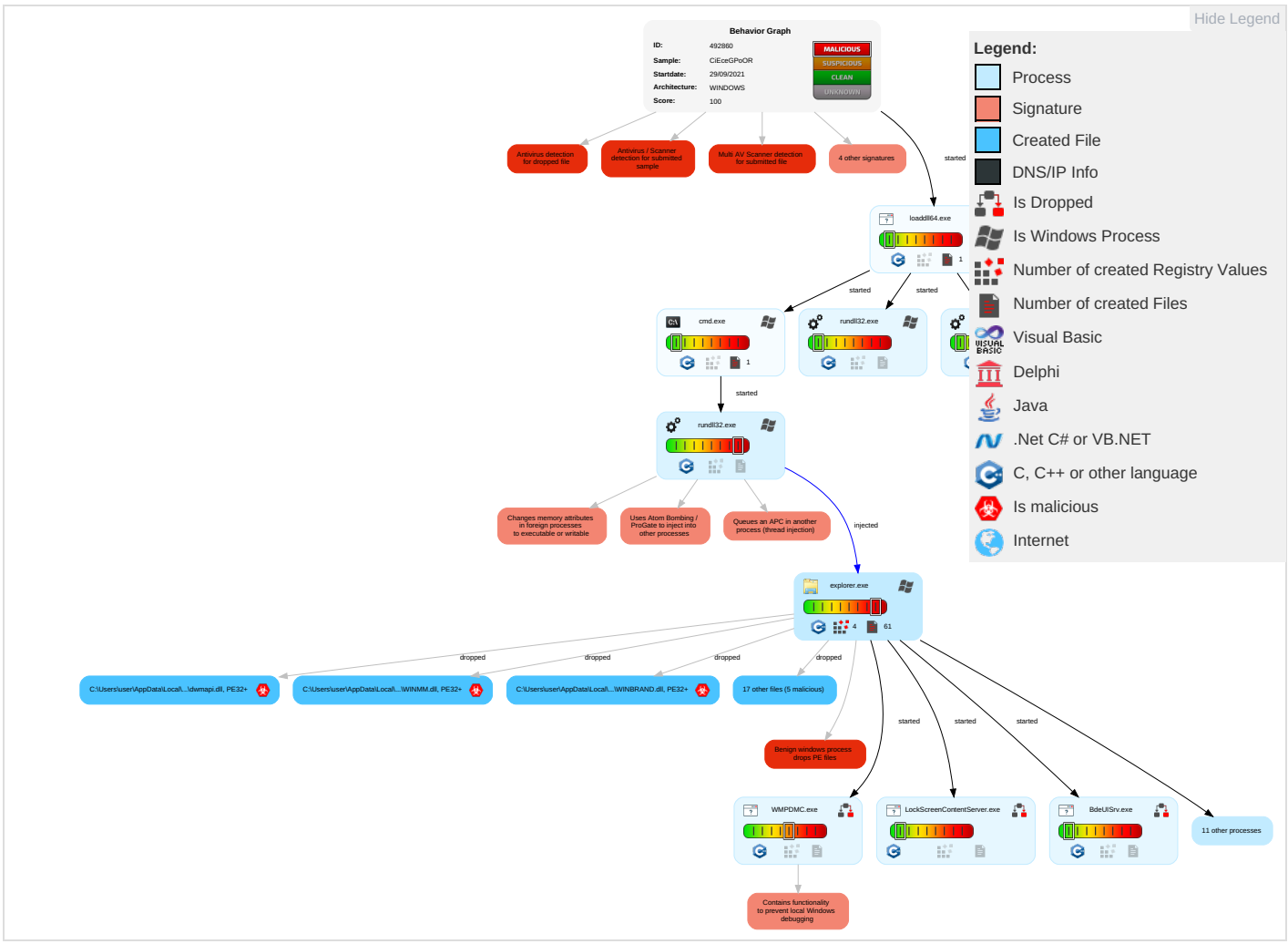
Contains functionality to prevent local Windows debugging

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	Comma and Co
Valid Accounts 1	Command and Scripting Interpreter 1 2	Valid Accounts 1	Valid Accounts 1	Masquerading 1 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Screen Capture 1	Exfiltration Over Other Network Medium	Encrypt Channe
Default Accounts	Service Execution 2	Windows Service 3	Access Token Manipulation 1 1	Valid Accounts 1	LSASS Memory	Security Software Discovery 4 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Junk Da
Domain Accounts	Native API 1	DLL Side-Loading 1	Windows Service 3	Virtualization/Sandbox Evasion 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganc
Local Accounts	Exploitation for Client Execution 1	Logon Script (Mac)	Process Injection 4 1 2	Access Token Manipulation 1 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protoco Imperso
Cloud Accounts	Cron	Network Logon Script	DLL Side-Loading 1	Process Injection 4 1 2	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channe
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multibar Commu
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	System Information Discovery 3 5	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commo Used Pc
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Rundll32 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicat Layer P
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Pr
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Timestomp 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tra Protoco
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	DLL Side-Loading 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Pro

