ID: 492554
Sample Name: Y7KrNvSxWx
Cookbook: default.jbs
Time: 20:04:54
Date: 28/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report Y7KrNvSxWx 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 5
Sigma Overview 5
Jbx Signature Overview 5
AV Detection: 5
E-Banking Fraud: 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
URLs from Memory and Binaries 9
Contacted IPs 9
General Information 10
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 10
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 19
General 19
File Icon 19
Static PE Info 19
General 20
Entrypoint Preview 20
Rich Headers 20
Data Directories 20
Sections 20
Resources 21
Imports 21
Exports 21
Version Infos 21
Possible Origin 22
Network Behavior 22
Network Port Distribution 22
UDP Packets 22
Code Manipulations 22
Statistics 22
Behavior 22
System Behavior 22
Analysis Process: loaddll64.exe PID: 2288 Parent PID: 6428 22
General 22
File Activities 22
Analysis Process: cmd.exe PID: 2468 Parent PID: 2288 23
General 23
File Activities 23
Analysis Process: rundll32.exe PID: 6724 Parent PID: 2288 23
General 23
File Activities 23
File Read 23
Analysis Process: rundll32.exe PID: 6964 Parent PID: 2468 23
General 23
File Activities 24
File Read 24

Analysis Process: explorer.exe PID: 3440 Parent PID: 6724 24
General 24
File Activities 24
File Created 24
File Deleted 24
File Written 24
File Read 24
Registry Activities 24
Key Created 24
Key Value Created 24
Analysis Process: rundll32.exe PID: 6676 Parent PID: 2288 24
General 24
File Activities 25
File Read 25
Analysis Process: rundll32.exe PID: 2904 Parent PID: 2288 25
General 25
File Activities 25
File Read 25
Analysis Process: SndVol.exe PID: 2176 Parent PID: 3440 25
General 25
Analysis Process: SndVol.exe PID: 2444 Parent PID: 3440 25
General 25
File Activities 26
File Read 26
Analysis Process: bdeunlock.exe PID: 6612 Parent PID: 3440 26
General 26
Analysis Process: bdeunlock.exe PID: 6604 Parent PID: 3440 26
General 26
File Activities 26
File Read 26
Analysis Process: SystemPropertiesPerformance.exe PID: 5548 Parent PID: 3440 26
General 26
Analysis Process: SystemPropertiesPerformance.exe PID: 5532 Parent PID: 3440 27
General 27
File Activities 27
File Read 27
Analysis Process: GamePanel.exe PID: 5824 Parent PID: 3440 27
General 27
Analysis Process: GamePanel.exe PID: 6444 Parent PID: 3440 27
General 27
File Activities 28
File Read 28
Analysis Process: tcmsetup.exe PID: 3324 Parent PID: 3440 28
General 28
Analysis Process: tcmsetup.exe PID: 1916 Parent PID: 3440 28
General 28
Analysis Process: wscript.exe PID: 2584 Parent PID: 3440 28
General 28
Analysis Process: wscript.exe PID: 4312 Parent PID: 3440 29
General 29
Analysis Process: BitLockerWizardElev.exe PID: 4640 Parent PID: 3440 29
General 29
Analysis Process: BitLockerWizardElev.exe PID: 1636 Parent PID: 3440 29
General 29
Analysis Process: upfc.exe PID: 5152 Parent PID: 3440 30
General 30
Analysis Process: upfc.exe PID: 5816 Parent PID: 3440 30
General 30
Analysis Process: SystemPropertiesDataExecutionPrevention.exe PID: 6060 Parent PID: 3440 30
General 30
Disassembly 31
Code Analysis 31

Windows Analysis Report Y7KrNvSxWx

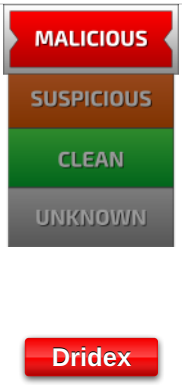
Overview

General Information

Sample Name:	Y7KrNvSxWx (renamed file extension from none to dll)
Analysis ID:	492554
MD5:	ecdfff8b0ece217…
SHA1:	9359770d71e743..
SHA256:	dc684f824a7deaf..
Tags:	Dridex exe
Infos:	

Most interesting Screenshot:

Detection

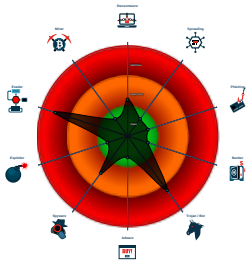


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected Dridex unpacked file
- Multi AV Scanner detection for subm…
- Benign windows process drops PE f…
- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Changes memory attributes in foreig…
- Machine Learning detection for samp…
- Queues an APC in another process …
- Machine Learning detection for dropp…
- Contains functionality to automate e…
- Uses Atom Bombing / ProGate to in…
- Queries the volume information (nam…

