ID: 492431
Sample Name: P7n0h6OhYp
Cookbook: default.jbs
Time: 17:44:10
Date: 28/09/2021
Version: 33.0.0 White Diamond

Table of Contents

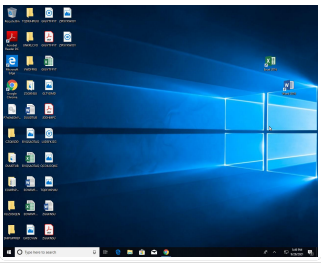
Windows Analysis Report P7n0h6OhYp

Overview

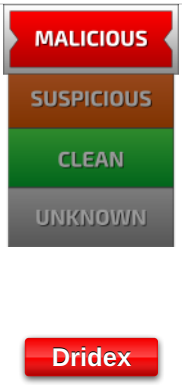
General Information

Sample Name:	P7n0h6OhYp (renamed file extension from none to dll)
Analysis ID:	492431
MD5:	718a7d9b1fe55a7.
SHA1:	5d870aeb7951ab..
SHA256:	d485423afb5929d.
Tags:	Dridex exe
Infos:	

Most interesting Screenshot:



Detection

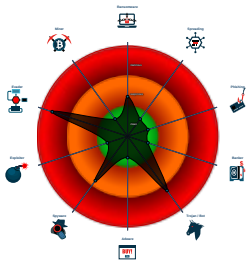


Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected Dridex unpacked file
- Multi AV Scanner detection for subm…
- Benign windows process drops PE f…
- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Changes memory attributes in foreig…
- Queues an APC in another process …
- Uses Atom Bombing / ProGate to in…
- Queries the volume information (nam…
- Contains functionality to check if a d…
- Contains functionality to query locale…
- May sleep (evasive loops) to hinder …
- Contains functionality to shutdown / …
- Uses code obfuscation techniques (…
- PE file contains sections with non-s…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 5036 cmdline: loaddll64.exe 'C:\Users\user\Desktop\P7n0h6OhYp.dll' MD5: E0CC9D126C39A9D2FA1CAD5027EBBD18)
  - cmd.exe (PID: 644 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\P7n0h6OhYp.dll',#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 5044 cmdline: rundll32.exe 'C:\Users\user\Desktop\P7n0h6OhYp.dll',#1 MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 3240 cmdline: rundll32.exe C:\Users\user\Desktop\P7n0h6OhYp.dll,IsInteractiveUserSession MD5: 73C519F050C20580F8A62C849D49215A)
    - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - RdpSa.exe (PID: 716 cmdline: C:\Windows\system32\RdpSa.exe MD5: 0795B6F790F8E52D55F39E593E9C5BBA)
      - RdpSa.exe (PID: 2564 cmdline: C:\Users\user\AppData\Local\1wgM9CYx\RdpSa.exe MD5: 0795B6F790F8E52D55F39E593E9C5BBA)
      - dxgiadaptercache.exe (PID: 6132 cmdline: C:\Windows\system32\dxgiadaptercache.exe MD5: 3E73262483D4FB1BB88BA1B2B9BB3D5A)
      - dxgiadaptercache.exe (PID: 1308 cmdline: C:\Users\user\AppData\Local\aDD0Ov\dxgiadaptercache.exe MD5: 3E73262483D4FB1BB88BA1B2B9BB3D5A)
      - GamePanel.exe (PID: 668 cmdline: C:\Windows\system32\GamePanel.exe MD5: 4EF330EFAE954723B1F2800C15FDA7EB)
      - GamePanel.exe (PID: 4140 cmdline: C:\Users\user\AppData\Local\Rn1XW4tG\GamePanel.exe MD5: 4EF330EFAE954723B1F2800C15FDA7EB)
      - SystemSettingsRemoveDevice.exe (PID: 1036 cmdline: C:\Windows\system32\SystemSettingsRemoveDevice.exe MD5: 87AF711D6518C0CF91560D7C98301BBB)
      - SystemSettingsRemoveDevice.exe (PID: 5192 cmdline: C:\Users\user\AppData\Local\tiy3x\SystemSettingsRemoveDevice.exe MD5: 87AF711D6518C0CF91560D7C98301BBB)
      - lpksetup.exe (PID: 4976 cmdline: C:\Windows\system32\lpksetup.exe MD5: 8E2C63E761A22724382338F349C55014)
      - lpksetup.exe (PID: 4968 cmdline: C:\Users\user\AppData\Local\A7mgbJ\lpksetup.exe MD5: 8E2C63E761A22724382338F349C55014)
      - Narrator.exe (PID: 5480 cmdline: C:\Windows\system32\Narrator.exe MD5: 56036993FB96C42F30C443A11BD56F4D)
      - Narrator.exe (PID: 5616 cmdline: C:\Users\user\AppData\Local\ocY6\Narrator.exe MD5: 56036993FB96C42F30C443A11BD56F4D)
      - WindowsActionDialog.exe (PID: 5040 cmdline: C:\Windows\system32\WindowsActionDialog.exe MD5: 991359EE1E9C1958EB5D0F7314774123)
      - WindowsActionDialog.exe (PID: 1280 cmdline: C:\Users\user\AppData\Local\JrFH9qPBX\WindowsActionDialog.exe MD5: 991359EE1E9C1958EB5D0F7314774123)
      - sessionmsg.exe (PID: 1112 cmdline: C:\Windows\system32\sessionmsg.exe MD5: 1F7CEA0216DE48B877C16F95C7DA1F0F)
      - sessionmsg.exe (PID: 1268 cmdline: C:\Users\user\AppData\Local\NNw\sessionmsg.exe MD5: 1F7CEA0216DE48B877C16F95C7DA1F0F)
  - rundll32.exe (PID: 5816 cmdline: rundll32.exe C:\Users\user\Desktop\P7n0h6OhYp.dll,QueryActiveSession MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 4632 cmdline: rundll32.exe C:\Users\user\Desktop\P7n0h6OhYp.dll,QueryUserToken MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000018.00000002.383288122.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
0000001A.00000002.410742595.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000004.00000002.324777282.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000027.00000002.514121758.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000029.00000002.543009513.0000000140001000.00000020.00020000.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

E-Banking Fraud:

Yara detected Dridex unpacked file

HIPS / PFW / Operating System Protection Evasion:

Benign windows process drops PE files

Changes memory attributes in foreign processes to executable or writable

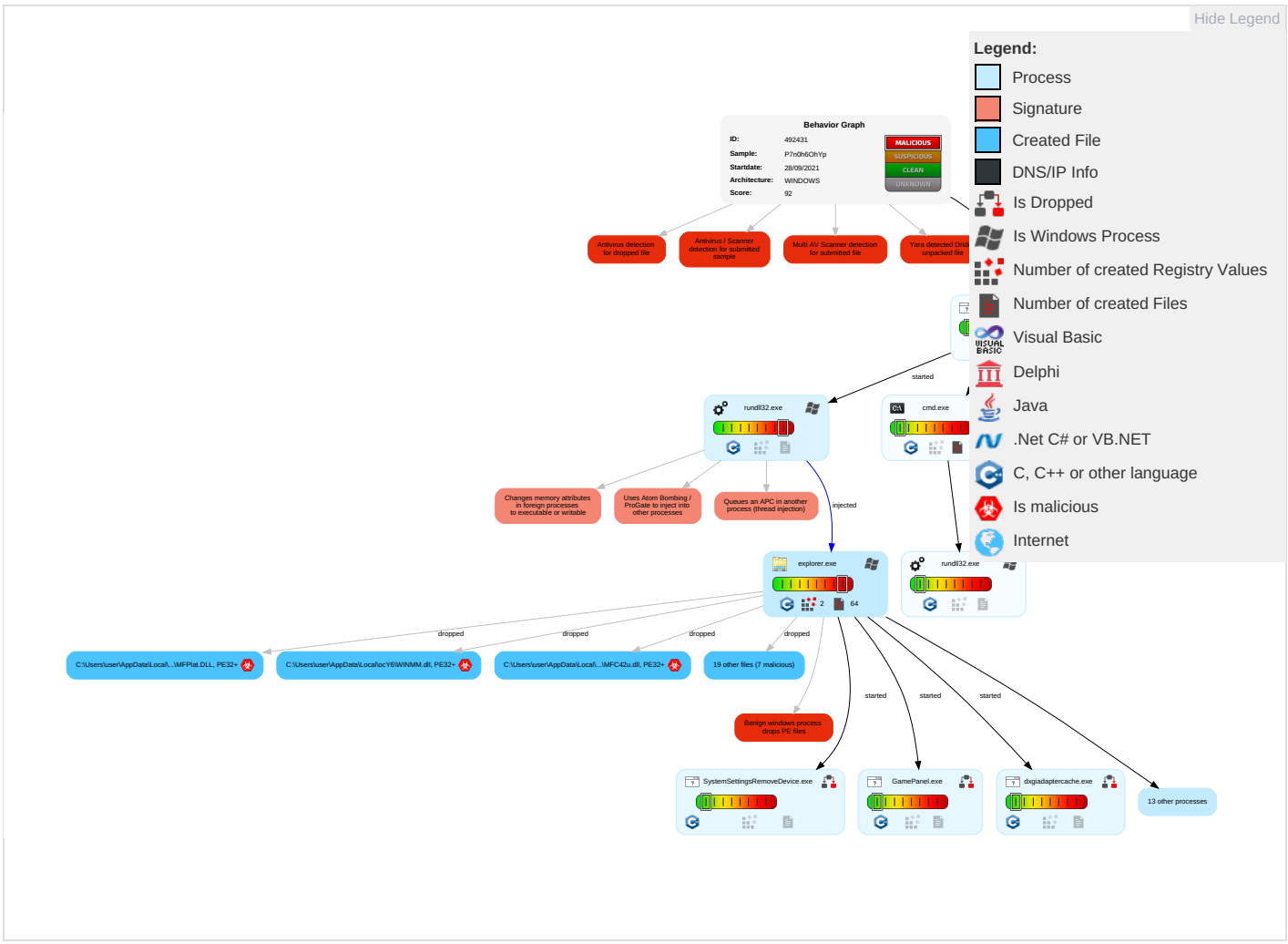
Queues an APC in another process (thread injection)

Uses Atom Bombing / ProGate to inject into other processes

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Valid Accounts	Native API 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	Input Capture 3 1	System Time Discovery 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encryp Chann
Default Accounts	Exploitation for Client Execution 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Screen Capture 1	Exfiltration Over Bluetooth	Junk D
Domain Accounts	Command and Scripting Interpreter 2	Logon Script (Windows)	Access Token Manipulation 1	Obfuscated Files or Information 3	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Input Capture 3 1	Automated Exfiltration	Stegar
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 3 1 2	Software Packing 2	NTDS	System Information Discovery 3 6	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protoc Impers
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Security Software Discovery 4 1	SSH	Keylogging	Data Transfer Size Limits	Fallba Chann
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiba Comm
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1 1	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applica Layer
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Access Token Manipulation 1	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web P
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 3 1 2	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tr Protoc
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Rundll32 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Pr

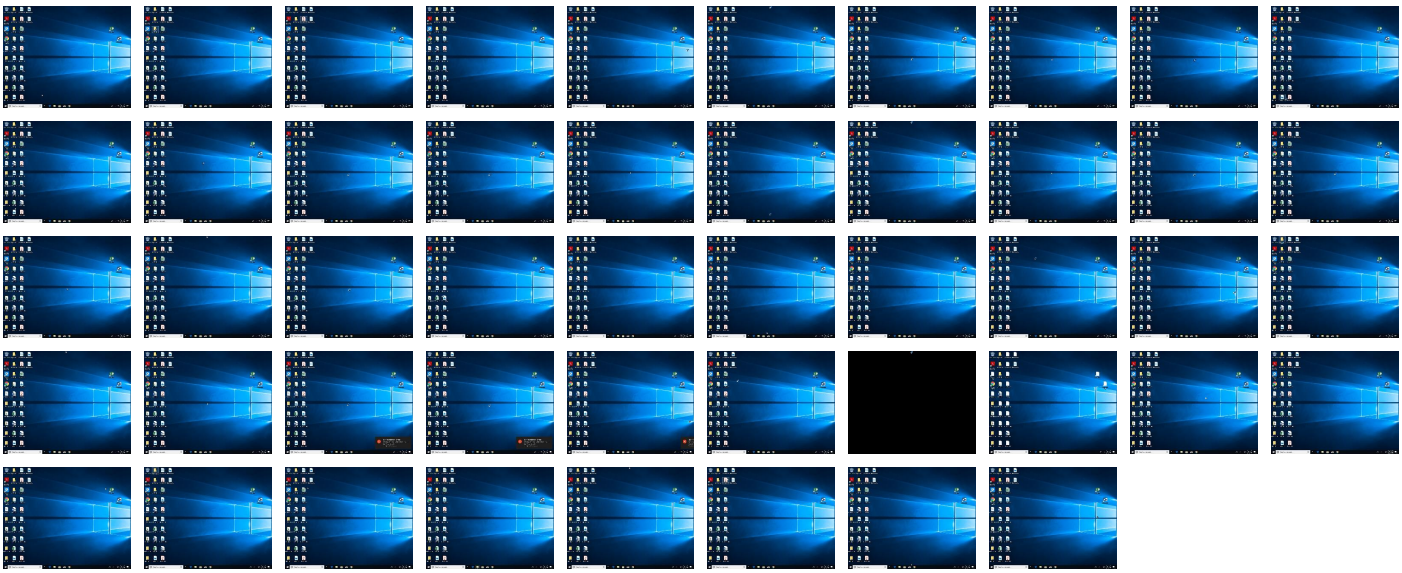
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
P7n0h6OhYp.dll	66%	Virustotal		Browse
P7n0h6OhYp.dll	60%	Metadefender		Browse
P7n0h6OhYp.dll	76%	ReversingLabs	Win64.Infostealer.Dridex	
P7n0h6OhYp.dll	100%	Avira	TR/Crypt.ZPACK.Gen	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\1wgM9CYx\WINSTA.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\NNw\DUser.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\ocY6\WINMM.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\Rn1XW4tG\UxTheme.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\aDD0Ov\dxgi.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\4PmTNr\SYSDM.CPL	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\j3KBEEMS\MFC42u.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\A7mgbJ\dpx.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\JrFH9qPBX\DUI70.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\JrFH9qPBX\DUI70.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\pEPyA\MFPlat.DLL	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\1wgM9CYx\RdpSa.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\1wgM9CYx\RdpSa.exe	0%	ReversingLabs		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\4PmTNr\SystemPropertiesComputerName.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\4PmTNr\SystemPropertiesComputerName.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\A7mgbJ\lpksetup.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\A7mgbJ\lpksetup.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
30.2.SystemSettingsRemoveDevice.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
41.2.sessionmsg.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.2.dxgiadaptercache.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
39.2.WindowsActionDialog.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
10.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
34.2.lpksetup.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.2.RdpSa.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
26.2.GamePanel.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.2.loaddll64.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://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:	492431
Start date:	28.09.2021
Start time:	17:44:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 16m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	P7n0h6OhYp (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:	mal92.troj.evad.winDLL@49/23@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 17.1% (good quality ratio 11.4%) • Quality average: 55.1% • Quality standard deviation: 44.7%
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\1wgM9CYx\RdpSa.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows

C:\Users\user\AppData\Local\1wgM9CYx\RdpSa.exe	
Category:	dropped
Size (bytes):	43008
Entropy (8bit):	5.898730459072675
Encrypted:	false
SSDEEP:	768:2nweYBCOBU+khtTMstnGUEqbfynaDWVVVFZ5i7t4AYRyF:TiaU+1qDya6VV7Z5SudyF
MD5:	0795B6F790F8E52D55F39E593E9C5BBA
SHA1:	6A9991A1762AAC176E3F47AB210CC121E038E4F9
SHA-256:	DF5B698983C3F08265F2FB0B74046CD7E68568190F329C8331CCA4761256D33B
SHA-512:	72D332EBDD1B9B40E18F565DACC200E5B710A91D803D536A0CF127C74622EED12A5EC855B9040F4A1FA8A44584E4E97E7E6C490B88DB3BDAFE61EA3FBF26AB59
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....$.....-.G.i.).i.).i.).`..o.)...*.k.)...-.}.)....,}.)...(.|.).i.(..)... .}.).....h.)...+.h.).Richi.)..... PE..d..... "..... j...@..... q..... @..... |..... `..... ..... <..... @...T..... @..... .....@..... text....h..... j..... ..`.rdata..n'..... (...n..... @..@.data..... @....pdata..<..... @..@.rsrc..... .....@..@.reloc..... @..B.....

C:\Users\user\AppData\Local\1wgM9CYx\WINSTA.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1228800
Entropy (8bit):	5.569298691821607
Encrypted:	false
SSDEEP:	12288:ZVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:YfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	9446475335E74BA8A8FBB0863D2FA19E
SHA1:	EECFA79E25A906C917F69F7AD13A9BAB343D3324
SHA-256:	7D42C3126F5D68841B75860988EED65ED25C60B0BF8C440DF69D1989F2237DDA
SHA-512:	2EFE24102003E7EFE2C09C3113AADFDEA7F46A9A9F1FED4A843C5C7B7B18D7A88E7B4283246F1E0B1447C5D842FCF40C3B03483A2168038EF77396B0AD9AE5AB
Malicious:	**true**
Antivirus:	• Antivirus: Avira, 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..... m....c..... h..... $#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,..... A..@.rsrc..... @..@.reloc..$#.......0..... @..B.qkm....J....@..... @..... @..@.cvjb...f...

