ID: 492692
Sample Name: rPP7AHsBQt
Cookbook: default.jbs
Time: 22:57:37
Date: 28/09/2021
Version: 33.0.0 White Diamond

Table of Contents

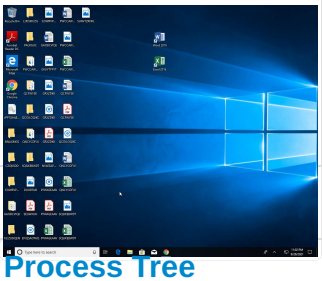
Windows Analysis Report rPP7AHsBQt

Overview

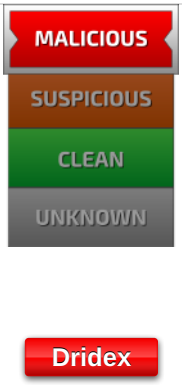
General Information

Sample Name:	rPP7AHsBQt (renamed file extension from none to dll)
Analysis ID:	492692
MD5:	6966f6e2c68c1f5..
SHA1:	c10eace5e0b5c0...
SHA256:	67e634c8f431ed6.
Tags:	Dridex exe
Infos:	

Most interesting Screenshot:



Detection

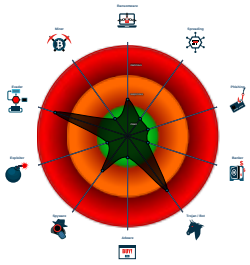


Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- Queues an APC in another process …
- Windows Update Standalone Installe…
- Uses Atom Bombing / ProGate to in…
- Queries the volume information (nam…
- Contains functionality to check if a d…
- May sleep (evasive loops) to hinder …

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 5548 cmdline: loaddll64.exe 'C:\Users\user\Desktop\rPP7AHsBQt.dll' MD5: E0CC9D126C39A9D2FA1CAD5027EBBD18)
  - cmd.exe (PID: 4312 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\rPP7AHsBQt.dll',#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 5560 cmdline: rundll32.exe 'C:\Users\user\Desktop\rPP7AHsBQt.dll',#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 2716 cmdline: rundll32.exe C:\Users\user\Desktop\rPP7AHsBQt.dll,HidD_FlushQueue MD5: 73C519F050C20580F8A62C849D49215A)
    - explorer.exe (PID: 3292 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - RDVGHelper.exe (PID: 6456 cmdline: C:\Windows\system32\RDVGHelper.exe MD5: 0BF1E2262C95164A0B244174167FBD85)
      - RDVGHelper.exe (PID: 6464 cmdline: C:\Users\user\AppData\Local\2YZyR\RDVGHelper.exe MD5: 0BF1E2262C95164A0B244174167FBD85)
      - wusa.exe (PID: 6884 cmdline: C:\Windows\system32\wusa.exe MD5: 04CE745559916B99248F266BBF5F9ED9)
      - wusa.exe (PID: 6940 cmdline: C:\Users\user\AppData\Local\v74M\wusa.exe MD5: 04CE745559916B99248F266BBF5F9ED9)
      - Dxpserver.exe (PID: 3476 cmdline: C:\Windows\system32\Dxpserver.exe MD5: DCCB1D350193BE0A26CEAFF602DB848E)
      - Dxpserver.exe (PID: 4116 cmdline: C:\Users\user\AppData\Local\30KRxXoL\Dxpserver.exe MD5: DCCB1D350193BE0A26CEAFF602DB848E)
      - InfDefaultInstall.exe (PID: 6700 cmdline: C:\Windows\system32\InfDefaultInstall.exe MD5: 5FDB30927E9D4387D777443BF865EEFD)
      - InfDefaultInstall.exe (PID: 6708 cmdline: C:\Users\user\AppData\Local\AzSj\InfDefaultInstall.exe MD5: 5FDB30927E9D4387D777443BF865EEFD)
      - sethc.exe (PID: 7036 cmdline: C:\Windows\system32\sethc.exe MD5: 1C0BF0B710016600C9D9F23CC7103C0A)
      - sethc.exe (PID: 7068 cmdline: C:\Users\user\AppData\Local\hxqisrGT\sethc.exe MD5: 1C0BF0B710016600C9D9F23CC7103C0A)
      - DevicePairingWizard.exe (PID: 6340 cmdline: C:\Windows\system32\DevicePairingWizard.exe MD5: E23643C785D498FF73B5C9D7EA173C3D)
      - DevicePairingWizard.exe (PID: 5596 cmdline: C:\Users\user\AppData\Local\9Q3FqD\DevicePairingWizard.exe MD5: E23643C785D498FF73B5C9D7EA173C3D)
  - rundll32.exe (PID: 1748 cmdline: rundll32.exe C:\Users\user\Desktop\rPP7AHsBQt.dll,HidD_FreePreparsedData MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5480 cmdline: rundll32.exe C:\Users\user\Desktop\rPP7AHsBQt.dll,HidD_GetAttributes MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
00000004.00000002.346721215.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
0000001C.00000002.402645228.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000024.00000002.460431340.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
0000001F.00000002.434908663.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000008.00000002.259769048.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
Click to see the 6 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

E-Banking Fraud:

Yara detected Dridex unpacked file

Persistence and Installation Behavior:

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

HIPS / PFW / Operating System Protection Evasion:

Benign windows process drops PE files

Changes memory attributes in foreign processes to executable or writable

Queues an APC in another process (thread injection)