Classification



- **System is w10x64**
- loaddll64.exe (PID: 2288 cmdline: loaddll64.exe 'C:\Users\user\Desktop\Y7KrNvSxWx.dll' MD5: E0CC9D126C39A9D2FA1CAD5027EBBD18)
  - cmd.exe (PID: 2468 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\Y7KrNvSxWx.dll',#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 6964 cmdline: rundll32.exe 'C:\Users\user\Desktop\Y7KrNvSxWx.dll',#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 6724 cmdline: rundll32.exe C:\Users\user\Desktop\Y7KrNvSxWx.dll,CloseDriver MD5: 73C519F050C20580F8A62C849D49215A)
    - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - SndVol.exe (PID: 2176 cmdline: C:\Windows\system32\SndVol.exe MD5: CDD7C7DF2D0859AC3F4088423D11BD08)
      - SndVol.exe (PID: 2444 cmdline: C:\Users\user\AppData\Local\KXZtu\SndVol.exe MD5: CDD7C7DF2D0859AC3F4088423D11BD08)
      - bdeunlock.exe (PID: 6612 cmdline: C:\Windows\system32\bdeunlock.exe MD5: FAB70105E2075EEC9C249A4D499CAE7C)
      - bdeunlock.exe (PID: 6604 cmdline: C:\Users\user\AppData\Local\mlAKVTuFf\bdeunlock.exe MD5: FAB70105E2075EEC9C249A4D499CAE7C)
      - SystemPropertiesPerformance.exe (PID: 5548 cmdline: C:\Windows\system32\SystemPropertiesPerformance.exe MD5: F325976CDC0F7E9C680B51B35D24D23A)
      - SystemPropertiesPerformance.exe (PID: 5532 cmdline: C:\Users\user\AppData\Local\UjbH0ZEv\SystemPropertiesPerformance.exe MD5: F325976CDC0F7E9C680B51B35D24D23A)
      - GamePanel.exe (PID: 5824 cmdline: C:\Windows\system32\GamePanel.exe MD5: 4EF330EFAE954723B1F2800C15FDA7EB)
      - GamePanel.exe (PID: 6444 cmdline: C:\Users\user\AppData\Local\cZk0IMu\GamePanel.exe MD5: 4EF330EFAE954723B1F2800C15FDA7EB)
      - tcmsetup.exe (PID: 3324 cmdline: C:\Windows\system32\tcmsetup.exe MD5: 0DDA495155D552D024593C4B3246C8FA)
      - tcmsetup.exe (PID: 1916 cmdline: C:\Users\user\AppData\Local\2oEy\tcmsetup.exe MD5: 0DDA495155D552D024593C4B3246C8FA)
      - wscript.exe (PID: 2584 cmdline: C:\Windows\system32\wscript.exe MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
      - wscript.exe (PID: 4312 cmdline: C:\Users\user\AppData\Local\NakOm\wscript.exe MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
      - BitLockerWizardElev.exe (PID: 4640 cmdline: C:\Windows\system32\BitLockerWizardElev.exe MD5: 3104EA9ECCA9ED71A382CCAAD618CEAE)
      - BitLockerWizardElev.exe (PID: 1636 cmdline: C:\Users\user\AppData\Local\Uh9eo\BitLockerWizardElev.exe MD5: 3104EA9ECCA9ED71A382CCAAD618CEAE)
      - upfc.exe (PID: 5152 cmdline: C:\Windows\system32\upfc.exe MD5: 4CEED46DDAB911AE1298422BFB12460C)
      - upfc.exe (PID: 5816 cmdline: C:\Users\user\AppData\Local\mFxP\upfc.exe MD5: 4CEED46DDAB911AE1298422BFB12460C)
      - SystemPropertiesDataExecutionPrevention.exe (PID: 6060 cmdline: C:\Windows\system32\SystemPropertiesDataExecutionPrevention.exe MD5: 1A34577AEDE83993615D7F2E37024D4D)
  - rundll32.exe (PID: 6676 cmdline: rundll32.exe C:\Users\user\Desktop\Y7KrNvSxWx.dll,DefDriverProc MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 2904 cmdline: rundll32.exe C:\Users\user\Desktop\Y7KrNvSxWx.dll,DriverCallback MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.456385826.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000003.00000002.355433336.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000024.00000002.625281639.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000028.00000002.681547027.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000014.00000002.514246640.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	

Click to see the 8 entries

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

E-Banking Fraud:

Yara detected Dridex unpacked file

HIPS / PFW / Operating System Protection Evasion:

Benign windows process drops PE files

Changes memory attributes in foreign processes to executable or writable

Queues an APC in another process (thread injection)

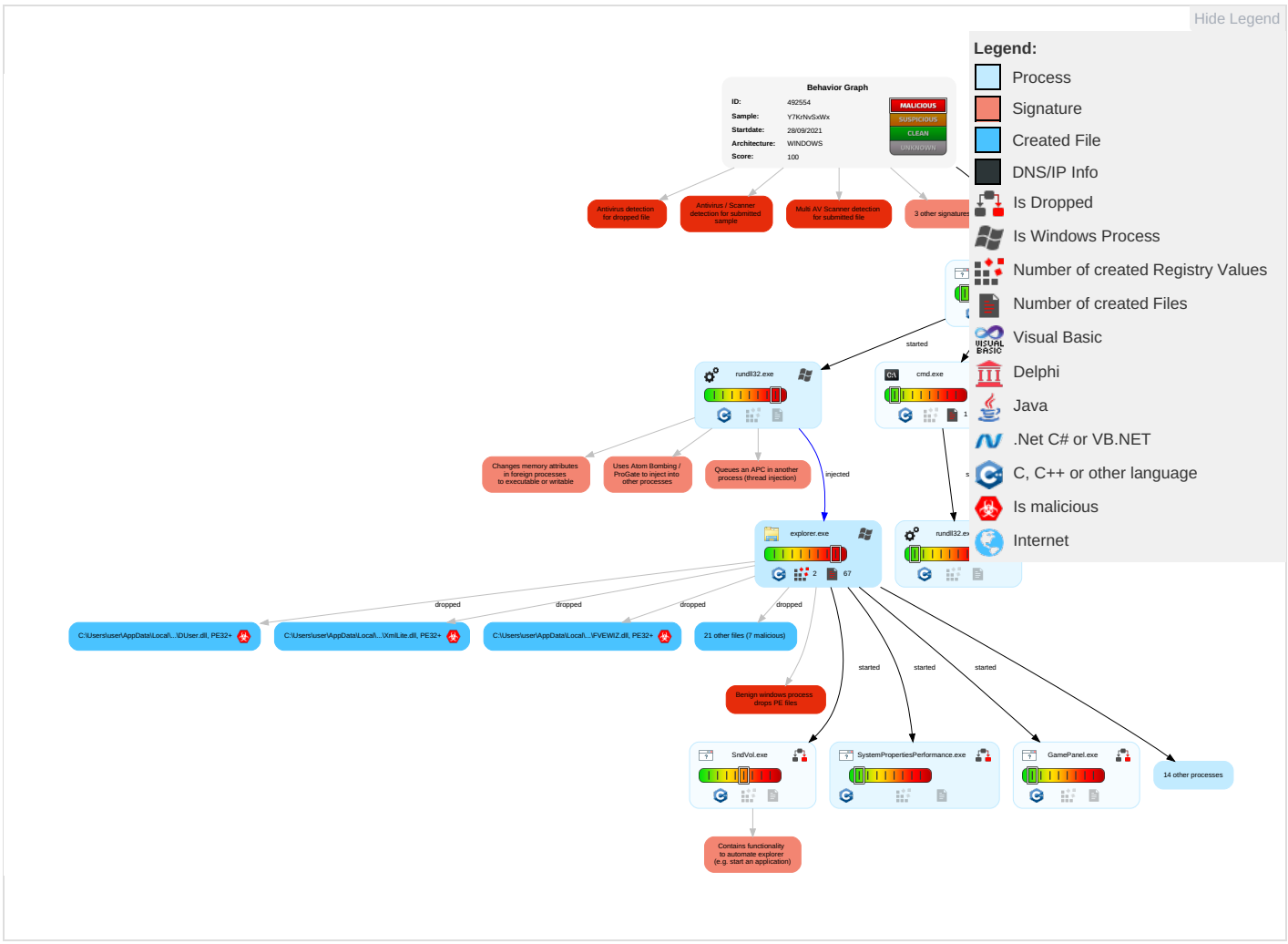
Contains functionality to automate explorer (e.g. start an application)

