ID: 492806
Sample Name: A1ogRC4R34
Cookbook: default.jbs
Time: 01:51:45
Date: 29/09/2021
Version: 33.0.0 White Diamond

Table of Contents

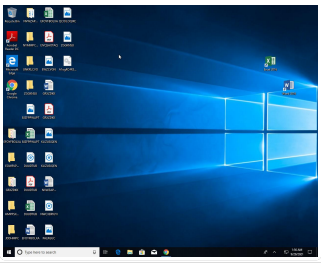
Windows Analysis Report A1ogRC4R34

Overview

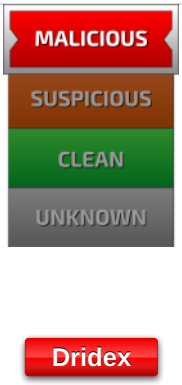
General Information

Sample Name:	A1ogRC4R34 (renamed file extension from none to dll)
Analysis ID:	492806
MD5:	5edd6ba336c4de..
SHA1:	af181a8f3fe25a5…
SHA256:	eda8c025e5f5f67..
Tags:	Dridex exe
Infos:	

Most interesting Screenshot:



Detection

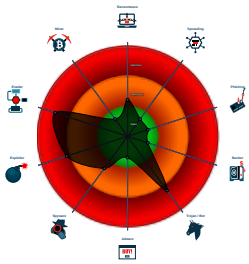


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- Accesses ntoskrnl, likely to find offs…
- Uses Atom Bombing / ProGate to in…
- Queries the volume information (nam…
- Uses code obfuscation techniques (…
- PE file contains sections with non-s…
- Queries the installation date of Wind…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 7096 cmdline: loaddll64.exe 'C:\Users\user\Desktop\A1ogRC4R34.dll' MD5: E0CC9D126C39A9D2FA1CAD5027EBBD18)
  - cmd.exe (PID: 3192 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\A1ogRC4R34.dll',#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 6396 cmdline: rundll32.exe 'C:\Users\user\Desktop\A1ogRC4R34.dll',#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6408 cmdline: rundll32.exe C:\Users\user\Desktop\A1ogRC4R34.dll,LogonIdFromWinStationNameA MD5: 73C519F050C20580F8A62C849D49215A)
    - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - rdpinit.exe (PID: 6372 cmdline: C:\Windows\system32\rdpinit.exe MD5: EF7C9CF6EA5B8B9C5C8320990714C35D)
      - rdpinit.exe (PID: 5620 cmdline: C:\Users\user\AppData\Local\fID\rdpinit.exe MD5: EF7C9CF6EA5B8B9C5C8320990714C35D)
      - DmNotificationBroker.exe (PID: 4592 cmdline: C:\Windows\system32\DmNotificationBroker.exe MD5: 1643D5735213BC89C0012F0E48253765)
      - DmNotificationBroker.exe (PID: 5212 cmdline: C:\Users\user\AppData\Local\uBsjD\DmNotificationBroker.exe MD5: 1643D5735213BC89C0012F0E48253765)
      - BitLockerWizardElev.exe (PID: 4916 cmdline: C:\Windows\system32\BitLockerWizardElev.exe MD5: 3104EA9ECCA9ED71A382CCAAD618CEAE)
      - BitLockerWizardElev.exe (PID: 6400 cmdline: C:\Users\user\AppData\Local\r7RKh\BitLockerWizardElev.exe MD5: 3104EA9ECCA9ED71A382CCAAD618CEAE)
      - wusa.exe (PID: 3676 cmdline: C:\Windows\system32\wusa.exe MD5: 04CE745559916B99248F266BBF5F9ED9)
      - wusa.exe (PID: 964 cmdline: C:\Users\user\AppData\Local\H3fqckDRC\wusa.exe MD5: 04CE745559916B99248F266BBF5F9ED9)
      - SystemPropertiesAdvanced.exe (PID: 6548 cmdline: C:\Windows\system32\SystemPropertiesAdvanced.exe MD5: 82ED6250B9AA030DDC13DC075D2C16E3)
      - SystemPropertiesAdvanced.exe (PID: 6656 cmdline: C:\Users\user\AppData\Local\3HlyM7czl\SystemPropertiesAdvanced.exe MD5: 82ED6250B9AA030DDC13DC075D2C16E3)
      - unregmp2.exe (PID: 7140 cmdline: C:\Windows\system32\unregmp2.exe MD5: 9B517303C58CA8A450B97B0D71594CBB)
  - rundll32.exe (PID: 6492 cmdline: rundll32.exe C:\Users\user\Desktop\A1ogRC4R34.dll,LogonIdFromWinStationNameW MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 3684 cmdline: rundll32.exe C:\Users\user\Desktop\A1ogRC4R34.dll,RemoteAssistancePrepareSystemRestore MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000028.00000002.476229981.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000007.00000002.248393203.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000003.00000002.327777249.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000018.00000002.356788011.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
0000001F.00000002.390772898.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
Click to see the 5 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