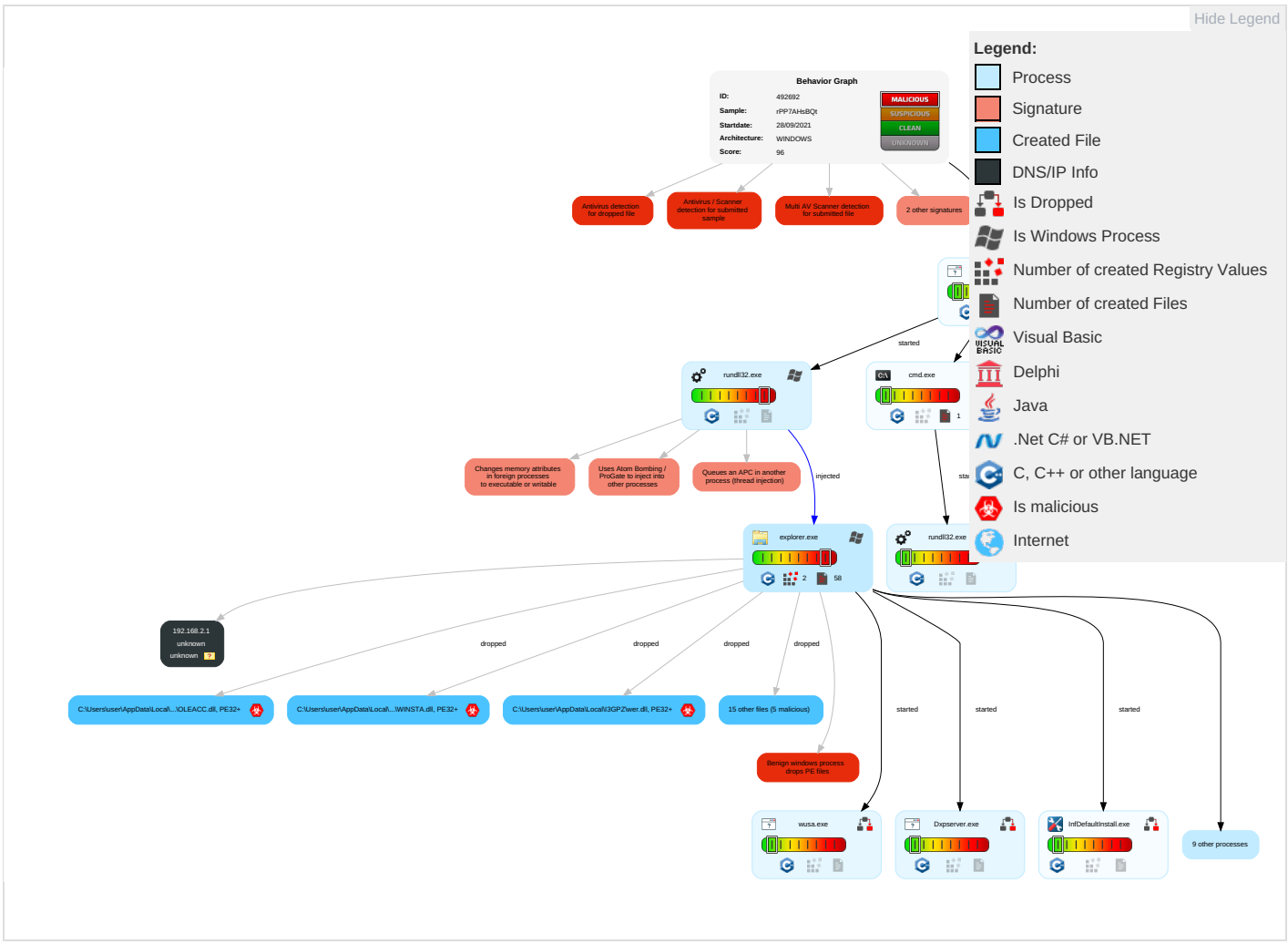
Uses Atom Bombing / ProGate to inject into other processes

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comman and Cont

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comman and Cont
Valid Accounts 1	Command and Scripting Interpreter 1 2	Valid Accounts 1	Valid Accounts 1	Masquerading 1	Input Capture 1	System Time Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel
Default Accounts	Exploitation for Client Execution 1	Boot or Logon Initialization Scripts	Access Token Manipulation 1 1	Valid Accounts 1	LSASS Memory	Security Software Discovery 2 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Junk Data
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 3 1 3	Virtualization/Sandbox Evasion 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganog
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Imperson
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 3 1 3	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	System Information Discovery 2 5	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonl Used Por
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Rundll32 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicatio Layer Pro
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Prot
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Timestomp 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Trans Protocols