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	Netv Effe
Valid Accounts	Command and Scripting Interpreter 2	Windows Service 1	Windows Service 1	Masquerading 1 1	Input Capture 1 1	System Time Discovery 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Inse Netv Com
Default Accounts	Service Execution 1	Application Shimming 1	Process Injection 3 1 2	Virtualization/Sandbox Evasion 1	LSASS Memory	Security Software Discovery 3 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Junk Data	Expl Redi Calls
Domain Accounts	Exploitation for Client Execution 1	Logon Script (Windows)	Application Shimming 1	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Expl Trac Loca
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 3 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Man Devi Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Deni Serv
External Remote Services	Scheduled Task	Startup Items	Startup Items	Rundll32 1	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 2	Proc Filesystem	System Information Discovery 3 5	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dow Inse Prot
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Timestomp 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogu Base

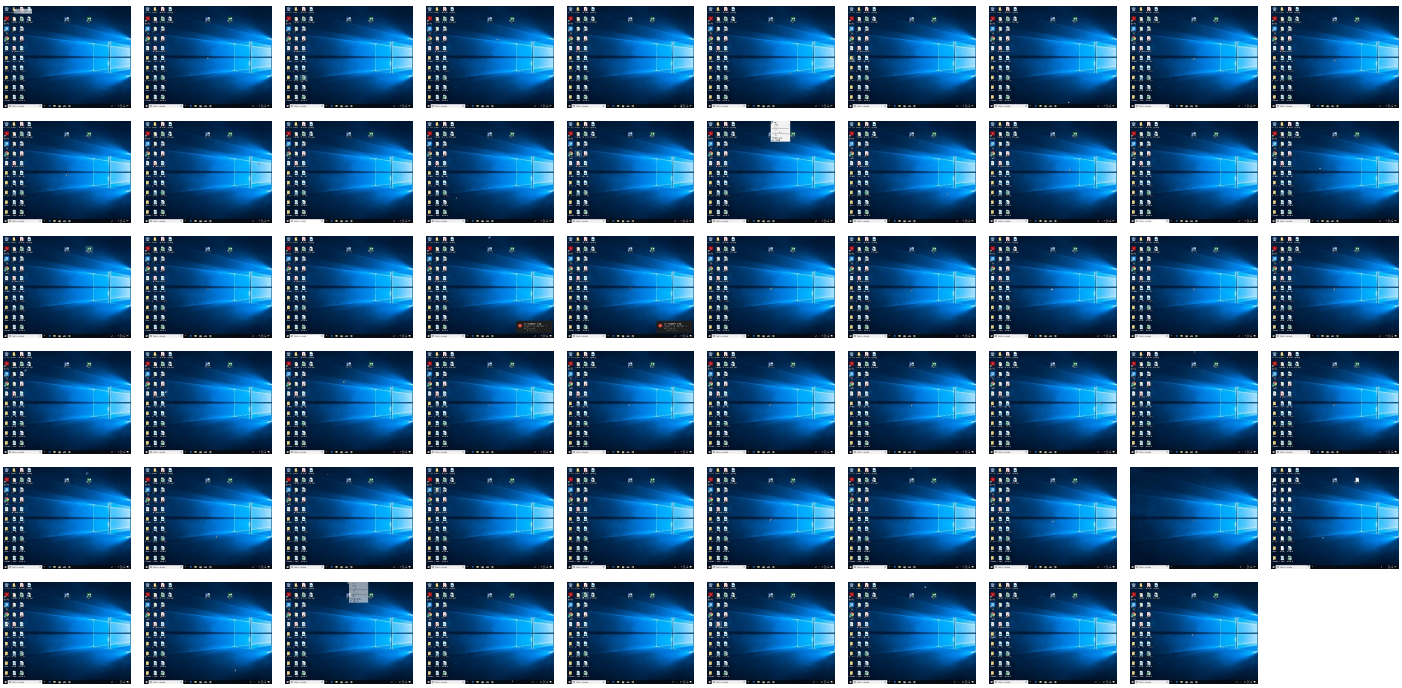
Behavior Graph



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
Y7KrNvSxWx.dll	65%	Virustotal		Browse
Y7KrNvSxWx.dll	78%	ReversingLabs	Win64.Infostealer.Dridex	
Y7KrNvSxWx.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
Y7KrNvSxWx.dll	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\KXZtu\dwmapi.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\KAG\SYSDM.CPL	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\FvTQVxZ\UxTheme.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\mFxP\XmlLite.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\5JXP\VERSION.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\mlAKVTuFf\DUser.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\5JXP\VERSION.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\2oEy\TAPI32.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\KAG\SYSDM.CPL	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\KXZtu\dwmapi.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\IcLt\WTSAPI32.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\Uh9eo\FVEWIZ.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\KXZtu\dwmapi.dll	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\KAG\SYSDM.CPL	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\FvTQVxZ\UxTheme.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\mFxP\XmlLite.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\5JXP\VERSION.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\mlAKVTuFf\DUser.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\5JXP\VERSION.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\2oEy\TAPI32.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\KAG\SYSDM.CPL	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\KXZtu\dwmapi.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\IcLt\WTSAPI32.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Uh9eo\FVEWIZ.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\2oEy\tcmsetup.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\2oEy\tcmsetup.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\2oEy\tcmsetup.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\5JXP\iexpress.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\5JXP\iexpress.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\FvTQVxZ\FileHistory.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\FvTQVxZ\FileHistory.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\IcLt\BdeUISrv.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\IcLt\BdeUISrv.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
7.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
40.2.upfc.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
20.2.bdeunlock.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
33.2.tcmsetup.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
17.2.SndVol.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
25.2.SystemPropertiesPerformance.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
38.2.BitLockerWizardElev.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
36.2.wscript.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
30.2.GamePanel.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://schemas.micro	0%	Avira URL Cloud	safe	
http://https://www.xboxlive.comMBI_SSLhttps://profile.xboxlive.com/users/me/profile/settings?settings=GameD	0%	Avira URL Cloud	safe	