Exploits:

Accesses ntoskrnl, likely to find offsets for exploits

E-Banking Fraud:

Yara detected Dridex unpacked file

HIPS / PFW / Operating System Protection Evasion:

Benign windows process drops PE files

Changes memory attributes in foreign processes to executable or writable

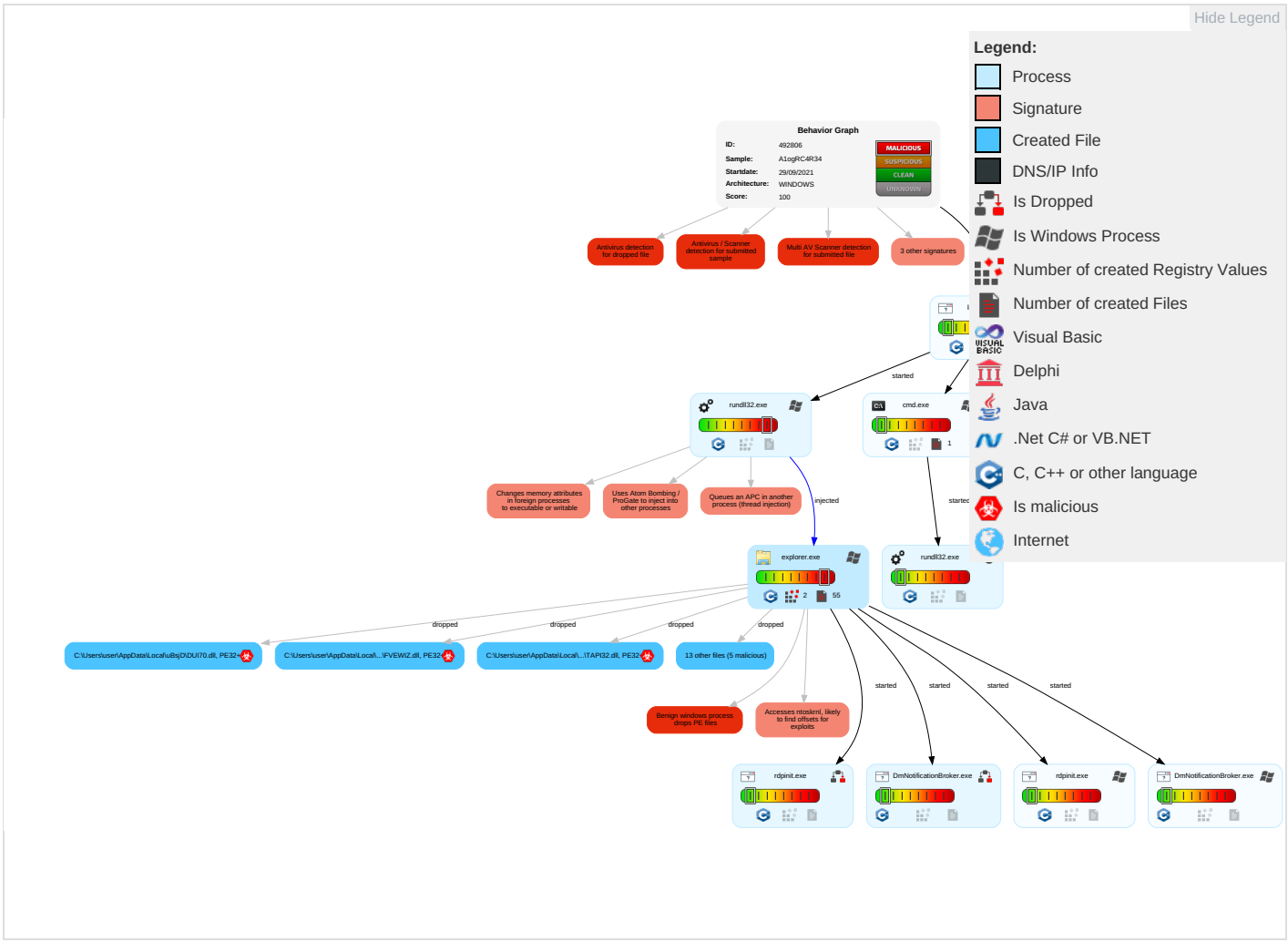
Queues an APC in another process (thread injection)