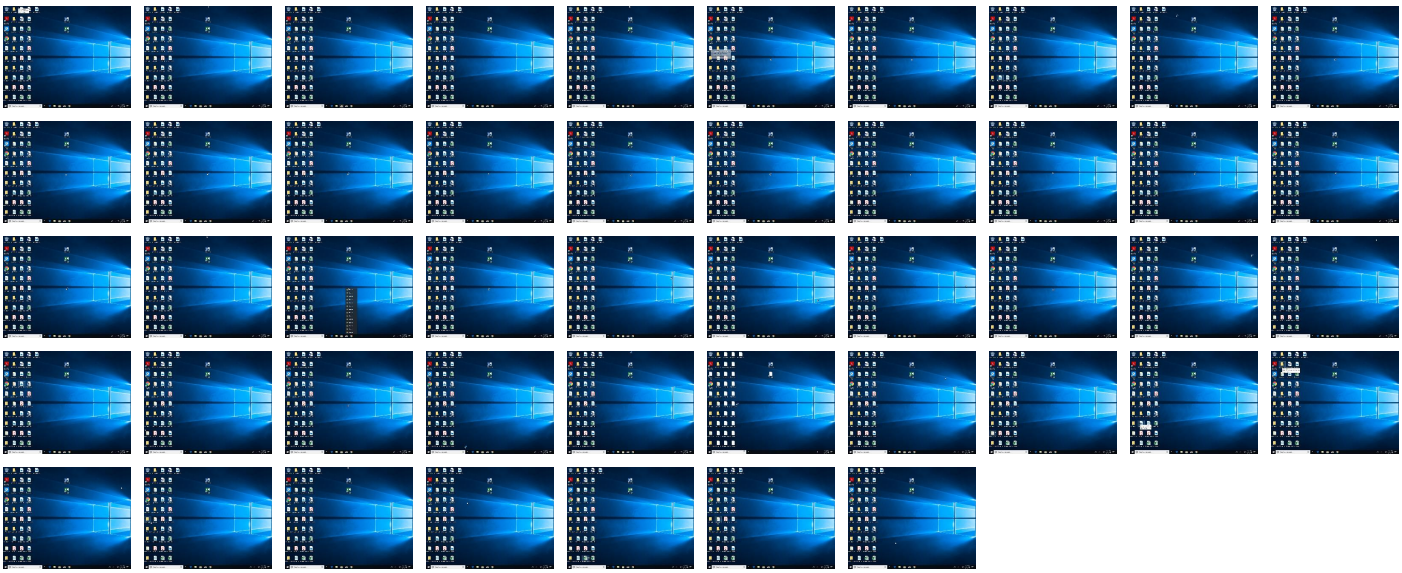
Behavior Graph



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
rPP7AHsBQt.dll	60%	Metadefender		Browse
rPP7AHsBQt.dll	76%	ReversingLabs	Win64.Infostealer.Dridex	
rPP7AHsBQt.dll	100%	Avira	TR/Crypt.ZPACK.Gen	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\9Q3FqD\MFC42u.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\CDG6Inqi\VERSION.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\30KRxXoL\dwmapi.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\I3GPZ\wer.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\2YZyR\WTSAPI32.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\hxqisrGT\OLEACC.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\QpqMx\WINSTA.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\AzSj\newdev.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\2YZyR\WTSAPI32.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\2YZyR\RDVGHelper.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\2YZyR\RDVGHelper.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\30KRxXoL\Dxpserver.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\30KRxXoL\Dxpserver.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\9Q3FqD\DevicePairingWizard.exe	0%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\9Q3FqD\DevicePairingWizard.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\AzSj\InfDefaultInstall.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\AzSj\InfDefaultInstall.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.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
5.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.2.wusa.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
23.2.RDVGHelper.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
31.2.Dxpserver.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
36.2.InfDefaultInstall.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
38.2.sethc.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
41.2.DevicePairingWizard.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

Source	Detection	Scanner	Label	Link
http://schemas.microsoft.coG	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

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:	492692
Start date:	28.09.2021
Start time:	22:57:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 21s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	rPP7AHsBQt (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:	mal96.troj.evad.winDLL@41/19@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 64.5% (good quality ratio 57.4%) • Quality average: 83.3% • Quality standard deviation: 34%
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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\2YZyR\RDVGHelper.exe	4CYPSBYNYQ.dll	Get hash	malicious	Browse	
	RVoWoXkXlE.dll	Get hash	malicious	Browse	
	DC2zX44MQr.dll	Get hash	malicious	Browse	
	itB5x2K4T3.dll	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	hR33M29cgO.dll	Get hash	malicious	Browse	
	ujc4RSCWM6.dll	Get hash	malicious	Browse	
	VJRmwvPkMp.dll	Get hash	malicious	Browse	
	zW80EdEp4O.dll	Get hash	malicious	Browse	
	BUal7Z7t7a.dll	Get hash	malicious	Browse	
	RG2JwdyFZp.dll	Get hash	malicious	Browse	
	xmNOO4kr1W.dll	Get hash	malicious	Browse	
	J68J8AW3wu.dll	Get hash	malicious	Browse	
	eIqCS9Cchl.dll	Get hash	malicious	Browse	
	0oSZeHvzK2.dll	Get hash	malicious	Browse	
	6mRFq6lDxY.dll	Get hash	malicious	Browse	
	hwhmwAJCgs.dll	Get hash	malicious	Browse	
	FzIHOw5IB1.dll	Get hash	malicious	Browse	
	TBt2yq48s1.dll	Get hash	malicious	Browse	
	ElRN8C51mm.dll	Get hash	malicious	Browse	
	peUe7aKWzZ.dll	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\2YZyR\RDVGHelper.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	107008
Entropy (8bit):	6.213211715541241
Encrypted:	false
SSDEEP:	1536:jZPv9YEIT8g15BZNWNBWNK5/FzUJmufD6o6ffv+Difx1P4dirH+Z3sUS+CvilU/s:lPBLBBbWDwff22J1Puq+y+HUk
MD5:	0BF1E2262C95164A0B244174167FBD85
SHA1:	81BD08AD31BF2665F298406F843924588BB7606B
SHA-256:	6B35C354C480D232A96EF73EABA268EF7D94F30A3D3A1161B69081B048A27E29
SHA-512:	FD01664A377359E72A67F52E8DFFDD237E24F8ACC158B3A478F71CAAC1CE2EDDB19B15E1FC66CB73E77DDED564D6A98FD3064BDA20419D8C949505457721BI5C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: 4CYPSBYNYQ.dll, Detection: malicious, Browse • Filename: RVoWoXkXlE.dll, Detection: malicious, Browse • Filename: DC2zX44MQr.dll, Detection: malicious, Browse • Filename: itB5x2K4T3.dll, Detection: malicious, Browse • Filename: hR33M29cgO.dll, Detection: malicious, Browse • Filename: ujc4RSCWM6.dll, Detection: malicious, Browse • Filename: VJRmwvPkMp.dll, Detection: malicious, Browse • Filename: zW80EdEp4O.dll, Detection: malicious, Browse • Filename: BUal7Z7t7a.dll, Detection: malicious, Browse • Filename: RG2JwdyFZp.dll, Detection: malicious, Browse • Filename: xmNOO4kr1W.dll, Detection: malicious, Browse • Filename: J68J8AW3wu.dll, Detection: malicious, Browse • Filename: eIqCS9Cchl.dll, Detection: malicious, Browse • Filename: 0oSZeHvzK2.dll, Detection: malicious, Browse • Filename: 6mRFq6lDxY.dll, Detection: malicious, Browse • Filename: hwhmwAJCgs.dll, Detection: malicious, Browse • Filename: FzIHOw5IB1.dll, Detection: malicious, Browse • Filename: TBt2yq48s1.dll, Detection: malicious, Browse • Filename: ElRN8C51mm.dll, Detection: malicious, Browse • Filename: peUe7aKWzZ.dll, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....L.....g.....g.....g.....g.....g.....g.w....g.....Rich..... ....PE..d.....o....."......B...b.....`G.....@.....`..... .....T.....$.....T.....g.....h..... .....text....@.....B..... ..`.rdata...A...`...B...F.....@..@.data.....@....pdata..T.....@..@.rsrc.....@..@.r eloc..$.....@..B..... .....