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:	492554
Start date:	28.09.2021
Start time:	20:04:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Y7KrNvSxWx (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@52/25@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 21.1% (good quality ratio 11.8%) • Quality average: 44.8% • Quality standard deviation: 44.6%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\2oEy\TAPI32.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1257472
Entropy (8bit):	5.475685685411727
Encrypted:	false
SSDEEP:	12288:rVl0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:qfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	1F0F43376BD11D400DCCDDCD81B21F94
SHA1:	5EAA2AF81A4FE3BDE246B3FD7DF1CFC7D05A9A72
SHA-256:	6ED5FE6184CA21B30D493C05C4C87A56B921CC94958AE01E89E56D5E100049D9
SHA-512:	4224BE24874CD605E4662B124EF38A59E0278E6FAF8D21CB6DB4641C2C9942A40CA8E88CB58901E0087DDFDCF07CFDEE1BC2288CD20039789FB3AC931A91A10
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.&..DN^......" .....p.....@.....0.....@lx}..b.....V....c.....h.....$#..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\2oEy\tcmsetup.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	4.999998588063228
Encrypted:	false
SSDEEP:	192:DIzBdu2Mhf/+G1jQ0pwPYqLmdO0O7RgZiLtzADWO4hxDcUh6UdBndOvfSWG0oW:GMVJjQ0dg0O7yk5ciJcUhLiSWG0oW
MD5:	0DDA495155D552D024593C4B3246C8FA
SHA1:	7501A7AD5DAA41462BEFF9127154BAF261A24A5B
SHA-256:	D3074CBD29678CA612C1F8AA93DE1F5B75108BE8187F0F2A2331BC302AD48CD9
SHA-512:	9159D8AF457591256BA87443E89ECE942DE40B8FF39586116C2026330B8AE9C20F96905547E87D98508951D2B4687069EFD018CC9E4A6C94A6C26D4B587F41B3
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....$.....Z...Z...Z..[...Z..[...Z..[...Z..[...Z...Z...Z..[...Z.:Z...Z..[...ZRich...Z.....PE..d....E.H....."..... ....@.....`..... .....9..x....p..P....`..D..... ....5..T.....0.....1.....text..... ..`.rdata..&....0.....@..@.data... ....P.....0.....@....pdata..D....`.....2.....@..@.rsrc...P....p.....4.....@..@.reloc.. .....>.....@..B.....

C:\Users\user\AppData\Local\5JXP\VERSION.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1253376
Entropy (8bit):	5.4525540502592165
Encrypted:	false
SSDEEP:	12288:zVl0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:ifP7fWsK5z9A+WGAW+V5SB6Ct4bnb

C:\Users\user\AppData\Local\5JXP\VERSION.dll	
MD5:	10C9880AF256B85D5A97543A9032990E
SHA1:	4D733236EDA9C1C78475ACF1B1288F62187F8FCA
SHA-256:	C28A08796B1EAEB99ED06084E855B205318C2339B44D15CB957CFF2050199218
SHA-512:	6A6A9F06F5401A2E740F3F4CD36255CF8CA8057BC3BFF43AA80023CFE00559DE709C440E1B4D32A31776427F39E2F41AE6D87687B7DF6BB775699649A682BC70
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.& ..DN^....." .....p.....@..... .....@lx}..b.....+....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\5JXP\iexpress.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	165888
Entropy (8bit):	6.756750968049146
Encrypted:	false
SSDEEP:	3072:oV6Rb3NlzO8Lwmq1cXNDnGOb+ahXNqJohePnq45L840:Y6TdOQXNDGOb+asEwv5L
MD5:	5EF563C2A4E7B7F4100ECD13B304FC48
SHA1:	4609D795D758A16B8703CA2E01F250D33816CB81
SHA-256:	2DFA704A6C0DAAEF91BEF043BA6E3F5B5D2516C97AFFBD39EC2C7278497B1688
SHA-512:	C372777121C0924519FC2EFDFF461B97B048D845AF14142680A4E95B9679D65583332788322CC87B98D3B1D8E28D0B1AFF74881B63BDA17434E4A8187B6D7CA9
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....$.....a.....d.....d.....d.....d.....dd.....d.....Rich..... .....PE..d....1....."..... .....@.....`..... .....W...p.....T.....@.....@...(.... .....text..... ..`.rdata.....0.....@..@.data...42...0.....@....pdata.....p.....&.....@..@.rsrc....W.....X.....@ ..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\FvTQVxZ\FileHistory.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	246784
Entropy (8bit):	6.054877934071265
Encrypted:	false
SSDEEP:	3072:5WQz0maAVV604aFUxzYuVD8o+otIxAGQW7A70TshCbdmyTVulAyXRON:5WZmxPZUxzYuVD8ortIxAGJKSuCbd
MD5:	989B5BDB2BEAC9F894BBC236F1B67967
SHA1:	7B964642FEE2D6508E66C615AA6CF7FD95D6196E
SHA-256:	FF1DE8A606FDB6A932E7A3E5EE5317A6483F08712DE93603C92C058E05A89C0C
SHA-512:	0360C9FE88743056FD25AC17F12087DAD026B033E590A93F394B00EB486A2F5E2331EDCCA9605AA7573D892FBA41557C9E0EE4FAC69FCA687D6B6F144E5E524
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....$.....m.s..k ..k ..k .hh!..k .^. ..k .ho!..k .hb!..k .hj!..k ..j #.k .hn!..k .h. ..k .h i!..k Rich..k .....PE..d....."....t...X.....{.....@..... .....\....`..... .....0..... ..8.....$... ...T..... .....H.....text...{m.....n..... ..`.nep.....r..... ..`.rdata...i.....j...x.....@..@.data... .....@....pdata..8.... ....@..@.rsrc.....0.....@..@.reloc..$.....@..B..... .....

C:\Users\user\AppData\Local\FvTQVxZ\UxTheme.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1253376
Entropy (8bit):	5.465059455756909

C:\Users\user\AppData\Local\FvTQVxZ\UxTheme.dll

Encrypted:	false
SSDEEP:	12288:sVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:ZfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	5DF5594539B2BE546567D24A31615566
SHA1:	96289E84A7565C8E5BB8342BD09023BA40D38F22
SHA-256:	C22641414C517DC57F59192D4B26514FD7173C16DB37FEE61C35C744AB9CDD01
SHA-512:	FAEEA042AE4CA60AAA52C1B6E92555309F1381EADA4E80D352CA8B1B95C861265B44AB888933F35554B6F47C8C2225353ED5820F829C884756A9386240EDA6A(
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.&..DN^....." .....p.....@..... .....@lx}..b.....c.....h.....$#..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\IcLt\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
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\IcLt\WTSAPI32.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1253376
Entropy (8bit):	5.461750054653759
Encrypted:	false
SSDEEP:	12288:ZVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:YfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	7E325FBCE0C44335A3D0A1A8F2145EAB
SHA1:	916B0D89C40D3D3E4C6611F05BDB88826AD4D92B
SHA-256:	6713740BA566CB93B7DD769B45F87B808AA1DA40FC273F3FA0B34D81329C88BE
SHA-512:	6F3D574D1DC2435CD142043887D87B30A5B45E0D18BD370629A2FC3F371E75072C82B531909689D23B46B52E444F00C3ED16954C1F204DD9A7A4EEF74F8213BE
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.&..DN^....." .....p.....@..... .....@lx}..b.....c.....h.....$#..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\KAG\SYSDM.CPL