Uses Atom Bombing / ProGate to inject into other processes

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Eff
Valid Accounts	Command and Scripting Interpreter 2	Path Interception	Exploitation for Privilege Escalation 1	Masquerading 1 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Re Tra Wit Aut
Default Accounts	Exploitation for Client Execution 1	Boot or Logon Initialization Scripts	Process Injection 3 1 2	Process Injection 3 1 2	LSASS Memory	Security Software Discovery 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Re Wi Wit Aut
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Ob De Clo Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rundll32 1	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 2	LSA Secrets	System Information Discovery 2 5	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Timestomp 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	

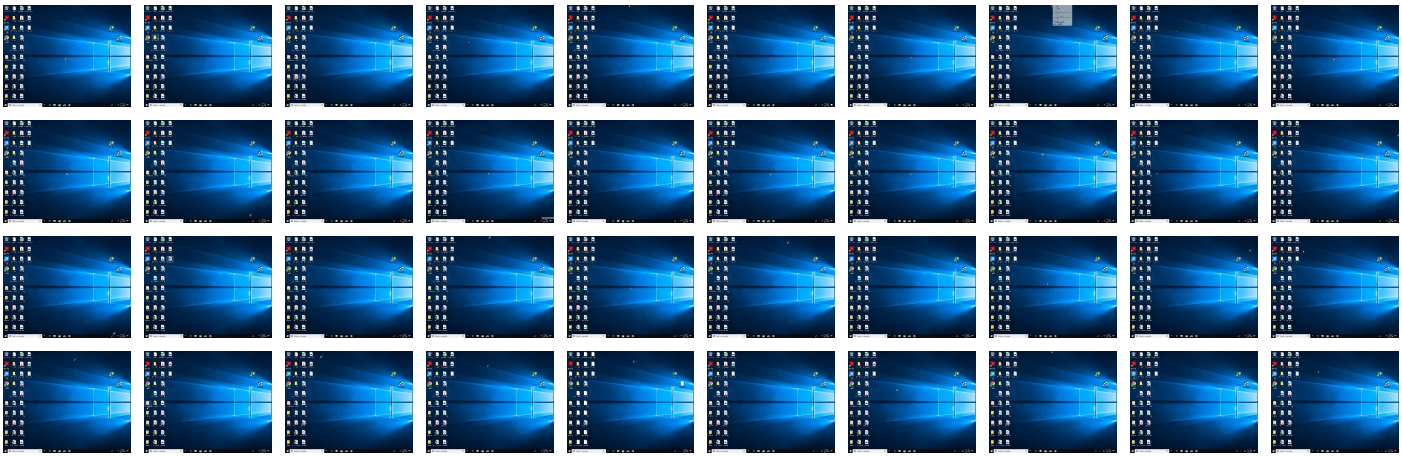
Behavior Graph



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
A1ogRC4R34.dll	62%	Virustotal		Browse
A1ogRC4R34.dll	57%	Metadefender		Browse
A1ogRC4R34.dll	76%	ReversingLabs	Win64.Infostealer.Dridex	
A1ogRC4R34.dll	100%	Avira	TR/Crypt.ZPACK.Gen	

Source	Detection	Scanner	Label	Link
A1ogRC4R34.dll	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\VcAfkDB\VERSION.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\fID\WINSTA.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\uBsjD\DUI70.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\r7RKh\FVEWIZ.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\kyOlt4HX\TAPI32.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\SaryWtyzg\WINMM.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\H3fqckDRC\dpx.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\3HlyM7czl\SYSDM.CPL	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\VcAfkDB\VERSION.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\fID\WINSTA.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\uBsjD\DUI70.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\r7RKh\FVEWIZ.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\kyOlt4HX\TAPI32.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\SaryWtyzg\WINMM.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\H3fqckDRC\dpx.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\3HlyM7czl\SYSDM.CPL	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\3HlyM7czl\SystemPropertiesAdvanced.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\3HlyM7czl\SystemPropertiesAdvanced.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\3HlyM7czl\SystemPropertiesAdvanced.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\H3fqckDRC\wusa.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\H3fqckDRC\wusa.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\H3fqckDRC\wusa.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\SaryWtyzg\PresentationSettings.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\SaryWtyzg\PresentationSettings.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
7.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
31.2.DmNotificationBroker.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.2.rdpinit.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.loaddll64.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:	492806
Start date:	29.09.2021
Start time:	01:51:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	A1ogRC4R34 (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.expl.evad.winDLL@38/17@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 8.6% (good quality ratio 6.9%) • Quality average: 72.7% • Quality standard deviation: 40.6%
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\3HlyM7czl\SYSDM.CPL

