ID: 492086
Sample Name: X5C9EzCB7A
Cookbook: default.jbs
Time: 10:48:48
Date: 28/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Windows Analysis Report X5C9EzCB7A

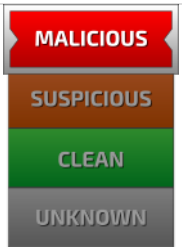
Overview

General Information

Sample Name:	X5C9EzCB7A (renamed file extension from none to dll)
Analysis ID:	492086
MD5:	dc4fca98a02c5cc..
SHA1:	4cecd255d9176ff..
SHA256:	ae087f890f576dc..
Tags:	exe
Infos:	

Most interesting Screenshot:

Detection



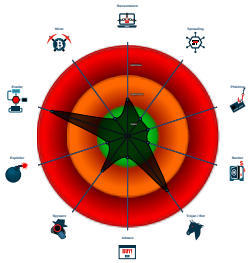
Dridex

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

Signatures

- Yara detected Dridex unpacked file
- Multi AV Scanner detection for subm…
- Benign windows process drops PE f…
- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Changes memory attributes in foreig…
- Machine Learning detection for samp…
- DLL side loading technique detected
- Queues an APC in another process …
- Machine Learning detection for dropp…
- Windows Update Standalone Installe…
- Uses Atom Bombing / ProGate to in…

Classification



- **System is w10x64**
- loaddll64.exe (PID: 2368 cmdline: loaddll64.exe 'C:\Users\user\Desktop\X5C9EzCB7A.dll' MD5: A84133CCB118CF35D49A423CD836D0EF)
  - cmd.exe (PID: 5760 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\X5C9EzCB7A.dll',#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 5356 cmdline: rundll32.exe 'C:\Users\user\Desktop\X5C9EzCB7A.dll',#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 2192 cmdline: rundll32.exe C:\Users\user\Desktop\X5C9EzCB7A.dll,AddGadgetMessageHandler MD5: 73C519F050C20580F8A62C849D49215A)
    - explorer.exe (PID: 3292 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - wermgr.exe (PID: 6572 cmdline: C:\Windows\system32\wermgr.exe MD5: FF214585BF10206E21EA8EBA202FACFD)
      - wermgr.exe (PID: 6600 cmdline: C:\Users\user\AppData\Local\M5A\wermgr.exe MD5: FF214585BF10206E21EA8EBA202FACFD)
      - WFS.exe (PID: 6640 cmdline: C:\Windows\system32\WFS.exe MD5: CD6ACF3B997099B6CFB2417D3942F755)
      - WFS.exe (PID: 6652 cmdline: C:\Users\user\AppData\Local\QEkvVts\WFS.exe MD5: CD6ACF3B997099B6CFB2417D3942F755)
      - wusa.exe (PID: 6888 cmdline: C:\Windows\system32\wusa.exe MD5: 04CE745559916B99248F266BBF5F9ED9)
      - wusa.exe (PID: 6912 cmdline: C:\Users\user\AppData\Local\8FwY\wusa.exe MD5: 04CE745559916B99248F266BBF5F9ED9)
  - rundll32.exe (PID: 1596 cmdline: rundll32.exe C:\Users\user\Desktop\X5C9EzCB7A.dll,AddLayeredRef MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 2840 cmdline: rundll32.exe C:\Users\user\Desktop\X5C9EzCB7A.dll,AdjustClipInsideRef MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 4156 cmdline: rundll32.exe C:\Users\user\Desktop\X5C9EzCB7A.dll,AttachWndProcA MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 2888 cmdline: rundll32.exe C:\Users\user\Desktop\X5C9EzCB7A.dll,AttachWndProcW MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 2916 cmdline: rundll32.exe C:\Users\user\Desktop\X5C9EzCB7A.dll,AutoTrace MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 1064 cmdline: rundll32.exe C:\Users\user\Desktop\X5C9EzCB7A.dll,BeginHideInputPaneAnimation MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6288 cmdline: rundll32.exe C:\Users\user\Desktop\X5C9EzCB7A.dll,BeginShowInputPaneAnimation MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6360 cmdline: rundll32.exe C:\Users\user\Desktop\X5C9EzCB7A.dll,BuildAnimation MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6388 cmdline: rundll32.exe C:\Users\user\Desktop\X5C9EzCB7A.dll,BuildDropTarget MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6404 cmdline: rundll32.exe C:\Users\user\Desktop\X5C9EzCB7A.dll,BuildInterpolation MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6428 cmdline: rundll32.exe C:\Users\user\Desktop\X5C9EzCB7A.dll,CacheDWriteRenderTarget MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6484 cmdline: rundll32.exe C:\Users\user\Desktop\X5C9EzCB7A.dll,ChangeCurrentAnimationScenario MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6524 cmdline: rundll32.exe C:\Users\user\Desktop\X5C9EzCB7A.dll,ClearPushedOpacitiesFromGadgetTree MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6620 cmdline: rundll32.exe C:\Users\user\Desktop\X5C9EzCB7A.dll,ClearTopmostVisual MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6752 cmdline: rundll32.exe C:\Users\user\Desktop\X5C9EzCB7A.dll,CreateAction MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000020.00000002.357738953.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000013.00000002.294331565.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
0000001B.00000002.332178412.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000000.00000002.452046176.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000019.00000002.324869275.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
Click to see the 16 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

System Summary:

PE file contains section with special chars

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

DLL side loading technique detected

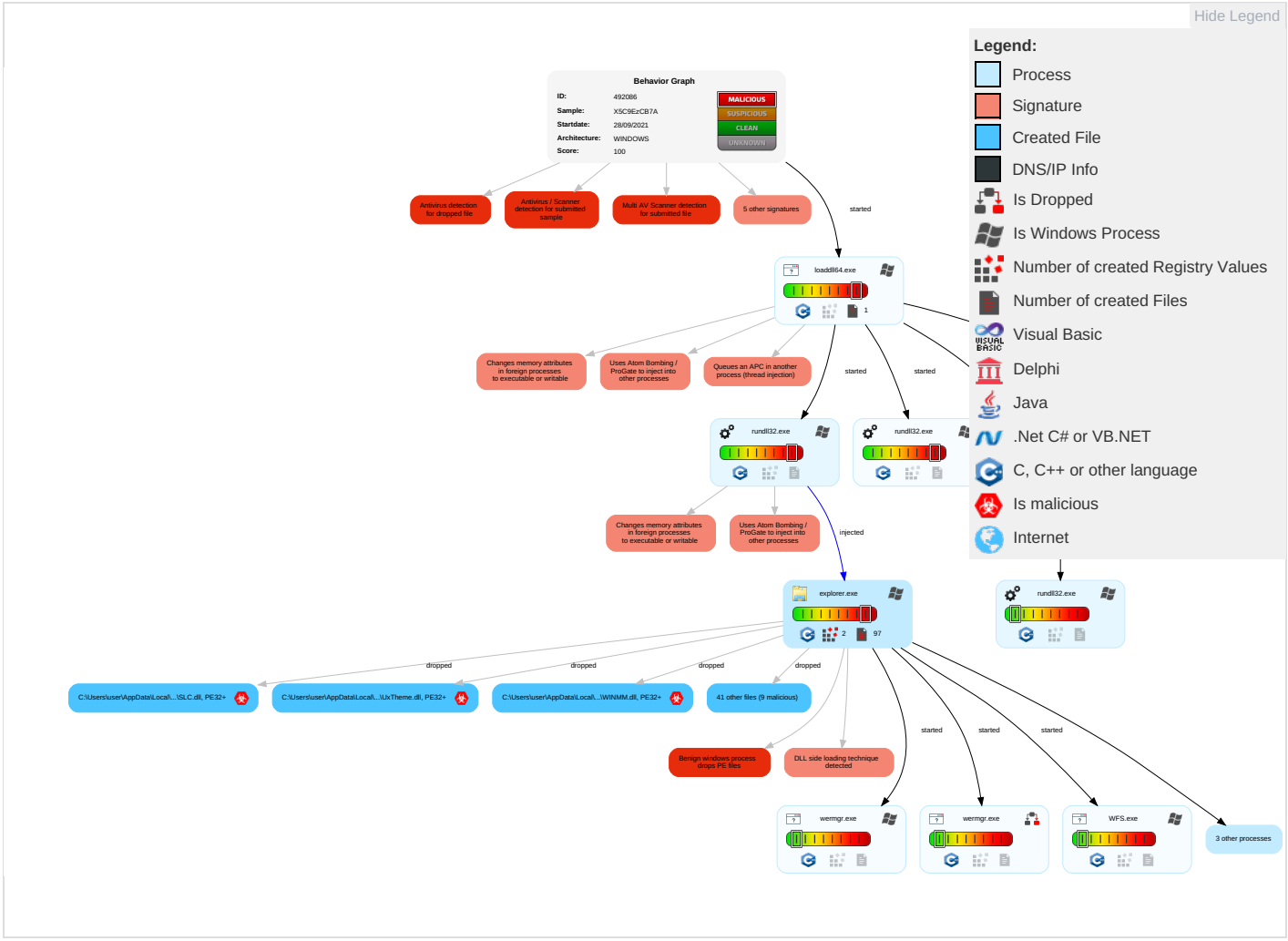
Queues an APC in another process (thread injection)