C:\Users\user\AppData\Local\2YZyR\WTSAPI32.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1781760
Entropy (8bit):	4.12006401986381
Encrypted:	false

C:\Users\user\AppData\Local\2YZyR\WTSAPI32.dll	
SSDEEP:	12288:OVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:TfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	00AED0EC34CFF50E3619BF8D25D97B52
SHA1:	DBFAC54FBF1A32D749AA02C0BE92943FCEB27847
SHA-256:	F4DF23DDEDE2B0C6EAFE9CDD3B02A701F433CBCCD30E9E75D2F8B6E767C56D1B
SHA-512:	4F32E6C34262317DBDB0DCA25C62788AAE5F8E179A663DE0414F4EEE80BEAEB9E11B32FE6DBD00129896989ECB6D82A7F22D17EC5F301067860649DA6FFAF14
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.#..DN^....." .....p.....@.....0.....@lx}..b..... .....c.....h.....$#..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\30KRxXoL\Dxpserver.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	304640
Entropy (8bit):	5.920357039114308
Encrypted:	false
SSDEEP:	6144:SidsFxbUPoT/FPrriCEe+oiXoGJm7JwQ9oWxDEHZwj:xaFxbFDBsBo6maPWxDcwj
MD5:	DCCB1D350193BE0A26CEAFF602DB848E
SHA1:	02673E7070A589B5BF6F217558A06067B388A350
SHA-256:	367CEA47389B6D5211595AE88454D9589AA8C996F5E765904FFEDE434424AF22
SHA-512:	ECD3C32E2BED31FC6328CA4B171B5D2503A2795324667F67FF48A67DF7C8B88760A62C0119A173487B9886E6AF3994025A85E42B064BEA38A466A6848AF65541
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9. E}.N.}.N.}.N...M.~.N...J.d.N...K.{.N...O.X.N.}.O.F.N...G.[.N....|.N..L.|.N.Rich}.N.....PE..d....z....."..... .....`.....@..... .....|....0..H..... .....p...`...T.....<.....=.....text...<..... ..`.rdata..6.....@..@.data.....@....pdata.. .....@..@.rsrc...H....0.....@..@.reloc..p.....@..B.....

C:\Users\user\AppData\Local\30KRxXoL\dwmapi.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1781760
Entropy (8bit):	4.118074670013424
Encrypted:	false
SSDEEP:	12288:6VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:nfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	120EA6047784304E8B9D9B314F5A5F7A
SHA1:	D5AB85335BDF4D948E00BCE3FF956AE83290CB8F
SHA-256:	E2A042740FCFBFCFD12B5D4F078BD806A24BC434F01B881F3DB799AE72564AC6
SHA-512:	763498B2F8F4B1861E7AF7BC89488D3492FECF60A3175CAFEED5F3C5B4002C1266D22F28694D146CC075760BCF05324B9756255140D1AD697838692B3AB40D7E
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.#..DN^....." .....p.....@.....0.....@lx}..b..... ..&....c.....h.....$#..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\9Q3FqD\DevicePairingWizard.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	92160
Entropy (8bit):	5.664138088677901
Encrypted:	false
SSDEEP:	1536:D/BmrFjio5/vzDSPwiEKi3xGyibqZ3qOT3:9mp5SwiEKWZiTo3
MD5:	E23643C785D498FF73B5C9D7EA173C3D
SHA1:	56296F1D29FC2DCBFAA1D991C87B10968C6D3882

C:\Users\user\AppData\Local\9Q3FqD\DevicePairingWizard.exe	
SHA-256:	40F423488FC0C13DED29109F8CC1C0D2CCE52ECB1BD01939EF774FE31014E0F4
SHA-512:	22E29A06F19E2DA941A707B8DA7115E0F5962617295CC36395A8E9B2A98F0239B6519B4BF4AB1DC671DEF8CD558E8F59F4E50C63130D392D1E085BBF6B710914
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%...a...a...a...h...o.....b.....r.....i.....j...a.....c.....j.`.....`...Richa..... .....PE..d...x.1".....".....\.....b.....@.....H...`..... .....|..T.....`r.....`s..8 .....text....[.....\..... ..`.rdata...-...p.....`.....@..@.data... .....@....pdata.....@..@.rsrc.....@..@.re loc.....f.....@..B..... .....