C:\Users\user\AppData\Local\4PmTNr\SYSDM.CPL	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1224704
Entropy (8bit):	5.550400298505411
Encrypted:	false
SSDEEP:	12288:OVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:TfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	D2C51612B8B57401F713D8F071BFF4A8
SHA1:	469C602B01FC845F75925383CA82C47572C11E33
SHA-256:	6BE3E11BD01ED11EA0E16FF7236148E9121CD9FA5443617ECD3A4051B4587EB2
SHA-512:	77C3BEE1D42A55D5AED6DCCCDD1ECEB423603E38F40768E7CB19BB62E3A20EFBC05E13C585794A9B426394E0219BBC1D38CEB5266168D20BD963793D12B62F9
Malicious:	**true**
Antivirus:	• Antivirus: Avira, 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\4PmTNr\SystemPropertiesComputerName.exe	
Process:	C:\Windows\explorer.exe

C:\Users\user\AppData\Local\4PmTNr\SystemPropertiesComputerName.exe	
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	83968
Entropy (8bit):	7.0666667890606005
Encrypted:	false
SSDEEP:	1536:/pmuZctREC/rMcgEPJV+G57ThjEC0kzJP+V5Jp:xHczECTMpuDhjRVJGr
MD5:	BEE134E1F23AFD3AE58191D265BB9070
SHA1:	52178976E1B4405157042CD3A095BE6D7975609A
SHA-256:	7F258CE17EA09F076A767A2D3CC0A06F3AEF07169BFD6A16265B8958758FD799
SHA-512:	AEDFF7C45288A1CF69616B9887FC091F0913BEFA0EA7642C6A18DB50E4D6369CDC73730B8E6BE4FEDB4EB5EC28729AED39845B2E6F0C0685EBFF60106B54C1A9
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....$.....%...a..[a..[a..[h..[o..[..Z`..[..Zc..[..Zp..[a..[C..[..Zd..[..Z`..[..q[`..[..Z`..[Richa..[.....PE..d....F$.....".....>.....@.....`..... .....&.....P..H'...@..... ...".T..... .....!..8.....text..... ..`.rdata..N.... .....@..@.data.....0.....@....pdata.....@.....@..@.rsrc...H'...P...(..... .....@..@.reloc.. .....F.....@..B..... .....

C:\Users\user\AppData\Local\A7mgbJ\dpx.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1224704
Entropy (8bit):	5.5489777308997486
Encrypted:	false
SSDEEP:	12288:wVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:1fP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	1FC2D12E05D6165CF883A06F0773D56C
SHA1:	C8D122CEC8C54514279E5784F8F118AC71143F1F
SHA-256:	501457FF96C202C5D2DCD3B17AD157821A890B1922A51457FB4B5898A22D0A7D
SHA-512:	82590111BC62F9D941EB2D18ACAD42B5C9AEF1FCE760E59B36339BCB7BA9E5A76F49BB09B9AEA16D174D6ECB9C091E40DD4BE5927C147B2513A04C5A0150ED5A
Malicious:	**true**
Antivirus:	• Antivirus: Avira, 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\A7mgbJ\lpksetup.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	732160
Entropy (8bit):	6.573630291630044
Encrypted:	false
SSDEEP:	12288:U4O7JpqBbsczjBmavlNRO5Gy1ay0OBegtkGyLY9d/Dz/sJ+lGDyYgWPL/kc7yfnQ:U40JpqtZzjBRvI5Gdy0OjtwLY9BDz/PW
MD5:	8E2C63E761A22724382338F349C55014
SHA1:	30C7F92A6E88C368B091E39665545EAFA8A6561F
SHA-256:	4CA6E16BEB57278E60E3EDCBCECDA1442AA344C424421E4B078F1213E6B99376
SHA-512:	92F289DDBD9D1E5103C36308DA84779708A292DC54F49A0A1B79D65C563378BBF08C98F3732F25365CCF8175589D8E6187CEE2A694AE5FB73CA9E85AECFF4CF
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....W..6...e...e...e..%e3..e|.d...e|.d...e|.d...e|.d...e...ec..e|.d6..e|.le. ..e|.d...eRich...e.....PE..d.....e....."....,..P.....@.....`..... .....H?.....g..T.....y.. (....x.....y..P.....text....+..... ..`.rdata..\....@.....0.....@..@.data...`[...0.....@....pdata..H?.....@.....@..@.rsrc..... .....^.....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\JrFH9qPBX\DUI70.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1507328
Entropy (8bit):	5.9083215743400475
Encrypted:	false
SSDEEP:	12288:+VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1D:jfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	1F157DCF2EA98E51B56AA2BDAC6965F1
SHA1:	0A5B46F1186CB468E4D4170131D81ACD53780DE8
SHA-256:	EEEAE364DE658FBB44E163EE517DDD26113AE82209537985019508F27BB56839
SHA-512:	C05CD804C03C5A6DD90D48DCB622519476A7DCAB76CB16C3156A911C912D2AD58F057C9E95471D2DD7BF6180F4ACCFA3562A5AD006971BE3A460E3867FFD2E
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.#..DN^....." .....p.....@.....@lx}..b.....dQ...c.....h.....$#..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\JrFH9qPBX\WindowsActionDialog.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	59392
Entropy (8bit):	5.897489723280295
Encrypted:	false
SSDEEP:	1536:VgSmVr7b1rKOX4TfOwQaq1WWhrIWSNJy8e:eZVrAThqLfSNwV
MD5:	991359EE1E9C1958EB5D0F7314774123
SHA1:	6456AEA32407B0AEEDD347AFAE5BB12BAB781863
SHA-256:	9F8E465348DBB165B7B0E6A72FCC78D2CE79FB897B1514490CD0DDAB021EA500
SHA-512:	EE6D10A0B75829AAAB55CB9F9EDA967D763F7CACD09F944A9C40B8E5ADDD6BBB6970F069FC64FA1807B547134B3558667A680174AB0366D11A068C6DD70BC3F3
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... .%.A.v.A.v.A.v.9Wv.A.v.%.w.A.v.%.w.A.v.%.w.A.v.%.w.A.v.A.v.A.v.%.w.A.v.%;v.A.v.%.w.A.vRich.A.v.....PE..d....i....."..... .j.....@.....@.....'..... .....h.... .....0.....p...T.....H.....text..... ..`.imrsiv.....rdata...H.....J.....@..@.data.....@....pdata.....@..@.rsrc..... .....@..@.reloc.....0.....@..B.....

C:\Users\user\AppData\Local\NNw\DUser.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1228800
Entropy (8bit):	5.556665134508183
Encrypted:	false
SSDEEP:	12288:KVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:XfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	8BE2E7C88B219670F9D927F52CBF64AB
SHA1:	FD54D3C22B126F4D05FA1C8C86553BF7F578211E
SHA-256:	53D9DF119574CA82FAB8D369AE5FFFB51E359963D19443B4789FC8AB0F7A1229
SHA-512:	64349D7B8524EC1BD86699AA98D669F9450BC8461D9A2B46A26423E7B519E66BD5E96AD15FE3706E1571663F6E4A4ACC796F54E59B62FF98837975EC8D0FCD3I
Malicious:	**true**
Antivirus:	• Antivirus: Avira, 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\NNw\sessionmsg.exe	
Process:	C:\Windows\explorer.exe

C:\Users\user\AppData\Local\NNw\sessionmsg.exe	
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	74440
Entropy (8bit):	6.20617662830101
Encrypted:	false
SSDEEP:	1536:uC9DVLLFwi//NFlWPP0mTluh1AzxJIdqqP86mSsrvNJYKPd:L3FR/F7+0mTwhswdqqk6mS4RF
MD5:	1F7CEA0216DE48B877C16F95C7DA1F0F
SHA1:	BBF654AC3D1EEC107CF18B9A7AF15FA1ED0F6075
SHA-256:	0E585A4A11586B921D103433AFA215EC419A5ED2940EFD084A47B871F43CC786
SHA-512:	3E724732D4EAA863263D2D4259FF2DF8132486418D23DBBE572E72B766416F2F7100C54EC5F776085F3EB04C33521D50895DDA1DE2947814AB67FEED55E89F50
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....:...[...[...[..?...[..?...[..?...[..?...[...[...[..?...[..?<..[..?...[..Rich.[..... .....PE..d.....#E.....".....|.....y.....@.....s,..... .....P..`....@..l.....$...p.....`...T..... .....text....{.....|..... ..`.imrsiv.....rdata...Y.....Z.....@..@.data....0.....@....pdata..l....@.....@..@.rs rc...`....P.....@..@.reloc.....p.....@..B..... .....

C:\Users\user\AppData\Local\Rn1XW4tG\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:	C122CD7A245EF6A6A7B7DECAB6500BDC11E4C57B8E35F8462CC0615E44E54071E6BF79B69BB8519470ACBAF0D2E62ABC45C38CBF0606261792EDB4A84790E 61
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\Rn1XW4tG\UxTheme.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1224704
Entropy (8bit):	5.563729164487592
Encrypted:	false
SSDEEP:	12288:IVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:dfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	EF86C1D91B1F2E166ABA2D6B26A78954
SHA1:	17E7E4E3E5256A7FC6B71685FB664A508D667F0F
SHA-256:	BFAAF4481E907EDBA8750C33DDE921D2082BED81360E489755BFB90741BA863C
SHA-512:	E8FECED9F2F869A137E9EB0B34AF4AD5F52707980E3FC680BA4626A62239BBD4BA2BD8A2853EA7FBDA4857835ABA3B26A2690247624CFC3DE7CE2DBD3A36A 2F9
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|..... .....PE..d.# ..DN^....." .....p.....@.....@\|x}..b..... .....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\aDD0Ov\dxgi.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1224704

C:\Users\user\AppData\Local\aDD0Ov\dxgi.dll	
Entropy (8bit):	5.551938872046831
Encrypted:	false
SSDEEP:	12288:AVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:lfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	8F188E3515ABBE7DEF3D367E6FF172EA
SHA1:	BADD8B732673F23A47684975FB1AD72F80A62B4A
SHA-256:	07640C740940FAC78881C737B4372A4BD5468801250A384936A5BE4718C1AB50
SHA-512:	1005C91C926389B9E6F5236B1386048A459A57CF8B7811DD0CA1B48A164BFA4AB5848A722453AF1D0654B0BF790EF071D692479EE0587E5B99E98FDB8FDEB5C/
Malicious:	**true**
Antivirus:	• Antivirus: Avira, 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\aDD0Ov\dxgiadaptercache.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	45568
Entropy (8bit):	5.76587079771977
Encrypted:	false
SSDEEP:	768:amW9V/ozvl7zYwl625N5s/NSUDUaDXqtqaBlrr8Nwcq40Jsbr8JWPgsygYADRBd8:xFzvllQ4cSUDJDdaT+weYWqfwzd8
MD5:	3E73262483D4FB1BB88BA1B2B9BB3D5A
SHA1:	27938C7A5DD113EC9EC644048070B9F1BCA7DEAA
SHA-256:	5E51AB3594D8B1E451DA1180FAF2A0E6D597725B8E63C4928B66E1DBA5D9CB86
SHA-512:	E0426B343455E022D03D9C1DDA49125E13E1354AD6DED20E64CEC83E71DCCC907EC0D1D510578E698A7F511EE428A819A7DA701B096E812E780B27BF26E71B2
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....}.y...*...*...*.d'*...*.x.+...*.x.+...*.x.+...*...*...*.x.+...*.x.+...*.xl*...*.xK*...*.x.+...*Rich...*.....PE..d....2.....".....l...J.....h.....@.....`..... ..... .....\...`...T.....text....k.....l..... ..`.rdata.../.....0...p.....@..@.data.....@....pdata.....@..@.rsrc... .....@..@.reloc..\.....@..B.....

C:\Users\user\AppData\Local\j3KBEEMS\MFC42u.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1249280
Entropy (8bit):	5.572733209255193
Encrypted:	false
SSDEEP:	12288:kVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1/f:BfP7fWsK5z9A+WGAW+V5SB6Ct4bnb/
MD5:	81AEBC0D9D866D52F0D2603386185771
SHA1:	110C09770C10EF6E43CD94DA6D6C1D17422299A0
SHA-256:	690F82C84EF602EB4D2DAC3E25C42A21D07054A498BF987E5273266EBCB03828
SHA-512:	8B23322C46EC3160D400AEB8F45E0DF6E6424030DF4BD5FD87062C72BF7DA3AF56A182DB4C0F0441544B805E92F78827BE40DBDFEBAE3C0F1E9FE7DEB2B4D7B1
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.#..DN^....." .....p.....@.....@lx}..b.....l...c.....h.....$#..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\j3KBEEMS\irftp.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	184832
Entropy (8bit):	5.862106385432374
Encrypted:	false

C:\Users\user\AppData\Local\j3KBEEMS\irftp.exe	
SSDEEP:	3072:gzPq/xfWlkWmvIGaYLZ4yjchpChlyelcU4uuh0SEslWsXxgCzX0Fhf8LL8FT7:Eq5fWlkjuYLLtHyeFSEiXxZzb8FT
MD5:	F1C2D10CA8161DB689CD4FDE756E2DBB
SHA1:	C41E86E9755824D3775E2AD6CAC9A46C7AA1C417
SHA-256:	8854450FEAD134B24FABF4B805434FCFDDF25D2179048410728F8901E0FE0906
SHA-512:	5EBB1AD4261C689E22FE34CFB0C18D71451DD4F3694D8F521D181EB42FF90582D8EF8C8AB43BFC59D224452944D9602DB1030B633856E139442EEF0C2F4428F5
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PU...4}..4}..4}.{P~..4}.{Py..4}.{Px..4}.{P|..4}..4|.c5}.{Pt.74}.{P...4}.{P...4}.Rich.4}.....PE..d....v.4....."......6.....4.....@.....`..... .....T...,....p..0....`..t.....p.....T..... .....@i.....@j.....text....4.....6..... ..`.rdata.....P.....:.....@..@.data....|.....@....pdata..t...`.....@..@.rsrc. ..0....p.....@..@.reloc.....p.....@..B..... .....

C:\Users\user\AppData\Local\ocY6\Narrator.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	349696
Entropy (8bit):	6.567354682144278
Encrypted:	false
SSDEEP:	3072:2v1g/YrkRsWlO3nWOgV1M2uMFS/BaMiXbAJUoTq7XLtqkXIJA9QD4hLtcRiWh6f3:2vSckvCWOgB6YsyzZBL+RQFgZKUV
MD5:	56036993FB96C42F30C443A11BD56F4D
SHA1:	93367421725D818963F337F179EE61710BB2ABD3
SHA-256:	D3A728CFC32D43A9C96A45EFE6B3B7A21A8435F758C1C382978047982B6ADBB0
SHA-512:	E3DBC40DC7717BB9EC31657126FFA29D69362EE570BAC3D5B31918876261CF9E6954FDB31C2145788FF186E01A29A1696B914B626797CC8BC46F5FCB43D90F2
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....E[...[...[...R.B.S...4...U...4...X...4...E...4...B...[.....4...q...4..,.Z...4.. .Z...4...Z...Rich[.....PE..d.....".....V.....5.....@.....GV....`..... .....H>..T.....T..... .....P.....text....U.....V..... ..`.rdata..p2...p...4...Z.....@..@.data...h.....@....pdata.....@..@. rsrc.....@..@.reloc.....N.....@..B..... .....

C:\Users\user\AppData\Local\ocY6\WINMM.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1228800
Entropy (8bit):	5.55817362410966
Encrypted:	false
SSDEEP:	12288:tVl0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:0fP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	787D5F31C2547CD098B78D078B242B65
SHA1:	8E00544A583694062D1668BD905E4F1692EC7CCF
SHA-256:	FC40BA104B2291E47E261DBE6E89B0C770AED13CD4580388C7F888341F972BF6
SHA-512:	BAD736ED84B4E58B0A833524433266B6F68830C6091C68188D884140C05C108BF59C3F1A27F5A7D06328E1717C7B59A98015B8431261C34F05EAD35B7C408C98
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.# ..DN^....." .....p.....@.....@lx}..b.....h....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\pEPyA\MFPlat.DLL	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1228800
Entropy (8bit):	5.576641063701175
Encrypted:	false
SSDEEP:	12288:mVl0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:7fP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	4D31651F601785EAF47A2DF7A5D44267
SHA1:	90A06F9253AC25DC67482A1F2D3B71C12C4A5917
SHA-256:	7AE428CD9BBAC8C2A562D975D36CFF88208DB205C9A5F1BF081B5D7AD22FE4BB

C:\Users\user\AppData\Local\pEPyA\MFPlat.DLL	
SHA-512:	47049EF459195EAE51DF6232ADA30CD7C40A92568F21CFEBCA4078231C1865D58917BC7F4DE28B9535C87220B607DF5B01A98D5B0C8F699443E43BA2D0A4C59
Malicious:	**true**
Antivirus:	• Antivirus: Avira, 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\pEPyA\mfpmp.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	49688
Entropy (8bit):	6.083384253651048
Encrypted:	false
SSDEEP:	768:vcqpeHOwVxW4zmjjJF686T/5Lel2fBetjEWI9Whu3H1PcSP:vcEoVxJodg/tfiEAhu3VPcSP
MD5:	7C3D09D6DB5DB4A272FCF4C1BB3986BD
SHA1:	F0C392891B6D73EADB20F669A29064910507E55E
SHA-256:	E459FF6CBA8C93589B206C07BDCCD2E6C57766BE6BB4754F2FB1DEF9EF2E3BDE
SHA-512:	6CFE325CD0A78D6ACC9473BA51069E234CB0F9A47F285A6204EE787902C77005491B41C301DD38602CC387329F214E700F9203E4ECE5077E58D30276821640E4
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0._.Q`..Q`..Q`..)...Q`..5c..Q`..5d..Q`..Qa..Q`..5a..Q`..5e..Q`..5n..Q`. .5...Q`..5b..Q`.Rich.Q`.....PE..d...^.A.....".....R...V.....P).....@.....s.....`..... .....h.....`.....$.....`z..T..... .....Pq.....`r.....H...`.....text....Q.....R..... ..`.rdata..T-...p.....V.....@..@.data.....@....pdata.....@..@.didat ..0.....@....rsrc...`.....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\tiy3x\DUI70.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1507328
Entropy (8bit):	5.908335102849305
Encrypted:	false
SSDEEP:	12288:+VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1g:jfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	03459CA27218008A2DAFBFDAE2268861
SHA1:	D31BFAF58897CB3EACC804C704969708AC369F32
SHA-256:	3E676DE9818A5E127DB08FC15A6594EEF78A8019AEE85D91922E884D4ED661BE
SHA-512:	C91700FF267F818BAAFBEA36C523C1DD66BCB1374780E8E1272427EFEED86037C99060D155B53CBD58B89C1480526CA2AE55CDE3DB71E0EE75544A1BC890C0 F
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.# ..DN^......" .....p.....@.....@lx}..b.....dQ...c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\tiy3x\SystemSettingsRemoveDevice.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	39304
Entropy (8bit):	6.292969415106569
Encrypted:	false
SSDEEP:	768:miVyKshA4p2nOCD6DjOxMtjlQfU7r5YdGiEh07tvNZRAER1PnX:QhlkOO74XU7i8iEG7HZR/PX
MD5:	87AF711D6518C0CF91560D7C98301BBB
SHA1:	81B7B8261A33D4D983DFDC47A716686118F582F9
SHA-256:	1B6381E83463416D9BE6656A81978B2EBA21587BBDE18E8CFEFA1C0F45378AAC
SHA-512:	E4534E5A205D44579AB60FAA5B19A2034C688D191ABB8670CD77696ABB000A949F5ABC996E0989FD74B4DFBE43C863FF66FDA9C623B045A771283B1955D28C3
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\tiy3x\SystemSettingsRemoveDevice.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....R|.PR|.PR|.P[..P~|.P=..QQ|.P=..Q@|.P=..QW|.P=..QC|.PR|.P.|.P=..QZ|.P=.dPS|.P=..QS|.PRichR|.P.....PE..d....G.j.....".....<...>.....B.....@.....SC..... .....p.....v...#....h....j..T.....`.....a..`.....text...n:.....<..... ..`.imrsiv.....P.....rdata..8...`.. ...@.....@..@.data.....`.....@....pdata.....b.....@..@.rsrc.....f.....@..@.reloc..h.....t.....@..B.....

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\89dad5d484a9f889a3a8dfca823edc3e_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	4447
Entropy (8bit):	5.4784075377314725
Encrypted:	false
SSDEEP:	48:JKKgU4Bzv1cL0zELQOzER45GgGKKgU4x3tseyhmyTsKbpQ4t2SIE:JJgqYzELhbGgGJgsbQKbp2Sx
MD5:	2DCE33567875F640E362573FD1B0F774
SHA1:	5FEBFBD4D394AD711E2BA6F7AA5F8EFA8767E9F5
SHA-256:	1E6543A033B33D7DA75925DB458C0C1E4AD3822783D07BA89F1DCB232059493E
SHA-512:	29504AF0F93BE599C4EB174BACC386B5E255A32172CF40412F831AF5191954CF66A9DDB310C573B94B1EC9F2A1E0FB9680016ACD309A49DBC9CEB7D656224CE8
Malicious:	false
Reputation:	unknown
Preview:	.....user.....user.....RSA1.....#...yg..{m.T.q.>...h..0.....U.D....k...i#x...k.>....* $M..DH.-M[.u..-'....Z.V.....Z6\|1....!.'!...M3.@E..I. H...P.!.....z..O.....-.[Rp8O.-Q....?....,...C.r.y.p.t.o.A.P.I. .P.r.i.v.a.t.e. .K.e.y....f..... .....$S...V(....H.qP.9.&...j..F|.,R..... .....|.cl.....tK.1a...hS...$T6...z.....P.x....O.....+...7_T\'..3..Q.....*.L>..f..].&Z. L.6....k.d.Z.`.M.u./0...G....r.(F..4y6...aI4..7oU.k...;.;.I.O.~D.E....:..F8.,....C..u..Nv8..\|....''&..U.....@.l@[.F_..2..4S..;&GL].....%.....>}t....o-.y...w.gM.pN...n.*.Z.....M,DnA.k(...Qa.qo(....t...:H.Q.....4d.V. +..C.$.P.^rr.C>....D4....~v.{.....6_W.|Q..._X2..q..F...W...o..@.6.6X...)...`..#...%^.f7....z}Ms.Y@.N.z.....0.....0..r.~.....O%%.....1.,z....@.Q...Z.j..^./..Z.s....yd!.[..U..~...%...5.=..8`U.P!.%y.xi.i=....\...n?.J.Yy{p.R.9.....*.#..

Static File Info

General

File type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Entropy (8bit):	5.574688553617224
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:	P7n0h6OhYp.dll
File size:	1220608
MD5:	718a7d9b1fe55a72cfa586e869236df8
SHA1:	5d870aeb7951ab6af0900ba837924f79e3716936
SHA256:	d485423afb5929de201a0fee5476c8b6d7d1a1868b537d7730db9b3e67d6a222
SHA512:	f07f61cee0c57c40ee9bce3682d10faa5987a317b3e06fcdf7da0e4a5bc6a42bb52008077fecf940e8237161587ff5f0fb2f022542f5715f7f0d339d56efe32a
SSDEEP:	12288:0VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:xfP7fWsK5z9A+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
.qzu	0x119000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tbbd	0x11a000	0x1f7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.shoovi	0x11b000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.wbmgl	0x11c000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.aobcn	0x11d000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.xdno	0x11e000	0x1f2a	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ipsw	0x120000	0x389	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.cqpqq	0x121000	0x573	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.skzqoj	0x122000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.nvjg	0x123000	0xd33	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.bbt	0x124000	0x2da	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.wsg	0x125000	0x389	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vqdhza	0x126000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.mgf	0x127000	0x1f2a	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.xusvuv	0x129000	0x8fe	0x1000	False	0.256591796875	data	3.73840094584	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	

Language of compilation system	Country where language is spoken	Map

Network Behavior

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: 5036 Parent PID: 6088

General

Start time:	17:45:08
Start date:	28/09/2021
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe 'C:\Users\user\Desktop\P7n0h6OhYp.dll'
Imagebase:	0x7ff705830000
File size:	1136128 bytes
MD5 hash:	E0CC9D126C39A9D2FA1CAD5027EBBD18
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000001.00000002.267714415.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 644 Parent PID: 5036

General

Start time:	17:45:08
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\P7n0h6OhYp.dll',#1
Imagebase:	0x7ff7eef80000
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: 3240 Parent PID: 5036

General

Start time:	17:45:08
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\P7n0h6OhYp.dll,IsInteractiveUserSession
Imagebase:	0x7ff6c6680000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000004.00000002.324777282.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 5044 Parent PID: 644

General

Start time:	17:45:09
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe 'C:\Users\user\Desktop\P7n0h6OhYp.dll',#1
Imagebase:	0x7ff6c6680000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000005.00000002.247365585.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3472 Parent PID: 3240

General

Start time:	17:45:10
Start date:	28/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff693d90000
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: 5816 Parent PID: 5036

General

Start time:	17:45:12
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\P7n0h6OhYp.dll,QueryActiveSession
Imagebase:	0x7ff797770000
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: 00000008.00000002.254598295.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 4632 Parent PID: 5036

General

Start time:	17:45:15
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\P7n0h6OhYp.dll,QueryUserToken
Imagebase:	0x7ff6c6680000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000000A.00000002.261507768.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: RdpSa.exe PID: 716 Parent PID: 3472

General

Start time:	17:45:48
Start date:	28/09/2021
Path:	C:\Windows\System32\RdpSa.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\RdpSa.exe
Imagebase:	0x7ff7f3240000
File size:	43008 bytes
MD5 hash:	0795B6F790F8E52D55F39E593E9C5BBA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: RdpSa.exe PID: 2564 Parent PID: 3472

General

Start time:	17:45:49
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\1wgM9CYx\RdpSa.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\1wgM9CYx\RdpSa.exe
Imagebase:	0x7ff73a1b0000
File size:	43008 bytes
MD5 hash:	0795B6F790F8E52D55F39E593E9C5BBA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000015.00000002.354057356.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

File Activities Show Windows behavior

File Read

Analysis Process: dxgiadaptercache.exe PID: 6132 Parent PID: 3472

General

Start time:	17:46:01
Start date:	28/09/2021
Path:	C:\Windows\System32\dxgiadaptercache.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\dxgiadaptercache.exe
Imagebase:	0x7ff6ca3d0000
File size:	45568 bytes
MD5 hash:	3E73262483D4FB1BB88BA1B2B9BB3D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dxgiadaptercache.exe PID: 1308 Parent PID: 3472

General

Start time:	17:46:01
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\aDD0Ov\dxgiadaptercache.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\aDD0Ov\dxgiadaptercache.exe
Imagebase:	0x7ff64dc50000
File size:	45568 bytes
MD5 hash:	3E73262483D4FB1BB88BA1B2B9BB3D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000018.00000002.383288122.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities Show Windows behavior

File Read

Analysis Process: GamePanel.exe PID: 668 Parent PID: 3472

General

Start time:	17:46:14
Start date:	28/09/2021
Path:	C:\Windows\System32\GamePanel.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\GamePanel.exe

Imagebase:	0x7ff74c0a0000
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: 4140 Parent PID: 3472

General

Start time:	17:46:16
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\Rn1XW4tG\GamePanel.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Rn1XW4tG\GamePanel.exe
Imagebase:	0x7ff7a3570000
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: 0000001A.00000002.410742595.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Read

Analysis Process: SystemSettingsRemoveDevice.exe PID: 1036 Parent PID: 3472

General

Start time:	17:46:27
Start date:	28/09/2021
Path:	C:\Windows\System32\SystemSettingsRemoveDevice.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SystemSettingsRemoveDevice.exe
Imagebase:	0x7ff6f45e0000
File size:	39304 bytes
MD5 hash:	87AF711D6518C0CF91560D7C98301BBB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: SystemSettingsRemoveDevice.exe PID: 5192 Parent PID: 3472

General

Start time:	17:46:34
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\tiy3x\SystemSettingsRemoveDevice.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\tiy3x\SystemSettingsRemoveDevice.exe
Imagebase:	0x7ff6c5e60000
File size:	39304 bytes
MD5 hash:	87AF711D6518C0CF91560D7C98301BBB

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.00000002.449151118.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Read

Analysis Process: lpksetup.exe PID: 4976 Parent PID: 3472

General

Start time:	17:46:45
Start date:	28/09/2021
Path:	C:\Windows\System32\lpksetup.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\lpksetup.exe
Imagebase:	0x7ff6cdd60000
File size:	732160 bytes
MD5 hash:	8E2C63E761A22724382338F349C55014
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: lpksetup.exe PID: 4968 Parent PID: 3472

General

Start time:	17:46:46
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\A7mgbJ\lpksetup.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\A7mgbJ\lpksetup.exe
Imagebase:	0x7ff75ca20000
File size:	732160 bytes
MD5 hash:	8E2C63E761A22724382338F349C55014
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000022.00000002.476637367.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: Narrator.exe PID: 5480 Parent PID: 3472

General

Start time:	17:46:58
Start date:	28/09/2021
Path:	C:\Windows\System32\Narrator.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\Narrator.exe
Imagebase:	0x7ff7058a0000
File size:	349696 bytes

MD5 hash:	56036993FB96C42F30C443A11BD56F4D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: Narrator.exe PID: 5616 Parent PID: 3472

General

Start time:	17:46:59
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\ocY6\Narrator.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\ocY6\Narrator.exe
Imagebase:	0x7ff69a2a0000
File size:	349696 bytes
MD5 hash:	56036993FB96C42F30C443A11BD56F4D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WindowsActionDialog.exe PID: 5040 Parent PID: 3472

General

Start time:	17:47:00
Start date:	28/09/2021
Path:	C:\Windows\System32\WindowsActionDialog.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\WindowsActionDialog.exe
Imagebase:	0x7ff761c50000
File size:	59392 bytes
MD5 hash:	991359EE1E9C1958EB5D0F7314774123
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: WindowsActionDialog.exe PID: 1280 Parent PID: 3472

General

Start time:	17:47:04
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\JrFH9qPBX\WindowsActionDialog.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\JrFH9qPBX\WindowsActionDialog.exe
Imagebase:	0x7ff639950000
File size:	59392 bytes
MD5 hash:	991359EE1E9C1958EB5D0F7314774123
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: 00000027.00000002.514121758.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: sessionmsg.exe PID: 1112 Parent PID: 3472

General

Start time:	17:47:15
Start date:	28/09/2021
Path:	C:\Windows\System32\sessionmsg.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\sessionmsg.exe
Imagebase:	0x7ff650f20000
File size:	74440 bytes
MD5 hash:	1F7CEA0216DE48B877C16F95C7DA1F0F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: sessionmsg.exe PID: 1268 Parent PID: 3472

General

Start time:	17:47:16
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\NNw\sessionmsg.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\NNw\sessionmsg.exe
Imagebase:	0x7ff7635c0000
File size:	74440 bytes
MD5 hash:	1F7CEA0216DE48B877C16F95C7DA1F0F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000029.00000002.543009513.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Disassembly

Code Analysis