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

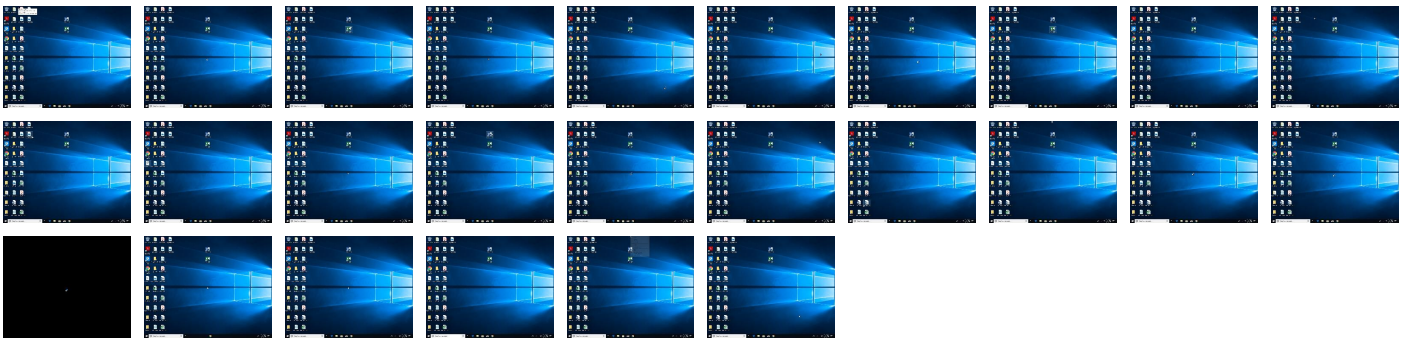
Behavior Graph



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
X5C9EzCB7A.dll	65%	Virustotal		Browse
X5C9EzCB7A.dll	57%	Metadefender		Browse
X5C9EzCB7A.dll	76%	ReversingLabs	Win64.Infostealer.Dridex	
X5C9EzCB7A.dll	100%	Avira	HEUR/AGEN.1114452	
X5C9EzCB7A.dll	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\9Krbbc\ACTIVEDS.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\8FwY\dpx.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\2vl\DUI70.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\0Nty\ReAgent.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\2vl\DUI70.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\M5A\wer.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\4DETSU\MFC42u.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\B8nn\XmlLite.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\Mnd\VERSION.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\4DETSU\MFC42u.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\Mnd\VERSION.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\2vl\DUI70.dll	100%	Avira	HEUR/AGEN.1114452	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\QEkvVts\WINMM.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\T6Vn91tw0\SLC.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\Nom\WTSAPI32.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\SB1jY1h\UxTheme.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\9Krbbc\ACTIVEDS.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\8FwY\dpx.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\2vl\DUI70.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\0Nty\ReAgent.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\2vl\DUI70.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\M5A\wer.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\4DETSU\MFC42u.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\B8nn\XmlLite.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Mnd\VERSION.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\4DETSU\MFC42u.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Mnd\VERSION.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\2vl\DUI70.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\QEkvVts\WINMM.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\T6Vn91tw0\SLC.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Nom\WTSAPI32.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\SB1jY1h\UxTheme.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\0Nty\recdisc.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\0Nty\recdisc.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\0Nty\recdisc.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\2vl\LicensingUI.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\2vl\LicensingUI.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\2vl\LicensingUI.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\4DETSU\FXSCOVER.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
31.2.wermgr.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.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
29.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
27.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
40.2.wusa.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
6.2.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
34.2.WFS.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
35.2.rundll32.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
24.2.rundll32.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
25.2.rundll32.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

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	492086
Start date:	28.09.2021
Start time:	10:48:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	X5C9EzCB7A (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@91/45@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 45.6% (good quality ratio 43.1%) • Quality average: 91.3% • Quality standard deviation: 25.6%
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\0Nty\ReAgent.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2121728
Entropy (8bit):	3.564329528703889
Encrypted:	false
SSDEEP:	12288:OVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:TfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	0F2CD68909E4CA4CB2925A2D530E611D
SHA1:	C797BFE2EB15E848B6F88E55873C03656F2399F1
SHA-256:	8E807BDF55D7676C4D761950196962D65D9202DE71C74542CA46C30DF3EA85C8
SHA-512:	0CEF9556A0802A23CEE42E76E2A749A7530E7B72F5F1E64462AEF6B9C5ADA48E02353910A2820CB7A64D72763A16094B0AB73335997BEEA8F77C19691F78073D
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.+ ..DN^....." .....@.....p.....@.....` .....@lx}..b.....P .....c.....h.....$#..... ..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\0Nty\recdisc.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	192512
Entropy (8bit):	6.154101271794163
Encrypted:	false
SSDEEP:	3072:H4SpDkUbgEHxW3BIovAuegPO8evTq2VC:H4/3BdFegEv+2V
MD5:	D2AEFB37C329E455DC2C17D3AA049666
SHA1:	69C5182FDC8A86009113EE721C8F1632F7B3D2DB
SHA-256:	A65F86E8EC62BEB3019E368E506DAB21FF872097EBF3FAEB4A3B23F2A08DFCE9
SHA-512:	DD5D63D79FD9E43560291687E0B41B71D6ECA55F033FE94BAA4FAF4CB967F6480CAC4F5481B3102F0589A65AFA473F5637B1C31C522329A275461F3D8C4353A3
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown

C:\Users\user\AppData\Local\0Nty\recdisc.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....e_...1...1...1..|....1..`5...1..`2...1..`4...1..`0...1...0...1..`8...1..`...1..`3 ...1.Rich..1.....PE..d...+38.....".....@.....@.....`..... .....|..... ..0.....0.....0m..T.....9.. (....8.....9.....text..... ..`.rdata...f...0...h.....@..@.data...`a.....Z.....@....pdata.....@..@.rsrc...0.... ... .@..@.reloc.....0.....@..B..... .....

C:\Users\user\AppData\Local\2vl\DUI70.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2404352
Entropy (8bit):	4.094137841436053
Encrypted:	false
SSDEEP:	12288:dVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1T:EfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	B6247D6791F82E58D5D33122BD0F7C54
SHA1:	CC03732CEC968973E9F1AF26AFBEEB5D0F55FC3F
SHA-256:	7AD71B0114C68798E5B61F406FCEDEA1F12F3BD2C70EDC0C35C35A4EADAF9F7C
SHA-512:	889B7AD402B8A162EC9C277BD08F227AEE9AB566B28721964F38A50D8A1DADA3FC4F99ECF361167586B4269D935BFD6A2A8465FDE6514E95F08528016CE268D
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, 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.....P .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\2vl\LicensingUI.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	146776
Entropy (8bit):	6.610587238297347
Encrypted:	false
SSDEEP:	3072:bjUURMlqPDQJX08E16Oa1bwcdnaevk2i2tMZd:39ilq7AxE4OaR1aymv
MD5:	BA2B32F8E3717F4A9CA3D400410E539A
SHA1:	87FFA0CBBE8B528E2263EE7121264011D1F5C5A4
SHA-256:	EC53F4520A49115D6E6CEE8CF896BCCA84E425BFB76E3FA904665F2A2F957BC8
SHA-512:	FC5DA9B26C395CA2191C4FDC0F06F37D75D67404D49C38EF75189ACC0817D02CED290559848C687DD74DD33F62DC36F1AD15A017E4977014CFE83025D22F59
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5T..[...[...[.....[...X...[...._...[...^...[...Z...[...Z...[...R...[.....[...Y...[.Rich.. [.....PE..d.....Y.....".....x.....@.....p.....9..... .....P..H....@..@.....X'...`.P.....T.....(..... .....text...,..... ..`.imrsiv.....rdata..rV.....X.....@..@.data.....0.....@....pdata..@....@..... .....@..@.rsrc...H....P.....@..@.reloc..P....`.....@..B..... .....