C:\Users\user\AppData\Local\9Q3FqD\MFC42u.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1806336
Entropy (8bit):	4.151016544012089
Encrypted:	false
SSDEEP:	12288:kVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1Mh:BfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	3F5481C3CF2BB7FAAFEEFB882A08F15D
SHA1:	B4FB8B3B5DE6F799F30A7B16D69D7B14A8A99119
SHA-256:	A20E653ECB06D68CF4D410F1BF596E0D924ADC851E8287E140427D6382F9601D
SHA-512:	7115E2589D5195D04556909B122FDE4AC1B803343005159B274644535580F6A166C3CA16881DE70CBBE53E2F498FE27538786A129D52AE28B42089F4A3EBFDD1
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....|...|...|....K.#}...'...}.....{}....X.#}....f..|....g..}..*...a|.....}....N..}..*... E}..[.I.E|...'..U}....N.+}..[.K.P|..[.K./}...I.h}..u.Y.k|.....|..W"...|..b.L.t|...|...}.....N|..2%...|..Rich.|.....PE..d.# ..DN^....." .....p.....p.....@.....@lx}..b..... ...l...c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\AzSj\InfDefaultInstall.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	13312
Entropy (8bit):	4.871127662725052
Encrypted:	false
SSDEEP:	192:kXe0PT5V21py9AA/lvmBfXWqFwO6Wdz3ios9aW/GW:kXe5pgAMhAXWq6OFZcaW/GW
MD5:	5FDB30927E9D4387D777443BF865EEFD
SHA1:	E802BE85298183F050141EAEB87930657A8E07A6
SHA-256:	C57CE112AB04B00CC7270B6D76F005FFB8E2ED3ADC6904CF5C5F184EE077FA32
SHA-512:	776F5B5640C22373E641DE4C3C6F4C7DFF0CD39662108B8DFA070EE0A867B3A6401976BD2B78BC766D469105AF2E6E466C4140FFE40C49146BB6B09591676773
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....mo..mo..mo..j..mo..l..mo..k..mo..n..mo..mn..mo..g..mo.... .mo..m..mo.Rich.mo.....PE..d.....K.....".....&.....@.....@.....p.....?:....`..... .....&.....P.....@.....`.. ....#..T..... ....!.....text...@..... ..`.rdata..... .....@..@.data.....0..... .....@....pdata.....@.....".....@..@.rsrc.... ....P.....$.....@..@.reloc.. ....`.....2.....@..B..... .....

C:\Users\user\AppData\Local\AzSj\newdev.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1781760
Entropy (8bit):	4.114146296909227
Encrypted:	false
SSDEEP:	12288:FVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:cfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	D3B5C0D22ED8729DA2FAD2B5D1E5932A
SHA1:	66679B519C5CB18C370DA672A9FC16A76CEEA6E7
SHA-256:	CFE9832E3DD1A7E2FEDAB63B25CB7C8EB95EFF8A0D5607B7D54C97258350EC7B
SHA-512:	9D2A70ECA5CDECE764EDFAE3D6C71B9D61E582469EDE505555068DBEF0FF006694550C7E653513C98BCC3B6363B8BD0549C8AB6B7159E08296845C64CED053 7
Malicious:	**true**

C:\Users\user\AppData\Local\AzSj\newdev.dll	
Antivirus:	• Antivirus: Avira, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.#..DN^......" .....p.....@.....0.....@lx}..b..... ..]....c.....h.....$#..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\CDG6Inqi\VERSION.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1781760
Entropy (8bit):	4.112814429004735
Encrypted:	false
SSDEEP:	12288:0VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:xfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	422CF18F068925A7705B12D5EAB257B2
SHA1:	4E1B2934052304DABEC01A71EAD49AEFE67E7D12
SHA-256:	06778AE98D60D4D961C551CA1004830899F54BE06226E2249BF547F930BA43E1
SHA-512:	FEE21A47E88855116FE44A021F6F5BD4524568941FA54A552E857951E08A27E0869F102A45608AFB56C17D1120EA69116B5E0DF41DFF8FFD8002FB7FD0A0D4C7
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.#..DN^......" .....p.....@.....0.....@lx}..b..... ..+....c.....h.....$#..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\CDG6Inqi\wscript.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	163840
Entropy (8bit):	5.729539450068024
Encrypted:	false
SSDEEP:	1536:8HSpBlnak9UH8bCAHZ1LQ434syPz7M5hh/kzhwS827HuYHwHugXEYJ6S7775MWUn:aC4HWCp/fM5hvNebgXEYJN73uWUZxtt
MD5:	9A68ADD12EB50DDE7586782C3EB9FF9C
SHA1:	2661E5F3562DD03C0ED21C33E2888E2FD1137D8C
SHA-256:	62A95C926C8513C9F3ACF65A5B33CBB88174555E2759C1B52DD6629F743A59ED
SHA-512:	156CAED6E1BF27B275E4BA0707FB550F1BF347A26361D6D3CAD12C612C327686950B47B6C5487110CF8B35A490FAADC812ADE3777FFF7ED76A528D970914A6E
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....n.....Rich.....PE..d....U.E....."....2...R.....@*.....@.....8w...`.....8...8.....T.....T.....text..."1.....2..... ..`.rdata..F....P.....6.....@..@.data.....@....pdata.....@..@.rsrc.....@..@.reloc..T.....t.....@..B.....