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2170880
Entropy (8bit):	3.4921794252523632
Encrypted:	false
SSDEEP:	12288:fVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:WfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	0BDAF2F3724797EAF4254B3B131700E6
SHA1:	4E9489103C1BE75098B7D9382F436D39BB65D828
SHA-256:	866FBAEAE3267C7FA20C1F9C8A0D0CFC1699B6D98793FBDE193BC28936F7DAC8
SHA-512:	68100D08A418F66E25BA08668E43AC77D151190CB5E0028B86E287763631B466E8FC86F0376C22ABD5E14A57B1014C90B4CFE8A0EB3B0836C0C2EEDE0A7C766
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.0..DN^....." .....p.....@..... !.....@lx}..b.....!.....c.....h.....$#..... .....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\3HlyM7czl\SystemPropertiesAdvanced.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	83968
Entropy (8bit):	7.065147438048501
Encrypted:	false
SSDEEP:	1536:UfuZktREC/rMcgEPJV+G57ThjEC0kzJP+V5JI:VkzECTMpuDhjRVJG3
MD5:	82ED6250B9AA030DDC13DC075D2C16E3
SHA1:	BC2BDCF474A7315232136B29291166E789D1F280
SHA-256:	F321BB53BBC41C2CBFFABC56837F9FA723AA0C6ACB68A0C200CBC7427202DC9E
SHA-512:	94D34293F070F6505D6922977AC1EF8E08DB0D92DCA8823BCF7376FD81B3AA80D2BD0FEF21FC74BCE08EEBF82DF09114A71792945DE4E3BB1FD0929538DF48B
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%...a..[a..[a..[h..[o..[..Z`..[..Zc..[..Zp..[a..[C..[..Zd..[..Z`..[..q[`..[..Z`..[Richa..[.....PE..d.....o....."....."....>.....@.....AS....`..... .....&.....P..0'...@..... ...."..T.....!..8.....text..... ..`.rdata..N.... .....@..@.data.....0.....@....pdata.....@.....@..@.rsrc...0'...P...(.....@..@.reloc.. .....F.....@..B.....

C:\Users\user\AppData\Local\H3fqckDRC\dpx.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2166784
Entropy (8bit):	3.4966791942802127
Encrypted:	false
SSDEEP:	12288:KVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:XfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	623DB87A3F248EA64BE5D903D21E9FB6
SHA1:	F816BA14F36DF9361B275670075534F8CEBB0A02

C:\Users\user\AppData\Local\H3fqckDRC\dpx.dll	
SHA-256:	2FECFF3A874320ACB1D2B749243CAF4714BA9507435EB066CD719435AED7E9D7
SHA-512:	5AF3F294602CA4366663183A77F8FEA2A3A871228C911A0CB8D3772442F74FEAC3EF1989C9AEBFEC2C3D4C50AFC321EDA05A3D321BCE8841D2A06EB497312B 1
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d./ ..DN^....." .....p.....@.....!.....@lx}..b.....,o.....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\H3fqckDRC\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
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;..-..~..~..~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\SaryWtyzg\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:	6528C86BA0272274A907F8559DFD79C55D1A6BAF3A4545EF3F6CDC4C790CC9FBDB7A3A8A2E72D0ED39651975DF5967608111448D1351BDC659E8F0F5E8C7244
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....$....._.">.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.....@..@.rsr c.....@..@.reloc.....b.....@..B..... .....

C:\Users\user\AppData\Local\SaryWtyzg\WINMM.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2174976
Entropy (8bit):	3.501635076472576
Encrypted:	false
SSDEEP:	12288:9VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:kfP7fWsK5z9A+WGAW+V5SB6Ct4bnb