C:\Users\user\AppData\Local\4DETSU\FXSCOVER.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	232960
Entropy (8bit):	5.805361894084464
Encrypted:	false
SSDEEP:	6144:v4J/ihC4Tb5//Jfl+QL+ooODUwq306Q/:v4khC4h/qiooT06Q/
MD5:	BEAB16FEFCB7F62BBC135FB87DF7FDF2
SHA1:	EAF18190494496329573CAA3F95CACA6EF0FB6F6
SHA-256:	E3C66F68737611DFD051F1D6EEB371FDE89B129925A85695B9F90CDE3E04BD96

C:\Users\user\AppData\Local\4DETSU\FXSCOVER.exe	
SHA-512:	FF4E756B1D928C97523ADE2B30FAB56219659AA22E7F5D71CB3238A2C39E1C704C6A046C2DC14FA5207CE8E8C75CD7EF5416B36A1452D97D929A5686C75D2C3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....).I.H...H...H...,...H...,...H...,...H...H...K...,...H...,...H...,...H..Rich.H.....PE..d.....3.....".....@.....0...`..... .....h1...`.....T.....c..(....b..... .....d.....text...~..... ..`.rdata..... .....@..@.data.....@.....&.....@....pdata.....`.....6.....@..@.rsrc...h1.....2...N..... ..@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\4DETSU\MFC42u.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2146304
Entropy (8bit):	3.60023617437132
Encrypted:	false
SSDEEP:	12288:mVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1K47:7fP7fWsK5z9A+WGAW+V5SB6Ct4bnbK
MD5:	44E6F4AE82E198545E40858C95CB304A
SHA1:	64799A505F32C595AB858A3F0DA66C69CC9C19DE
SHA-256:	A469E652E33BA0D7E248176ABCB460912B7EF9AFEE0B976D6ADB0BB26601D353
SHA-512:	B042C71C2B6DF38EF60A6371610699A5EBA0CE85CF5E894E82F3F3B352FC4D61E78BD1B3BC0E06768BBAA1CCA8B4A52AD2B2A8B801B6E6054A840509EB9B44B3
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.+..DN^....." .....p.....@..... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\8FwY\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):	3.5583371704739357
Encrypted:	false
SSDEEP:	12288:sVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:ZfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	84A402DFBA64739AF98A797BFF68AB60
SHA1:	C5734661A0BA49350157E021989BDB768178E607
SHA-256:	6AC1496F60796CA15B0DBB61A0C2D81D6CD406B4A273BC2E036EE2CC94C7A333
SHA-512:	127438FE3F4D1570234EC12CBA62994CBB5ED94D5519BAE69E9A993E59C58FC91FA6C6F97CA24E2320F94AF0481F039652926E5F0B8276F1B798C8D104BB7D53
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.+..DN^....." .....@.....p.....@.....` .....@\|x}..b.....P .....c.....h.....$#..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\8FwY\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

C:\Users\user\AppData\Local\8FwY\wusa.exe	
SHA1:	76FA00103A89C735573D1D8946D8787A839475B6
SHA-256:	1D86701A861FFA88FE050A466E04281A4809C334B16832A84231DC6A5FBC4195
SHA-512:	B4D2EF6B90164E17258F53BCAF954076D02EDB7F496F4F79B2CF7848B90614F6160C8EB008BA5904521DD8B1449840B2D7EE368860E58E01FBEAB9873B654B3A
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;..-..~..~..~v./~}.~....}.~....i.~....{.~....d.~..~w.~....k.~..C~~.~.... ~.~Rich..~.....PE..d.....TS....."....`...X.....f.....@.....g.....`..... .....I.....T...p.....`....?..T.....Pq..(. ..Pp.....xq..@.....text...3^.....`..... ..`.rdata..^....p.....d.....@..@.data.....`.....T.....@....pdata.....p.....X.....@..@.rsrc....T .....V...^.....@..@.reloc..`.....@..B..... .....

C:\Users\user\AppData\Local\9Krbbc\ACTIVEDS.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2121728
Entropy (8bit):	3.5609800893226784
Encrypted:	false
SSDEEP:	12288:XVl0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:efP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	2A0973FA588371BB4A19B6CC0C7E00ED
SHA1:	B441B28BA295D9223EEB4CCC6660177EEA7FEED7
SHA-256:	C063B7251B7AB553053CFCCE861C04C285D08830127403E2D0C888A48F71453D
SHA-512:	548B9DB967268DD17727AABD4A7A2A739236D4674C76A13D78C0ADAA4F74EBFDE7A0D755A0D2CA3B1559C9EB68EF24C3124363687FF8D33F806E8F3B67DCC5 E5
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.+ ..DN^....." .....@.....p.....@.....` .....@lx}..b.....P .y....c.....h.....$#..... ..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\9Krbbc\SppExtComObj.Exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	577024
Entropy (8bit):	7.365924302927238
Encrypted:	false
SSDEEP:	12288:KEpKNOQ/1mgFgnHF+2ryqfut4iob3vBzx4PQpIQbwhsi:lpKbbFgl+2OqfuqiOb3JUFs
MD5:	809E11DECADAEBE2454EFEDD620C4769
SHA1:	A121B9FC2010247C65CE8975FE4D88F5E9AC953E
SHA-256:	8906D8D8BCD7C8302A3E56EA2EBD0357748ACC9D3FDA91925609C742384B9CC2
SHA-512:	F78F46437C011C102A9BCEC2A8565EDC75500C9448AC17457FF44D3C8DB1980F772C0D1546F1DEE0F8A6F2C7273A5A915860B768DE9BB24EBEFE2907CE18B0 F
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%.].a.3.a.3.a.3.h.u.3...6.`.3...7.t.3...2.n.3.a.2...3...=.r.3...0.e.3... .`.3...1.`.3.Richa.3.....PE..d...b....."....0.....@.....CS P.....3..... .....Y..h.....J.....T..... .....S.....z..`.....text..... ..`?g_Encry.-..... ..`.rdata..._.....`.....@..@.data.....p.....V.....@....pdata...J..... L...d.....@..@.rsrc.....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\B8nn\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

C:\Users\user\AppData\Local\B8nn\Dxpserver.exe

SHA-512:	ECD3C32E2BED31FC6328CA4B171B5D2503A2795324667F67FF48A67DF7C8B88760A62C0119A173487B9886E6AF3994025A85E42B064BEA38A466A6848AF65541
Malicious:	false
Reputation:	unknown
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\B8nn\XmlLite.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2121728
Entropy (8bit):	3.5589287422510516
Encrypted:	false
SSDEEP:	12288:pVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:IfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	CF749BC5C2122F394AF6B2AA66EF71CD
SHA1:	0369F942C144F4B33B596FD0EBB58F71B2F6D26B
SHA-256:	14375D79237DA8A731ED43252FBFC4B53EED438945A2097C14FB4160EFAA2D73
SHA-512:	97E95B61EBAE640C6C8752859093671B81C7F49DBCE10035D956EB147A207D4390F767472CFE9CE710B611E63CBE9F484D135496AFE6B34DD4C954118A5B98C
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.+ ..DN^....." .....@.....p.....@..... ` .....@lx}..b.....P .....c.....h.....$#..... ..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\Bun\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
SHA-256:	40F423488FC0C13DED29109F8CC1C0D2CCE52ECB1BD01939EF774FE31014E0F4
SHA-512:	22E29A06F19E2DA941A707B8DA7115E0F5962617295CC36395A8E9B2A98F0239B6519B4BF4AB1DC671DEF8CD558E8F59F4E50C63130D392D1E085BBF6B710914
Malicious:	false
Reputation:	unknown
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\Bun\MFC42u.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2146304
Entropy (8bit):	3.5999443255720154
Encrypted:	false
SSDEEP:	12288:9VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:kfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	B8583BCD3646915D6FA965A033928155
SHA1:	A8A80A042BFB3F23980F78B5695411BE670C1DC0
SHA-256:	13BC74B3E5A8341A886C3C0F444783F611803D73BAA20202F18340FA5E48CA0D
SHA-512:	243E32A0A7FA8278CFD8EB838A8C6BB240043F21CAD1E33D20DA54CF2E3E3A5899BF45A23E6D4A7E1D7F2FADA7016E5F22AE9FE5A2D42651BD243C5EA16A68 AB
Malicious:	false

C:\Users\user\AppData\Local\Bun\MFC42u.dll	
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.+..DN^....." .....p.....@..... .....@lx}..b.....P ..l...c.....h.....$#..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\LnjKLu\DUI70.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2404352
Entropy (8bit):	4.094232719670622
Encrypted:	false
SSDEEP:	12288:rVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1bT:qfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	BA00B1255006B5B8A6F65DC6D2A59DAE
SHA1:	8CEC4C49EDF68431C794817D93C0FFCE933B4E2B
SHA-256:	095A00A6D3B5FDF367B389858F6F7CE9ED2483D26B878681DEEE96CE6F9EB1E6
SHA-512:	051D058BCBF12614CB08E393FEB4E938AC21A7EA4098157394BB962E4DA01EBD1C00DB28F0A51A17F439B5B62A415569B3B417DD1BDED5D702CC141A5E86BB1A
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.....P .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\LnjKLu\ProximityUxHost.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	264480
Entropy (8bit):	6.478365286411354
Encrypted:	false
SSDEEP:	6144:xSt+s2GFGbqEuzhJONjx9UVuCuHpwqr/vt9r+ULJBaBpcIFz:xStzFGbGhoPgMHpwqrHthUB6IF
MD5:	E7F0E9B3779E54CD271959C600A2A531
SHA1:	8006E2D1AA91798E48D8BFDE1EBF94A2D6BA6C0A
SHA-256:	155CE33E0E145314FE9D8911BE69B8CBBD2AC09B7B6D98363F9BAA277C71954E
SHA-512:	E10C3FD9C5F34260323CEC9E8EEDF2290F40254F0FFDCA582DB57D113B32871793CDFFF03D55941EF5E79FA8141803AB353BA4938357A4555233F2D090045338
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B..B..B..K.`.&..-..A..-...U..-...K..-..U..B..t..-...]..-...C..-..C..RichB.....PE..d...;.*Q....."..... .....@..... .....&..... .....H.....T..... +.....Pa..T.....p3..(...p2.....3. .....text..... ..`.imrsiv.....rdata..... .....@..@.data...x.....@....pdata..T.....@..@.rsrc...H.....@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\M5A\wer.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2125824
Entropy (8bit):	3.5693057153343792
Encrypted:	false
SSDEEP:	12288:5VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:4fP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	5F5B4F0BE7EDE9E5A344DF47CE0CDB88
SHA1:	25DA7FA0704227C2CA6F0F54EF5C73DF862198B2
SHA-256:	B582E1DF3773DD2B0345F7CFD286B8F8B18975849320C1EE87D827AB590CAA82
SHA-512:	7DB53F0BAE6E8E5F1499512097A6CBED579B98973A555AC5C590E720CA30FA241D7EC63FFDF565B5B8000127172EF21B110DCEEF3FFF7FDA3DB977C4ABF26F8
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown

C:\Users\user\AppData\Local\M5A\wer.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.+..DN^....." .....P.....p.....@.....p .....@lx}..b.....P .W....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\M5A\wermgr.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	209312
Entropy (8bit):	6.796289498157116
Encrypted:	false
SSDEEP:	6144:swTMBboFMSuc/9NPXWPJROo/wVJyB60OHyLC7vs:swTMB02SD/mXO64c2Hyw
MD5:	FF214585BF10206E21EA8EBA202FACFD
SHA1:	1ED4AE92D235497F62610078D51105C4634AFADE
SHA-256:	C48C430EB07ACC2FF8BDDD6057F5C9F72C2E83F67478F1E4A1792AF866711538
SHA-512:	24073F60B886C58F227769B2DD7D1439DF841784E43E753265DA761801FDA58FBEEDAC4A642E0A6ABDA40A6263153FAA1A9540DF6D35E38BF0EE5327EA55B4FE
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....(j.jl..jl..jl..c1...l...-..il...-..ql..jl...H...-..ml...-..`l...-..Kl...-..kl...-..kl..Richjl.....PE..d...p....."....,.....`(.....@.....p.....`..... .... ..0:.....!...`..\...@...T.....`Q.....`R.....t.....text...++.....,..... ..`.imrsiv.....@.....rdata.....P.....0.....@..@.data...X.....@....pdata.....@.@.@.didat..@.....@....rsrc...0:... ...<.....@..@.reloc..\....`.....@..B..... .....

C:\Users\user\AppData\Local\Mnd\VERSION.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2121728
Entropy (8bit):	3.559794578495645
Encrypted:	false
SSDEEP:	12288:kVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:BfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	1AE7DB0FD99F869562057B3685B4419F
SHA1:	B403937ABF171D7B76725FBDC003872D45C67502
SHA-256:	4FC37EF78A0B1F816556CF10A9942939832F72EF321F24B6BAF0152EDEB45D48
SHA-512:	55EFF618F7B54BEB965B7BFCC615351D00D9988504E9166E371EC9FDA7F4D9A9B305D2CC01EA2E9D4D70888403AF1AD5833DDB9DEA31DF8B5A6AD97E5032D6
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.+..DN^....." .....@.....p.....@.....` .....@lx}..b.....P .+....c.....h.....$#..... ..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\Mnd\wextract.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	143872
Entropy (8bit):	6.942627183104786
Encrypted:	false
SSDEEP:	3072:0BuGag041hcWp1icKAArDZz4N9GhbkUNEk95l:5hudp0yN90vE
MD5:	ED93B350C8EEFC442758A00BC3EEDE2D
SHA1:	ADD14417939801C555BBBFFAF7388BD13DE2DE42
SHA-256:	ABD6D466E30626636D380A3C9FCC0D0B909C450F8EA74D8963881D7C46335CED
SHA-512:	7BA8D1411D9AEE3447494E248005A43F522CA684839FCD4C4592946B12DC4E73B1FF86D8E843B25A73E3F2463955815470304E4F219B36DBC94870BEBF700581
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Mnd\wextract.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....e.....`.....`.....`.....`.....`.....`0.....`.....Rich..... .....PE..d...._{.....".....r.....w.....@.....R...`..... ....T..... ... .text....q.....r..... ..`.rdata..".....$...v.....@..@.data.....@....pdata.....@..@.rsrc.....@..@.reloc.. .....0.....@..B..... .....

C:\Users\user\AppData\Local\Nom\WTSAPI32.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2121728
Entropy (8bit):	3.5662350439042503
Encrypted:	false
SSDEEP:	12288:aVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:HfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	6AABBD46074D1F4BA508D5F48258EEEF
SHA1:	0D326013154DD896F67F2808340896E6B886DEE6
SHA-256:	CFD9A093AB4005696F5B11CD2599CED5A3DBC69F30E704BD5136B4B500FD140F
SHA-512:	0B975F80B2D713F97E5344B8702F888F97511967C93C9487E286A40B228AD0DF293094E0E2CB5D5FB1E7D5223BF15F919D86B6D689CFFF52B25646CCAA9EC629
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.+ ..DN^....." .....@.....p.....@.....` .....@lx}..b.....P .....c.....h.....$#..... ..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\Nom\mblctr.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	799744
Entropy (8bit):	6.62164167843942
Encrypted:	false
SSDEEP:	12288:y9Pyqz1mcI6upViTf8+RrhGi51qviizQBODAKylkm5ZUxXrc5Zh5ZG5Ze:yHz1m9dpVQRhL5kRzAKcjY8poA
MD5:	0CE1C2D873D151A19FB993139D19E68B
SHA1:	269BDAE3FBF1BE67FCC779720EF5C647AF98DC16
SHA-256:	DCDE80BC80BAD4FCEA64567B14C23595C407705E94EC2D1D39C8944039292904
SHA-512:	93D0ACC3C24D8E9388B7428320F4D16624E276B912914AF3D0ECBEC720491E546A619D000DF41C53DBB37F84B4CB1DF11C291908B05086BB49916E7F2BF9089
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;.4.Zag.Zag.Zag.".g.Zag.>bf.Zag.>ef.Zag.>df.Zag.>`f.Zag.Z`g.[ag.>hf.Zag.>.g.Zag.>cf.ZagRich.Zag.....PE..d....7>....."....t.....@.....%o...`..... .....S..p..... ....p..... 0..T.....text...Q..... ..`.rdata..>.....@..@.data.....l.....@....pdata.....x..... .....@..@.rsrc.....@..@.reloc.....p.....0.....@..B..... .....

C:\Users\user\AppData\Local\O8JNmHZW\VERSION.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2121728
Entropy (8bit):	3.55979090810396
Encrypted:	false
SSDEEP:	12288:5VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:4fP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	17E3E019DB12FE19F8993A2A664B0AF1
SHA1:	8436E71B27FF8EAF67D07D4F9BECB8175253F604
SHA-256:	54F90A3391C70E1C1D51E347C3BBFFD8146814C3B9098DCE738680F1CFFFB1CD
SHA-512:	D86F9AC95D1326CED1F9C43F5008BB121A52515C8BB503181634CDA3A961DDE3103CCA5FC78BB7C8561DF18F5C3CAEE3D13152E87DD673E8FCC8A0EAC7F67 1A
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\O8JNmHZW\VERSION.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.+ ..DN^....." .....@.....p.....@.....` .....@lx}..b.....P .+....c.....h.....$#..... ..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\O8JNmHZW\cmstp.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	92672
Entropy (8bit):	5.749238064237604
Encrypted:	false
SSDEEP:	1536:7oIXq0f2yF9sDb/RjxgnvkmVUqAVnKUMjbWg+I/87BM/Z4j8Qi1Yv9V:0Izw/RooolWIk7BM/ZNQi1EV
MD5:	2A9828E0C405422D166E0141054A04B3
SHA1:	84AA48946D4F9A9DFE4C1AF6F96C44B643229A73
SHA-256:	94152FB98573FE31C0CE49D260D760DD173741D663414DE718A37AAC7E8EF11F
SHA-512:	B9B0472706C11D3AECDAB055D4CF319EDD50E8C97B7099D1DC7B768812E804975392E327A1E62301077AB92C1CA97E706628B07172892AB09753FBDD9A07277
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....I....X...X...X...Y...X...Y...X...Y...X...Y...X...XQ..X...Y...X...X...X ...Y...XRich...X.....PE..d....mg.....".....@.....`..... .....M.....p.....X....B..T..... .....H.....text..... ..`.rdata..''l.....n.....@..@.data.....`.....R.....@....pdata.....p.....T.....@..@.rsrc..... .....Z.....@..@.reloc..X.....h.....@..B..... .....

C:\Users\user\AppData\Local\QEkvVts\WFS.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	930304
Entropy (8bit):	5.99262413442194
Encrypted:	false
SSDEEP:	12288:YVpcWBIX7oU/HEx5a/DTROFJTl7XjY5uUMUd1vLf1k+xt4vFe:spnBUoR5AfRElITjY5umjz1ivFe
MD5:	CD6ACF3B997099B6CFB2417D3942F755
SHA1:	7376A8000CB7B5CE0F5DA783BAF9F9C2C36F1670
SHA-256:	B699695F47AA8E8B70A21267BA1648B59B33BD677E29D334BC73EBB1A4B81F3E
SHA-512:	F301F0D87CB5FFFFB88AB0B86035DA7705DED1121107D2FDF7A9132F8DFBDEFFAFBE452E3BC7ACEAD1A0E368815127942B2E642B214EA83D90E97B015C766D E0
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....OR...3.,.3.,.3.,dW.-3.,dW.-3.,dW.-3.,dW.-$3.,.3.,o7.,dW.-q3 .,dW.,.3.,dW.-3.,Rich.3.,.....PE..d...d.D.....".....F.....@.....`..... .....`.....0...%.....@A.....`..D ..`@.. T.....Y..(... .....Y..8... W.....text...2..... ..`.rdata.....@..@.data..../..... .....@....pdata..@A.....B..... ..@..@.didat..... .....@....rsrc....%...0...&.....@..@.reloc..D ..`..."....@..B..... .....

C:\Users\user\AppData\Local\QEkvVts\WINMM.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2125824
Entropy (8bit):	3.568769494855891
Encrypted:	false
SSDEEP:	12288:/VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:2fP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	852F5FE3F15F82DBD91A3A5FFE27C781
SHA1:	E6E7BE15DE046D247F7FCBAF62825E9DD0E93390
SHA-256:	85AAB65BC8DC5D02ACF566A14555F5544EE15550506660CCD240DA786AAB04F3
SHA-512:	C69C2777FDC4E94F549D0E686B77A1D6F9F18664E6ED8A58D478D7299CF88A99A831D2209F054A4555F84CBAF6E796656F3C04AD26650E3862DCB64AEABF0C7
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown

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

C:\Users\user\AppData\Local\SB1jY1h\AtBroker.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	62976
Entropy (8bit):	5.750635515620841
Encrypted:	false
SSDEEP:	768:LqMH7HUyeCtu1URDrYxfxyLzkd0S2B3ZEI1yfdc9X1vV09SOI9HiEiOpF1QtNcEd:L3RtZkNxCk61BW6901I9HDF1QH8ST
MD5:	E2C775244B3951A401A9083DD742029A
SHA1:	B4DC87649038B7A4E86B5D6AEBAAD975ECE2F477
SHA-256:	80CC3FB17D8CBB4A68F27C607A8D1C0208CEE892F6D2A2E222E18B23D4E0FC76
SHA-512:	CCFABD50BF7F1F9D2DBF3D0F7FFC5A9C862F623472F9AE51A2F4EDB88EF06BCE23731A925405ACF5BF4BB466EA862413EA01B23177C710CA5FE97EA97E6B832C
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....5`..q.b.q.b.q.b..ea.r.b..ef.d.b..eg.y.b..ec.b.b.q.c...b..ek.~.b..e..p.b..e`.p.b.Richq.b.....PE..d...=..~....."....d.....@.....@.....`..... ..... ..8.....0.....p...T..... p.....p...@.....text..... ..`.rdata..8B.....D.....@..@.data.....@....pdata.....@..@.rsrc...8.... ....@..@.reloc.....0.....@..B..... .....

C:\Users\user\AppData\Local\SB1jY1h\UxTheme.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2121728
Entropy (8bit):	3.5684926622805717
Encrypted:	false
SSDEEP:	12288:BVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:wfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	158C1DF1885FC864E485F6ACE03E43AA
SHA1:	874621AD6CC12CA767A8693033BBEA1EEDEE25C1
SHA-256:	0CDC4C9C52D67E9FAB9EBDC2C39F0D1D1D1042776B2CAA9C5AF3833817526427
SHA-512:	CF090C69481BF910DF5EF588B6AE59BB75479083EFD37113EFFCAEEB5E4576390E04F2C5D758599090C7A51C7FF87DCDE40B7FDFC97B83486F8DDCACA53FC9F9
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.+..DN^....." .....@.....p.....@.....` .....@lx}..b.....P .....c.....h.....$#..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\T6Vn91tw0\SLC.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2121728
Entropy (8bit):	3.5626898520741004
Encrypted:	false
SSDEEP:	12288:IVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1l1:dfP7fWsK5z9A+WGAW+V5SB6Ct4bnbl1
MD5:	9B62B394C76C05624097101E4F503CF9
SHA1:	82B5529C75A10E3DFF42DB4B241071ACECDCB071
SHA-256:	D606489B4DD836A90E668FB799E13EC617BA7F12CE5EED969E6B887AF1551B47
SHA-512:	231E2B9A2C9CD9EE4C8BEA451214745CD050D0FBA355254BBFBDC1700C18BE156A09EDD9A55353F9F861DD1F960F295E17170CCA07112D7396940D03638B762
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown

C:\Users\user\AppData\Local\T6Vn91tw0\SLC.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.+..DN^....." .....@.....p.....@.....` .....@lx}..b.....P .3....c.....h.....$#..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\T6Vn91tw0\slui.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	445952
Entropy (8bit):	6.661655128700218
Encrypted:	false
SSDEEP:	6144:q++gR8ZWU7WZ1rpvJw1DouE71kL3qY/W5R02qO7VKCyWQp:MgzKWZ1VJwEmDq3nyR
MD5:	96A8EF9387619D17BB30B024DDF52BF3
SHA1:	02DFA07143911500925C6298864477296F414AB0
SHA-256:	ECC41BB93E0E1EA63A1027D551BA0FCE503E53EF1BA2E70944FD7E7C7C9A9B8A
SHA-512:	01701BCFB3D3F09DF86CAF75ED76DC82A4B1480A284AB68FB4B7E4941466DB1ED23187B4D2E51B63C7526123EB4647FB5D155F31832E9ED7F4DBADF78F1F94EA
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....*...n.rMn.rMn.rMg..Mr.rM..qLm.rM..vLx.rM..wLj.rM..sL{.rMn.sM..rM..|Lv.rM...Mo.rM..pLo.rMRichn.rM.....PE..d...O.h{....."....."....0.....@..... .....`..... .....-.....` .....T.....(.....text...&..... ..`.rdata.....@..@.data.....P.....*.....@....pdata.....`.....0.....@..@.rsrc.....J.....@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\byYs\DUI70.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2404352
Entropy (8bit):	4.0941855774712055
Encrypted:	false
SSDEEP:	12288:jVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ19Z:yfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	27B08379E48FF2EA436796B3BA872FB3
SHA1:	7F0271B8E7D0C700499802459171313 2F9C7F449
SHA-256:	0A5AC48F07DD100A1BF602A1D8B0FD6ED3B31315BCD6CED03FA7A9A8B55C5551
SHA-512:	41D34A6B0BD2F36365D0C71D5E8D35C83AA55F3C3D82EACE7C2898CC69665C13AE998FD72BACFC8747D1309B4B10DE90323D084D38ED4C64AB511C3797BB8BE
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.....P .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\byYs\wlrmdr.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	65704
Entropy (8bit):	5.834154867756865
Encrypted:	false
SSDEEP:	1536:B14+6gGQ7ubZiQ+KytHIyObsvqr9PxDt8PcPs:QgGIu1iFtHJLu9ZDt8kU
MD5:	4849E997AF1274DD145672A2F9BC0827
SHA1:	D24E9C6079A20D1AED8C1C409C3FC8E1C63628F3
SHA-256:	B43FC043A61BDBCF290929666A62959C8AD2C8C121C7A3F36436D61BBD011C9D
SHA-512:	FB9227F0B758496DE1F1D7CEB3B7A5E847C6846ADD360754CFB900358A71422994C4904333AD51852DC169113ACE4FF3349520C816E7EE796E0FBE6106255AEF
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\byYs\wlrmdr.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....j.s... ... ... .s\ ... .o.!... .o.!... .o.!... .o.!... ... t.. .o.!... .o0 ... .o.!... Rich ... .PE..d....2.....".....4.....:.....@.....@.....b.....P.....xg.....$...0.....y..T.....f.....g..x. .....text....3.....4..... ..`.imrsiv.....P.....rdata..J2...`...4...8.....@..@.data...h.....l.....@....pdata.....n.....@..@.rsr c...xg.....h...r.....@..@.reloc.....0.....@..B..... .....

C:\Users\user\AppData\Local\gxzS7\credui.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2121728
Entropy (8bit):	3.5615439297314184
Encrypted:	false
SSDEEP:	12288:xVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:AfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	D8BF7ED579BFB7A50E4A529F70CF3992
SHA1:	AFD198A7352054DF47F147F47ED0CC2F136284FD
SHA-256:	CC7BF835073F601CE20178DE8B86547E4D481735D22E35AB94FF7A18B24B3262
SHA-512:	8530CFD8BDBC0B1B20EAA392A1977FCC5F3F12E022570287612CA4BE2AE6622B8B236D460EF5420ABF115AEAC237BBFFF7453337DF9E5DDFFAB13085AA83F3 45
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.+ ..DN^....." .....@.....p.....@.....` .....@lx}..b.....P .....c.....h.....$#..... ..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\gxzS7\perfmon.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	175616
Entropy (8bit):	6.895507339523819
Encrypted:	false
SSDEEP:	3072:uVt2h5auVI9cMHFO+ZyGghtYIo9piswTogiqQKy349:uVMzVIOMHFhyhqIo9s37iTK24
MD5:	BD9ABDEA680B56534CE7627E39270A7C
SHA1:	24FCF3E615F5E7F434244D90AE5C4EB90F7C5EB5
SHA-256:	EB9FF0CDA3E15147BB0FE00984B75C5F7B04644957CCAC135996AC18C1FD3EED
SHA-512:	CEFA87534CB62E705EEE00CE5FA7C73083562A6B97E5D9D0106A3BCB3499A1F7FE997376DB22F73BB4F19DA66E6CE65FE85E2DF1FD06051CC19C006B590824 7
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....H....f..f..f.c...f.c...f.c...f.c...f..f..f.c...f.c. ..f.c...f.Rich.f.....PE..d.....i6... .....".....$.....P.....@.....9....`..... .....D.....@.....0.....p...T.....`.....`.....t ext..... ..`.rdata...x.....z.....@..@.data..... .....@....pdata.....0.....@..@.rsrc.....@.....@..@.reloc..... ...@..B..... .....

C:\Users\user\AppData\Local\h1G\ACTIVEDS.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2121728
Entropy (8bit):	3.5609838856348315
Encrypted:	false
SSDEEP:	12288:nVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:OfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	B5AADBED0CF9FCBC4DF667183EBCF3CC
SHA1:	BE5445DE7B7CFC449DB9EE4AA01B4EF85EC46F6C
SHA-256:	0EDAE1B408B6ABCDF430CED04BE928D26B007F50BF8AD0DA8D2D95F029682CA4
SHA-512:	9828D153CEC7FF5F61EEF3E480196854170EE8101FEDC14DC63517578601DCCB7C83627F7843A6FC57CA4DEF4D46A43FF899DB3379E43272828F1B3DFBC9170
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.+ ..DN^....." .....@.....p.....@.....` .....@lx}..b.....P .y....c.....h.....$#..... ..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\h1G\ACTIVEDS.dll	

C:\Users\user\AppData\Local\h1G\AgentService.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1189376
Entropy (8bit):	6.169931271903684
Encrypted:	false
SSDEEP:	24576:+pL4Q4y94x7ZWe6b1B5I2M62kM0s1vt2txc/viVO1IORNfLc:uL4Q3S9b6b1UA9MPwOR5c
MD5:	F7E36C20DB953DFF4FDDB817904C0E48
SHA1:	8C6117B5DD68D397FD7C32F4746FB9B353D5DAE5
SHA-256:	2C5EDE0807D8A5EC4B6E0FE0C308B37DBBDE12714FD9ADC4CE3EF4E0A5692207
SHA-512:	32333A33DECD1AF0915FFDC48DA99831DA345010A91630C5245F2548939E33157F6151F596C09D0BEEAC3F15F08F79D4EEF4FAA4158BA023DEDFC4F6F6F56DF
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....:K..[%M.[%M.[%M.?&L.[%M.? L.[%M.?!L.[%M.?$L.[%M.[$M .Z%M.?,L.[%M.?.M.[%M.?'L.[%MRich.[%M.....PE..d...m.>l....."....B.....@.....=...`..... .....P.. ... .....x.....`..`...p-..T.....pI..(...pH.....I.....text...L..... ..`.rdata..| .....".....@..@.data...@....@...r..."....@....pdata ...x.....z.....@..@.rsrc... ....P.....@..@.reloc..`...`.....@..B..... .....

C:\Users\user\AppData\Local\iU8z5\wer.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2125824
Entropy (8bit):	3.5692811602312817
Encrypted:	false
SSDEEP:	12288:1VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:sfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	0F2F06886BBAF597A92F52E906C4CE03
SHA1:	CFDCD31E7AE917F24C94DAFD832E2AABC846AE15
SHA-256:	DBF19D0AF4D465C1C986B3CAD125C54A3204DF84007D1104F583035F8B622B46
SHA-512:	2226AF343434512F1DFA11910678A3E99EC3A0F022D43CD3FE8C4AED85834FBCA8C16F28E547FE7F014056B6F84A16489A84752259AEB3AC7185F3DA44F5E8DE
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.+ ..DN^....." .....P.....p.....@.....p .....@lx}..b.....P .W....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\iU8z5\wermgr.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	209312
Entropy (8bit):	6.796289498157116
Encrypted:	false
SSDEEP:	6144:swTMBboFMSuc/9NPXWPJROo/wVJyB60OHyLC7vs:swTMB02SD/mXO64c2Hyw
MD5:	FF214585BF10206E21EA8EBA202FACFD
SHA1:	1ED4AE92D235497F62610078D51105C4634AFADE
SHA-256:	C48C430EB07ACC2FF8BDDD6057F5C9F72C2E83F67478F1E4A1792AF866711538
SHA-512:	24073F60B886C58F227769B2DD7D1439DF841784E43E753265DA761801FDA58FBEEDAC4A642E0A6ABDA40A6263153FAA1A9540DF6D35E38BF0EE5327EA55B4F E
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....(j.jl..jl..jl..c1...l...-..il...-..ql..jl...H...-..ml...-..`l...-..Kl...-..kl...-..kl..Rich jl.....PE..d...p.....".....,.....`(.....@.....p.....`..... ... ..0:.....!...`..\...@...T.....`Q.....`R.. ...t.....text...++.....,..... ..`.imrsiv.....@.....rdata.....P.....0.....@..@.data...X.....@....pdata.....@. .@.didat..@.....@....rsrc...0:... ...<.....@..@.reloc..\....`.....@..B..... .....

C:\Users\user\AppData\Local\kOjpxXR\SnippingTool.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	3292160
Entropy (8bit):	4.311007815185121
Encrypted:	false
SSDEEP:	24576:+oNva52v20/OB1b1v+YMTvlcZbbAbn3ltpG:VNtv20/OB1hXulc10L4tp
MD5:	9012F9C6AC7F3F99ECDD37E24C9AC3BB
SHA1:	7B8268C1B847301C0B5372C2A76CCE326C74991E
SHA-256:	4E30A8C88C755944145F2BC6C935EE5107C56832772F2561229E20CEAB1D10D2
SHA-512:	B76D2BE02A22990E224DBC5AED9E5B701EAC52C1376529DE3E90B084CD6860B88D746CD61093E93FC932E12FBAF45B4CA342CC0D9C9DAE4EAFE05921D83A797
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....$...w...w...w...w...w...v...w...v...w...v...w...v...w...w'..w...v...w ..mw...w..ow...w...v...wRich...w.....PE..d....i....."....v/....0.....@.....2.....I.2...`..... .....P..(;...0.....2.|...`...T.... .....(.....text...9..... ..`.rdata.....@..@.data....0.....@....pdata.....0.....@..@.rsrc...(;...P...<.....@..@.reloc..|.....2.....82.....@..B..... .....

C:\Users\user\AppData\Local\kOjpxXR\dwmapi.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2121728
Entropy (8bit):	3.564430230982269
Encrypted:	false
SSDEEP:	12288:BVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:wfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	1DF68F7322A2C246D8E8E030719ABADD
SHA1:	25A86D132BFC21D4890018962C3578365E8C0757
SHA-256:	AED0A6E8AC8AB86A2EB2888077512E0615DCF2820C45464A227384E7B02A735A
SHA-512:	247971E464A8F5939FC1C9478A8E3F44D6218503E0E4187CC630727C6D7BF546151429EBD627573C5FB39F4F924FDABA1719633EE23B4540B4B42EB4D60CE72F
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.+ ..DN^....." .....@.....p.....@.....` .....@lx}..b.....P .&....c.....h.....$#..... ..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\kkXbTNX3S\VERSION.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2121728
Entropy (8bit):	3.5597998659110672
Encrypted:	false
SSDEEP:	12288:zVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:ifP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	EA53E60CCD953EACD6E4EC1A093544CF
SHA1:	3DFF3F21F3A31769BB487A8F34207F629CC6F2A9
SHA-256:	6224FA0A9E564D0859E1D6951AAD9B2E5CC0BFA867E10085F9FF669424E54D94
SHA-512:	D8E91C06007B40F244EA5E27692362964056501EA78CDAE2120A0E232716DC4EDA850766218FE6B8DACADBCC3748C11DAB790EC996C99D32279F6D22B71809C
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.+ ..DN^....." .....@.....p.....@.....` .....@lx}..b.....P .+....c.....h.....$#..... ..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\kkXbTNX3S\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

C:\Users\user\AppData\Local\kkXbTNX3S\wscript.exe	
Encrypted:	false
SSDEEP:	1536:8HSpBlnak9UH8bCAHZ1LQ434syPz7M5hh/kzhwS827HuYHwHugXEYJ6S7775MWUn:aC4HWCp/fM5hvNebgXEYJN73uWUZxtt
MD5:	9A68ADD12EB50DDE7586782C3EB9FF9C
SHA1:	2661E5F3562DD03C0ED21C33E2888E2FD1137D8C
SHA-256:	62A95C926C8513C9F3ACF65A5B33CBB88174555E2759C1B52DD6629F743A59ED
SHA-512:	156CAED6E1BF27B275E4BA0707FB550F1BF347A26361D6D3CAD12C612C327686950B47B6C5487110CF8B35A490FAADC812ADE3777FFF7ED76A528D970914A6E
Malicious:	false
Reputation:	unknown
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\ySbBY3WaF\SndVol.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	259904
Entropy (8bit):	5.955701055747905
Encrypted:	false
SSDEEP:	3072:UfYIZJbRydnidilSnGvLqeD358rwW39nuyHjVozZcxSHfcBL1ljbEyB7HbIa+:Uf9JonidFnqLV358rNnJqcRcy10/
MD5:	CDD7C7DF2D0859AC3F4088423D11BD08
SHA1:	128789A2EA904F684B5DF2384BA6EEF4EB60FB8E
SHA-256:	D98DB8339EB1B93A7345EECAC2B7290FA7156E3E12B7632D876BD0FD1F31EC66
SHA-512:	A093BF3C40C880A80164F2CAA87DF76DCD854375C5216D761E60F3770DFA04F4B02EC0CA6313C32413AC99A3EBDC081CF915A7B468EE3CED80F9B1ECF4B498 4
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<.BL]..L]..L]..E%...]..#9..O]..#9..U]..#9..F]..#9..W]..L]...\..#9..o].. #9k.M]..#9..M]..RichL].....PE..d...wJSn....."....@.....@..... .....p.... ..@.....@+...0..... ..U..T.....p&..(...p%.....&.....P.....text..... ..`.imrsiv.....rdata..... .....@..@.data.....@.. ..pdata.....@..@.didat.....@....rsrc...@.... .....@..@.reloc.....0.....@..B..... .....

C:\Users\user\AppData\Local\ySbBY3WaF\UxTheme.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2121728
Entropy (8bit):	3.5685074321676984
Encrypted:	false
SSDEEP:	12288:tVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:0fP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	268ECB8D07BC2F31469FF3C825FCAF4C
SHA1:	ECCC90BBF20D68C77BAD0C39E75F6467FE1EC101
SHA-256:	C337124A0D68D9356040E1F5C514934208901DE875459FA463C232F306FB16C2
SHA-512:	8603B6E4DEA1B0C56D9C8A4AA943B0696723063F495DB74E6D4FF8C85FCBFD4D71DE885520523F935391B2AACE4E86FEB2D3BB4CCCA78054EB4B7870D9A400 E0
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.+ ..DN^....." .....@.....p.....@.....` .....@lx}..b.....P .....c.....h.....$#..... ..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

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):	5.480575242471079
Encrypted:	false
SSDEEP:	96:edCYIIR00Oj1NZ7BuyPvYVQx6dCYiLaefYWtGzOY6GzD:eIInC1Nn2JuJQWYzZ6G/
MD5:	D94FDB48B116A14A2F2563F7E1AA8183

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\eb42b1a5c308fc11edf1ddbdd25c8486_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
SHA1:	44E8DD08F074C105FD001FEFF961C42E4BCDB7F6
SHA-256:	0AC6FF1517064A3976B4B1951CA95A302C7FDE49080C5DB4C8DC278C444DC7B1
SHA-512:	96A4F43372E69D652FC7F776D65EC598B19699923C4E2F12076690104B40CADFAB2CC4FF297E11BA63D4F78FA5A4FB35EE037DC27E538DA75AE75265E95DAE4A
Malicious:	false
Reputation:	unknown
Preview:	.....user.....user.....RSA1.....W$s66.o.4.....wK8tY...I...'..}q...?.9..vFr...7x..0..[b.(..J...x...iM:.A}.Z...5nM{.....[....z..'.3}{..<."......!X.....z..O.....F.M.6.K./.v.....,...C.r.y.p.t.o.A.P.I. .P.r.i.v.a.t.e. .K.e.y....f..... ....z9o$au.7..aF&..h. ..I\..[&Y.aM..... ...8....PB.....(.]..E.vh..u.....=...M..rs.C....1./iw.}.!i[].k?..C.p...2.Q..._....-.....-.W..tW.a.(&.T.....dJ...{KE.C.....KU.bqO../t..a/=.^.PRgsG,.c.I.....?.7z..e..U..uE0(K._.:Q.P....KZ..7..z<...7.%g.c.v..T.f...[.....5..g...33...?..JC-.;d..N<.E..,.....0.^.Qa:I.....7s.&..P...O.t.=.!....~...+I..e..>..<J...~.d...1b..b...m..4!..h...ZKr..J....`z..c..%.DB..s...M.....@....4..y.....r...f.....M.7t..n.!$".%.....-..9....'....8.j.-f....n.0.....VN...|...>2.....{...4...{.....rVL.,q..KA...../)...T.t...V.t_..o.1.