C:\Users\user\AppData\Local\I3GPZ\wbengine.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1535488
Entropy (8bit):	6.5079506357027785
Encrypted:	false
SSDEEP:	24576:UgSNpxTPrVDqUtzohGP5ilEI1T4N9sS4aC+369riDQMbbKoLtHWwtPJhVx8OIC9h:UtNpxTPrVuUtMhGRuEAc3sfaYhiDXmod
MD5:	6E235F75DF84C387388D23D697D6540B
SHA1:	A97DE324726F3ECBA383863CB643E4AD5DADB4DC
SHA-256:	7113DD02243E9368EF3265CF5A7F991F9B4D69CAB70B1A446062F8DD714AFC8E
SHA-512:	F294A7F7AD6FAD1E2F2E82123AFB78B76E56C603EF3FA37CDD73992DE91640EB55E2F002072DD57B850B1D7E9162F49B4DE973CFE71DF35DAD958B439E1F28A
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....|r..|r..|r..q..|r..v..|r..w..|r..s..|r..|s..}r..{.M|r..r..|r.....|r..p..|r.Rich.|r.....PE..d...!....."....z.....p.....@.....v....`..... .....|..... ...u.....@...T.....=..(....<.....(=.....text..... ..`.rdata..b.... .....@..@.data....&.....@....pdata...u... ...v.....@..@.rsrc.....Z.....@..@.reloc.....f.....@..B.....

C:\Users\user\AppData\Local\I3GPZ\wer.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1785856
Entropy (8bit):	4.122378222596304
Encrypted:	false
SSDEEP:	12288:7VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:afP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	6D04485BF586C674E145F2F40AB3C577
SHA1:	12065B852C5AAD44370755290123E4EEC3A0BFBA
SHA-256:	CC04B9DE9881C5F6B5B320AAE8CB4DE4CE2C7C32F8BBEC92C72DAD59F59685EE
SHA-512:	959D86E8CCB86137AA97F58C7B8424764EC0DEB524809505AFEF170097801389F78415AE4FDB439C3D2815D2BE797959FBF6DE15C48A18312D9C3723667D2C99
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.#..DN^..... " ....p.....@.....@.....@lx}..b..... ..W....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\QpqMx\RdpSaUacHelper.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	29184
Entropy (8bit):	5.483991269470949
Encrypted:	false
SSDEEP:	384:x1i6wkbsVQCy+MmItEV3DAOnKjXxyWzyWpaTeinj7qHk9FyMWagW:x1TwgsmCRMmIcTRnKbQW/kj7uk2U
MD5:	DA88A7B872B1A52F2465D12CFBA4EDAB
SHA1:	8421C2A12DFF33B827E8A6F942C2C87082D933DB
SHA-256:	6A97CF791352C68EFFEFCBE3BB23357A76D93CB51D08543ED993210C56782627
SHA-512:	CA96D8D423235E013B228D05961ED5AA347D25736F8DFC4C7FEB81BFA5A1193D013CD29AA027E1793D6835E52F6557B3491520D56DE7C09F0165F1D5C8FD9ED
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....& ..bA..bA..bA..k9..`A...%..cA...%..`A...%..pA...%..uA..bA...A...%..hA...%p.cA...%..cA..RichbA.....PE..d...?.1V....."....6...>..... =.....@.....f....`..... .....4k.....f..T.....U.....V.....text....4.....6..... ..`.rdata...'...P...(...:.....@..@.data.....b.....@....pdata.....d.....@..@..@.rsrc.....f.....@..@.reloc.....p.....@..B.....

C:\Users\user\AppData\Local\QpqMx\WINSTA.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1785856
Entropy (8bit):	4.130571614423483
Encrypted:	false
SSDEEP:	12288:vVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:GfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	5343AEA48CE4722D13097BBF228724E0
SHA1:	D2FA1C270C847B97C8C170C4D7EA2D80470600F7
SHA-256:	819E3D7921B463B88EBB76E6C7C97880A6CCFD5F4F530A4F707EC4D1B2143D7B
SHA-512:	322512540578740AF0AC1C4959B288A08B0CFB820FBE94852BB3F165A05A433911F92B8CAE10FEF67F973F53D5A8919954540D062E6B5A53CC67956438CBF35F
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.#..DN^..... " ....p.....@.....@.....@lx}..b..... ..m....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\hxqisrGT\OLEACC.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1781760
Entropy (8bit):	4.1144286325107045
Encrypted:	false

C:\Users\user\AppData\Local\hxqisrGT\OLEACC.dll	
SSDEEP:	12288:aVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:HfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	40558B8832E21854D8782294C56CFF29
SHA1:	C0D4D63CF9B0803AA202861D6C6767E8C6DAB11D
SHA-256:	9201A707728F3D83E5787741F4FF978AF65DC004E85A51B0851B9DA53A4DA2DE
SHA-512:	8886F06A86DFD0F30DCC07E9179F68003EDEC537597BE16F36EC74750F95F2A21908F04F139FB09EC63F4C207599657D784026E6E07E78C48435F220E08EDD4D
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.#..DN^....." .....p.....@.....0.....@lx}..b..... .....c.....h.....$#..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\hxqisrGT\sethc.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	284160
Entropy (8bit):	6.85709982153028
Encrypted:	false
SSDEEP:	6144:z1dgUn5C1AlGr66uFz2LJGRg4kLNnei36cw:XiKFCdUc
MD5:	1C0BF0B710016600C9D9F23CC7103C0A
SHA1:	EFA944D43F76AEA0C72A5C7FB3240ADC55E7DAE8
SHA-256:	AEA110EE0865635EE764B1B40409DB3A3165E57EFFF4CAF942BCD8982F3063C5
SHA-512:	775F075A9D43A887B1AFB000E5E2CBC8EF514C4B1864C694977342307C61173DACC5BA8E5D47002870687B24914B3E6D2D0EB48BF99517822511A8BA2A122515
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r../6q.\|6q.\|6q.\|Y..}5q.\|Y..} q.\|Y..}1q.\|Y..}-q.\|6q.\|8p.\|Y..}$q.|Y.[|7q.|Y..}7q.|Rich6q.|.....PE..d.... ....."..... .....@..... ..`..... .....P.....`..h'...P.....x.....T..... .....0.....0.....text..... ..`.rdata...j.....l.....@..@.data...8....0.....@....pdata.....P.....$.....@..@.rsrc...h'...`... (...,.....@..@.reloc..x.....T.....@..B.....

C:\Users\user\AppData\Local\v74M\WTSAPI32.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1781760
Entropy (8bit):	4.120050321896044
Encrypted:	false
SSDEEP:	12288:8VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:JfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	9DDB78BD96C660A463481D09DD4F4564
SHA1:	1A01B02E0E8DD5E040EA22DDB751B8A0052823C1
SHA-256:	24D3AB5E4FD539E035CEB9FE4311C0F8DC19FEEE0C07C08429CAD81FEB386D19
SHA-512:	172A2B8CB9E650BBFF677263567B68132514BD23E2B21101037819A54F1B41B9A2983DA37D101B69E8A110C667CCB9A66DA00722A94F9DE4DBE79486D8D90812
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.#..DN^....." .....p.....@.....0.....@lx}..b..... .....c.....h.....$#..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\v74M\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

C:\Users\user\AppData\Local\v74M\wusa.exe	
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\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\eb42b1a5c308fc11edf1ddbdd25c8486_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	4462
Entropy (8bit):	5.464123225028128
Encrypted:	false
SSDEEP:	48:eq8hbUtZS9Ok9c3cIz2XwQ8KdIoiIEOBAUq8hbU0C1Dtm+7bHjGo973/YVFJ:eV5iZL3d6F8mfNV59C1DtbPao9wVFJ
MD5:	AB09C0D653A04FE6626151A759C9807C
SHA1:	B672006CC0146E3408482C264F8C01EEAAA62843
SHA-256:	9BCAEE6BF895589362D63560EA6B703BDA67147311A2FABCDB1590FC19E09C09
SHA-512:	451CA012C1DB77B533FCAA32D7AEB6F2103621AE5855CFC15E7533500643AC7438A11437656486B9C06B0D00A63DF5D5AB28F0C99A9B0915C0BD57CF696BCBF
Malicious:	false
Preview:	.....user.....user.....RSA1.....9.h.U.....sr.k.....JAS..7#.Qt...{.....E.{./.O.....oO..pu..w.\R^._w.....k.....=5.c\IG .7E5@me...n....d."..bNd....x.S.....z..O.....F..yQ.C..8..m.....,...C.r.y.p.t.o.A.P.I. .P.r.i.v.a.t.e. .K.e.y....f..... ...F.j5.._Z.LuT...OTfb...f.Q..... ..._1.S...]F.r..) ..C[..N^.fxT.]N.....y.9..~...1...%.$.l<.5....2....z..Q.....#./..$4.....6...d[....Z?.D@..=.7.[....\.....sU^.33.]]....G..Tr...t.'&....f.f. .....g1..4....R...t0a.V.....rm.dZ....<..o..k;....us!.|... .RM.....r..A.>8%.q....Q..."...o.....0..-O.E.....vU...;...._:`..+.:.....!.....G_.....k._/.<..KP..n.3F..<.....o.+..... .&.tUx..>0.&..`Ar.,...\l..=..8.Y..#.....I ..'.k4.W..(....."DQd.5G...- 4.%{z.N..`...r..n.....nF...x.8..1~..p`.s-...9..*.....=3..".E..E...)...VU.J.<o..*.?.z.g...`bt..K..D....G....|..

Static File Info

General

File type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Entropy (8bit):	4.124181284517686
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:	rPP7AHsBQt.dll
File size:	1777664
MD5:	6966f6e2c68c1f536d63b50bb966c031
SHA1:	c10eace5e0b5c0531895ed1d02332e3e8bd0fd32
SHA256:	67e634c8f431ed69d672dca57c2bd493772b24fdee37432aa8fc3e1822f0b804
SHA512:	365cefcf86f2d1b12e59d819c3dda9733003592a6a3cbf010b15d543547f2de2038dc659301a3f454881b76c644d929bb24c382bb70b349a621f95047457c19f
SSDEEP:	12288:RVl0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:gfP7fWsK5z9A+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

General

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	0x64fd0	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
.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
.tblq	0x110000	0x5a7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.hcmjm	0x111000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.nagyk	0x157000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.jrucz	0x158000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rnr	0x159000	0x3fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ths	0x15a000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vyfudm	0x15b000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bejn	0x15c000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.lxdw	0x15d000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.uffn	0x15e000	0x3ba	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.cbmla	0x15f000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.fcy	0x160000	0x451c2	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.aady	0x1a6000	0x706	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pqe	0x1a7000	0x1e66	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.zfem	0x1a9000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ila	0x1aa000	0x1af	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ygqg	0x1ab000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.onr	0x1ac000	0x3ba	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.brn	0x1ad000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.zch	0x1ae000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.yithue	0x1af000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.jxyn	0x1b0000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bvk	0x1b1000	0x5a7	0x1000	False	0.189453125	data	2.59802364405	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: 5548 Parent PID: 3316

General

Start time:	22:58:35
Start date:	28/09/2021
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe 'C:\Users\user\Desktop\rPP7AHsBQt.dll'
Imagebase:	0x7ff7ea5b0000
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: 00000001.00000002.273240568.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 4312 Parent PID: 5548

General

Start time:	22:58:36
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\rPP7AHsBQt.dll',#1