C:\Users\user\AppData\Local\SaryWtyzg\WINMM.dll	
MD5:	2AB1771EACAAB67C8DBCC40CC742146C
SHA1:	630753BE4D7354238AD511DEF9BEF46504102D67
SHA-256:	AEEEF877DA29CDBC34426C62C3C264346FE8570AA553056C8C6BB4D3758EAC1F
SHA-512:	A139373330E6607A61709BD5D9D1ADFCEEF8F6DEBE62ECE092C67267BA1171C2B40360BDAE286C7FC66C7027C6389F5C06C93CDA95389CE8A3DB54150F07AC E
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.0 ..DN^....." .....p.....@.....0!.....@lx}..b.....!.h....c.....h.....$#..... ....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\VcAfkDB\VERSION.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2170880
Entropy (8bit):	3.492654327259235
Encrypted:	false
SSDEEP:	12288:8VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:JfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	0F593199E2816C0C8B8ED747CE1BEB85
SHA1:	423FD306E81B4F2D7FEF4D9F4F163BF5EE93EE7C
SHA-256:	B69C3AA0F262596A156376EA2931FC2324451A064F751DCE655F280650B046E5
SHA-512:	EC2234B909D85C89EE40C548CFC926D036A27B265F9793455AB6F2363AC66F81838F1D9288ECDB1BDEDA7D0C70A54EA8319BF6D0852C98FD24978A288BCABD C
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.0 ..DN^....." .....p.....@..... !.....@lx}..b.....!.+....c.....h.....$#..... ....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\VcAfkDB\unregmp2.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	254976
Entropy (8bit):	5.093220071075157
Encrypted:	false
SSDEEP:	3072:1t+/6BNqqNRhdutq4jCoNhdxtYEbvyIwYKO8/+9vAwk4OdamabJ9:3Bhhd+7QKb
MD5:	9B517303C58CA8A450B97B0D71594CBB
SHA1:	BE75E3F10E17400DA7C0FAF70BF16EE7D0AA93A8
SHA-256:	2A38BFC3813D7E845F455B31DF099C8A6E657EF4556BFF681315F86A883A3314
SHA-512:	6A47EC7800E1F1FCDBB44A018147CE4A87FF0F5B94597B182AAE4E8545D9B18FAAAA07379BA1086D8F7785F0F66C36E4B6C68FCF49130333B8A9DC3A9E9E08E 8
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....|.R.....y.....y.....y.....y.....w....y.....yf.....y.....Rich..... .....PE..d....Q&....."....."....^.....@.....0.....A....`..... .....0.....T.....V..(....U.....V..... .....text...w..... ..`.rdata..4.....@..@.data....8.....&.....@....pdata..0.....@..@.rsrc.....@..@.relo c.....@..B..... .....

C:\Users\user\AppData\Local\fID\WINSTA.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2174976
Entropy (8bit):	3.5091748741070106
Encrypted:	false
SSDEEP:	12288:0VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:xfP7fWsK5z9A+WGAW+V5SB6Ct4bnb

C:\Users\user\AppData\Local\fID\WINSTA.dll	
MD5:	6F22D93755FC031456BE2557F243015B
SHA1:	FC3E0F51E986057956F65B48296CB1AA197E8116
SHA-256:	EA2649CC270C4676E22323536EF5CFF6BA657383CFDDF1EF700E6CCE00ED9E11
SHA-512:	70CE3B19AA4485D82C7FB8E910CC789F7D004592AA8FD21DA1D25B600A2E699E00CB6577731CE81F226EFE451FB971C277055DF9FE667675B954E8F1AE0EB66
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.0 ..DN^....." .....p.....@.....0!.....@lx}..b.....!.m....c.....h.....$#..... ....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\fID\rdpinit.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	327168
Entropy (8bit):	6.414070673036673
Encrypted:	false
SSDEEP:	6144:fOzsB7eGjsO+VxyQ/qY4gCJkxkVPXqdzVxNwK3S3drxhUS4eMZfCZc/o:fOzsB7eGjb+VxynJkxkZ6dzV63drxhlF
MD5:	EF7C9CF6EA5B8B9C5C8320990714C35D
SHA1:	9CBD44DE4761F9383F2E0352035D52B86ECE80C2
SHA-256:	0FD9B6C366E042ED83BFC53C5EA1AAF43F13F53D97F220B5571681BB766C33FA
SHA-512:	C2F5E902DF725BC05F03052042767635689A35226CA1C3436ADF4835C57666B3E815FD386B80517734AC3B71F2FB15E48CE2F6739D669B5F68F4A8989713E8FC
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s.....S...S...S.j.S...S.v.R...S.v.R...S.v.R...S.v.R...S...S...S.v.R...S .vmS...S.v.R...SRich...S.....PE..d...q....."....f..... .....@.....p.....+..... .....@....@.....d .....`..x.....T..... .....text...<..... ..`.imrsiv.....rdata.....@..@.data....:.....@....pdata..d ..... ".....@..@.rsrc.....@.....@..@.reloc..x...`.....@..B..... .....

