ID: 492789
Sample Name: yWteP7e12z
Cookbook: default.jbs
Time: 01:30:21
Date: 29/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report yWteP7e12z 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 4
Sigma Overview 5
Jbx Signature Overview 5
AV Detection: 5
E-Banking Fraud: 5
System Summary: 5
HIPS / PFW / Operating System Protection Evasion: 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted IPs 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 11
Static File Info 18
General 18
File Icon 18
Static PE Info 18
General 18
Entrypoint Preview 18
Rich Headers 19
Data Directories 19
Sections 19
Resources 20
Imports 20
Exports 20
Version Infos 20
Possible Origin 20
Network Behavior 20
Network Port Distribution 20
UDP Packets 21
Code Manipulations 21
Statistics 21
Behavior 21
System Behavior 21
Analysis Process: loaddll64.exe PID: 6928 Parent PID: 5496 21
General 21
File Activities 21
Analysis Process: cmd.exe PID: 4668 Parent PID: 6928 21
General 21
File Activities 22
Analysis Process: rundll32.exe PID: 4536 Parent PID: 6928 22
General 22
File Activities 22
File Read 22
Analysis Process: rundll32.exe PID: 4528 Parent PID: 4668 22
General 22
File Activities 22
File Read 22

Analysis Process: explorer.exe PID: 3352 Parent PID: 4536 22
General 22
File Activities 23
File Created 23
File Deleted 23
File Written 23
File Read 23
Registry Activities 23
Key Created 23
Key Value Created 23
Analysis Process: rundll32.exe PID: 6568 Parent PID: 6928 23
General 23
File Activities 23
File Read 23
Analysis Process: rundll32.exe PID: 3912 Parent PID: 6928 23
General 23
File Activities 24
File Read 24
Analysis Process: recdisc.exe PID: 6628 Parent PID: 3352 24
General 24
Analysis Process: SnippingTool.exe PID: 7044 Parent PID: 3352 24
General 24
Analysis Process: SnippingTool.exe PID: 6200 Parent PID: 3352 24
General 24
File Activities 25
File Read 25
Analysis Process: raserver.exe PID: 3604 Parent PID: 3352 25
General 25
Analysis Process: raserver.exe PID: 2992 Parent PID: 3352 25
General 25
File Activities 25
File Read 25
Analysis Process: ddodiag.exe PID: 5808 Parent PID: 3352 25
General 25
Analysis Process: ddodiag.exe PID: 5828 Parent PID: 3352 26
General 26
File Activities 26
File Read 26
Analysis Process: dccw.exe PID: 2364 Parent PID: 3352 26
General 26
Analysis Process: SppExtComObj.Exe PID: 6280 Parent PID: 3352 26
General 26
Analysis Process: SppExtComObj.Exe PID: 5620 Parent PID: 3352 27
General 27
File Activities 27
File Read 27
Analysis Process: WMPDMC.exe PID: 6628 Parent PID: 3352 27
General 27
Analysis Process: WMPDMC.exe PID: 6480 Parent PID: 3352 27
General 27
Analysis Process: wscript.exe PID: 5532 Parent PID: 3352 28
General 28
Analysis Process: wscript.exe PID: 5012 Parent PID: 3352 28
General 28
Analysis Process: BdeUISrv.exe PID: 5368 Parent PID: 3352 28
General 28
Analysis Process: BdeUISrv.exe PID: 6080 Parent PID: 3352 29
General 29
Disassembly 29
Code Analysis 29

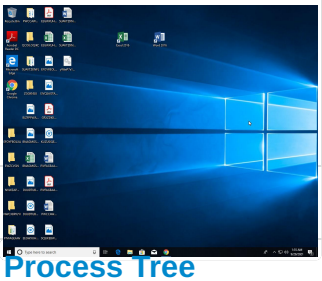
Windows Analysis Report yWteP7e12z

Overview

General Information

Sample Name:	yWteP7e12z (renamed file extension from none to dll)
Analysis ID:	492789
MD5:	a75be08d11b502..
SHA1:	c47a48e04dc106..
SHA256:	7500211dd9ce4e..
Tags:	Dridex exe
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

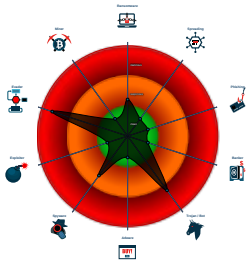
Dridex

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…
- Queues an APC in another process …
- Machine Learning detection for dropp…
- Contains functionality to prevent loc…
- Uses Atom Bombing / ProGate to in…
- PE file contains section with special…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 6928 cmdline: loaddll64.exe 'C:\Users\user\Desktop\yWteP7e12z.dll' MD5: E0CC9D126C39A9D2FA1CAD5027EBBD18)
  - cmd.exe (PID: 4668 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\yWteP7e12z.dll',#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 4528 cmdline: rundll32.exe 'C:\Users\user\Desktop\yWteP7e12z.dll',#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 4536 cmdline: rundll32.exe C:\Users\user\Desktop\yWteP7e12z.dll,BeginBufferedAnimation MD5: 73C519F050C20580F8A62C849D49215A)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - recdisc.exe (PID: 6628 cmdline: C:\Windows\system32\recdisc.exe MD5: D2AEFB37C329E455DC2C17D3AA049666)
      - SnippingTool.exe (PID: 7044 cmdline: C:\Windows\system32\SnippingTool.exe MD5: 9012F9C6AC7F3F99ECDD37E24C9AC3BB)
      - SnippingTool.exe (PID: 6200 cmdline: C:\Users\user\AppData\Local\S8mrk1\SnippingTool.exe MD5: 9012F9C6AC7F3F99ECDD37E24C9AC3BB)
      - raserver.exe (PID: 3604 cmdline: C:\Windows\system32\raserver.exe MD5: DE2022F0B86E33875D8A40B65550CFEB)
      - raserver.exe (PID: 2992 cmdline: C:\Users\user\AppData\Local\eQL\raserver.exe MD5: DE2022F0B86E33875D8A40B65550CFEB)
      - ddodiag.exe (PID: 5808 cmdline: C:\Windows\system32\ddodiag.exe MD5: 3CE911D7C12A2EFA9108514013BD17FE)
      - ddodiag.exe (PID: 5828 cmdline: C:\Users\user\AppData\Local\Iz08tEz\ddodiag.exe MD5: 3CE911D7C12A2EFA9108514013BD17FE)
      - dccw.exe (PID: 2364 cmdline: C:\Windows\system32\dccw.exe MD5: 341515B9556F37E623777D1C377BCFAC)
      - SppExtComObj.Exe (PID: 6280 cmdline: C:\Windows\system32\SppExtComObj.Exe MD5: 809E11DECADAEBE2454EFEDD620C4769)
      - SppExtComObj.Exe (PID: 5620 cmdline: C:\Users\user\AppData\Local\jYs4ma0u\SppExtComObj.Exe MD5: 809E11DECADAEBE2454EFEDD620C4769)
      - WMPDMC.exe (PID: 6628 cmdline: C:\Windows\system32\WMPDMC.exe MD5: 4085FDA375E50214142BD740559F5835)
      - WMPDMC.exe (PID: 6480 cmdline: C:\Users\user\AppData\Local\92ea6x\WMPDMC.exe MD5: 4085FDA375E50214142BD740559F5835)
      - wscript.exe (PID: 5532 cmdline: C:\Windows\system32\wscript.exe MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
      - wscript.exe (PID: 5012 cmdline: C:\Users\user\AppData\Local\JFuMqIg\wscript.exe MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
      - BdeUISrv.exe (PID: 5368 cmdline: C:\Windows\system32\BdeUISrv.exe MD5: 25D86BC656025F38D6E626B606F1D39D)
      - BdeUISrv.exe (PID: 6080 cmdline: C:\Users\user\AppData\Local\2lBRPi\BdeUISrv.exe MD5: 25D86BC656025F38D6E626B606F1D39D)
  - rundll32.exe (PID: 6568 cmdline: rundll32.exe C:\Users\user\Desktop\yWteP7e12z.dll,BeginBufferedPaint MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 3912 cmdline: rundll32.exe C:\Users\user\Desktop\yWteP7e12z.dll,BeginPanningFeedback MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.290585928.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000002.00000002.384630779.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000020.00000002.502508138.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000022.00000002.529404050.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000029.00000002.583509816.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
Click to see the 7 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

E-Banking Fraud:

Yara detected Dridex unpacked file

System Summary:

PE file contains section with special chars

HIPS / PFW / Operating System Protection Evasion:

Benign windows process drops PE files

Changes memory attributes in foreign processes to executable or writable

Queues an APC in another process (thread injection)

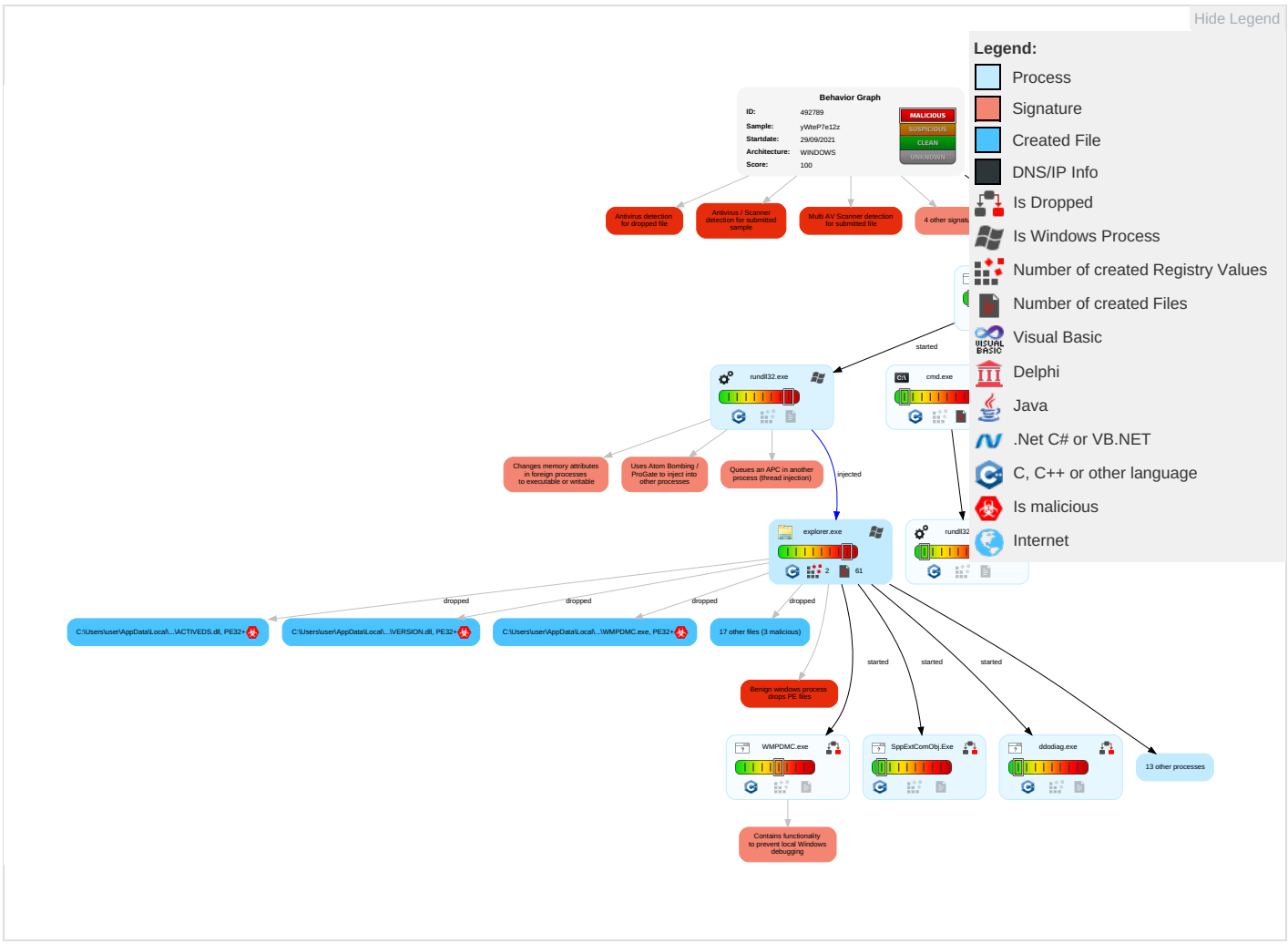
Contains functionality to prevent local Windows debugging

Uses Atom Bombing / ProGate to inject into other processes

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Native API 1	Windows Service 1	Windows Service 1	Deobfuscate/Decode Files or Information 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop Insecure Network Communic
Default Accounts	Exploitation for Client Execution 1	Boot or Logon Initialization Scripts	Process Injection 4 1 2	Obfuscated Files or Information 3	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Screen Capture 1	Exfiltration Over Bluetooth	Junk Data	Exploit SS Redirect P Calls/SMS
Domain Accounts	Command and Scripting Interpreter 2	Logon Script (Windows)	Logon Script (Windows)	Software Packing 2	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Steganography	Exploit SS Track Dev Location
Local Accounts	Service Execution 2	Logon Script (Mac)	Logon Script (Mac)	Timestomp 1	NTDS	System Information Discovery 3 5	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Security Software Discovery 4 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 4 1 2	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi- Access Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Rundll32 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrad Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cel Base Stati

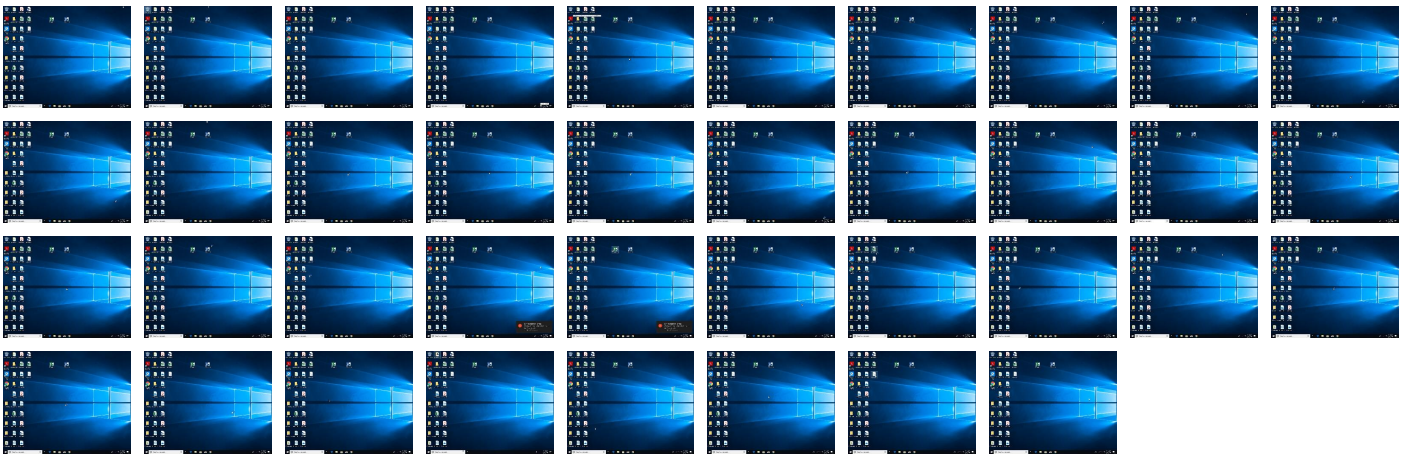
Behavior Graph



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
yWteP7e12z.dll	64%	Virustotal		Browse
yWteP7e12z.dll	78%	ReversingLabs	Win64.Infostealer.Dridex	
yWteP7e12z.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
yWteP7e12z.dll	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\JFuMqIg\VERSION.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\2IBRPi\WTSAPI32.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\2Pnr0hm64\XmlLite.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\2Pnr0hm64\XmlLite.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\2IBRPi\WTSAPI32.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\2Pnr0hm64\XmlLite.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\jYs4ma0u\ACTIVEDS.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\7YI8zy\OLEACC.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\7YI8zy\OLEACC.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\7YI8zy\OLEACC.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\JFuMqIg\VERSION.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\2IBRPi\WTSAPI32.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\2Pnr0hm64\XmlLite.dll	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\2Pnr0hm64\XmlLite.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\2IBRPi\WTSAPI32.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\2Pnr0hm64\XmlLite.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\jYs4ma0u\ACTIVEDS.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\7YI8zy\OLEACC.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\7YI8zy\OLEACC.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\7YI8zy\OLEACC.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\2Pnr0hm64\MusNotifyIcon.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\2Pnr0hm64\MusNotifyIcon.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\2IBRPi\BdeUISrv.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\2IBRPi\BdeUISrv.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\7YI8zy\sethc.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\7YI8zy\sethc.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\92ea6x\WMPDMC.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\92ea6x\WMPDMC.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
34.2.WMPDMC.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
32.2.SppExtComObj.Exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
28.2.ddodiag.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
19.2.SnippingTool.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
9.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
26.2.raserver.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
41.2.BdeUISrv.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
8.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
37.2.wscript.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	492789
Start date:	29.09.2021
Start time:	01:30:21

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	yWteP7e12z (renamed file extension from none to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	41
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@49/21@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 25.6% (good quality ratio 19.6%) • Quality average: 55.9% • Quality standard deviation: 39.2%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\2Pnr0hm64\MusNotifyIcon.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	348248
Entropy (8bit):	4.476463179941575
Encrypted:	false
SSDEEP:	3072:h+3PxWVjjy9Vya+bgdI/uQmyDbT/j0MQXOAfib98:h+5WVje+UdI/uQmyDbDWOAfH
MD5:	56EB45AF6E8DAC3DE13BFBDDD23471FD
SHA1:	B6CD69E22DF2AC6220DDE6BD5B96D0333C81664E
SHA-256:	96C7678DFB92B3666D5A41BB251EE21DF24D7C3F32E0115BB302438F364DFA7D
SHA-512:	4062829F81BF34C25ECDE96D46BC55A9CB40E3D0B78E73C07245DCCE42B7F60EE169A8545518F758E52215E9ABA3E62BEC02E7D4F5B5AE79DA690518920E974B
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....R...R...R...[.....=..Q...=..E...R.....=..C...=..E...=..]...=.r.S...=..S...RichR.....PE..d...R....."......P.....@.....).....`..... .....H.....H....P..@...."..X....p.....P...T.....d.....e..`.....text...<N.....P..... ..`.rdata..T....`.....T.....@..@.data...(....@.....&.....@....pdata..@....P.....(.....@..@.didat.....p.....:.....@....rsrc...H.....<.....@..@.reloc.....p..... .....@..B.....

C:\Users\user\AppData\Local\2Pnr0hm64\XmlLite.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2109440
Entropy (8bit):	3.576077189317853
Encrypted:	false
SSDEEP:	12288:pVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:IfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	8D382555F4058C485E44A6F1746DF8AE
SHA1:	CA1DD960D00123E12458CE1E1C56B9DB7E06623E
SHA-256:	E266F25DE43726B4AEDFEF41B4561CA93156A5DB9FDE2EE68E2A9790DBF93A7F
SHA-512:	361C29520A7B22149F1F7D24831C06BA90514381F53918B4FB4F74FA8A8E456BAF216F6DE4F7538C7ECC21038A449C2419A4301B6551216AB593C1ED69F5C7AC
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.)..DN^....." .....p.....@.....0 .....@lx}..b..... .....c.....h.....$#..... .....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\2IBRPi\BdeUISrv.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	52736
Entropy (8bit):	5.7946530792580475
Encrypted:	false
SSDEEP:	768:NS51B2sZMD1mYu/Lr7p0dHkf9abpWnGjTopPjZdWC2bNrHuOKAh/4J99j4ktPUww:J/Yn/Lr7qwYb7/oRjeJh2991t8Yte
MD5:	25D86BC656025F38D6E626B606F1D39D
SHA1:	673F32CCA79DC890ADA1E5A2CF6ECA3EF863629D
SHA-256:	202BEC0F63167ED57FCB55DB48C9830A5323D72C662D9A58B691D16CE4DB8C1E
SHA-512:	D4B4BC411B122499E611E1F9A45FD40EC2ABA23354F261D4668BF0578D30AEC5419568489261FC773ABBB350CC77C1E00F8E7C0B135A1FD4A9B6500825FA6E0
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown

C:\Users\user\AppData\Local\2lBRPi\BdeUISrv.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....3..hw.;w.;w.;~.";u.;...:t.;...:`.;...:q.;...:d.;w.;.;.:.:.;..N;v.;...:v.;Richw.; .....PE..d...X.....".....v...\.....0y.....@..... .....Db....`..... .....p.....x.....T..... .....text...At.....v..... ..`.rdata...3.....4...z.....@..@.data.....@....pdata.....@..@.rsrc.....@..@. reloc..x.....@..B..... .....

C:\Users\user\AppData\Local\2lBRPi\WTSAPI32.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2109440
Entropy (8bit):	3.583353111174115
Encrypted:	false
SSDEEP:	12288:0VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:xfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	860C08B5CFEB671CA94A0CEC612CA670
SHA1:	584648309587E969A66C78F2DB9E995BA138DB1A
SHA-256:	C1C3B44B2E6EE00A256E4B6ECDFF26E4EE3C6F89C5B88026EA2C929D95CD0719
SHA-512:	AD81404B4AEE0F8C268D87ED57DC7A8093E87C9DF454CDC324DD3432DC9E6125FF9ED376ECA36C456AAF0B7FA81A077E9AB86BA0698CF8A396844619861650D
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.) ..DN^....." .....p.....@.....0 .....@lx}..b..... .....c.....h.....$#..... .....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\7YI8zy\OLEACC.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2109440
Entropy (8bit):	3.5783451393964993
Encrypted:	false
SSDEEP:	12288:NVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:UfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	B882DA1C973F306CE92DF7B397F79477
SHA1:	D3A451F40911018FD3FB3827CBC794A91D50C0BF
SHA-256:	BDC8B5C0E124749EFD29F926C5DEB99D4D6111E37C290354EB69BBD43891BE43
SHA-512:	59381D442B6D01629468C9DEE364976C73AF67162C03F112835E50FB3C5A3652E17325BF79FD5DA50D8E8231B8C6208010D1DD4398935884D78C67243F0C3D7D
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.) ..DN^....." .....p.....@.....0 .....@lx}..b..... .....c.....h.....$#..... .....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\7YI8zy\sethc.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	284160
Entropy (8bit):	6.85709982153028
Encrypted:	false
SSDEEP:	6144:z1dgUn5C1AlGr66uFz2LJGRg4kLNnei36cw:XiKFCdUc
MD5:	1C0BF0B710016600C9D9F23CC7103C0A
SHA1:	EFA944D43F76AEA0C72A5C7FB3240ADC55E7DAE8
SHA-256:	AEA110EE0865635EE764B1B40409DB3A3165E57EFFF4CAF942BCD8982F3063C5

C:\Users\user\AppData\Local\7YI8zy\sethc.exe	
SHA-512:	775F075A9D43A887B1AFB000E5E2CBC8EF514C4B1864C694977342307C61173DACC5BA8E5D47002870687B24914B3E6D2D0EB48BF99517822511A8BA2A122515
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....r../6q.\|6q.\|6q.\|6q.\|Y..}5q.\|Y..} q.\|Y..}1q.\|Y..}-q.\|6q.\|8p.\|Y..}$q.|Y.[|7q.| Y..}7q.|Rich6q.|.....PE..d.... .....".....@.....`..... .....P.....`..h'...P.....x.....T..... .....0.....0.....text..... ..`.rdata...j.....l.....@..@.data...8....0.....@....pdata.....P.....$.....@..@.rsrc...h'...`... (...,.....@..@.reloc..x.....T.....@..B..... .....

C:\Users\user\AppData\Local\92ea6x\OLEACC.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2109440
Entropy (8bit):	3.578353842294324
Encrypted:	false
SSDEEP:	12288:hVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:QfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	562B44A22DF95EC9CAB4D5FE434F6B79
SHA1:	B8C66B70032983B0F6767CA39D5ED53BE1090E83
SHA-256:	157395ACD40DFE6078A29173CBEFF6E17E522607CB4D92C9AA9E64A1CFA4616F
SHA-512:	B76402269EB0CED9A0788BEFC131ABBAD97A2BC53DAA0FBACF51AA3D5A745DC56DEB3CD1AF871F4FC03F95781B22A1D6BC40AFAC938AE1327FF3D0EE9BC3 9F27
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.) ..DN^..... " .....p.....@.....0 .....@lx}..b..... .....c.....h.....$#..... ....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\92ea6x\WMPDMC.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1517568
Entropy (8bit):	6.62150533612437
Encrypted:	false
SSDEEP:	24576:esSffc55l2PlDph6LYq3BRf6Te8+n3wAJF1/Mk+F6uwY6V0qRr8kmHVJZh/u:cct2PpphUlxRn3wAblMk+F6+6S2r8/Hu
MD5:	4085FDA375E50214142BD740559F5835
SHA1:	22D548F1E0F4832AAEE3D983A156FDABD3021DA4
SHA-256:	93F61516B7FD3CE8F1E97F25B760BDF62AE58CC7714B559FEFC2C75AD1130804
SHA-512:	7712F8E551D475A9D2FF3BED9992A2B3D53AB01F61DCB7313320181F9EB6B5B84558CCA45AE95150267128C8B228F806F869157B7F4961755076DD83F02E3BDF
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....@.....-.....*.....+...../..../.A....'.X.....,....Rich..... .....PE..d...D..9....." ....@.....`..... ..... ..x.....l.....0...S..`Y..T.....G..(....F.....8G..... .....text..... ..`.rdata..Pg.....h.....@..@.data...p=...@.....,.....@....pdata..l.....D.....@..@.didat.....@.... rsrc...x.... .....@..@.reloc...S...0...T.....@..B..... .....

C:\Users\user\AppData\Local\Iz08tEz\XmlLite.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2109440
Entropy (8bit):	3.576061001877867
Encrypted:	false
SSDEEP:	12288:uVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:zfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	4DFE07B3BCAFD9CE65D8C33C35692412
SHA1:	72E62D60652D8B8E0FFAEABE38E85DF7474DE3F0
SHA-256:	601E95E3207C0693E50E0DF68F2D3F4563365D832C22A28F18659B9F30C37DF5

C:\Users\user\AppData\Local\Iz08tEz\XmlLite.dll	
SHA-512:	020BA9DB617F445299631A8A9097AC67014B1FA640209B302A679474AF329CD25887295BCDBBCC1E4DD7DF66D818507232F3AF5879B3BB9DBDDDF6DE1F6B37F E
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.) ..DN^....." .....p.....@.....0 .....@lx}..b..... .....c.....h.....$#..... ....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\Iz08tEz\ddodiag.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	37888
Entropy (8bit):	5.0324146638870335
Encrypted:	false
SSDEEP:	768:li5tlKBaheiGK/hc3aZkLmMgMaouZl6i9Kott/D:/C0heiGK/hc3aZkLmMgMaouZl6i9t/D
MD5:	3CE911D7C12A2EFA9108514013BD17FE
SHA1:	2F739BD7731932A0BF13A3B8526FC867EC41C63E
SHA-256:	FC55CB5FF243496B039D3DB181BD846BDD38D11C7D52E4BA20D882B65FBE1C3B
SHA-512:	33F4FD94916DB3F0BC4E138DD88125D9B45108F7EECFDE0A54BE1901F4BE3F1966BC0FE9278A919A3D94AEC53A8269ACA9451EBA7D53C82BF64CC215522AD7 8E
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....X.=...S...S...S.s.P...S.s.W...S.s.V...S.s.R...S...R.$.S.s.Z...S.s....S.s .Q...S.Rich..S.....PE..d...~3....."....."....&...p.....p/.....@.....q...`..... .....~..d.....p.....(...`z..T..... E..... F.....text...P%.....&..... ..`.rdata.."D...@...F...*.....@..@.data.....p.....@....pdata.....@..@.rsrc...p.... .....@..@.reloc..(.....@..B.....

C:\Users\user\AppData\Local\JFuMqIg\VERSION.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2109440
Entropy (8bit):	3.5769403032587643
Encrypted:	false
SSDEEP:	12288:BVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:wfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	D76C4636DA44EBABF1FC1E81811471E0
SHA1:	3191D457033E6D791CDBE097A3D1ADC3F7284491
SHA-256:	E06D76E1543A31F7BC71EA29D772368867B8A971C303B5CA10EE224F69D814AE
SHA-512:	8A57090E6156AD7D73CC637E6BDA63F74E896F8A6A53581A2A4D12996AFB49CBE9B27DD18AD2DB2FEE6E9CC1750F81CB1640394BC0C95C88085AFE1AA9CE1 D5
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.) ..DN^....." .....p.....@.....0 .....@lx}..b..... .+....c.....h.....$#..... ....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\JFuMqIg\wscript.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	163840
Entropy (8bit):	5.729539450068024
Encrypted:	false
SSDEEP:	1536:8HSpBlnak9UH8bCAHZ1LQ434syPz7M5hh/kzhwS827HuYHwHugXEYJ6S7775MWUn:aC4HWCp/fM5hvNebgXEYJN73uWUZxtt
MD5:	9A68ADD12EB50DDE7586782C3EB9FF9C
SHA1:	2661E5F3562DD03C0ED21C33E2888E2FD1137D8C
SHA-256:	62A95C926C8513C9F3ACF65A5B33CBB88174555E2759C1B52DD6629F743A59ED
SHA-512:	156CAED6E1BF27B275E4BA0707FB550F1BF347A26361D6D3CAD12C612C327686950B47B6C5487110CF8B35A490FAADC812ADE3777FFF7ED76A528D970914A6E
Malicious:	false

C:\Users\user\AppData\Local\JFuMqIg\wscript.exe	
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\S8mrk1\OLEACC.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2109440
Entropy (8bit):	3.578355139397792
Encrypted:	false
SSDEEP:	12288:qVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:3fP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	D37540715730618EC4C8D8320D14BA1F
SHA1:	61DE879F216BFDFC426752CA83E326632F229203
SHA-256:	828D0A3C802DBDB43DB11772E7AB9432AC794124F5C1766D7B89802A35094B7B
SHA-512:	20ACED35734330011806C82F3523BF15B3E3CB5E2FCBDBA861A9FB4496F6249198AFCBCCA0271E65B3184B555041E122C76D67991E7903FD3F31FF6A3FE9B3A5
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.) ..DN^....." .....p.....@.....0 .....@lx}..b..... .....c.....h.....$#..... ....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\S8mrk1\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:	B76D2BE02A22990E224DBC5AED9E5B701EAC52C1376529DE3E90B084CD6860B88D746CD61093E93FC932E12FBAF45B4CA342CC0D9C9DAE4EAFE05921D83A7 97
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\eQL\WTSAPI32.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2109440
Entropy (8bit):	3.583321391509454
Encrypted:	false
SSDEEP:	12288:aVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:HfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	4FBEA39A2FFB22CDAEB407491596D80B
SHA1:	EB0102854221347A1F395685A8B10591F0A7A275
SHA-256:	ABF264AEB0738742100E969CAFC9328B84070A69D87CF920CE1A83628E13D47D
SHA-512:	E72BDBFE7B1CA46C9003AEACC1CB3B2BF766D1F8BD915DC5DEA965A44554F08299816E7E5ECA11D71BF10EBE4C6418126ED1CAD2934DC30279A3B74A75B39 247
Malicious:	false
Reputation:	unknown

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

C:\Users\user\AppData\Local\eQL\raserver.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	128000
Entropy (8bit):	5.845576104002147
Encrypted:	false
SSDEEP:	3072:KPtuXlMcmw7mMH/5+fDxE/loYJZFr3kzH:plMcmzMH/5Sy/loYJZFSH
MD5:	DE2022F0B86E33875D8A40B65550CFEB
SHA1:	391DDE6C03A58D0FC0B4BF5AF46BD181584936C2
SHA-256:	95470F8DE7666C026DB37D2A754085BA3832358C422D6218126D293A67B2F60E
SHA-512:	903A9B137715B114D861BED86E4CAEB9772455DA6749E40C0DDA9758DEE5BDDF0DB3FB46B484556DD55162294C97A399105E3C3E8FDFC0D63F9A8967F99EDDA
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u.....3.....Rich.....PE..d....Z.....".....@.....u...`.....p.....6.....0.....T.....0D.....0E..X.....@.....text.....rdata.....0.....@..@.data... .....@....pdata.....@..@.didat.....@....rsrc....6.....8.....@..@.reloc.....0.....@..B.....

C:\Users\user\AppData\Local\jYs4ma0u\ACTIVEDS.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2109440
Entropy (8bit):	3.5780991878185837
Encrypted:	false
SSDEEP:	12288:oVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:9fP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	9E70F06EEB43B7684995C76AFF5E3B6F
SHA1:	3245C9D942678CAA6CC3B3FE91B84B8BBA961B0B
SHA-256:	8BADF14EA6C4EC41342CAB9CA944EA6D1CA4B76E3A65DFA11E94736B78E4E16F
SHA-512:	0FE463B9EDF9E3723E5E738F9D417D9CED2FE8D85BBC4CDA67CFA4FC02FE5835F9DC2CD0F126912343E5D314C2C3F6D4536D66EAD905A3AC827680373A6C439
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.)..DN^....." .....p.....@.....0 .....@lx}..b..... .y....c.....h.....$#..... .....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\jYs4ma0u\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:	F78F46437C011C102A9BCEC2A8565EDC75500C9448AC17457FF44D3C8DB1980F772C0D1546F1DEE0F8A6F2C7273A5A915860B768DE9BB24EBEFE2907CE18B0F
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\jYs4ma0u\SppExtComObj.Exe	
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\yoY8Y\XmlLite.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	2109440
Entropy (8bit):	3.576064881611147
Encrypted:	false
SSDEEP:	12288:fVI0W/TtlPLfJCm3WIYxJ9yK5lQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:WfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	960BA4F38C3F96CA6C088B732D12F98D
SHA1:	2282B2027E83696813DAE22FA050CBEE25641814
SHA-256:	60843D78DAAA68AB9F7A82D127138C6E67DD47F2CA7C1C47820CAD85FFA4879F
SHA-512:	E709B8EF755F827DC853BDD5DD69FE2863B1918FF9EED50815DC347D71236F8B1292ADFD176E4CE948192B34AECCD6F3BDF3B700ED241F7EDB79F37EE006F4B
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}....I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.) ..DN^..... " .....p.....@.....0 .....@lx}..b..... .....c.....h.....$#..... ....text..... ..`.rdata..,O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\yoY8Y\ddodiag.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	37888
Entropy (8bit):	5.0324146638870335
Encrypted:	false
SSDEEP:	768:li5tlKBaheiGK/hc3aZkLmMgMaouZl6i9Kott/D:/C0heiGK/hc3aZkLmMgMaouZl6i9t/D
MD5:	3CE911D7C12A2EFA9108514013BD17FE
SHA1:	2F739BD7731932A0BF13A3B8526FC867EC41C63E
SHA-256:	FC55CB5FF243496B039D3DB181BD846BDD38D11C7D52E4BA20D882B65FBE1C3B
SHA-512:	33F4FD94916DB3F0BC4E138DD88125D9B45108F7EECFDE0A54BE1901F4BE3F1966BC0FE9278A919A3D94AEC53A8269ACA9451EBA7D53C82BF64CC215522AD78E
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....X.=...S...S...S.s.P...S.s.W...S.s.V...S.s.R...S...R.$.S.s.Z...S.s....S.s .Q...S.Rich..S.....PE..d...~3.....".....&...p.....p/.....@.....q...`..... .....~..d.....p.....(...`z..T..... E..... F.....text...P%.....&..... ..`.rdata.."D...@...F...*.....@..@.data.....p.....@....pdata.....@..@.rsrc...p.... .....@..@.reloc..(.....@..B..... .....

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\414045e2d09286d5db2581e0d955d358_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	4442
Entropy (8bit):	5.464429481363534
Encrypted:	false
SSDEEP:	48:F3sV8UzB4ghZgNEDJN5G/3sV8Uwfg5p+sDw/RsSUZQKrt:F3sV8a26iQm3sV8SWsDOJ0Z
MD5:	F8E3EE8D7E508146B4D4A69987A397E0
SHA1:	117280869E2C01839C86F013FED869887721D73B
SHA-256:	B1C8DC44B2B3A83A1B831665D934AABEA14BE2F52C02D859C9728A1ED3AB64FB
SHA-512:	4835D8A9F18EA4755A5BDCB3D04F315BB9E528F90394CEE9C274F7188A5B59922ACD6088EDE6DA7CCFF9D7611CBF3A4E14AF8FD85D0EFC3F3760866B879BCABB
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\414045e2d09286d5db2581e0d955d358_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Preview:	.....user.....user.....RSA1.....1P...v.....@..|V..3..>.}.&....E. ..G .pd?...l..w.....!.W.}.....c9>T4.:...@....'Sl... x.7.e.J.....8.p..|....p]. .....z..O.....A\..1..F..::M...F.....,..C.r.y.p.t.o.A.P.I. .P.r.i.v.a.t.e. .K.e.y....f..... ....E#^.C.I...^0..rRQ2..... ...`....#.$.....9. .....0..... .....X.....p.....X-.....Qx.s.....{..@.....6w..N....>3Dp.Q...!.^....K.-q7.....`.....WOp..v$K.R..Y.1..U...cj.r`...^.1|_. X..).:.U^.SF.O=.....P;....w.zz.FV...h.)...0.O.&....i...#..... 6.W~.I.N\q.+.C.....>...S.....Y..].g.t.8.x... }..H..o..gC...9.>T:R....Oa].....,"..M..R%..b.L.....#..!i...5jTIp).$t&+.Ip..Jj...3.B.F.F...gv.o...J...n:..t....E..@.....kR.q6...T!.....v ?~. .s7.....LW=I.?.lu!....s..VH....T\|+/...t..F.....d.l.f..y.....$...|*...X....I...@..O}....Gi....Y+Z....q.(.5...%...+c.+3f+..

Static File Info

General

File type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Entropy (8bit):	3.58956560239292
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:	yWteP7e12z.dll
File size:	2105344
MD5:	a75be08d11b5028b6e0fa8be59676599
SHA1:	c47a48e04dc10641df07dba7dbbb73602e6615aa
SHA256:	7500211dd9ce4e45664ae07e4eb58ca361c4551f1c2b52d00bb0da547e9cdc2a
SHA512:	444d9ddbdbfac48953e01df6ed9376a78de22f6ae5d8155e5325a8482c228f96c099985ac4b9fd2e5447090380e535bdad59f59b7ebfa20578cd2038262a53b8
SSDEEP:	12288:LVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:KfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....|...|...|....K.#}...'...}.....{}....X.#}....f..|....g..}..*...a|.....}....N..}..*...E}..[.I.E|...'..U}....N.+}..[.K.P|.

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x140041070
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x140000000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE, DLL, LARGE_ADDRESS_AWARE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x5E4E44CC [Thu Feb 20 08:35:24 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	6668be91e2c948b183827f040944057f

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x40796	0x41000	False	0.776085486779	data	7.73364605679	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x42000	0x64f2c	0x65000	False	0.702390160891	data	7.86574512659	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa7000	0x178b8	0x18000	False	0.0694580078125	data	3.31515306295	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0xbf000	0x12c	0x1000	False	0.06005859375	PEX Binary Archive	0.581723022719	IMAGE_SCN_TYPE_DSECT, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.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
.wualk	0x15f000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.qwqp	0x160000	0x389	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.txp	0x161000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ezxpm	0x162000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.kdkmc	0x163000	0x736	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
.vwqjj	0x164000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ute	0x165000	0x9cd	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.hzotrb	0x166000	0x3ba	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.mkb	0x167000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.plbi	0x169000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.dmwl	0x16a000	0x2da	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.qorltm	0x16b000	0x141	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ubg	0x16c000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.lhm	0x16d000	0x1f2a	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.wojiyd	0x16f000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ekv	0x170000	0x389	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vmf	0x171000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rqv	0x172000	0x197d	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rseab	0x174000	0x543	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pxtlo	0x175000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.nri	0x1bb000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.fcbpa	0x201000	0x9cd	0x1000	False	0.323974609375	data	4.02720598472	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: 6928 Parent PID: 5496

General

Start time:	01:31:16
Start date:	29/09/2021
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe 'C:\Users\user\Desktop\yWteP7e12z.dll'
Imagebase:	0x7ff6440f0000
File size:	1136128 bytes
MD5 hash:	E0CC9D126C39A9D2FA1CAD5027EBBD18
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000000.00000002.311924847.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 4668 Parent PID: 6928

General

Start time:	01:31:17
Start date:	29/09/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\yWteP7e12z.dll',#1
Imagebase:	0x7ff786250000
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: 4536 Parent PID: 6928

General

Start time:	01:31:17
Start date:	29/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\yWteP7e12z.dll,BeginBufferedAnimation
Imagebase:	0x7ff7e9410000
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: 00000002.00000002.384630779.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 4528 Parent PID: 4668

General

Start time:	01:31:17
Start date:	29/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe 'C:\Users\user\Desktop\yWteP7e12z.dll',#1
Imagebase:	0x7ff7e9410000
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: 00000003.00000002.290585928.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3352 Parent PID: 4536

General

Start time:	01:31:19

Start date:	29/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff720ea0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
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: 6568 Parent PID: 6928

General

Start time:	01:31:20
Start date:	29/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\yWteP7e12z.dll,BeginBufferedPaint
Imagebase:	0x7ff7e9410000
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: 00000008.00000002.299168621.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 3912 Parent PID: 6928

General

Start time:	01:31:24
Start date:	29/09/2021

Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\yWteP7e12z.dll,BeginPanningFeedback
Imagebase:	0x7ff7e9410000
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: 00000009.00000002.305431916.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: recdisc.exe PID: 6628 Parent PID: 3352

General

Start time:	01:32:04
Start date:	29/09/2021
Path:	C:\Windows\System32\recdisc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\recdisc.exe
Imagebase:	0x7ff7400a0000
File size:	192512 bytes
MD5 hash:	D2AEFB37C329E455DC2C17D3AA049666
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: SnippingTool.exe PID: 7044 Parent PID: 3352

General

Start time:	01:32:04
Start date:	29/09/2021
Path:	C:\Windows\System32\SnippingTool.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SnippingTool.exe
Imagebase:	0x7ff75dea0000
File size:	3292160 bytes
MD5 hash:	9012F9C6AC7F3F99ECDD37E24C9AC3BB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: SnippingTool.exe PID: 6200 Parent PID: 3352

General

Start time:	01:32:06
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\S8mrk1\SnippingTool.exe

Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\S8mrk1\SnippingTool.exe
Imagebase:	0x7ff73d040000
File size:	3292160 bytes
MD5 hash:	9012F9C6AC7F3F99ECDD37E24C9AC3BB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000013.00000002.415702992.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities Show Windows behavior

File Read

Analysis Process: raserver.exe PID: 3604 Parent PID: 3352

General

Start time:	01:32:18
Start date:	29/09/2021
Path:	C:\Windows\System32\raserver.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\raserver.exe
Imagebase:	0x7ff7f7510000
File size:	128000 bytes
MD5 hash:	DE2022F0B86E33875D8A40B65550CFEB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: raserver.exe PID: 2992 Parent PID: 3352

General

Start time:	01:32:19
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\eQL\raserver.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\eQL\raserver.exe
Imagebase:	0x7ff74e110000
File size:	128000 bytes
MD5 hash:	DE2022F0B86E33875D8A40B65550CFEB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000001A.00000002.443389132.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities Show Windows behavior

File Read

Analysis Process: ddodiag.exe PID: 5808 Parent PID: 3352

General

Start time:	01:32:30
Start date:	29/09/2021
Path:	C:\Windows\System32\ddodiag.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\ddodiag.exe
Imagebase:	0x7ff7da9c0000
File size:	37888 bytes
MD5 hash:	3CE911D7C12A2EFA9108514013BD17FE
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: ddodiag.exe PID: 5828 Parent PID: 3352

General

Start time:	01:32:31
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\Iz08tEz\ddodiag.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Iz08tEz\ddodiag.exe
Imagebase:	0x7ff740980000
File size:	37888 bytes
MD5 hash:	3CE911D7C12A2EFA9108514013BD17FE
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000001C.00000002.469517159.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Read

Analysis Process: dccw.exe PID: 2364 Parent PID: 3352

General

Start time:	01:32:44
Start date:	29/09/2021
Path:	C:\Windows\System32\dccw.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\dccw.exe
Imagebase:	0x7ff722dc0000
File size:	657920 bytes
MD5 hash:	341515B9556F37E623777D1C377BCFAC
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: SppExtComObj.Exe PID: 6280 Parent PID: 3352

General

Start time:	01:32:46
Start date:	29/09/2021
Path:	C:\Windows\System32\SppExtComObj.Exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SppExtComObj.Exe
Imagebase:	0x7ff6c3600000
File size:	577024 bytes
MD5 hash:	809E11DECADAEBE2454EFEDD620C4769
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: SppExtComObj.Exe PID: 5620 Parent PID: 3352

General

Start time:	01:32:47
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\jYs4ma0u\SppExtComObj.Exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\jYs4ma0u\SppExtComObj.Exe
Imagebase:	0x7ff791460000
File size:	577024 bytes
MD5 hash:	809E11DECADAEBE2454EFEDD620C4769
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000020.00000002.502508138.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Read

Analysis Process: WMPDMC.exe PID: 6628 Parent PID: 3352

General

Start time:	01:32:58
Start date:	29/09/2021
Path:	C:\Windows\System32\WMPDMC.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WMPDMC.exe
Imagebase:	0x7ff74b5f0000
File size:	1517568 bytes
MD5 hash:	4085FDA375E50214142BD740559F5835
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: WMPDMC.exe PID: 6480 Parent PID: 3352

General

Start time:	01:32:59
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\92ea6x\WMPDMC.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\92ea6x\WMPDMC.exe
Imagebase:	0x7ff67b5f0000

File size:	1517568 bytes
MD5 hash:	4085FDA375E50214142BD740559F5835
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000022.00000002.529404050.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: wscript.exe PID: 5532 Parent PID: 3352

General

Start time:	01:33:11
Start date:	29/09/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wscript.exe
Imagebase:	0x7ff70a400000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: wscript.exe PID: 5012 Parent PID: 3352

General

Start time:	01:33:12
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\JFuMqIg\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\JFuMqIg\wscript.exe
Imagebase:	0x7ff6e8920000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000025.00000002.556857266.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: BdeUISrv.exe PID: 5368 Parent PID: 3352

General

Start time:	01:33:23
Start date:	29/09/2021
Path:	C:\Windows\System32\BdeUISrv.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\BdeUISrv.exe
Imagebase:	0x7ff609f50000
File size:	52736 bytes
MD5 hash:	25D86BC656025F38D6E626B606F1D39D
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: BdeUISrv.exe PID: 6080 Parent PID: 3352

General

Start time:	01:33:24
Start date:	29/09/2021
Path:	C:\Users\user\AppData\Local\2IBRPi\BdeUISrv.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\2IBRPi\BdeUISrv.exe
Imagebase:	0x7ff6e6d60000
File size:	52736 bytes
MD5 hash:	25D86BC656025F38D6E626B606F1D39D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000029.00000002.583509816.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

Disassembly

Code Analysis