Imagebase:	0x7ff7bf140000
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: 2716 Parent PID: 5548

General

Start time:	22:58:36
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\rPP7AHsBQt.dll,HidD_FlushQueue
Imagebase:	0x7ff60f080000
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: 00000004.00000002.346721215.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 5560 Parent PID: 4312

General

Start time:	22:58:36
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe 'C:\Users\user\Desktop\rPP7AHsBQt.dll',#1
Imagebase:	0x7ff60f080000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000005.00000002.252486367.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3292 Parent PID: 2716

General

Start time:	22:58:38
Start date:	28/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff662bf0000
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: 1748 Parent PID: 5548

General

Start time:	22:58:39
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\rPP7AHsBQt.dll,HidD_FreePreparsedData
Imagebase:	0x7ff60f080000
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: 00000008.00000002.259769048.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 5480 Parent PID: 5548

General

Start time:	22:58:43
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\rPP7AHsBQt.dll,HidD_GetAttributes
Imagebase:	0x7ff60f080000
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.00000002.266794445.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: RDVGHelper.exe PID: 6456 Parent PID: 3292

General

Start time:	22:59:23
Start date:	28/09/2021
Path:	C:\Windows\System32\RDVGHelper.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\RDVGHelper.exe
Imagebase:	0x7ff7f5b00000
File size:	107008 bytes
MD5 hash:	0BF1E2262C95164A0B244174167FBD85
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: RDVGHelper.exe PID: 6464 Parent PID: 3292

General

Start time:	22:59:24
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\2YZyR\RDVGHelper.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\2YZyR\RDVGHelper.exe
Imagebase:	0x7ff787770000
File size:	107008 bytes
MD5 hash:	0BF1E2262C95164A0B244174167FBD85
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: 00000017.00000002.375513310.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

File Activities

Show Windows behavior

File Read

Analysis Process: wusa.exe PID: 6884 Parent PID: 3292

General

Start time:	22:59:36
Start date:	28/09/2021
Path:	C:\Windows\System32\wusa.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wusa.exe
Imagebase:	0x7ff6d6a20000
File size:	308736 bytes
MD5 hash:	04CE745559916B99248F266BBF5F9ED9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: wusa.exe PID: 6940 Parent PID: 3292

General

Start time:	22:59:37
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\v74M\wusa.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\v74M\wusa.exe
Imagebase:	0x7ff6d6590000
File size:	308736 bytes
MD5 hash:	04CE745559916B99248F266BBF5F9ED9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000001C.00000002.402645228.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Read

Analysis Process: Dxpserver.exe PID: 3476 Parent PID: 3292

General

Start time:	22:59:50
Start date:	28/09/2021
Path:	C:\Windows\System32\Dxpserver.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\Dxpserver.exe
Imagebase:	0x7ff639f30000
File size:	304640 bytes
MD5 hash:	DCCB1D350193BE0A26CEAFF602DB848E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: Dxpserver.exe PID: 4116 Parent PID: 3292

General

Start time:	22:59:52
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\30KRxXoL\Dxpserver.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\30KRxXoL\Dxpserver.exe
Imagebase:	0x7ff7d7eb0000
File size:	304640 bytes
MD5 hash:	DCCB1D350193BE0A26CEAFF602DB848E
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.00000002.434908663.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

File Activities

Show Windows behavior

File Read

Analysis Process: InfDefaultInstall.exe PID: 6700 Parent PID: 3292

General

Start time:	23:00:03
Start date:	28/09/2021
Path:	C:\Windows\System32\InfDefaultInstall.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\InfDefaultInstall.exe
Imagebase:	0x7ff703950000
File size:	13312 bytes
MD5 hash:	5FDB30927E9D4387D777443BF865EEFD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: InfDefaultInstall.exe PID: 6708 Parent PID: 3292

General

Start time:	23:00:04
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\AzSj\InfDefaultInstall.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\AzSj\InfDefaultInstall.exe
Imagebase:	0x7ff6ee8a0000
File size:	13312 bytes
MD5 hash:	5FDB30927E9D4387D777443BF865EEFD
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: 00000024.00000002.460431340.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

File Activities Show Windows behavior

File Read

Analysis Process: sethc.exe PID: 7036 Parent PID: 3292

General

Start time:	23:00:16
Start date:	28/09/2021
Path:	C:\Windows\System32\sethc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\sethc.exe
Imagebase:	0x7ff64dfa0000
File size:	284160 bytes
MD5 hash:	1C0BF0B710016600C9D9F23CC7103C0A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sethc.exe PID: 7068 Parent PID: 3292

General

Start time:	23:00:16
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\hxqisrGT\sethc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\hxqisrGT\sethc.exe
Imagebase:	0x7ff61c020000
File size:	284160 bytes
MD5 hash:	1C0BF0B710016600C9D9F23CC7103C0A
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: 00000026.00000002.487070134.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: DevicePairingWizard.exe PID: 6340 Parent PID: 3292

General

Start time:	23:00:30
Start date:	28/09/2021
Path:	C:\Windows\System32\DevicePairingWizard.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\DevicePairingWizard.exe
Imagebase:	0x7ff61e4c0000
File size:	92160 bytes
MD5 hash:	E23643C785D498FF73B5C9D7EA173C3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: DevicePairingWizard.exe PID: 5596 Parent PID: 3292

General

Start time:	23:00:37
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\9Q3FqD\DevicePairingWizard.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\9Q3FqD\DevicePairingWizard.exe
Imagebase:	0x7ff6159d0000
File size:	92160 bytes
MD5 hash:	E23643C785D498FF73B5C9D7EA173C3D
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: 00000029.00000002.533624086.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

Disassembly

Code Analysis