C:\Users\user\AppData\Local\kyOlt4HX\TAPI32.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2174976
Entropy (8bit):	3.512499889839238
Encrypted:	false
SSDEEP:	12288:uVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:zfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	99671622AFF90CD9D173CA46E372D3AC
SHA1:	B689B8799C7A057958AF0BFAFF233142AC54F761
SHA-256:	578AD60043FB755F8546C8418C9D8FDE64D2C4BA9F4467CE812AA14D702FA855
SHA-512:	021357EAE61F5E372F5675788D0CDFA09A252238F808419E75912B53DC5507D26D6EB1B27B26000A699E53C0E831C6ADBFE66E4BA63577AB0FB129F6A9D44AC
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.0 ..DN^....." .....p.....@.....0!.....@lx}..b.....!.V....c.....h.....$#..... ....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\kyOlt4HX\tcmsetup.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	4.999998588063228
Encrypted:	false
SSDEEP:	192:DIzBdu2Mhf/+G1jQ0pwPYqLmdO0O7RgZiLtzADWO4hxDcUh6UdBndOvfSWG0oW:GMVJjQ0dg0O7yk5ciJcUhLiSWG0oW
MD5:	0DDA495155D552D024593C4B3246C8FA
SHA1:	7501A7AD5DAA41462BEFF9127154BAF261A24A5B

C:\Users\user\AppData\Local\kyOlt4HX\tcmsetup.exe	
SHA-256:	D3074CBD29678CA612C1F8AA93DE1F5B75108BE8187F0F2A2331BC302AD48CD9
SHA-512:	9159D8AF457591256BA87443E89ECE942DE40B8FF39586116C2026330B8AE9C20F96905547E87D98508951D2B4687069EFD018CC9E4A6C94A6C26D4B587F41B3
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Z...Z...Z..[...Z..[...Z..[...Z..[...Z...Z...Z..[...Z.:Z...Z..[...ZRich...Z.. .....PE..d....E.H....."..... ....@..... `..... .....9..x....p..P....`..D..... ....5..T.....0.....1.. .....text..... ..`.rdata..&....0.....@..@.data... ....P.....0.....@....pdata..D....`.....2.....@..@.rsrc...P....p.....4..... ....@..@.reloc.. .....>.....@..B..... .....

C:\Users\user\AppData\Local\r7RKh\BitLockerWizardElev.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	101888
Entropy (8bit):	6.95002760620154
Encrypted:	false
SSDEEP:	3072:k8kEZwnVS570M9kdatGCO+xmBc+hMPhPsx:1khVs7nyatGt+SYF
MD5:	3104EA9ECCA9ED71A382CCAAD618CEAE
SHA1:	9277108B7254F0C5BD241C2643902378925A8F9C
SHA-256:	D8CB004D4E8894AB4CA769C3CEC9A37B7FAB336DCDA1E6E9A15975DC64CEF370
SHA-512:	27C84C35461E37557BA27A7D9E9F86A47686DE73DDC74E001777F11EA8D5BE9B17604403875CF20124595010477F6F2ADDD797B9ACED79C514AEF2D2F1A019B
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.`M.h3M.h3M.h3"Jm2O.h3"Jk2O.h3"Jl2_.h3"Ji2F.h3M.i3 }.h3"Ja2L.h3"J.3L.h3"Jj2L.h3RichM.h3.....PE..d....C....."..... .....@.....0....`..... .....D,..x....`...c...P..... ..... ....(..T..... ..... .....!.....text..... ..`.rdata..... .....@..@.data.....@.....$.....@....pdata.....P.....&.... .....@..@.rsrc....c...`...d...(.....@..@.reloc.. .....@..B..... .....

C:\Users\user\AppData\Local\r7RKh\FVEWIZ.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2170880
Entropy (8bit):	3.4988987994424146
Encrypted:	false
SSDEEP:	12288:8VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:JfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	E618EE247E3251D556DAF3D3C658C0A9
SHA1:	177C80CA1FDA1BA71113C7A1F648D911E8A0C4C9
SHA-256:	101AF5D6FC2DAA1B700D779CDBB54D9255FDEA3718BE0FC9F672B807346298C6
SHA-512:	261E7DE708350CAC5E52860F9432CDB1DEDA7289168C4A10F26CD36EABFBA28CA4DD3BBAF9708C9110E3FD13F9D22E5789D112D682CCCEC243F62E1D3298030
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|..... .....PE..d.0 ..DN^....." .....p.....@..... !.....@lx}..b.....!.....c.....h.....$#..... ....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\uBsjD\DUI70.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2453504
Entropy (8bit):	4.027319224931197
Encrypted:	false
SSDEEP:	12288:1VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1XQ:sfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	6A41878B4C9B36A4455B22A8EBBC846F
SHA1:	CF9CFC24FDC9B744A867B81E452C18A04042A4E2
SHA-256:	BC2B240D729D4DB74F14D302EC83EBD06C1ED7F340CF7CA8BE11F0184B263CE0
SHA-512:	7526BAC5EBDF82F434BC5E753F038AF339ADE485F59108A90D3CBB1589397DE08BCDE4C390AA7008395974E1B56F290A7787BCBD5145074B367AE8C2DB0A3BB

C:\Users\user\AppData\Local\uBsjD\DUI70.dll	
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.0..DN^....." .....P!.....p.....@.....p%.....@lx}..b.....!.dQ...c.....h.....$#..... ....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\uBsjD\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:	F0BD45FE66EDC6F615C0125C1AE81E657CA26544544769651AB0623DD3C724F96D9D78835EF6B1D15083D1BB9D501F6DC48487DDA5C361CAFA96022D5F33A4
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....j.?H..lH..lH..lAs.lT..l'o.mJ..l'o.m[..lH..l...l'o.mC..l'o.mA..l'o.mA..l'ohll..l'o.ml..lRichH..l.....PE..d.....".....*...V.....&.....@.....n3..... .....x..... .....Po..T.....].....^..p.....text....(.....*..... ..`.imrsiv.....@.....rdata..P8...P...:.....@..@.data...(.....h.....@.....pdata.....j.....@..@.rsrc... .....n.....@..@.reloc.....z.....@..B.....

C:\Users\user\AppData\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):	5.481123367178235
Encrypted:	false
SSDEEP:	96:Jlj2Zt+j6ZP4zr1Q9Elj2Z0+ByNAI4v1lV3:O4tTgF8L40+8oXV3
MD5:	ED384AAFCE2EF80D0F36ED6D8B12E7B3
SHA1:	2D4B43B7864F08321B7702E6014A80D4BBAB0F24
SHA-256:	D55C29F6CD93EA549E21A9A294B036BB7621886B8DEDBDAFCA4BCFD287C0D8AD
SHA-512:	20B0483FBCA47C76328D8F0527C346DF626246EE0E70CACEC737C028CB6A9C2261C692BD07A00640459A96DBE0E1746D4DE44DDA6D1349F51CC7EF0B6ADE0E0C
Malicious:	false
Reputation:	unknown
Preview:	.....user.....user.....RSA1.....q00D..7..w.~.....;<.Y.....'7.....VVmp/..."F.Q...#B.....x.....K|..K.....~+:..:..%.J.+a(.....5...f.d...o...nV.....z..O.....D.Mb.G..m..#&....,...C.r.y.p.t.o.A.P.I. .P.r.i.v.a.t.e. .K.e.y....f..... ....v?..`.G:AsQ.!..9mB.....+...>..... ...!.Lt.}....S..!!.$'y.....D.$n.....4.A...A../.j.B.b.....6V:3..*0...`..Ep....6.s..8....3.?`....LS..}F..+..Q_G..~.:.....f..5...I..n.*`..t..i....f.~b.rQ.....#6.z...g...$.*y7...}B..>.Q6..,.....I_K.d.....>.....d_.<..M0....D.p..>i.T.J...Q...}.g~... V7x...I.[&"ptk..x^.X.....| @...~xB.....O.z...RA'^.}-..&....Ug._....f.....F~.q^....;/.H....t....8...A.ND.6...L.[j@...^.I..G.G^U=.[.2...k.7ln....@.:..l.8.....9@t..m...j.....-.....o-.t..4..V.k....k....u.....`.J.skr<.`jq?....._.i...\..g@{..B.I5|n)"..U+5.&.....I...W..:#.d..`..o/.....