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1253376
Entropy (8bit):	5.451863471275378

C:\Users\user\AppData\Local\KAG\SYSDM.CPL	
Encrypted:	false
SSDEEP:	12288:VVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:MfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	785FAB922A3D502B0BEA7ED0FA1A0A3D
SHA1:	622860AC01B70DA59EE4D8989B7DD2B2CA1AE591
SHA-256:	48070254D0EB21C9312FD4996A4DD9E4519478A4585634C7B513538DC2C9E5D5
SHA-512:	B71C9940A2957DC7E4B05F10479BCD80E5F0B6901AD83F697D6A0BABB200EEE7A36BD3F71FF3CDB030118475898B8EEE8DA3D173C19236968110EE0F42DA805D
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.&..DN^....." .....p.....@..... .....@lx}..b.....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\KAG\SystemPropertiesDataExecutionPrevention.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	83968
Entropy (8bit):	7.070618238949574
Encrypted:	false
SSDEEP:	1536:9ulZctREC/rMcgEPJV+G57ThjEC0kzJP+V5Jk:KczECTMpuDhjRVJGe
MD5:	1A34577AEDE83993615D7F2E37024D4D
SHA1:	73B845775507B0754F55507DE8250025E17A353F
SHA-256:	B3E7E41DBFC4D7E91BA6C5AEB6FD2D4C7D1B05F93F24FD591FDA9B0342761FA2
SHA-512:	703085DED509130ECE0430A27840A6648807639FF2AE1B4519C07FD13A9990D3FFEDD9B5F69FB5265B7067EC5BCF6C8B256C0F6EDF58E54EC678CC5E0ECE925
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%...a..[a..[a..[h..[o..[..Z`..[..Zc..[..Zp..[a..[C..[..Zd..[..Z`..[..q[`..[..Z`..[Richa..[.....PE..d...76....."....>.....@.....a....`..... .....&.....P...'...@..... ...."..T..... .....!..8.....text..... ..`.rdata..F.... .....@..@.data.....0.....@....pdata.....@.....@..@.rsrc...'...P...(..... .....@..@.reloc.. .....F.....@..B.....

C:\Users\user\AppData\Local\KXZtu\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
Malicious:	**true**
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\KXZtu\dwmapi.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1253376

C:\Users\user\AppData\Local\KXZtu\dwmapi.dll	
Entropy (8bit):	5.459202568986086
Encrypted:	false
SSDEEP:	12288:NVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:UfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	8567748CEEF8C27F7F9D2CC01C7FF8D8
SHA1:	54E17D05356982196640F79E7CA4E52EA39810BA
SHA-256:	5B901C10F6E9BE30CCFE17A8B4E2E2441B8760FC2FFAB75E023B8F8B20F7541F
SHA-512:	2DE32997A489520D7653206526853EDAC727DA0FE178E21103B589BD1E7742868C48B20EE204B683F806D5E7D1CF852DECBC32D75C2B326D29106321E028D70A
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.& ..DN^....." .....p.....@..... .....@lx}..b.....&....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\NakOm\VERSION.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1253376
Entropy (8bit):	5.452577152333679
Encrypted:	false
SSDEEP:	12288:5VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:4fP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	D111BFD3EEFF105A44B0B0F29184BA99
SHA1:	6DE0946646FB368B151628F4C89D8D2F2710D5C1
SHA-256:	0D9841379883D8FC6AECC01FA209FC1DDDC5534F04BE2C8EAB84671C8193F62B
SHA-512:	8A1FAEF5D1801C15220D29D6386ECB3177203BC72A9395FCDCD666E72ACDD2B6F3429B4BF2ABD6153909E380D9F62AC831DCA79B61264998835C0097D3B0B5 D
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.& ..DN^....." .....p.....@..... .....@lx}..b.....+....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\NakOm\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
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\Uh9eo\BitLockerWizardElev.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	101888
Entropy (8bit):	6.95002760620154

C:\Users\user\AppData\Local\Uh9eo\BitLockerWizardElev.exe	
Encrypted:	false
SSDEEP:	3072:k8kEZwnVS570M9kdatGCO+xmBc+hMPhPsx:1khVs7nyatGt+SYF
MD5:	3104EA9ECCA9ED71A382CCAAD618CEAE
SHA1:	9277108B7254F0C5BD241C2643902378925A8F9C
SHA-256:	D8CB004D4E8894AB4CA769C3CEC9A37B7FAB336DCDA1E6E9A15975DC64CEF370
SHA-512:	27C84C35461E37557BA27A7D9E9F86A47686DE73DDC74E001777F11EA8D5BE9B17604403875CF20124595010477F6F2ADDD797B9ACED79C514AEF2D2F1A019B
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.`M.h3M.h3M.h3"Jm2O.h3"Jk2O.h3"Jl2_.h3"Ji2F.h3M.i3 }.h3"Ja2L.h3"J.3L.h3"Jj2L.h3RichM.h3.....PE..d....C....."..... @.....0.....`..... .....D,..x....`...c...P..... ..... ....(..T..... ..... !.....text..... ..`.rdata..... .....@..@.data.....@.....$.....@....pdata.....P.....&.... .....@..@.rsrc....c..`...d...(.....@..@.reloc.. .....@..B..... .....

C:\Users\user\AppData\Local\Uh9eo\FVEWIZ.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1253376
Entropy (8bit):	5.461597709510602
Encrypted:	false
SSDEEP:	12288:vVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:GfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	3C1D465503B713020F78BCAA49872555
SHA1:	4C71E3773BA876868E0B0E1A780B088CC30B1F85
SHA-256:	D92C2EE583FCF742E9AC95FBEC82A44E9A577F5DAAEDCB21BC8559BEF43ABF27
SHA-512:	9C29500CCF6E64EB0CFE084ED073979A74803D9B50CB62D1CC172DE436E2E73905607C77CFC9455623A71E10671D049BAF37DE22B2D1B2D73148BBA71599B82
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.& ..DN^....." .....p.....@..... .....@lx}..b.....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\UjbH0ZEv\SYSDM.CPL	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1253376
Entropy (8bit):	5.451844365185671
Encrypted:	false
SSDEEP:	12288:wVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:1fP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	BEF736598FD9DBF745B5463549E3BF27
SHA1:	7833E3221FDC65ED0DBA03C0934CE444DEBF0B4B
SHA-256:	AC621540B0F1E3F7EA98A020E97608E5E2B97C39C963F52CF6FF13EAF05CC4A3
SHA-512:	A520E95DB93716516AD3FEBF77E171B53623092408BC570D5C6DEC41DEEAE1D7CFDA92BFEC1F29E1037B985ECBB952E09167F1694B36B5D4A665801531E053B A
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.& ..DN^....." .....p.....@..... .....@lx}..b.....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\UjbH0ZEv\SystemPropertiesPerformance.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	83968
Entropy (8bit):	7.071848641739436
Encrypted:	false
SSDEEP:	1536:5MVEZnXtREC/rMcgEPJV+G57ThjEC0kzJP+V5J9:3XzECTMpuDhjRVJGf
MD5:	F325976CDC0F7E9C680B51B35D24D23A