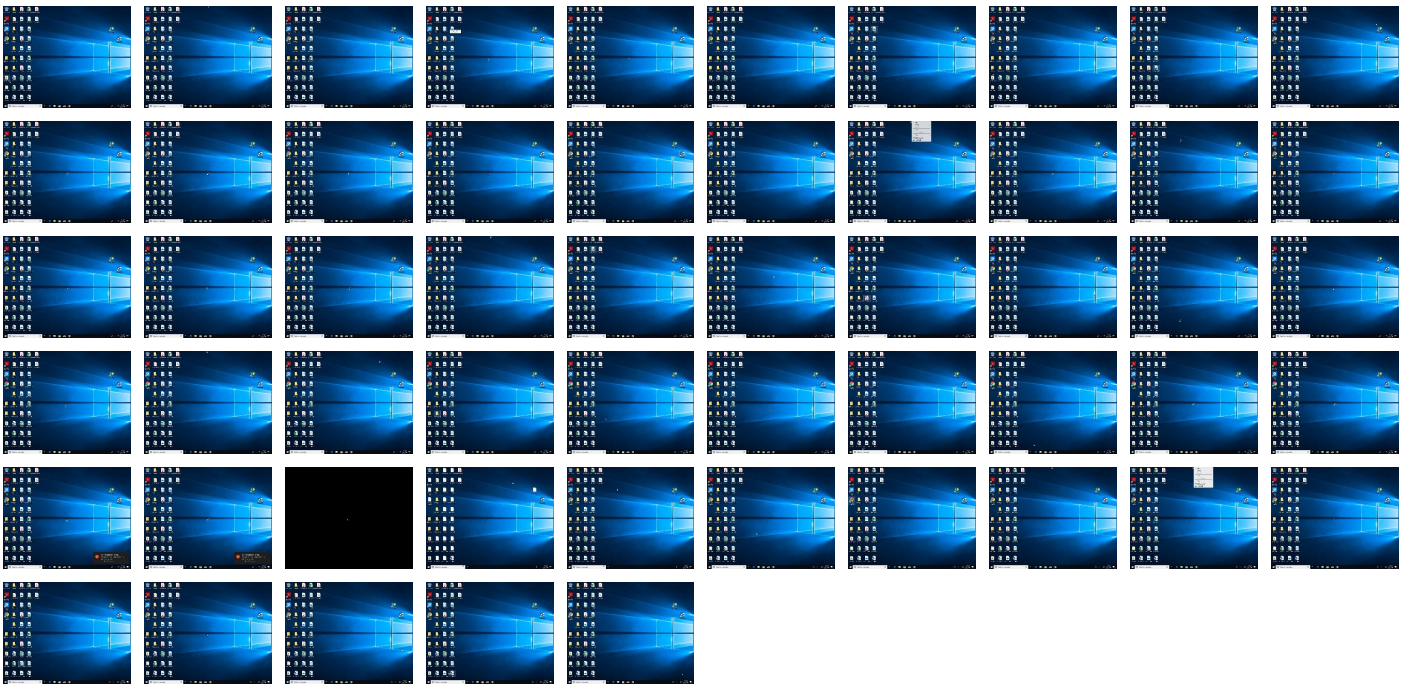
Behavior Graph



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
CiEceGPoOR.dll	57%	Metadefender		Browse
CiEceGPoOR.dll	80%	ReversingLabs	Win64.Infostealer.Dridex	
CiEceGPoOR.dll	100%	Avira	HEUR/AGEN.1114452	
CiEceGPoOR.dll	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\f49B\WTSAPI32.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\ukxAYmxLA\dwmapi.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\Dwpdl\SYSDM.CPL	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\qGdjcQqe\WINBRAND.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\Z7wAQ0\VERSION.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\Dwpdl\SYSDM.CPL	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\uHKs6l\WINMM.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\f49B\WTSAPI32.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\WMp\OLEACC.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\uHKs6l\WINMM.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\f49B\WTSAPI32.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\ukxAYmxLA\dwmapi.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Dwpdl\SYSDM.CPL	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\qGdjcQqe\WINBRAND.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Z7wAQ0\VERSION.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\DwpdI\SYSDM.CPL	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\uHKs6l\WINMM.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\f49B\WTSAPI32.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\WMp\OLEACC.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\uHKs6l\WINMM.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\DwpdI\SystemPropertiesRemote.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\DwpdI\SystemPropertiesRemote.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\WMp\WMPDMC.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\WMp\WMPDMC.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Z7wAQ0\AgentService.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Z7wAQ0\AgentService.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\f49B\BdeUISrv.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\f49B\BdeUISrv.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
37.2.AgentService.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.2.LockScreenContentServer.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.2.WMPDMC.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
39.2.wusa.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.loaddll64.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
32.2.mspaint.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
35.2.SystemPropertiesRemote.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.2.BdeUISrv.exe.140000000.0.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

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	492860
Start date:	29.09.2021
Start time:	03:54:34