Static File Info

General

File type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Entropy (8bit):	3.5201402860449647
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%

General

File name:	A1ogRC4R34.dll
File size:	2166784
MD5:	5edd6ba336c4de29f55cadfd2167a67e
SHA1:	af181a8f3fe25a515a8fe2a02559e5daceecf976
SHA256:	eda8c025e5f5f67ae92bee0ed77113e18f60e9465f43fc43e00664f5bea7c32d
SHA512:	01b133fad6f564e6736d5f7297284da9aa8cc67a1c28a57b7b7eb1989ee049318377df85fbbeda9f777c0d955f07706743dc2becc3994bf9727a8d040067f5d5
SSDEEP:	12288:JVl0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:ofP7fWsK5z9A+WGAW+V5SB6Ct4bnb
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
.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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.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
.fhgxfk	0x164000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.wqpbrq	0x1aa000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.xlhbgj	0x1ab000	0xebe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rzgl	0x1ac000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.yic	0x1ad000	0x1f7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.zfmbo	0x1ae000	0x1af	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.kurwl	0x1af000	0x3fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.crlsf	0x1b0000	0x1e66	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
.wrn	0x1b2000	0x6cd0	0x7000	False	0.00177873883929	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.blcv	0x1b9000	0x1af	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.roblb	0x1ba000	0x9cd	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.yblxa	0x1bb000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tfy	0x1bc000	0x9cd	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.wsmv	0x1bd000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.hrs	0x1be000	0x16c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ppapg	0x1bf000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.udm	0x1c0000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.fxc	0x1c2000	0x1f2a	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.fvxxk	0x1c4000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.zmj	0x1c5000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.zvz	0x1c6000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.xyiz	0x20c000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.gbzxp	0x20d000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.kkivgv	0x20e000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.evwibb	0x20f000	0x197d	0x2000	False	0.318115234375	data	4.72480866446	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: 7096 Parent PID: 5844

General

Start time:	01:52:38
Start date:	29/09/2021
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe 'C:\Users\user\Desktop\A1ogRC4R34.dll'
Imagebase:	0x7ff77a010000
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: 00000001.00000002.254502525.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 3192 Parent PID: 7096

General

Start time:	01:52:38
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\A1ogRC4R34.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: 6408 Parent PID: 7096

General

Start time:	01:52:39
Start date:	29/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\A1ogRC4R34.dll,LogonIdFromWinStationNameA
Imagebase:	0x7ff608cf0000
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: 00000003.00000002.327777249.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities — Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 6396 Parent PID: 3192

General

Start time:	01:52:39
Start date:	29/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe 'C:\Users\user\Desktop\A1ogRC4R34.dll',#1
Imagebase:	0x7ff608cf0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000004.00000002.234114370.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities — Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3472 Parent PID: 6408

General

Start time:	01:52:40

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: 6492 Parent PID: 7096

General

Start time:	01:52:42
Start date:	29/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\A1ogRC4R34.dll,LogonIdFromWinStationNameW
Imagebase:	0x7ff608cf0000
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: 00000006.00000002.241053387.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 3684 Parent PID: 7096

General

Start time:	01:52:45
Start date:	29/09/2021

Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\A1ogRC4R34.dll,RemoteAssistancePrepareSystemRestore
Imagebase:	0x7ff608cf0000
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: 00000007.00000002.248393203.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities Show Windows behavior

File Read

Analysis Process: rdpinit.exe PID: 6372 Parent PID: 3472

General

Start time:	01:53:25
Start date:	29/09/2021
Path:	C:\Windows\System32\rdpinit.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\rdpinit.exe
Imagebase:	0x7ff642f20000
File size:	327168 bytes
MD5 hash:	EF7C9CF6EA5B8B9C5C8320990714C35D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rdpinit.exe PID: 5620 Parent PID: 3472

General

Start time:	01:53:27
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\fID\rdpinit.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\fID\rdpinit.exe
Imagebase:	0x7ff785a80000
File size:	327168 bytes
MD5 hash:	EF7C9CF6EA5B8B9C5C8320990714C35D
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: 00000018.00000002.356788011.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities Show Windows behavior

File Read

Analysis Process: DmNotificationBroker.exe PID: 4592 Parent PID: 3472

General

Start time:	01:53:38
Start date:	29/09/2021
Path:	C:\Windows\System32\DmNotificationBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\DmNotificationBroker.exe
Imagebase:	0x7ff619e90000
File size:	32256 bytes
MD5 hash:	1643D5735213BC89C0012F0E48253765
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: DmNotificationBroker.exe PID: 5212 Parent PID: 3472

General

Start time:	01:53:42
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\uBsjD\DmNotificationBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\uBsjD\DmNotificationBroker.exe
Imagebase:	0x7ff69e090000
File size:	32256 bytes
MD5 hash:	1643D5735213BC89C0012F0E48253765
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000001F.00000002.390772898.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Read

Disassembly

Code Analysis