C:\Users\user\AppData\Local\UjbH0ZEv\SystemPropertiesPerformance.exe	
SHA1:	8BA00280B451378802DD2A06BB139B8BEA78C90C
SHA-256:	E24A61B15FD191DDC8A2CA82E22A759609E6099A832ADE0B5C0C6E0F1ABB05FE
SHA-512:	9D65A154758B5C38C09AACA1BB51E53FE6E8DEA374EAD88AEA33AB41525B3BB180211D6F6C93CA112197F7455842228960699DF471F47EE83DBC6CA59A5166EC
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....E.v..c...c...c.....c..n....c..n....c..n....c..n....c...c..''c..n....c..n...c..n.. ..c..Rich.c.....PE..d...0.....".....>.....@.....s...`..... .....<&.....P..P'...@..... ....#..T..... .....!..H.....text..... ..`.rdata..... .....@..@.data.....0.....@....pdata.....@.....@..@.rsrc...P'...P...(..... .....@..@.reloc.. .....F.....@..B..... .....

C:\Users\user\AppData\Local\cZk0IMu\GamePanel.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1292288
Entropy (8bit):	6.159394598062476
Encrypted:	false
SSDEEP:	24576:tg6uRV8QrFa8Zdntp/LEz2INhgITVXTvlHQroF:tgJVbFaqtpDEznyQVjvZQroF
MD5:	4EF330EFAE954723B1F2800C15FDA7EB
SHA1:	3E152C0B10E107926D6A213C882C161D80B836C9
SHA-256:	0494166D4AE6BB7925E4F57BB6DFAC629C95AE9E03DFC925F8232893236BD982
SHA-512:	C122CD7A245EF6A6A7B7DECAB6500BDC11E4C57B8E35F8462CC0615E44E54071E6BF79B69BB8519470ACBAF0D2E62ABC45C38CBF0606261792EDB4A84790EC61
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....T.ur.`.!.`.!.`.!...!P`.!... .`.!... .`.!... 4`.!... 9`.!.`.!de.!... .`.!...!.`.!...!.`.!... .`.!Rich.`.!.....PE..d.....".....H.....0.....@.....@..... .....u.....`.....:..p...T.....@..(...pp... .....8@..H... ...@.....text....F.....H..... ..`.imrsiv.....`.....rdata.....p.....L.....@..@.data.....@....pdata..`.....~..... .....@..@.didat.....p.....@....rsrc....u.....v.....@..@.reloc...:.....<...|.....@..B..... .....

C:\Users\user\AppData\Local\cZk0IMu\dwmapi.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1253376
Entropy (8bit):	5.459256653240629
Encrypted:	false
SSDEEP:	12288:GVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:bfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	1B6EF09343061B200F166C0058B23AE5
SHA1:	1116742823038C9EDC5E29E5E12496C174A79F7A
SHA-256:	28F70C785ACFDF24D35ECA3849A3060A170A3B2B3ECE5D12F31C4B331EA7F145
SHA-512:	9A8B33D74DA4937344BD1DC693E779A559A5D2E6D5F93D37CFEDD0B61C59DCFFF708CF7616D873FA6F73A6DF76A6F7558DCD342497A256770780CBB42B1A4FE
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....|...|...|....K.#}...'...}.....{}....X.#}....f..|....g..}..*...a|.....}....N..}..*... E}..[.I.E|...'..U}....N.+}..[.K.P|..[.K./}...I.h}..u.Y.k|.....|..W"...|..b.L.t|...|...}.....N|..2%...|..Rich.|.....PE..d.& ..DN^.....".....p.....@..... .....@Ix}..b.....&.....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\mFxP\XmlLite.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1253376
Entropy (8bit):	5.451309586899805
Encrypted:	false
SSDEEP:	12288:GVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:bfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	3094332DF5A7FD0DC27350FA12555706
SHA1:	2130132D8DF6A2542B177CE2606160C393BD589F
SHA-256:	9108849AF9ADEDABFF5D60B3612711290F0F06CB2088A3D4F1D03D2408C2C168
SHA-512:	7CED590EF762A332FBB1536833DEADCF50ADD35E309D1DE5692FA1AED1E5F320CA32615BFD00E95E433550B45DB1DBBF113ED844CBEEE098014BCB6C9698340

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

C:\Users\user\AppData\Local\mFxP\upfc.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	110632
Entropy (8bit):	6.598198265862064
Encrypted:	false
SSDEEP:	1536:IJY1Xjv7mjVN0OpMSzkqkWHL9yBpDdv7M8T84Rrrjbk9RP+S+sjT6NfPN:IJYtmj6C7HRM9S0trvkPHDjT6NfV
MD5:	4CEED46DDAB911AE1298422BFB12460C
SHA1:	2A3BFED90C680FC78E229091B6786AAF9655AA6B
SHA-256:	1A20F7A7BBAF5B7D4435471A2CF3EC96787B068F1A63CAA5DEDC52B8FAAA60C8
SHA-512:	AD49E1E2D5B0A21AD6F4B1A421659E5B743DF44F1272F5757C3772A9A5F7257C5938C864518F6A72BAE80E5CBE489544F9F4C4067A597CE8EFE67E2357C3B6B4
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s....Z...Z...Z..Z..Z...Z...Z...[...Z...[...Z...[...Z...[...Z...Z...Z...Z...Z...[...ZRich...Z.....PE..d...X%@\....."..... .....P.....@.....`..... .....Hw.....H.....(&.....T....b..T.....#... .....$.....text..... ..`.rdata...k... ...l.....@..@.data...h.....t.....@....pdata..H.....x.....@..@.rsrc..... .....@..@.reloc..T.....@..B..... .....