Static File Info

General

File type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Entropy (8bit):	3.5792852577015357
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:	X5C9EzCB7A.dll
File size:	2117632
MD5:	dc4fca98a02c5cc7ee5f565c56915c86
SHA1:	4cecd255d9176fff8d0ca18cd3dabd690ce02fbf
SHA256:	ae087f890f576dca43d22b3c527b5008547dacd68dfd61440c99370051cc853b
SHA512:	4954ed3d7ac9fcca73623f1d24a8aaa4ca88727a58a45382e897966311909d0c8d43d709d828e0d3211f6c478ee1ca2bf5970c476c5485a949f5cfbf033e9875
SSDEEP:	12288:YVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:NfP7fWsK5z9A+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

General

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
.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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.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
.txms	0x1a8000	0x3fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vqqm	0x1a9000	0x1af	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.cbwb	0x1aa000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.cti	0x1ab000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ktfjac	0x1ac000	0x3ba	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.hvmici	0x1ad000	0xbe9	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bvyyd	0x1ae000	0x1af	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.qhjn	0x1af000	0x1af	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bsvkca	0x1b0000	0x389	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.nvpgx	0x1b1000	0x2a2	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.yaa	0x1b2000	0x543	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.qsimby	0x1b3000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.dibg	0x1b5000	0x451c2	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.odxfk	0x1fb000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.zczpdd	0x1fd000	0x543	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.iceycz	0x1fe000	0x5a7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.lwp	0x1ff000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ejt	0x200000	0x543	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.gzpi	0x201000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.oima	0x203000	0x1124	0x2000	False	0.276733398438	data	3.64280372921	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: 2368 Parent PID: 4164

General

Start time:	10:49:47
Start date:	28/09/2021
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe 'C:\Users\user\Desktop\X5C9EzCB7A.dll'
Imagebase:	0x7ff7f9830000
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: 00000000.00000002.452046176.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 5760 Parent PID: 2368

General

Start time:	10:49:47
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\X5C9EzCB7A.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: 2192 Parent PID: 2368

General

Start time:	10:49:48
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\X5C9EzCB7A.dll,AddGadgetMessageHandler
Imagebase:	0x7ff7f1330000
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: 00000002.00000002.341553991.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 5356 Parent PID: 5760

General

Start time:	10:49:48
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe 'C:\Users\user\Desktop\X5C9EzCB7A.dll',#1
Imagebase:	0x7ff7f1330000
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: 00000003.00000002.249682229.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3292 Parent PID: 2192

General

Start time:	10:49:49
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: 1596 Parent PID: 2368

General

Start time:	10:49:51
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\X5C9EzCB7A.dll,AddLayeredRef
Imagebase:	0x7ff7f1330000
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: 00000006.00000002.256116400.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 2840 Parent PID: 2368

General

Start time:	10:49:54
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\X5C9EzCB7A.dll,AdjustClipInsideRef
Imagebase:	0x7ff7f1330000
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: 00000008.00000002.263669758.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 4156 Parent PID: 2368

General

Start time:	10:49:58
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\X5C9EzCB7A.dll,AttachWndProcA
Imagebase:	0x7ff7f1330000
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: 00000009.00000002.270725525.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 2888 Parent PID: 2368

General

Start time:	10:50:01
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false

Commandline:	rundll32.exe C:\Users\user\Desktop\X5C9EzCB7A.dll,AttachWndProcW
Imagebase:	0x7ff7f1330000
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.00000002.279755934.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 2916 Parent PID: 2368

General

Start time:	10:50:05
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\X5C9EzCB7A.dll,AutoTrace
Imagebase:	0x7ff7f1330000
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: 0000000E.00000002.287591369.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 1064 Parent PID: 2368

General

Start time:	10:50:09
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\X5C9EzCB7A.dll,BeginHideInputPaneAnimation
Imagebase:	0x7ff7f1330000
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: 00000013.00000002.294331565.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 6288 Parent PID: 2368

General

Start time:	10:50:12
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\X5C9EzCB7A.dll,BeginShowInputPaneAnimation
Imagebase:	0x7ff7f1330000
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: 00000015.00000002.302760143.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 6360 Parent PID: 2368

General

Start time:	10:50:16
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\X5C9EzCB7A.dll,BuildAnimation
Imagebase:	0x7ff7f1330000
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: 00000017.00000002.310372882.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 6388 Parent PID: 2368

General

Start time:	10:50:19
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\X5C9EzCB7A.dll,BuildDropTarget
Imagebase:	0x7ff7f1330000
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: 00000018.00000002.317261849.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 6404 Parent PID: 2368

General

Start time:	10:50:23
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\X5C9EzCB7A.dll,BuildInterpolation
Imagebase:	0x7ff7f1330000
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: 00000019.00000002.324869275.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 6428 Parent PID: 2368

General

Start time:	10:50:26
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\X5C9EzCB7A.dll,CacheDWriteRenderTarget
Imagebase:	0x7ff7f1330000
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: 0000001B.00000002.332178412.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 6484 Parent PID: 2368

General

Start time:	10:50:30
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\X5C9EzCB7A.dll,ChangeCurrentAnimationScenario
Imagebase:	0x7ff7f1330000
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.00000002.339544401.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 6524 Parent PID: 2368

General

Start time:	10:50:33
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\X5C9EzCB7A.dll,ClearPushedOpacitiesFromGadgetTree
Imagebase:	0x7ff7f1330000
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: 0000001D.00000002.399487635.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: wermgr.exe PID: 6572 Parent PID: 3292

General

Start time:	10:50:34
Start date:	28/09/2021
Path:	C:\Windows\System32\wermgr.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wermgr.exe
Imagebase:	0x7ff6251d0000
File size:	209312 bytes
MD5 hash:	FF214585BF10206E21EA8EBA202FACFD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: wermgr.exe PID: 6600 Parent PID: 3292

General

Start time:	10:50:36
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\M5A\wermgr.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\M5A\wermgr.exe
Imagebase:	0x7ff740970000
File size:	209312 bytes
MD5 hash:	FF214585BF10206E21EA8EBA202FACFD
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.00000002.353298117.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 6620 Parent PID: 2368

General

Start time:	10:50:37
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\X5C9EzCB7A.dll,ClearTopmostVisual
Imagebase:	0x7ff7f1330000
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: 00000020.00000002.357738953.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: WFS.exe PID: 6640 Parent PID: 3292

General

Start time:	10:50:39
Start date:	28/09/2021
Path:	C:\Windows\System32\WFS.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WFS.exe
Imagebase:	0x7ff7eb8a0000
File size:	930304 bytes
MD5 hash:	CD6ACF3B997099B6CFB2417D3942F755
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WFS.exe PID: 6652 Parent PID: 3292

General

Start time:	10:50:40
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\QEkvVts\WFS.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\QEkvVts\WFS.exe
Imagebase:	0x7ff7d5c70000
File size:	930304 bytes
MD5 hash:	CD6ACF3B997099B6CFB2417D3942F755
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: 00000022.00000002.363607406.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: rundll32.exe PID: 6752 Parent PID: 2368

General

Start time:	10:50:41
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe

Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\X5C9EzCB7A.dll,CreateAction
Imagebase:	0x7ff7f1330000
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: 00000023.00000002.367587367.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: wusa.exe PID: 6888 Parent PID: 3292

General

Start time:	10:50:43
Start date:	28/09/2021
Path:	C:\Windows\System32\wusa.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wusa.exe
Imagebase:	0x7ff6bc1b0000
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: 6912 Parent PID: 3292

General

Start time:	10:50:44
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\8FwY\wusa.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\8FwY\wusa.exe
Imagebase:	0x7ff6ee1f0000
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: 00000028.00000002.370038497.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Disassembly

Code Analysis