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	CiEceGPoOR (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:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@46/21@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 36.1% (good quality ratio 34.7%) • Quality average: 93.9% • Quality standard deviation: 22%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\DwpdI\SYSDM.CPL	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2256896
Entropy (8bit):	3.380894553174277
Encrypted:	false
SSDEEP:	12288:kVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:BfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	EE703BF34E61D2DC59F997A4B44A85C2
SHA1:	DF19CE64F479AC91DFDAD9914CC2259E6D46BFF9
SHA-256:	5FD55D6FFC125DF1D96DD190A7876A085DCF391DA84AD60CCD2F0CEB1A4A52A4
SHA-512:	2B905E221D96D91540AE4348889B6D41C31E5AA2C8F969C447FED2A342C2826FD73A5BD02BAA114194FA5D67DD7B99242954DC0325F0CF69474F21DCAC71E9D
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.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.7 ..DN^....." .....P.....p.....@.....p"....@lx}..b.....`"....c.....h.....$#..... ..... .....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\DwpdI\SystemPropertiesRemote.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	83968
Entropy (8bit):	7.06451035203089
Encrypted:	false
SSDEEP:	1536:g1cZZtREC/rMcgEPJV+G57ThjEC0kzJP+V5JO:NZzECTMpuDhjRVJG8
MD5:	70E55B55A17F1D1C4047CC678EB936F0
SHA1:	1E6EB17BE9961F27280EEF306490A42302495E69
SHA-256:	464B613BF38262C4C088068855B557082D1FCA8F697F8C99D77704471069C32B
SHA-512:	72349FD8FE3F64921ECC442CE2F89DB5831B1F573FB5B68F155FF311EF16555FBEEB0C620CA5DB1E165DA4F2620D0CC879A6DE39640268034B137D120DFCC37
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....$.....%...a..[a..[a..[h..[o..[..Z`..[..Zc..[..Zp..[a..[C..[..Zd..[..Z`..[..q[`..[..Z`..[Richa..[.....PE..d...XF....."....."....>.....@.....F....`..... .....&.....P.. '...@..... ...."..T..... .....!..8.....text..... ..`.rdata..V.... .....@..@.data.....0.....@....pdata.....@.....@..@.rsrc... '...P...(..... .....@..@.reloc.. .....F.....@..B.....

C:\Users\user\AppData\Local\WMp\OLEACC.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2256896
Entropy (8bit):	3.382690286745838
Encrypted:	false
SSDEEP:	12288:LVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:KfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	1B56C69AD8B525F4D3BF6E1AEDF17E6E
SHA1:	F512E6D87B458BC362A7B4EB432BBC55F99603CB
SHA-256:	933602A98EC630126C0FF2ECF13001BC8272AF5C780188955A8510404FAEF361
SHA-512:	8B631F3F51F32171BD82209B75EECA6731011DB3D01A676583D5A893C8ABBB78630F7F4211EE2DFA99482FAA042149977D299844424FB6A9BFC316DEE3EF6A1E
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown

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

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.7 ..DN^....." .....P.....p.....@.....p"....@lx}..b.....`"....c.....h.....$#..... ..... .....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\WMp\WMPDMC.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1517568
Entropy (8bit):	6.62150533612437
Encrypted:	false
SSDEEP:	24576:esSffc55l2PlDph6LYq3BRf6Te8+n3wAJF1/Mk+F6uwY6V0qRr8kmHVJZh/u:cct2PpphUlxRn3wAblMk+F6+6S2r8/Hu
MD5:	4085FDA375E50214142BD740559F5835
SHA1:	22D548F1E0F4832AAEE3D983A156FDABD3021DA4
SHA-256:	93F61516B7FD3CE8F1E97F25B760BDF62AE58CC7714B559FEFC2C75AD1130804
SHA-512:	7712F8E551D475A9D2FF3BED9992A2B3D53AB01F61DCB7313320181F9EB6B5B84558CCA45AE95150267128C8B228F806F869157B7F4961755076DD83F02E3BDF
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....@.....-.....*.....+...../...../.A....'.X.....,....Rich..... .....PE..d...D..9....."..... .....@.....`..... ..... ..x.....l.....0...S..`Y..T.....G..(....F.....8G..... .....text..... ..`.rdata..Pg.....h.....@..@.data...p=...@.....,.....@....pdata..l.....D.....@..@.didat.....@.... rsrc...x.... .....@..@.reloc...S...0...T.....@..B..... .....

C:\Users\user\AppData\Local\Z7wAQ0\AgentService.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1189376
Entropy (8bit):	6.169931271903684
Encrypted:	false
SSDEEP:	24576:+pL4Q4y94x7ZWe6b1B5l2M62kM0s1vt2txc/viVO1IORNfLc:uL4Q3S9b6b1UA9MPwOR5c
MD5:	F7E36C20DB953DFF4FDDB817904C0E48
SHA1:	8C6117B5DD68D397FD7C32F4746FB9B353D5DAE5
SHA-256:	2C5EDE0807D8A5EC4B6E0FE0C308B37DBBDE12714FD9ADC4CE3EF4E0A5692207
SHA-512:	32333A33DECD1AF0915FFDC48DA99831DA345010A91630C5245F2548939E33157F6151F596C09D0BEEAC3F15F08F79D4EEF4FAA4158BA023DEDFC4F6F6F56DF
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....$.....:K..[%M.[%M.[%M.?&L.[%M.? L.[%M.?!L.[%M.?$L.[%M.[$M .Z%M.?,L.[%M.?.M.[%M.?'L.[%MRich.[%M.....PE..d...m.>I....."....B.....@.....=...`..... .....P.. ... .....x.....`..`...p-..T.....pI..(...pH.....I.....text...L..... ..`.rdata..| ....."....@..@.data...@....@...r..".....@....pdata ...x.....z.....@..@.rsrc... ....P.....@..@.reloc..`...`.....@..B..... .....

C:\Users\user\AppData\Local\Z7wAQ0\VERSION.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2256896
Entropy (8bit):	3.3813315171863225
Encrypted:	false
SSDEEP:	12288:OVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:TfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	1561A1A689F95195D6D24DADD60ACA89
SHA1:	520410E244597D00A4FE8AACDBE064B3DD370F96
SHA-256:	DEAEE22737295F5A0F47F62C91F20CE80614BDBA967FED48C99ADADE428B1406
SHA-512:	6C95EB2724D51FF70FE663647B4D4BEA189A646D742AA6D2EFF9E3F5892BB5EB052351CCA58B189311D73CD883F2493B9F6AECABF7963210F8E787747443CED A
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%

C:\Users\user\AppData\Local\Z7wAQ0\VERSION.dll	
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.7 ..DN^....." .....P.....p.....@.....p"....@\|x}..b.....`".+....c.....h.....$#..... ..... .....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\f49B\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
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....$.....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\f49B\WTSAPI32.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2256896
Entropy (8bit):	3.3874708703184213
Encrypted:	false
SSDEEP:	12288:sVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:ZfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	2E52AF8975EFA854E1683B74463B6913
SHA1:	A463E30799756FBC830F2F2876EC30AC10CB26BA
SHA-256:	A51730C6B2A93621290BCAB6EC90D1FB72EC90D4C4E24B2A11CD04FF3C16909F
SHA-512:	D5A79940CE2FD45DD946E9D0192F8902B3DBEB44A49E77FDFB293398CB5AE873B1109B63CB066848BDF4962C4BF917381EB8F5BEC364CAAA8C14BF21E57F2C 89
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.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.7 ..DN^....." .....P.....p.....@.....p"....@\|x}..b.....`".....c.....h.....$#..... ..... .....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\igQ\WTSAPI32.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2256896
Entropy (8bit):	3.387421868586717
Encrypted:	false
SSDEEP:	12288:nVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:OfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	0D2066DE3B0C48AC2327A0FE775FFE6A
SHA1:	522F2FB0DBE0C7109DE245227FC8BFCAA943860A
SHA-256:	14DFF84D1E8A1AF2B2DC387E9484A9DA800214AC5496119DF35E59A0B556441F
SHA-512:	447D722785D2A33232F0B58B1EE4293F653C2A7F6C32AFB3737D0142FE80A665A86912E479D5780985E74C8F394B31175A65000EB0BD3C7AA788DD91587F98CF
Malicious:	false

C:\Users\user\AppData\Local\igQ\WTSAPI32.dll	
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.7 ..DN^....." .....P.....p.....@.....p"....@lx}..b.....`"....c.....h.....$#..... ..... .....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\igQ\wusa.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	308736
Entropy (8bit):	6.55894801361276
Encrypted:	false
SSDEEP:	6144:TozDd3UafMCFoMVclxM8cVM49UApxyN90vE:ToXd33MCFoqSxM5MmUAy90
MD5:	04CE745559916B99248F266BBF5F9ED9
SHA1:	76FA00103A89C735573D1D8946D8787A839475B6
SHA-256:	1D86701A861FFA88FE050A466E04281A4809C334B16832A84231DC6A5FBC4195
SHA-512:	B4D2EF6B90164E17258F53BCAF954076D02EDB7F496F4F79B2CF7848B90614F6160C8EB008BA5904521DD8B1449840B2D7EE368860E58E01FBEAB9873B654B3A
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;..-..~..~..~v./~}.~....}.~....i.~....{.~....d.~..~w.~....k.~..C~~.~.... ~.~Rich..~.....PE..d.....TS....."....`...X.....f.....@.....g....`..... .....I.....T...p.....`....?..T.....Pq..(. ..Pp.....xq..@.....text...3^.....`..... ..`.rdata..^....p.....d.....@..@.data.....`.....T.....@....pdata.....p.....X.....@..@.rsrc....T .....V...^.....@..@.reloc..`.....@..B..... .....

C:\Users\user\AppData\Local\pjo7Mc7Il\SYSDM.CPL	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2256896
Entropy (8bit):	3.3808861421525056
Encrypted:	false
SSDEEP:	12288:3VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:+fP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	3AA64EB2847BBCE9E3C31FA18E7B9F5D
SHA1:	E749026A2F54435991838F4EE146A346A342BA58
SHA-256:	178D81184F3C327ED2BF276E3D00E6C6F3415EEFEA6B3AD6487D038477FCEEDF
SHA-512:	EF128F3770DA7A1B2D2B7E05C305DE5FFECF1D6E4B74C72366A2A0B15545EC0F998DAF3C966E735F89337604B0739A81964C463C37F65127B2C2013D0B8918FE
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.7 ..DN^....." .....P.....p.....@.....p"....@lx}..b.....`"....c.....h.....$#..... ..... .....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\pjo7Mc7Il\SystemPropertiesRemote.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	83968
Entropy (8bit):	7.06451035203089
Encrypted:	false
SSDEEP:	1536:g1cZZtREC/rMcgEPJV+G57ThjEC0kzJP+V5JO:NZzECTMpuDhjRVJG8
MD5:	70E55B55A17F1D1C4047CC678EB936F0
SHA1:	1E6EB17BE9961F27280EEF306490A42302495E69
SHA-256:	464B613BF38262C4C088068855B557082D1FCA8F697F8C99D77704471069C32B
SHA-512:	72349FD8FE3F64921ECC442CE2F89DB5831B1F573FB5B68F155FF311EF16555FBEEB0C620CA5DB1E165DA4F2620D0CC879A6DE39640268034B137D120DFCC37
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%...a..[a..[a..[h..[o..[..Z`..[..Zc..[..Zp..[a..[C..[..Zd..[..Z`..[..q[`..[..Z`..[Richa..[.....PE..d...XF....."....."....>.....@.....F.....`..... .....&.....P.. '...@..... ...."..T..... .....!..8.....text..... ..`.rdata..V.... .....@..@.data.....0.....@....pdata.....@.....@..@.rsrc... '...P...(..... .....@..@.reloc.. .....F.....@..B..... .....

C:\Users\user\AppData\Local\qGdjcQqe\WINBRAND.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2256896
Entropy (8bit):	3.3812520581221097
Encrypted:	false
SSDEEP:	12288:VVl0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:MfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	06FA4A77517150DC152DD03EF202812D
SHA1:	9891B2A841F9EC52F80343AFC0676731492A8ABA
SHA-256:	EFD60F575EDAFA67104912C5398578C69CFCC4618ABD4A4AA29C8A7C1628122D
SHA-512:	B65C1944DD4E0BD2360BF3AAF884A7D6FA3E931EE521CF9A1F8256D7716FFA1DFA8330286BD67FFB48A5C1187AA61B6C4CD680C5B29757E9105EFAA6EABA26D9
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.7..DN^....." .....P.....p.....@.....p".....@lx}..b.....`".....c.....h.....$#..... .....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\qGdjcQqe\pwcreator.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	800768
Entropy (8bit):	5.701025089752158
Encrypted:	false
SSDEEP:	24576:TD+9c2wgjOGTtUNbYYotGatTAcBg9okYyW:kc2wg6GTtUNsAaScBgWDy
MD5:	BF33FA218E0B4F6AEC77616BE0F5DD9D
SHA1:	F3F0A424406B743410F6E5C72209979AC9537FAE
SHA-256:	E7760E07BE5CF608CC10FDDF0AB21E765F36962372BF9DA4360DCB196E08425D
SHA-512:	8BF912B8785DE97757F862A0C327A6BC921A895C79C8D6D593BA79C5450D12382A511BF974A2C01A183CCFA0F612AC4A80D6F346058ED1FB694ED71A43B1122
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... ...NI..NI..NI..MH..NI..JH..NI..KH..NI..OH..NI..OIa~NI..GH,.NI...I..NI..LH..NIRich..NI.....PE..d....._....."..... .....'.....@.....?...`..... .....x6..|.....a.....B.....p.....P...T.....P.....P...(.....text...Q..... ..`.rdata.....@..@.data...`...p.....T.....@....pdata...B.....D.....@..@.rsrc....a....b.....@..@.reloc.....p.....(.....@..B.....

C:\Users\user\AppData\Local\uHKs6l\Narrator.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	349696
Entropy (8bit):	6.567354682144278
Encrypted:	false
SSDEEP:	3072:2v1g/YrkRsWlO3nWOgV1M2uMFS/BaMiXbAJUoTq7XLtqkXIJA9QD4hLtcRiWh6f3:2vSckvCWOgB6YsyzZBL+RQFgZKUV
MD5:	56036993FB96C42F30C443A11BD56F4D
SHA1:	93367421725D818963F337F179EE61710BB2ABD3
SHA-256:	D3A728CFC32D43A9C96A45EFE6B3B7A21A8435F758C1C382978047982B6ADBB0
SHA-512:	E3DBC40DC7717BB9EC31657126FFA29D69362EE570BAC3D5B31918876261CF9E6954FDB31C2145788FF186E01A29A1696B914B626797CC8BC46F5FCB43D90F2
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....E[...[...[...R.B.S...4...U...4...X...4...E...4...B...[.....4...q...4..,.Z...4...Z...4...Z...Rich[.....PE..d.....".....V.....5.....@.....GV....`..... .....H>..T.....T..... .....P.....text....U.....V..... ..`.rdata..p2...p...4...Z.....@..@.data...h.....@....pdata.....@..@.rsrc.....@..@.reloc.....N.....@..B.....

C:\Users\user\AppData\Local\uHKs6l\WINMM.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped

C:\Users\user\AppData\Local\uHKs6l\WINMM.dll	
Size (bytes):	2260992
Entropy (8bit):	3.3902758972646265
Encrypted:	false
SSDEEP:	12288:UVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:RfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	BE85B26E12C6BFA0503499448FD81878
SHA1:	B12FDE317045637F7FF332C8FF422CFE5FFE7BDB
SHA-256:	9A6A55C16D44315902FAFB6FE507AF04CB7CD8A3F1286DB3C9ED030C6430947E
SHA-512:	B007EB34865787E8A40CFB6BD4F2D83F6985EA74E2A87ABB8CCBD1403D468607685E1863F155E956EBA3CDA04DCD3C0658DF140FF602D0E8864F5076DE638B5D
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.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.7..DN^......" .....`.....p.....@.....".....@lx}..b.....`".h....c.....h.....$#..... .....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\ukxAYmxLA\LockScreenContentServer.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	47600
Entropy (8bit):	6.182394161787695
Encrypted:	false
SSDEEP:	768:0SD9dkiWX/i7Ek29r9Hu53ldEkUZGYP7loL1Prco:pVKFudldlUZGYP7loPwo
MD5:	45E51238434FAF543D66E17EF3783413
SHA1:	1CE0BA884E5C2ADA74A34D10F32A5E7431C66411
SHA-256:	DAFF63C2C374463E0CF476B5CBADF2D58D0DADE0BB0C29DDAE543A69BA34FB93
SHA-512:	353467F3477B136909C1AD0206A3E9CA84AC9104B386529345BBEBABFCA1B3239F6C0B387C2C1018B937885144D43ACAADA264EB4D266B815A632A3DFEDEB331
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....4E..gE..gE..gL.4gg..g*..fG..g*..fQ..g*..fB..g*..fT..gE..g...g*..fC..g*.XgD..g*..fD..gRichE..g.....PE..d...|dV....."....>...Z.....@.....@.....`..... .....h..... .....#.....L....a..T. .....U..(....T.....U.....text....<.....>..... ..`.rdata..`@...P...B...B.....@..@.data.....@....pdata.....@..@.rsrc... .....@..@.reloc..L.....@..B.....

C:\Users\user\AppData\Local\ukxAYmxLA\dwmapi.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2256896
Entropy (8bit):	3.3857591682018664
Encrypted:	false
SSDEEP:	12288:iVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:/fP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	12B57CCEEB262F2166C8F5A2F255ABCE
SHA1:	C53EE689A89C945AE1065152258DDB0C49620E5D
SHA-256:	3DE50E5768723366E847A5F1076086F7DB7A6CDF9A564FF247043531B6162386
SHA-512:	08068C34FD911B25C43EC11E579C3D5CAD6AE8A27D6BA8D8B3F5267F59C3F0B700EA2FE135444D3B011D9A9DB63DADC5051204BB681703A02ED6FF22F6F70C8
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.7..DN^....." .....P.....p.....@.....p"....@lx}..b.....`".&....c.....h.....$#..... .....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\vbVu\WINMM.dll	
Process:	C:\Windows\explorer.exe

C:\Users\user\AppData\Local\vbVu\WINMM.dll	
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2260992
Entropy (8bit):	3.390257188753584
Encrypted:	false
SSDEEP:	12288:WVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:LfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	B6BF5C2E91887A902462C7E8621E0004
SHA1:	5EF91A0F0E0DBBB56E9B55EAD19BEAA3CA6C678B
SHA-256:	7A25516846C100F6954FA8A40D73F0834F3D8FC4BE872F53DDA16F11951B853C
SHA-512:	52E7431379523CC35512FF391FB86ADE97F5F8B89F0D96781A180C52EDDB33811D4BC84D31790B924FC560E1916C368EC060AFAD6115052E4967181CD6837EEE
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.7 ..DN^....." .....`.....p.....@....."....@lx}..b.....`".h....c.....h.....$#..... ....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\vbVu\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/gQw4MIlawYVb7jP8v
MD5:	99F86A0D360FD9A3FCAD6B1E7D92A90C
SHA1:	65F36247C0FFBB881947F68B352128C0C9CFCBE5
SHA-256:	D46519B76D09DFF8BC5C7B34A4E73AD8E7CF6E4C40BDAD6C769E34A099ECE017
SHA-512:	5071487AA218712FBA3A1FCEA6A810C3B27D26A145BC728315CA8078B6A88E51989038CAE4F5EE494B1FEE7515C6E86742D280D1A763B044BDBE7D2E360124A
Malicious:	false
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\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\89dad5d484a9f889a3a8dfca823edc3e_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	4447
Entropy (8bit):	5.485455297414369
Encrypted:	false
SSDEEP:	48:JZC1UowElfeoaBJOQfbe+uowEViZC1UowEsxOvNeGQotxnToRowEMhgB:JcB3lfefJOQfy+X3VicB3sU9fTou3MiB
MD5:	94883D0CAF88428A2154B4F79D3E2671
SHA1:	4990F6F80F7422B65130FF1D54DBB1B9EDE66F09
SHA-256:	BD29BBB8364271950A6B4BD3119F038011F0A5FF3042462D403784837EBA53CF
SHA-512:	9456E0E76003FC754D686752771E6A10C69F7D7666483A903C7591723B5E738F11A3F8CCD2DCF9C78059DF66853DA0E00B32CA9EB386ADE9F742D04D35C11923
Malicious:	false
Reputation:	unknown
Preview:	.....user.....user.....RSA1.....).....):...J..X.m1.).de._8.]..9..4.=s.s...lG.7G.Uf.J..+.....j.i.]A.%m+\-X.....{ ..b....em...S`.9.I...'..P.....z..O.....E..._D.2...".....,...C.r.y.p.t.o.A.P.I. .P.r.i.v.a.t.e. .K.e.y....f..... ...K..Ye..".....6.W.(.....2e.4=..... ....*zN.Z.....X.]{...=. H_.....1.u?.....+(...T.. 1..&.(.`!.....G.l.....uS...@..E..V.TZ....._.v.....ok.....&..>eL...`.C.}./Z..u/..^..0.#..ucJ.M9.s.=...N...*.L..L..]....d..b.E]..6...p....@7....Z..r..n.n.,v.5..asogC.... um+8..i.5..._)...O.s.H.c.....V.H...)..!.s{/...m.a.4..~!.../.#7..9....%-q0*....]..*...a.TN.. ..\..p..w..C...L.....+ .j.}1...%.|t.J...g.~... .>...}..!....r.c._.Y.zE}.3... ...=...r~M.1....E.Y#3.W. ..@....~.J...}.0.cU..o...m.7'..\y[..M.@! .....~L.&]).?+9..v,~.o.(.c...i....2.....H.L.u.;\q....U.I....f>..B`..5... #/[.

Static File Info

General

General

File type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Entropy (8bit):	4.317932567104927
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:	CiEceGPoOR.dll
File size:	2252800
MD5:	2ab698a4e7608708ae2a693966194322
SHA1:	300f4d7d2f462dac7e6ab333d8783bab4f371316
SHA256:	3e814c52ab51985ebaf91bff6baeb9eab08c85529bf09f4a069803a4ee984572
SHA512:	2bdce7f070a92e50089af42f087a18516cc465c45169d9877337f8cdd4d93abcdb227c0c55bc29625db1ad28c299f96c5482b0e4e8329a027b92a6aa9c420623
SSDEEP:	12288:wVI0W/TtlPLfJCm3WlYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1Cp3A:1fP7fWsK5z9A+WGAW+V5SB6Ct4bnbW
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....|...|...|....K.#}...'...}.....{}....X.#}....f..|....g..}..*...a|.....}....N..}..*...E}..[.I.E|...'..U}....N.+}..[.K.P|.

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x140041070
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x140000000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x5E4E44CC [Thu Feb 20 08:35:24 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:	6668be91e2c948b183827f040944057f

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x40796	0x41000	False	0.776085486779	data	7.73364605679	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x42000	0x64f2c	0x65000	False	0.702390160891	data	7.86574512659	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0xa7000	0x178b8	0x18000	False	0.0694580078125	data	3.31515306295	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0xbf000	0x12c	0x1000	False	0.06005859375	PEX Binary Archive	0.581723022719	IMAGE_SCN_TYPE_DSECT, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0xc0000	0x880	0x1000	False	0.139892578125	data	1.23838501563	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xc1000	0x2324	0x3000	False	0.0498046875	data	4.65321444248	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.qkm	0xc4000	0x74a	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.cvjb	0xc5000	0x1e66	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tlmkv	0xc7000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.wucsxe	0xc8000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.fltwtj	0x10e000	0x1267	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.sfplio	0x110000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rpg	0x111000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bewzc	0x157000	0x1124	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vksvaw	0x159000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.wmhg	0x15a000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.kswemc	0x15c000	0x36d	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.kaxfk	0x15d000	0x197d	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pjf	0x15f000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.retjqj	0x160000	0x7fd	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.mizn	0x161000	0x9cd	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrub	0x162000	0x197d	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.susbqq	0x164000	0x6cd0	0x7000	False	0.00177873883929	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.jeojcw	0x16b000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vwl	0x16c000	0xae7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.mub	0x16d000	0x6cd0	0x7000	False	0.00177873883929	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.xwxpmb	0x174000	0x573	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
.aea	0x175000	0x7fd	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.lwpch	0x176000	0x7fd	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.nzgp	0x177000	0x1f7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.qimx	0x178000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.jbqbr	0x179000	0x1f7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.kxxxil	0x17a000	0xbf6	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.drpaa	0x17b000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.lepjc	0x17c000	0x1f7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.txam	0x17d000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vqjcpr	0x1c3000	0x128f	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vvwma	0x1c5000	0x6cd0	0x7000	False	0.00177873883929	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pinm	0x1cc000	0x6ec	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.eowj	0x1cd000	0xbf6	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.dzlhaa	0x1ce000	0x896	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ncnf	0x1cf000	0x42a	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vqes	0x1d0000	0x1124	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rtu	0x1d2000	0x197d	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.qlvquw	0x1d4000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.nzjn	0x1d5000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.dfwg	0x1d7000	0x1e66	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.zypdk	0x1d9000	0x5a7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ufvfoh	0x1da000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.efst	0x1db000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.dfk	0x1dc000	0x5a7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.mxubr	0x1dd000	0x197d	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.zqcgin	0x1df000	0x2da	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
.cxkr	0x1e0000	0x451c2	0x46000	False	0.218610491071	data	5.76270152146	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

Version Infos

Possible Origin

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

Network Behavior

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: 4956 Parent PID: 804

General

Start time:	03:55:35
Start date:	29/09/2021
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe 'C:\Users\user\Desktop\CiEceGPoOR.dll'
Imagebase:	0x7ff7859f0000
File size:	1136128 bytes
MD5 hash:	E0CC9D126C39A9D2FA1CAD5027EBBD18

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: 00000000.00000002.274495775.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 4916 Parent PID: 4956

General

Start time:	03:55:36
Start date:	29/09/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\CiEceGPoOR.dll',#1
Imagebase:	0x7ff7eef80000
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 Show Windows behavior

Analysis Process: rundll32.exe PID: 4756 Parent PID: 4916

General

Start time:	03:55:36
Start date:	29/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe 'C:\Users\user\Desktop\CiEceGPoOR.dll',#1
Imagebase:	0x7ff786160000
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: 00000002.00000002.339185192.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 3228 Parent PID: 4956

General

Start time:	03:55:36

Start date:	29/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\CiEceGPoOR.dll,??0?$PatternProvider@VExpandCollapseProvider@DirectUI@@UIExpandCollapseProvider@@$00@DirectUI@@QEAA@XZ
Imagebase:	0x7ff786160000
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: 00000003.00000002.253536981.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3472 Parent PID: 4756

General

Start time:	03:55:38
Start date:	29/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: rundll32.exe PID: 2964 Parent PID: 4956

General

Start time:	03:55:40
Start date:	29/09/2021

Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\CiEceGPoOR.dll,??0?$PatternProvider@VGridItem Provider@DirectUI@@UIGridItemProvider@@$01@DirectUI@@QEAA@XZ
Imagebase:	0x7ff786160000
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: 00000007.00000002.260833878.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 5228 Parent PID: 4956

General

Start time:	03:55:43
Start date:	29/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\CiEceGPoOR.dll,??0?$PatternProvider@VGridProv ider@DirectUI@@UIGridProvider@@$02@DirectUI@@QEAA@XZ
Imagebase:	0x7ff786160000
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: 0000000A.00000002.268716589.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: BdeUISrv.exe PID: 7060 Parent PID: 3472

General

Start time:	03:56:20
Start date:	29/09/2021
Path:	C:\Windows\System32\BdeUISrv.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\BdeUISrv.exe
Imagebase:	0x7ff7312e0000
File size:	52736 bytes
MD5 hash:	25D86BC656025F38D6E626B606F1D39D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: BdeUISrv.exe PID: 7076 Parent PID: 3472

General

Start time:	03:56:21
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\f49B\BdeUISrv.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\f49B\BdeUISrv.exe
Imagebase:	0x7ff7caa60000
File size:	52736 bytes
MD5 hash:	25D86BC656025F38D6E626B606F1D39D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000016.00000002.369765886.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: WMPDMC.exe PID: 496 Parent PID: 3472

General

Start time:	03:56:33
Start date:	29/09/2021
Path:	C:\Windows\System32\WMPDMC.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WMPDMC.exe
Imagebase:	0x7ff6c7670000
File size:	1517568 bytes
MD5 hash:	4085FDA375E50214142BD740559F5835
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WMPDMC.exe PID: 476 Parent PID: 3472

General

Start time:	03:56:34
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\WMp\WMPDMC.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\WMp\WMPDMC.exe
Imagebase:	0x7ff71e310000
File size:	1517568 bytes
MD5 hash:	4085FDA375E50214142BD740559F5835
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: 00000018.00000002.396379510.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

File Activities Show Windows behavior

File Read

Analysis Process: LockScreenContentServer.exe PID: 3620 Parent PID: 3472

General

Start time:	03:56:45
Start date:	29/09/2021
Path:	C:\Windows\System32\LockScreenContentServer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\LockScreenContentServer.exe
Imagebase:	0x7ff605300000
File size:	47600 bytes
MD5 hash:	45E51238434FAF543D66E17EF3783413
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: LockScreenContentServer.exe PID: 5012 Parent PID: 3472

General

Start time:	03:56:46
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\ukxAYmxLA\LockScreenContentServer.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\ukxAYmxLA\LockScreenContentServer.exe
Imagebase:	0x7ff755d00000
File size:	47600 bytes
MD5 hash:	45E51238434FAF543D66E17EF3783413
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000001C.00000002.424243110.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities Show Windows behavior

File Read

Analysis Process: mspaint.exe PID: 6932 Parent PID: 3472

General

Start time:	03:56:59
Start date:	29/09/2021
Path:	C:\Windows\System32\mspaint.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\mspaint.exe

Imagebase:	0x7ff7308c0000
File size:	6780928 bytes
MD5 hash:	99F86A0D360FD9A3FCAD6B1E7D92A90C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: mspaint.exe PID: 6940 Parent PID: 3472

General

Start time:	03:57:00
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\vbVu\mspaint.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\vbVu\mspaint.exe
Imagebase:	0x7ff67b100000
File size:	6780928 bytes
MD5 hash:	99F86A0D360FD9A3FCAD6B1E7D92A90C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000020.00000002.455241434.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: SystemPropertiesRemote.exe PID: 5680 Parent PID: 3472

General

Start time:	03:57:13
Start date:	29/09/2021
Path:	C:\Windows\System32\SystemPropertiesRemote.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SystemPropertiesRemote.exe
Imagebase:	0x7ff74b730000
File size:	83968 bytes
MD5 hash:	70E55B55A17F1D1C4047CC678EB936F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: SystemPropertiesRemote.exe PID: 5868 Parent PID: 3472

General

Start time:	03:57:14
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\pjo7Mc7Il\SystemPropertiesRemote.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\pjo7Mc7Il\SystemPropertiesRemote.exe
Imagebase:	0x7ff7376b0000
File size:	83968 bytes
MD5 hash:	70E55B55A17F1D1C4047CC678EB936F0
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: 00000023.00000002.481917685.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: AgentService.exe PID: 6040 Parent PID: 3472

General

Start time:	03:57:26
Start date:	29/09/2021
Path:	C:\Windows\System32\AgentService.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\AgentService.exe
Imagebase:	0x7ff73ca90000
File size:	1189376 bytes
MD5 hash:	F7E36C20DB953DFF4FDDB817904C0E48
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: AgentService.exe PID: 6064 Parent PID: 3472

General

Start time:	03:57:28
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\Z7wAQ0\AgentService.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Z7wAQ0\AgentService.exe
Imagebase:	0x7ff7a3460000
File size:	1189376 bytes
MD5 hash:	F7E36C20DB953DFF4FDDB817904C0E48
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: 00000025.00000002.514511264.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: wusa.exe PID: 4368 Parent PID: 3472

General

Start time:	03:57:41
Start date:	29/09/2021
Path:	C:\Windows\System32\wusa.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wusa.exe
Imagebase:	0x7ff6293e0000
File size:	308736 bytes
MD5 hash:	04CE745559916B99248F266BBF5F9ED9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: wusa.exe PID: 4720 Parent PID: 3472

General

Start time:	03:57:42
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\igQ\wusa.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\igQ\wusa.exe
Imagebase:	0x7ff778ca0000
File size:	308736 bytes
MD5 hash:	04CE745559916B99248F266BBF5F9ED9
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: 00000027.00000002.541829732.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Disassembly

Code Analysis