C:\Users\user\AppData\Local\mlAKVTuFf\DUser.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1257472
Entropy (8bit):	5.458454067792567
Encrypted:	false
SSDEEP:	12288:iVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1+:/fP7fWsK5z9A+WGAW+V5SB6Ct4bnb+
MD5:	B02754D536507A54F3A3F136B7BE88FF
SHA1:	6E6497990A24673082451ADF644B862782593C57
SHA-256:	7F655543CD3FC9BD30CBF0FE12299A34DF1E676657B57787DEE156BC1DF576AA
SHA-512:	B7739F0FDD505C97F523A870744194947E33344F2D5EB8E381EE9D93DB0E97FE98C75245C239A85B3F815870A83BA1B9C3E26D970E1E73B5F5CD9D9FB897FA0
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\mlAKVTuFf\bdeunlock.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	286232
Entropy (8bit):	6.926729215014979
Encrypted:	false
SSDEEP:	6144:jjJkzmZ4CSal+EH+pDQh01TXRYJWEmTKBKt1Vs7nyatGt+SYFmW2kb/:jtgmSdal+EH+5QhWEmTKB2H+S+7b/
MD5:	FAB70105E2075EEC9C249A4D499CAE7C
SHA1:	B5B4216725F55A4E6AF9FB0BB7E0167CEED6081F
SHA-256:	7EA89BE1BBA6A7C2B08D70FA8E4CF036CB086ED162BCD22255E2BC0F926B22B2
SHA-512:	96327DEC3BCEE7A9934AAF27F1942030D46CEE693AF2562EE4972D5306DD3AD14F404762B99E581C0F0F563610EA097372044890EB19CE1C7A8F535A78D9E19A
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\mIAKVTuFf\bdeunlock.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....:..A~.~.~.~.~.~.w...v.~...}.}.~...z.l.~...{.x.~.....g.~.~.....~...w.i.~. ..~...~.....~...|...~.Rich~.~.....PE..d....X.....".....D.....pJ.....@.....i..... .....P.....T.....x.....2...,.....t.... ...T.....t.....u.....text...PB.....D..... ..`.imrsiv.....`.....rdata...c...p...d...H.....@..@.data.....@.... pdata.....@..@.rsrc....x.....z.....@..@.reloc..t.....0.....@..B..... .....

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\21c8026919fd094ab07ec3c180a9f210_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	4457
Entropy (8bit):	5.473312982000721
Encrypted:	false
SSDEEP:	96:xCOIz7wXyo8LqnOwzUbBCOIzO/Xj/w6OTmcLPxXS:0OIBgzwEOIEkRLRS
MD5:	2353DF7BE15A7D7836D6888AA678A989
SHA1:	A71A7834F1BA6097698B00A2657008E5ACE3C83B
SHA-256:	2BBF137AC5EB8418152EDE398C09325FA06065E92B4E1DB92B11D3A596159338
SHA-512:	EAC02C23E43916857946888DBA8EDEEC70D14447272272A0CDC831CD01D97015D502BE2D711A12751DB460B1F91E896900A28F8AE0A0B14844EBC9A4F9B2DB
Malicious:	false
Reputation:	unknown
Preview:	.....user.....user.....RSA1.....l..'.ZN.....9q8.w.Bo.....k.[..#.4..JZ...pJ.+..{{.v..T..^..?"...!.#.....M.`.VZ.?|...qn.I.. ..B....8_3)S...L....A.{..k.1.xW.....z..O.....C..J.QD.1.....,...C.r.y.p.t.o.A.P.I. .P.r.i.v.a.t.e. .K.e.y....f..... ...>M.K.(...\...p.hh].xC.....zrjg..... .....a.,d.s.|_Y.).c..{.. ....C..c.....P.....r..T\~.1# h.<Fg.v..t....].Vw...P.L`h..M..w.....w9.l..i.QU/...p.o....>.[..e...F.K=._-.....*..o9]..v'S%j6.&'..6..t.....y....xi..j.7g.E%.....f.Zem..{``(."..'...~.U..V)...R..U l.*n..hV.....f..5...L.f.....F.B. ..X.....R..B...Q.h`...d.+..../.>|.Qw.....Hd>.....r..A.d.....R..7...G..v.....(.....K.p.h....."0;e.0K.L.&~C..E.0a....._.d|.l.K.L..*...6..",.Bv*kk.5.c&j]U.s.U.n_.q.|G.-.W.Y_.....).....|.1...'....x..."...YtO*C=6.....I2r.@.B.^.3..1.G.Vd.._".Zv.Q...b"~..&QSc.z dA..

Static File Info

General

File type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Entropy (8bit):	5.487493969044098
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:	Y7KrNvSxWx.dll
File size:	1249280
MD5:	ecdfff8b0ece2175cd699e690de1fcaf
SHA1:	9359770d71e743832ca22597db917dfa817038b2
SHA256:	dc684f824a7deaf6028f6266b48cc3f982a4931ce2db003f692a448da8e255e3
SHA512:	106ecdecdc64b395ae74fd231dc858f0c18a75baba52729ec928451884462d7f5e828f20dd0de3fc750c817d96461708030679873d7a675327b35f51bb8fcc3d
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
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	0x64fcb	0x65000	False	0.702262047494	data	7.86510283498	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
.wnx	0x10e000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.weqy	0x10f000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.yby	0x110000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ormx	0x112000	0xbde	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
.dhclu	0x113000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.xmiul	0x114000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tlwcxe	0x115000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.get	0x116000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.hzrd	0x117000	0x1124	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.gulz	0x119000	0x1124	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ybavfq	0x11b000	0x1af	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.hzccq	0x11c000	0x1e66	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.kmnqh	0x11e000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.sqadf	0x11f000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.uans	0x120000	0x1f2a	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.gelkgq	0x122000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.jbviw	0x123000	0x21b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ypg	0x124000	0x2da	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.qqs	0x125000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.dsy	0x126000	0x2a2	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.fgy	0x127000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.onfp	0x128000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.clcj	0x129000	0x128f	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.fhc	0x12b000	0x3fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ghxb	0x12c000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.icyh	0x12d000	0x1f2a	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.wguyua	0x12f000	0x1278	0x2000	False	0.28125	data	3.91163132638	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: 2288 Parent PID: 6428

General

Start time:	20:05:54
Start date:	28/09/2021
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe 'C:\Users\user\Desktop\Y7KrNvSxWx.dll'
Imagebase:	0x7ff764910000
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: 00000000.00000002.377190564.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 2468 Parent PID: 2288

General

Start time:	20:05:55
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\Y7KrNvSxWx.dll',#1
Imagebase:	0x7ff7180e0000
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: 6724 Parent PID: 2288

General

Start time:	20:05:55
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\Y7KrNvSxWx.dll,CloseDriver
Imagebase:	0x7ff79a230000
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: 00000002.00000002.456385826.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 6964 Parent PID: 2468

General

Start time:	20:05:55
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe 'C:\Users\user\Desktop\Y7KrNvSxWx.dll',#1
Imagebase:	0x7ff79a230000
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: 00000003.00000002.355433336.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3440 Parent PID: 6724

General

Start time:	20:05:57
Start date:	28/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f22f0000
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: 6676 Parent PID: 2288

