ID: 492089
Sample Name: 3PgaI7gtQn
Cookbook: default.jbs
Time: 10:50:55
Date: 28/09/2021
Version: 33.0.0 White Diamond

Table of Contents

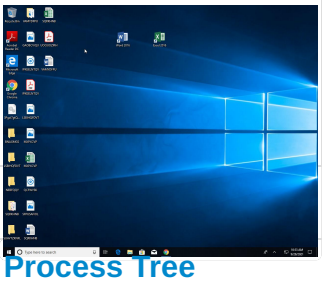
Windows Analysis Report 3PgaI7gtQn

Overview

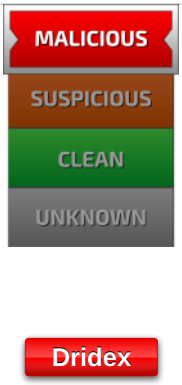
General Information

Sample Name:	3PgaI7gtQn (renamed file extension from none to dll)
Analysis ID:	492089
MD5:	8a6f4fe59b41d74..
SHA1:	064f5eca3efd02c..
SHA256:	d7cb31b51d497e..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

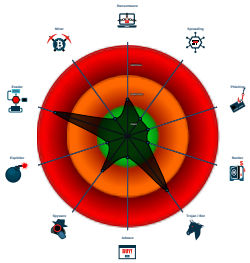


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- Uses Atom Bombing / ProGate to in…
- Queries the volume information (nam…
- Contains functionality to query locale…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 6272 cmdline: loaddll64.exe 'C:\Users\user\Desktop\3PgaI7gtQn.dll' MD5: A84133CCB118CF35D49A423CD836D0EF)
  - cmd.exe (PID: 2600 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\3PgaI7gtQn.dll',#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 1444 cmdline: rundll32.exe 'C:\Users\user\Desktop\3PgaI7gtQn.dll',#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 900 cmdline: rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,CopyPropVariant MD5: 73C519F050C20580F8A62C849D49215A)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - bdeunlock.exe (PID: 3976 cmdline: C:\Windows\system32\bdeunlock.exe MD5: FAB70105E2075EEC9C249A4D499CAE7C)
      - bdeunlock.exe (PID: 2912 cmdline: C:\Users\user\AppData\Local\bnfeSWnf\bdeunlock.exe MD5: FAB70105E2075EEC9C249A4D499CAE7C)
      - CameraSettingsUIHost.exe (PID: 6660 cmdline: C:\Windows\system32\CameraSettingsUIHost.exe MD5: 34F32BC06CDC7AF56607D351B155140D)
      - CameraSettingsUIHost.exe (PID: 6744 cmdline: C:\Users\user\AppData\Local\43ip\CameraSettingsUIHost.exe MD5: 34F32BC06CDC7AF56607D351B155140D)
      - pwcreator.exe (PID: 1848 cmdline: C:\Windows\system32\pwcreator.exe MD5: BF33FA218E0B4F6AEC77616BE0F5DD9D)
      - pwcreator.exe (PID: 4984 cmdline: C:\Users\user\AppData\Local\NfgW4al\pwcreator.exe MD5: BF33FA218E0B4F6AEC77616BE0F5DD9D)
      - lpksetup.exe (PID: 5944 cmdline: C:\Windows\system32\lpksetup.exe MD5: 8E2C63E761A22724382338F349C55014)
      - lpksetup.exe (PID: 4732 cmdline: C:\Users\user\AppData\Local\fbMtwkN2S\lpksetup.exe MD5: 8E2C63E761A22724382338F349C55014)
  - rundll32.exe (PID: 2824 cmdline: rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,CreatePropVariant MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 1572 cmdline: rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,CreatePropertyStore MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5184 cmdline: rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,DestroyPropVariant MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 2872 cmdline: rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,FormatTagFromWfx MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6116 cmdline: rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,GetAMSubtypeFromD3DFormat MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 7164 cmdline: rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,GetD3DFormatFromMFSubtype MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5560 cmdline: rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,MFAddPeriodicCallback MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5568 cmdline: rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,MFAllocateSerialWorkQueue MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 4100 cmdline: rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,MFAllocateWorkQueue MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 3416 cmdline: rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,MFAllocateWorkQueueEx MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6764 cmdline: rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,MFAppendCollection MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6704 cmdline: rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,MFAverageTimePerFrameToFrameRate MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6700 cmdline: rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,MFBeginCreateFile MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 4200 cmdline: rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,MFBeginGetHostByName MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 2464 cmdline: rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,MFBeginRegisterWorkQueueWithMMCSS MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6832 cmdline: rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,MFBeginRegisterWorkQueueWithMMCSSEx MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 1492 cmdline: rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,MFBeginUnregisterWorkQueueWithMMCSS MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 7040 cmdline: rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,MFCalculateBitmapImageSize MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 2124 cmdline: rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,MFCalculateImageSize MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.710759124.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000024.00000002.812744317.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000015.00000002.820144134.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
0000001F.00000002.800645636.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000010.00000002.733013846.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	

Click to see the 21 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

HIPS / PFW / Operating System Protection Evasion:

Benign windows process drops PE files

Changes memory attributes in foreign processes to executable or writable

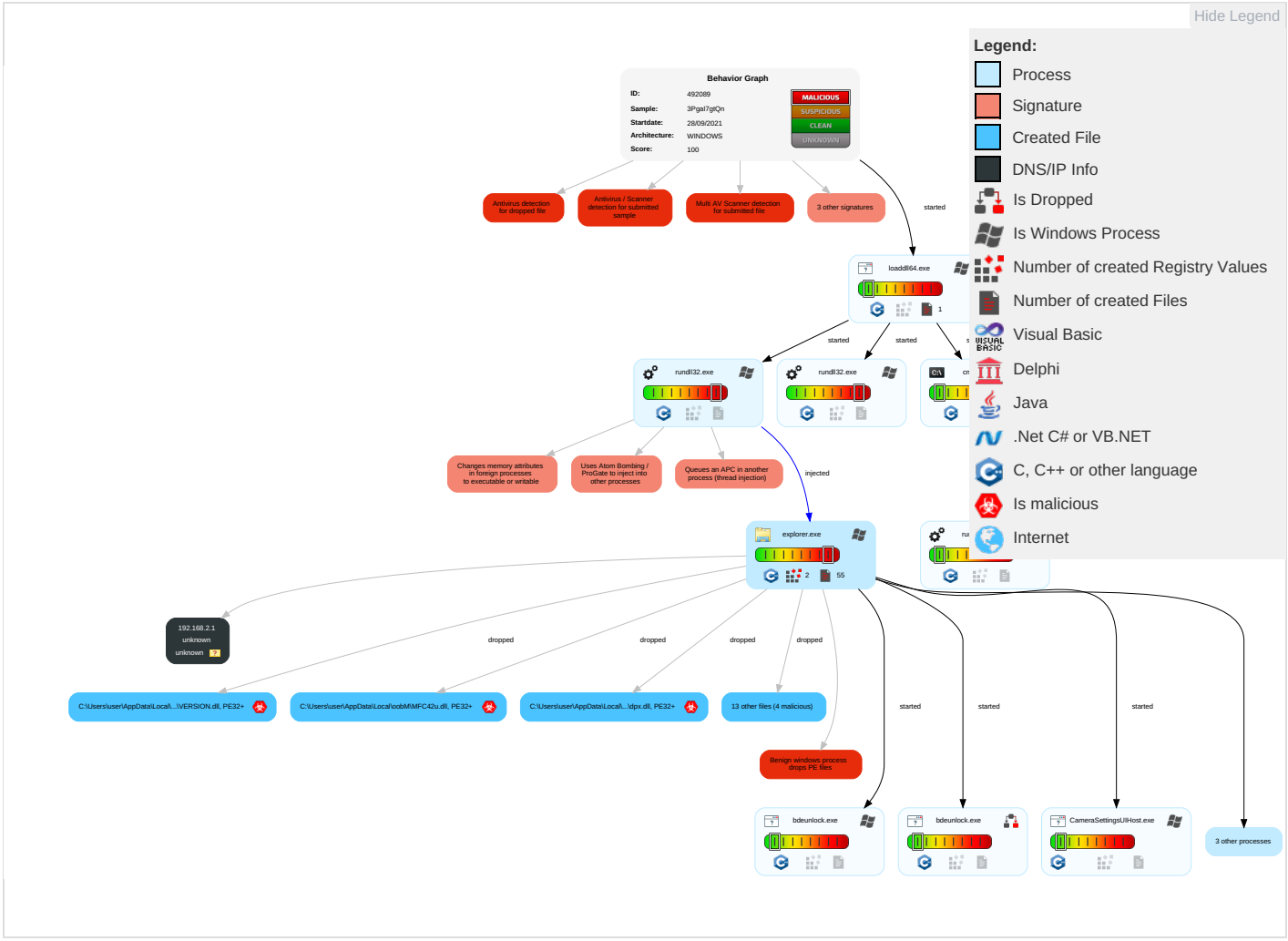
Queues an APC in another process (thread injection)

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
Valid Accounts	Command and Scripting Interpreter 2	Application Shimming 1	Access Token Manipulation 1	Masquerading 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdro Insecure Network Communi
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Process Injection 3 1 2	Virtualization/Sandbox Evasion 1	LSASS Memory	Security Software Discovery 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit S Redirect I Calls/SM
Domain Accounts	Exploitation for Client Execution 1	Logon Script (Windows)	Application Shimming 1	Access Token Manipulation 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 3 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulat Device Communi
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	System Information Discovery 3 5	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Rundll32 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access P
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Timestomp 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue C Base Stat

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
3PgaI7gtQn.dll	69%	Virustotal		Browse
3PgaI7gtQn.dll	54%	Metadefender		Browse
3PgaI7gtQn.dll	76%	ReversingLabs	Win64.Infostealer.Dridex	
3PgaI7gtQn.dll	100%	Avira	HEUR/AGEN.1114452	
3PgaI7gtQn.dll	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\fbMtwkN2S\dpx.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\43ip\DUI70.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\oobM\MFC42u.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\aPIxGSGX\XmlLite.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\HxApBjE\NETPLWIZ.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\NfgW4al\WINBRAND.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\zshP\VERSION.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\43ip\DUI70.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\fbMtwkN2S\dpx.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\43ip\DUI70.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\oobM\MFC42u.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\aPIxGSGX\XmlLite.dll	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\HxApBjE\NETPLWIZ.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\NfgW4al\WINBRAND.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\zshP\VERSION.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\43ip\DUI70.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\43ip\CameraSettingsUIHost.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\43ip\CameraSettingsUIHost.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\HxApBjE\Netplwiz.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\HxApBjE\Netplwiz.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\NfgW4al\pwcreator.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\aPIxGSGX\ddodiag.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\aPIxGSGX\ddodiag.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
30.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
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
16.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
13.2.rundll32.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
20.2.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
17.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
11.2.rundll32.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
23.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
35.2.pwcreator.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
32.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
31.2.CameraSettingsUIHost.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
19.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
27.2.bdeunlock.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.2.rundll32.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

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	492089
Start date:	28.09.2021
Start time:	10:50:55
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	3PgaI7gtQn (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:	40
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@69/17@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 15.8% (good quality ratio 13.4%) • Quality average: 77.9% • Quality standard deviation: 37.1%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI
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\43ip\CameraSettingsUIHost.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	32104
Entropy (8bit):	6.224595599643794
Encrypted:	false
SSDEEP:	768:HYxSW1tZfZjtM2mpgc8WtCpZswKro1PDg:HhAhty8WteuwKrwPDg
MD5:	34F32BC06CDC7AF56607D351B155140D
SHA1:	88EF25BC91BCC908AF743ECA254D6251E5564283
SHA-256:	47238D9ED75D01FD125AC76B500FEEF7F8B27255570AD02D18A4F049B05DF3BD
SHA-512:	D855414779125F4E311ACF4D5EFC8ACA4452323CABD1694798CA90FD5BD76DC70B5D06790A2AE311E7DD19190DCCB134F6EF96AB1B7CF5B8A40AD642B72D5 44
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....$....._Lp..-...-...-...U...-..tl...-..tl...-..tl...-..tl...-...-..K-..tl...-..tl..-..tl...-..Rich.- .....PE..d....\YN....."....*...2.....0.....@..... ....._.....Z..h#.....X..T.....`S..(...`R..... .....S.....text....(.....*..... ..`.imrsiv.....@.....rdata.....P.....@..@.data.....p.....J.....@....pdata.....L..... .....@..@.rsrc.....P.....@..@.reloc.....X.....@..B.....

C:\Users\user\AppData\Local\43ip\DUI70.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2408448
Entropy (8bit):	4.088464785484027
Encrypted:	false
SSDEEP:	12288:NVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1ymulOt:UfP7fWsK5z9A+WGAW+V5SB6Ct4bnbMK
MD5:	4121EE4C9F38EE65D7E1D3F39CE327A4
SHA1:	D85D7FBF8CDD63C2D7D2024C22EA63423D9292BB
SHA-256:	2E195E740BA535D55EFA59E4342EA5D76F2DAD519494BD8F6AA7BB715AA308B0
SHA-512:	A4F246AD5BCB81B9730C7B8814DD2F6B4E62CC839A177B4CDE98DADC09401C1E027AC696C06C01676C7F47F7FB9C03426938006F2C5CE0EC7B278C60A6A469 B
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.' ..DN^....." ....p.....@.....$.....@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\HxApBjE\NETPLWIZ.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows

C:\Users\user\AppData\Local\HxApBjE\NETPLWIZ.dll	
Category:	dropped
Size (bytes):	2125824
Entropy (8bit):	3.5527133641756206
Encrypted:	false
SSDEEP:	12288:oVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:9fP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	7C2DFAC0CE010C8A44E593D1103BDA97
SHA1:	406EE28D9C04ED4F287A4792BD201668CF8CBC1D
SHA-256:	4FDB143C3627C8EA9C51899CA42246922F08A4873E8B2ED2BA11BD5AAE8221C8
SHA-512:	6FE9C8618DE0338E993AC4744E7DB6B0F55C4B96271205E96A7A7CC720F9914EDFE7D019B98AB70EC3479FB83AE41BBAB818A238CD249E195BDCE4D338305DD4
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.'..DN^....." .....P.....p.....@.....p .....@lx}..b.....` .....c.....h.....$#..... .....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\HxApBjE\Netplwiz.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	39424
Entropy (8bit):	5.640119387300135
Encrypted:	false
SSDEEP:	768:Sm6uxIL0DPeyQvEsNN6hU2hGGalaQkQcryUJU3fUrh6WeENiJDBPrxZt4W:p6MMD6hlBBjrywUKeWSDBPrxZaW
MD5:	A513A767CC9CC3E694D8C9D53B90B73E
SHA1:	F10B719117D26DAFCC9DBE54E9F9D78A0F80EE2A
SHA-256:	C9F7AC4322504D7EC8305973951A66FBE34E55E34A59409B5B574D627A474369
SHA-512:	03BBBC076D3497E35952143085B9DCC83EDE855A00A190F05712FC91F0C0C4301995D0123EBDCA75A59B93C51358EAD5C4030F8EE9C33F9D1BF1A0EDBC52FD4
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....$.....;.K.U.K.U.K.U.B..G.U.$.P.J.U.$.V.H.U.$.Q.Y.U.$.T.F.U.K.T...U.$.\.J.U.$...J.U.$.W.J.U.RichK.U.....PE..d...v....."....n.....@6.....@.....`..... .....L.....F...p..... .....4....F..T.....@.....A.....text....- ..`.rdata..t....@.....2.....@..@.data.....`.....J.....@....pdata.....p..... ..L.....@..@.rsrc....F.....H...P.....@..@.reloc..4.....@..B..... .....

C:\Users\user\AppData\Local\NfgW4al\WINBRAND.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2125824
Entropy (8bit):	3.5537457737561593
Encrypted:	false
SSDEEP:	12288:MVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:5fP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	0FA8A4183C28C71FE734D6065497ADDE
SHA1:	D22C41D6DF53577BD9013BB5AD02074576800F6C
SHA-256:	43DE8467A04ED6F74B09C66F09EE6FEF2BE1A5120C9B20C792B1CA98B117E400
SHA-512:	AAE25C32715162F02FA2FEB437F4DF35015C68C9003F906CBFED45BFCD744F6AC724247B126882FD82E30037C68407C58704ACCF226B9F50325563344848D8D1
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.'..DN^....." .....P.....p.....@.....p .....@lx}..b.....` .....c.....h.....$#..... .....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\NfgW4al\pwcreator.exe	

C:\Users\user\AppData\Local\NfgW4al\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
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
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\aPIxGSGX\XmlLite.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2125824
Entropy (8bit):	3.5529782689844396
Encrypted:	false
SSDEEP:	12288:KVl0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:XfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	2BF02D76D58256D262FCEE3D70F9BA42
SHA1:	095C42C35275909EBC554B07B7B30DDF75843A27
SHA-256:	A7FDE865CA3F382F9B288ECD01366EB88F5C53C3B8B03266DABDAB89C4E9690B
SHA-512:	F5F8B185E62AF9104AB601877CFD3A2E4DF71BFF626A75ED00711108FFCBF81EE0C36E7575BCF0E4692BF0A124236F621E1F28037ACD3DF551D568DF99949623
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.' ..DN^....." .....P.....p.....@.....p .....@lx}..b.....` .....c.....h.....$#..... ..... .....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\aPIxGSGX\ddodiag.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	37888
Entropy (8bit):	5.0324146638870335
Encrypted:	false
SSDEEP:	768:li5tlKBaheiGK/hc3aZkLmMgMaouZl6i9Kott/D:/C0heiGK/hc3aZkLmMgMaouZl6i9t/D
MD5:	3CE911D7C12A2EFA9108514013BD17FE
SHA1:	2F739BD7731932A0BF13A3B8526FC867EC41C63E
SHA-256:	FC55CB5FF243496B039D3DB181BD846BDD38D11C7D52E4BA20D882B65FBE1C3B
SHA-512:	33F4FD94916DB3F0BC4E138DD88125D9B45108F7EECFDE0A54BE1901F4BE3F1966BC0FE9278A919A3D94AEC53A8269ACA9451EBA7D53C82BF64CC215522AD7 8E
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....$.....X.=...S...S...S.s.P...S.s.W...S.s.V...S.s.R...S...R.$.S.s.Z...S.s....S.s .Q...S.Rich..S.....PE..d...~3.....".....&...p.....p/.....@.....q....`..... .....~..d.....p.....(...`z..T..... E..... F.....text...P%.....&..... ..`.rdata..."D...@...F...*.....@..@.data.....p.....@....pdata.....@..@.rsrc...p.... .....@..@.reloc..(.....@..B..... .....

C:\Users\user\AppData\Local\bnfeSWnf\DUI70.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2408448
Entropy (8bit):	4.088173474060694
Encrypted:	false
SSDEEP:	12288:EVl0W/TtlPLfJCm3WIYxJ9yK5lQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ15sZz:hfP7fWsK5z9A+WGAW+V5SB6Ct4bnb5U
MD5:	5B66C49965E3F6B0E1B462A795619EB4
SHA1:	8639F82F4D16E35FEDC7A5778F7F43A252CFB6EE
SHA-256:	2FADF48DCCD8B10EADDA1405AA2D7E764E0563D22C589729D30FA419DEC50112
SHA-512:	0F3D0B89CED60B6725DA24FC5D973EB1EB0FF81ECEE2FCBCD15885BDD47D3011D53B4B390B018C4B81CE36654EDC6AE348DE8B404CE9187814733F179CA53EA
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.'..DN^....." ....p.....@.....$.....@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\bnfeSWnf\bdeunlock.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	286232
Entropy (8bit):	6.926729215014979
Encrypted:	false
SSDEEP:	6144:jjJkzmZ4CSal+EH+pDQh01TXRYJWEmTKBKt1Vs7nyatGt+SYFmW2kb/:jtgmSdal+EH+5QhWEmTKB2H+S+7b/
MD5:	FAB70105E2075EEC9C249A4D499CAE7C
SHA1:	B5B4216725F55A4E6AF9FB0BB7E0167CEED6081F
SHA-256:	7EA89BE1BBA6A7C2B08D70FA8E4CF036CB086ED162BCD22255E2BC0F926B22B2
SHA-512:	96327DEC3BCEE7A9934AAF27F1942030D46CEE693AF2562EE4972D5306DD3AD14F404762B99E581C0F0F563610EA097372044890EB19CE1C7A8F535A78D9E19A
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....:..A~.~.~.~.~.~.w...v.~...}.}.~...z.l.~...{.x.~.....g.~.~.....~...w.i.~...~...~.....~...|...~.Rich~.~.....PE..d....X.....".....D.....pJ.....@.....i..... .....P.....T.....x.....2...,.....t....T.....t.....u.....text...PB.....D..... ..`.imrsiv.....`.....rdata...c...p...d...H.....@..@.data.....@....pdata.....@..@.rsrc....x.....z.....@..@.reloc..t.....0.....@..B.....

C:\Users\user\AppData\Local\fbMtwkN2S\dpx.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2121728
Entropy (8bit):	3.5580591254970417
Encrypted:	false
SSDEEP:	12288:1Vl0W/TtlPLfJCm3WIYxJ9yK5lQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:sfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	11691B104F078DBB489FADF628AE5C83
SHA1:	5A8564886486825568354 6E5465E14D0E29427AF
SHA-256:	3619646B47E58F21DE52463FE7F6ECBA59173E10C6AED207D7B7D9425D3287C7
SHA-512:	A3909BD47F0ED501EE9B60D60260C1313E885CC7791A3700306DC607F6C07D1AB6EB0423CDC32385D1EFB3819733D5A6D5C090B89C14CD44B721EEE8F3BDEE8
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\fbMtwkN2S\lpksetup.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows

C:\Users\user\AppData\Local\fbMtwkN2S\lpksetup.exe	
Category:	dropped
Size (bytes):	732160
Entropy (8bit):	6.573630291630044
Encrypted:	false
SSDEEP:	12288:U4O7JpqBbsczjBmavlNRO5Gy1ay0OBegtkGyLY9d/Dz/sJ+lGDyYgWPL/kc7yfnQ:U40JpqtZzjBRvI5Gdy0OjtwLY9BDz/PW
MD5:	8E2C63E761A22724382338F349C55014
SHA1:	30C7F92A6E88C368B091E39665545EAFA8A6561F
SHA-256:	4CA6E16BEB57278E60E3EDCBCECDA1442AA344C424421E4B078F1213E6B99376
SHA-512:	92F289DDBD9D1E5103C36308DA84779708A292DC54F49A0A1B79D65C563378BBF08C98F3732F25365CCF8175589D8E6187CEE2A694AE5FB73CA9E85AECFF4CF
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....W..6...e...e...e..%e3..e|.d...e|.d...e|.d...e|.d...e...ec..e|.d6..e|.Ie. ..e|.d...eRich...e.....PE..d.....e.....".....,...P.....@.....`..... .....H?.....g..T.....y.. (....x.....y..P.....text....+.....,..... ..`.rdata..\....@.....0.....@..@.data...`[...0.....@....pdata..H?.....@.....@..@.rsrc..... .....^.....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\oobM\MFC42u.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2150400
Entropy (8bit):	3.5942759550882832
Encrypted:	false
SSDEEP:	12288:BVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1u:wfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	DB0FB2C1640C7E176AD5B8C83BE68823
SHA1:	86452C8617E4F9FAC9AB219DE1E45F3F8285541C
SHA-256:	5782DEB31D2ED74626BFE53E3D100DF785A536EB164898D4EFF01A017A96DBFD
SHA-512:	8E03D8A585C337A7D36446E274C64B3DB1E1E21A983FFD2BA5C1D374A4382A685C7CAB2F5EBA84A42DCB6D902CB96F2FD5D131862AE9029A5C354CD849708C 7
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.' ..DN^.....".....p.....@..... .....@lx}..b.....` ..I...c.....h.....$#..... ..... .....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\oobM\mmc.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1859584
Entropy (8bit):	6.170036018738162
Encrypted:	false
SSDEEP:	24576:jkx6/5L0DOw7CYHrgS3TY8hVLujvKfukMo7wMo7DH:jx/VoCYLgS3JhNQval7e7DH
MD5:	BA80301974CC8C4FB9F3F9DDB5905C30
SHA1:	382008FBA9480F6568DB3E1F335D080192DE62CA
SHA-256:	683C0CB518B3FE31CFFA7FCF79F5EFC18D355C6D52734757758ED26AE5950037
SHA-512:	50B9F485F2C0291FF724E33133A1C5941ECA367C0EA03ACFB3560756848183B7301165E4A4D8E9B813142872A14CE95D97DAAFE355EBB9C7AEA5F6252A1045DA
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qd.T...T...T...]h..V...;t..W...;t..q...;t..Z...;t..C...T.....;t..?...;t..U...;t ..U...RichT.....PE..d...2.....".....t.....@.....@.....0=.....xK.....0..@F...@..$.....9.....T..... .....X..(...@1.....}..p...D.....text...@r.....t..... ..`.rdata.....x.....@..@.data.....x.....@....pdata..$....@.....@.. @.didat..... .....@....rsrc...@F...0...H.....@..@.reloc...9.....:...&.....@..B..... .....

C:\Users\user\AppData\Local\zshP\VERSION.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2125824
Entropy (8bit):	3.5538487124192493

C:\Users\user\AppData\Local\zshP\VERSION.dll	
Encrypted:	false
SSDEEP:	12288:uVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:zfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	2393DBDB7B83B4F04D36585D7BD53D12
SHA1:	6763ADDEF91982DBC7A1C8FD23653BB470BBA183
SHA-256:	82E108220C59CA7F0733EBC7BE4B484A040DBF2AE89061599CA60C1951D4206B
SHA-512:	9A1EAB4660873C76A882ADA54F163825C71E3D4F96D3F682531B47E6F69F5FEDF32E3CE572FE39D02572CCC7515CD559B135CE9BEC5E6F3DBDBF825244FC36B
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.'..DN^......" .....P.....p.....@.....p .....@lx}..b.....` .+....c.....h.....$#..... .....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\zshP\sigverif.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	74752
Entropy (8bit):	6.227529985586147
Encrypted:	false
SSDEEP:	1536:yGD6cQz4lg9F+JrM+FqrEGtxzAZT3WuEs:Uccg9kC+FqrEGkB7
MD5:	8BADFA1EAEC018D2EDFE5630577F0B0F
SHA1:	43091FDC6B068E36FE0AE374A0C096C8912ACD5B
SHA-256:	DA824555DB880996AEF4DF4C68B499139040A4EA68D533E676059A12C8563BEB
SHA-512:	080FED8F14CD192CDD4602504E82F8906B64EA9991D81C07B4BDF63BFABD2B257D7355E6546A83B223F817E231C5496362D73D2E6001B83D81F8CE704EE9165
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<...R_..R_..R_..W^..R_..Q^..R_..V^..R_..S^..R_..S_..R_..Z^..R_..._..R_..P^..R_Rich..R_.....PE..d....{.T....."....r.....`x.....@.....p.....&x....`..... .....d.....`.....`.. .....T..... .....text....p.....r..... ..`.rdata...$.....&...v.....@..@.data.....@....pdata.....@..@.rsrc...`..... .....@..@.reloc.. ....`....."....@..B.....

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\bc49718863ee53e026d805ec372039e9_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	4442
Entropy (8bit):	5.475608894086636
Encrypted:	false
SSDEEP:	48:jZnGgUWSn/oB2Nagg5JtGgWHTMVZnGgUWs6cVfKJlD9Ow1K0sjOWLek:jZGg1iaBodTsZGg6Xl7DEB
MD5:	265559C6982B3A4CF08B093CA2B36B05
SHA1:	38AB5D305B69D0CB9EE68066CD9BF77529AB3DDF
SHA-256:	CAD2600DEE248B2D18B8CDAA66194C1580B21F01FDDBFCD51D0C3912059EFB99
SHA-512:	E9845473C172D7C81326A242EC78D102A9FF2693E2848577907DD944CAB0AD62E0DF6C543EEE744C1802DEF402749557F493AE23622B664A94BC9CB704DCAC7
Malicious:	false
Reputation:	unknown
Preview:	.....user.....user.....RSA1.....].~."l..I..Ee..Y.M4..|.....Box.....bUB5..3...!....I.@.....i.E..|W..#v.J.. bJ0#..v.3.'....!\OBL7....Wj....S....m.Y...e.j.....z..O.....K.cY..C....a.....,...C.r.y.p.t.o.A.P.I. .P.r.i.v.a.t.e. .K.e.y....f..... .....iX....c...."..Jq....Xp..(p.ty..... .....Z....TT=..He....?.....8..a.#X.s..g..._.....:uG.9.....[.R...._..D.!.....\.A.&...~.F..C.....4...'....0.H4k..BLP..M...e~...._..?..4Q.*...2]..]L0=.sf.6..8..w....o.>..!...../.o.i...A{*.Q.GH.v...c.;. ..h.w|)..I..k.Ka.B.....)LF.N.}I.4D..k$._..0.Q..ID.By..\...S.....Y-.i2.J%].h..q...2.i..w.."=KZ..B.1..9[H.QW.....3Z.;C`.....>.._%..c...[#D..gh...`...X")R<...~8..6K....%.....&.\.[.7$..q.I..[....cx..J..2.b....s....$.....m7...PB.....c..]7....rZ|.w#f4..z..U..}.U/p..`..].??.d..^Y....N..[r....yD....G...q..>..#t...i.....}M.`

Static File Info

General

File type:	PE32+ executable (DLL) (console) x86-64, for MS Windows

General

Entropy (8bit):	3.5870494758907925
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:	3PgaI7gtQn.dll
File size:	2121728
MD5:	8a6f4fe59b41d74501e04f1b451dc57d
SHA1:	064f5eca3efd02c5f40a8c9e7fedb86aa40eeed0
SHA256:	d7cb31b51d497eaac81246a38db0abd05398832fb301cb1b97d1ca979df2a4ca
SHA512:	4dfb736dc4e967f964d4a8eac22808fd7249fe39500752bf8b2cc9c197107bc6347ba7da07f20dda47b7d7bd14217792a81222e60f7d648918a93f222ab8084c
SSDEEP:	12288:1VI0W/TtlPLfJCm3WIYxJ9yK5lQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:sfP7fWsK5z9A+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

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
.favk	0x160000	0x1f7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vhtukj	0x161000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.hmbyox	0x1a7000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.djv	0x1a8000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.hpern	0x1a9000	0x706	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.czzwqg	0x1aa000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.jxjvn	0x1ab000	0xbf6	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.jfsnsk	0x1ac000	0x1f7	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
.nzvifv	0x1ad000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tops	0x1ae000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.lrjye	0x1b0000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.qwdob	0x1b1000	0x6cd0	0x7000	False	0.00177873883929	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.xcq	0x1b8000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ifxvj	0x1b9000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.fgpyt	0x1ba000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tgzhe	0x1bc000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.oocus	0x1bd000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ybtor	0x203000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.gxixek	0x204000	0x1f2a	0x2000	False	0.413330078125	data	5.51434056843	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: 6272 Parent PID: 6460

General

Start time:	10:51:52
Start date:	28/09/2021
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe 'C:\Users\user\Desktop\3PgaI7gtQn.dll'
Imagebase:	0x7ff690cb0000
File size:	140288 bytes
MD5 hash:	A84133CCB118CF35D49A423CD836D0EF
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: 00000000.00000002.826268433.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 2600 Parent PID: 6272

General

Start time:	10:51:53
Start date:	28/09/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\3PgaI7gtQn.dll',#1
Imagebase:	0x7ff622070000
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: 900 Parent PID: 6272

General

Start time:	10:51:53
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false

Commandline:	rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,CopyPropVariant
Imagebase:	0x7ff6d7cd0000
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: 00000002.00000002.760994382.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 1444 Parent PID: 2600

General

Start time:	10:51:53
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe 'C:\Users\user\Desktop\3PgaI7gtQn.dll',#1
Imagebase:	0x7ff6d7cd0000
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: 00000003.00000002.666186606.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 900

General

Start time:	10:51:54
Start date:	28/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000
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: 2824 Parent PID: 6272

General

Start time:	10:51:56
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,CreatePropVariant
Imagebase:	0x7ff6d7cd0000
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: 00000006.00000002.673965568.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities — Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 1572 Parent PID: 6272

General

Start time:	10:52:00
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,CreatePropertyStore
Imagebase:	0x7ff6d7cd0000
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: 00000007.00000002.681251793.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities — Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 5184 Parent PID: 6272

General

Start time:	10:52:03
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,DestroyPropVariant
Imagebase:	0x7ff6d7cd0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000008.00000002.688453025.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 2872 Parent PID: 6272

General

Start time:	10:52:07
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,FormatTagFromWfx
Imagebase:	0x7ff6d7cd0000
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: 00000009.00000002.698430783.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 6116 Parent PID: 6272

General

Start time:	10:52:10
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,GetAMSubtypeFromD3DFormat

Imagebase:	0x7ff6d7cd0000
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.00000002.703548461.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 7164 Parent PID: 6272

General

Start time:	10:52:14
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,GetD3DFormatFromMFSubtype
Imagebase:	0x7ff6d7cd0000
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: 0000000B.00000002.710759124.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 5560 Parent PID: 6272

General

Start time:	10:52:17
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,MFAddPeriodicCallback
Imagebase:	0x7ff6d7cd0000
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: 0000000D.00000002.718583222.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 5568 Parent PID: 6272

General

Start time:	10:52:21
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,MFAllocateSerialWorkQueue
Imagebase:	0x7ff6d7cd0000
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: 0000000F.00000002.726244001.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 4100 Parent PID: 6272

General

Start time:	10:52:24
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,MFAllocateWorkQueue
Imagebase:	0x7ff6d7cd0000
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: 00000010.00000002.733013846.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 3416 Parent PID: 6272

General

Start time:	10:52:28
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,MFAllocateWorkQueueEx
Imagebase:	0x7ff6d7cd0000
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: 00000011.00000002.741881097.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 6764 Parent PID: 6272

General

Start time:	10:52:32
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,MFAppendCollection
Imagebase:	0x7ff6d7cd0000
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: 00000013.00000002.749401860.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 6704 Parent PID: 6272

General

Start time:	10:52:35
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,MFAverageTimePerFrameToFrameRate
Imagebase:	0x7ff6d7cd0000
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: 00000014.00000002.756539402.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 6700 Parent PID: 6272

General

Start time:	10:52:38
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,MFBeginCreateFile
Imagebase:	0x7ff6d7cd0000
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: 00000015.00000002.820144134.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: bdeunlock.exe PID: 3976 Parent PID: 3424

General

Start time:	10:52:40
Start date:	28/09/2021
Path:	C:\Windows\System32\bdeunlock.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\bdeunlock.exe
Imagebase:	0x7ff6563e0000
File size:	286232 bytes
MD5 hash:	FAB70105E2075EEC9C249A4D499CAE7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 4200 Parent PID: 6272

General

Start time:	10:52:42
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,MFBeginGetHostByName
Imagebase:	0x7ff6d7cd0000
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: 00000017.00000002.776537982.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: bdeunlock.exe PID: 2912 Parent PID: 3424

General

Start time:	10:52:46
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\bnfeSWnf\bdeunlock.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\bnfeSWnf\bdeunlock.exe
Imagebase:	0x7ff77b970000
File size:	286232 bytes
MD5 hash:	FAB70105E2075EEC9C249A4D499CAE7C
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: 0000001B.00000002.783009139.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 2464 Parent PID: 6272

General

Start time:	10:52:47
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,MFBeginRegisterWorkQueueWithMMCSS
Imagebase:	0x7ff6d7cd0000
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: 0000001C.00000002.783658899.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: CameraSettingsUIHost.exe PID: 6660 Parent PID: 3424

General

Start time:	10:52:50
Start date:	28/09/2021
Path:	C:\Windows\System32\CameraSettingsUIHost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\CameraSettingsUIHost.exe
Imagebase:	0x7ff72c230000
File size:	32104 bytes
MD5 hash:	34F32BC06CDC7AF56607D351B155140D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: rundll32.exe PID: 6832 Parent PID: 6272

General

Start time:	10:52:51
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,MFBeginRegisterWorkQueueWithMMCSSEx
Imagebase:	0x7ff6d7cd0000
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: 0000001E.00000002.794067616.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: CameraSettingsUIHost.exe PID: 6744 Parent PID: 3424

General

Start time:	10:52:55
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\43ip\CameraSettingsUIHost.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\43ip\CameraSettingsUIHost.exe
Imagebase:	0x7ff7fd010000
File size:	32104 bytes
MD5 hash:	34F32BC06CDC7AF56607D351B155140D
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.00000002.800645636.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: rundll32.exe PID: 1492 Parent PID: 6272

General

Start time:	10:52:55
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\3PgaI7gtQn.dll,MFBeginUnregisterWorkQueueWithMMCSS
Imagebase:	0x7ff6d7cd0000
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: 00000020.00000002.802131007.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: pwcreator.exe PID: 1848 Parent PID: 3424

General

Start time:	10:52:58
Start date:	28/09/2021
Path:	C:\Windows\System32\pwcreator.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\pwcreator.exe
Imagebase:	0x7ff7f0e90000
File size:	800768 bytes
MD5 hash:	BF33FA218E0B4F6AEC77616BE0F5DD9D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: pwcreator.exe PID: 4984 Parent PID: 3424

General

Start time:	10:52:58
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\NfgW4al\pwcreator.exe

Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\NfgW4al\pwcreator.exe
Imagebase:	0x7ff647f70000
File size:	800768 bytes
MD5 hash:	BF33FA218E0B4F6AEC77616BE0F5DD9D
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: 00000023.00000002.812206472.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, ReversingLabs

Disassembly

Code Analysis