General

Start time:	20:05:59
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\Y7KrNvSxWx.dll,DefDriverProc
Imagebase:	0x7ff79a230000
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: 00000006.00000002.363238472.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 2904 Parent PID: 2288

General

Start time:	20:06:02
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\Y7KrNvSxWx.dll,DriverCallback
Imagebase:	0x7ff79a230000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000007.00000002.370198156.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: SndVol.exe PID: 2176 Parent PID: 3440

General

Start time:	20:06:46
Start date:	28/09/2021
Path:	C:\Windows\System32\SndVol.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SndVol.exe
Imagebase:	0x7ff7da4c0000
File size:	259904 bytes
MD5 hash:	CDD7C7DF2D0859AC3F4088423D11BD08
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: SndVol.exe PID: 2444 Parent PID: 3440

General

Start time:	20:06:48
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\KXZtu\SndVol.exe
Wow64 process (32bit):	false

Commandline:	C:\Users\user\AppData\Local\KXZtu\SndVol.exe
Imagebase:	0x7ff6249b0000
File size:	259904 bytes
MD5 hash:	CDD7C7DF2D0859AC3F4088423D11BD08
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000011.00000002.488077444.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities Show Windows behavior

File Read

Analysis Process: bdeunlock.exe PID: 6612 Parent PID: 3440

General

Start time:	20:06:59
Start date:	28/09/2021
Path:	C:\Windows\System32\bdeunlock.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\bdeunlock.exe
Imagebase:	0x7ff7fd2d0000
File size:	286232 bytes
MD5 hash:	FAB70105E2075EEC9C249A4D499CAE7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: bdeunlock.exe PID: 6604 Parent PID: 3440

General

Start time:	20:07:00
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\mlAKVTuFf\bdeunlock.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\mlAKVTuFf\bdeunlock.exe
Imagebase:	0x7ff68d870000
File size:	286232 bytes
MD5 hash:	FAB70105E2075EEC9C249A4D499CAE7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000014.00000002.514246640.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities Show Windows behavior

File Read

Analysis Process: SystemPropertiesPerformance.exe PID: 5548 Parent PID: 3440

General

Start time:	20:07:12
Start date:	28/09/2021
Path:	C:\Windows\System32\SystemPropertiesPerformance.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SystemPropertiesPerformance.exe
Imagebase:	0x7ff6c5320000
File size:	83968 bytes
MD5 hash:	F325976CDC0F7E9C680B51B35D24D23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: SystemPropertiesPerformance.exe PID: 5532 Parent PID: 3440

General

Start time:	20:07:13
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\UjbH0ZEv\SystemPropertiesPerformance.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\UjbH0ZEv\SystemPropertiesPerformance.exe
Imagebase:	0x7ff6a7b90000
File size:	83968 bytes
MD5 hash:	F325976CDC0F7E9C680B51B35D24D23A
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: 00000019.00000002.545893721.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Read

Analysis Process: GamePanel.exe PID: 5824 Parent PID: 3440

General

Start time:	20:07:26
Start date:	28/09/2021
Path:	C:\Windows\System32\GamePanel.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\GamePanel.exe
Imagebase:	0x7ff7c2e80000
File size:	1292288 bytes
MD5 hash:	4EF330EFAE954723B1F2800C15FDA7EB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: GamePanel.exe PID: 6444 Parent PID: 3440

General

Start time:	20:07:26
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\cZk0IMu\GamePanel.exe

Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\cZk0IMu\GamePanel.exe
Imagebase:	0x7ff71bac0000
File size:	1292288 bytes
MD5 hash:	4EF330EFAE954723B1F2800C15FDA7EB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000001E.00000002.571934505.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Read

Analysis Process: tcmsetup.exe PID: 3324 Parent PID: 3440

General

Start time:	20:07:39
Start date:	28/09/2021
Path:	C:\Windows\System32\tcmsetup.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\tcmsetup.exe
Imagebase:	0x7ff7d6bb0000
File size:	16384 bytes
MD5 hash:	0DDA495155D552D024593C4B3246C8FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: tcmsetup.exe PID: 1916 Parent PID: 3440

General

Start time:	20:07:39
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\2oEy\tcmsetup.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\2oEy\tcmsetup.exe
Imagebase:	0x7ff6e3310000
File size:	16384 bytes
MD5 hash:	0DDA495155D552D024593C4B3246C8FA
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: 00000021.00000002.598954103.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Virustotal, Browse • Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: wscript.exe PID: 2584 Parent PID: 3440

General

Start time:	20:07:51

Start date:	28/09/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wscript.exe
Imagebase:	0x7ff7639c0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: wscript.exe PID: 4312 Parent PID: 3440

General

Start time:	20:07:52
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\NakOm\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\NakOm\wscript.exe
Imagebase:	0x7ff68af10000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000024.00000002.625281639.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: BitLockerWizardElev.exe PID: 4640 Parent PID: 3440

General

Start time:	20:08:05
Start date:	28/09/2021
Path:	C:\Windows\System32\BitLockerWizardElev.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\BitLockerWizardElev.exe
Imagebase:	0x7ff6283d0000
File size:	101888 bytes
MD5 hash:	3104EA9ECCA9ED71A382CCAAD618CEAE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: BitLockerWizardElev.exe PID: 1636 Parent PID: 3440

General

Start time:	20:08:05
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\Uh9eo\BitLockerWizardElev.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Uh9eo\BitLockerWizardElev.exe
Imagebase:	0x7ff6173e0000
File size:	101888 bytes
MD5 hash:	3104EA9ECCA9ED71A382CCAAD618CEAE
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000026.00000002.654598508.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: upfc.exe PID: 5152 Parent PID: 3440

General

Start time:	20:08:17
Start date:	28/09/2021
Path:	C:\Windows\System32\upfc.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\upfc.exe
Imagebase:	0x7ff629050000
File size:	110632 bytes
MD5 hash:	4CEED46DDAB911AE1298422BFB12460C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: upfc.exe PID: 5816 Parent PID: 3440

General

Start time:	20:08:18
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\mFxP\upfc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\mFxP\upfc.exe
Imagebase:	0x7ff7299b0000
File size:	110632 bytes
MD5 hash:	4CEED46DDAB911AE1298422BFB12460C
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: 00000028.00000002.681547027.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: SystemPropertiesDataExecutionPrevention.exe PID: 6060 Parent PID: 3440

General

Start time:	20:08:30
Start date:	28/09/2021
Path:	C:\Windows\System32\SystemPropertiesDataExecutionPrevention.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SystemPropertiesDataExecutionPrevention.exe
Imagebase:	0x7ff7aec30000
File size:	83968 bytes
MD5 hash:	1A34577AEDE83993615D7F2E37024D4D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis