ID: 492695
Sample Name: PSnPApRPsG
Cookbook: default.jbs
Time: 23:00:25
Date: 28/09/2021
Version: 33.0.0 White Diamond

Table of Contents

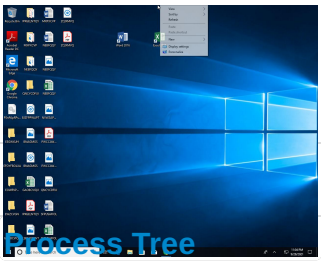
Windows Analysis Report PSnPApRPsG

Overview

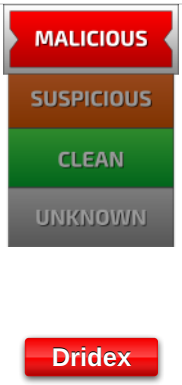
General Information

Sample Name:	PSnPApRPsG (renamed file extension from none to dll)
Analysis ID:	492695
MD5:	ed37656551984c..
SHA1:	1475e0b8fd14a3a.
SHA256:	4bbd6db4f6bdad3.
Tags:	Dridex exe
Infos:	

Most interesting Screenshot:



Detection

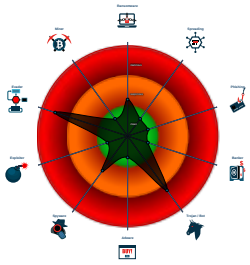


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- Uses Atom Bombing / ProGate to in…
- Queries the volume information (nam…
- Contains functionality to check if a d…

Classification



- **System is w10x64**
- loaddll64.exe (PID: 7012 cmdline: loaddll64.exe 'C:\Users\user\Desktop\PSnPApRPsG.dll' MD5: E0CC9D126C39A9D2FA1CAD5027EBBD18)
  - cmd.exe (PID: 7056 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\PSnPApRPsG.dll',#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 7092 cmdline: rundll32.exe 'C:\Users\user\Desktop\PSnPApRPsG.dll',#1 MD5: 73C519F050C20580F8A62C849D49215A)
      - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - tcmsetup.exe (PID: 6868 cmdline: C:\Windows\system32\tcmsetup.exe MD5: 0DDA495155D552D024593C4B3246C8FA)
        - tcmsetup.exe (PID: 6980 cmdline: C:\Users\user\AppData\Local\72PXeqK\tcmsetup.exe MD5: 0DDA495155D552D024593C4B3246C8FA)
        - RdpSaUacHelper.exe (PID: 5052 cmdline: C:\Windows\system32\RdpSaUacHelper.exe MD5: DA88A7B872B1A52F2465D12CFBA4EDAB)
        - RdpSaUacHelper.exe (PID: 6204 cmdline: C:\Users\user\AppData\Local\hUhx9Ta\RdpSaUacHelper.exe MD5: DA88A7B872B1A52F2465D12CFBA4EDAB)
        - msdt.exe (PID: 1568 cmdline: C:\Windows\system32\msdt.exe MD5: 8BE43BAF1F37DA5AB31A53CA1C07EE0C)
        - msdt.exe (PID: 5628 cmdline: C:\Users\user\AppData\Local\nmYaGulOu\msdt.exe MD5: 8BE43BAF1F37DA5AB31A53CA1C07EE0C)
        - bdechangepin.exe (PID: 6688 cmdline: C:\Windows\system32\bdechangepin.exe MD5: 013D00A367D851B0EC869F209337754E)
        - bdechangepin.exe (PID: 6608 cmdline: C:\Users\user\AppData\Local\RjGeORx\bdechangepin.exe MD5: 013D00A367D851B0EC869F209337754E)
        - ProximityUxHost.exe (PID: 4584 cmdline: C:\Windows\system32\ProximityUxHost.exe MD5: E7F0E9B3779E54CD271959C600A2A531)
        - ProximityUxHost.exe (PID: 5376 cmdline: C:\Users\user\AppData\Local\yC4r\ProximityUxHost.exe MD5: E7F0E9B3779E54CD271959C600A2A531)
        - psr.exe (PID: 3064 cmdline: C:\Windows\system32\psr.exe MD5: 3B8262EB45E790BF7FA648CEE2CCCB7B)
        - psr.exe (PID: 5152 cmdline: C:\Users\user\AppData\Local\Tp5KLY\psr.exe MD5: 3B8262EB45E790BF7FA648CEE2CCCB7B)
        - psr.exe (PID: 1716 cmdline: C:\Windows\system32\psr.exe MD5: 3B8262EB45E790BF7FA648CEE2CCCB7B)
        - psr.exe (PID: 5520 cmdline: C:\Users\user\AppData\Local\ifnj9zHVv\psr.exe MD5: 3B8262EB45E790BF7FA648CEE2CCCB7B)
        - wlrmdr.exe (PID: 5688 cmdline: C:\Windows\system32\wlrmdr.exe MD5: 4849E997AF1274DD145672A2F9BC0827)
        - wlrmdr.exe (PID: 5696 cmdline: C:\Users\user\AppData\Local\PVSXo\wlrmdr.exe MD5: 4849E997AF1274DD145672A2F9BC0827)
        - DevicePairingWizard.exe (PID: 5468 cmdline: C:\Windows\system32\DevicePairingWizard.exe MD5: E23643C785D498FF73B5C9D7EA173C3D)
        - DevicePairingWizard.exe (PID: 2832 cmdline: C:\Users\user\AppData\Local\YaR\DevicePairingWizard.exe MD5: E23643C785D498FF73B5C9D7EA173C3D)
        - PresentationSettings.exe (PID: 2108 cmdline: C:\Windows\system32\PresentationSettings.exe MD5: 76086DD04B6760277A2B897345A0B457)
        - PresentationSettings.exe (PID: 1072 cmdline: C:\Users\user\AppData\Local\br5u0t\PresentationSettings.exe MD5: 76086DD04B6760277A2B897345A0B457)
    - rundll32.exe (PID: 7120 cmdline: rundll32.exe C:\Users\user\Desktop\PSnPApRPsG.dll,??0?$PatternProvider@VExpandCollapseProvider@DirectUI@@UIExpandCollapseProvider@@$00@DirectUI@@QEAA@XZ MD5: 73C519F050C20580F8A62C849D49215A)
    - rundll32.exe (PID: 4388 cmdline: rundll32.exe C:\Users\user\Desktop\PSnPApRPsG.dll,??0?$PatternProvider@VGridItemProvider@DirectUI@@UIGridItemProvider@@$01@DirectUI@@QEAA@XZ MD5: 73C519F050C20580F8A62C849D49215A)
    - rundll32.exe (PID: 6328 cmdline: rundll32.exe C:\Users\user\Desktop\PSnPApRPsG.dll,??0?$PatternProvider@VGridProvider@DirectUI@@UIGridProvider@@$02@DirectUI@@QEAA@XZ MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.677061553.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000009.00000002.691449064.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000028.00000002.1082755771.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000017.00000002.846583663.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000026.00000002.1056321571.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
Click to see the 10 entries				

Sigma Overview

System Summary:

Sigma detected: Possible Applocker Bypass

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

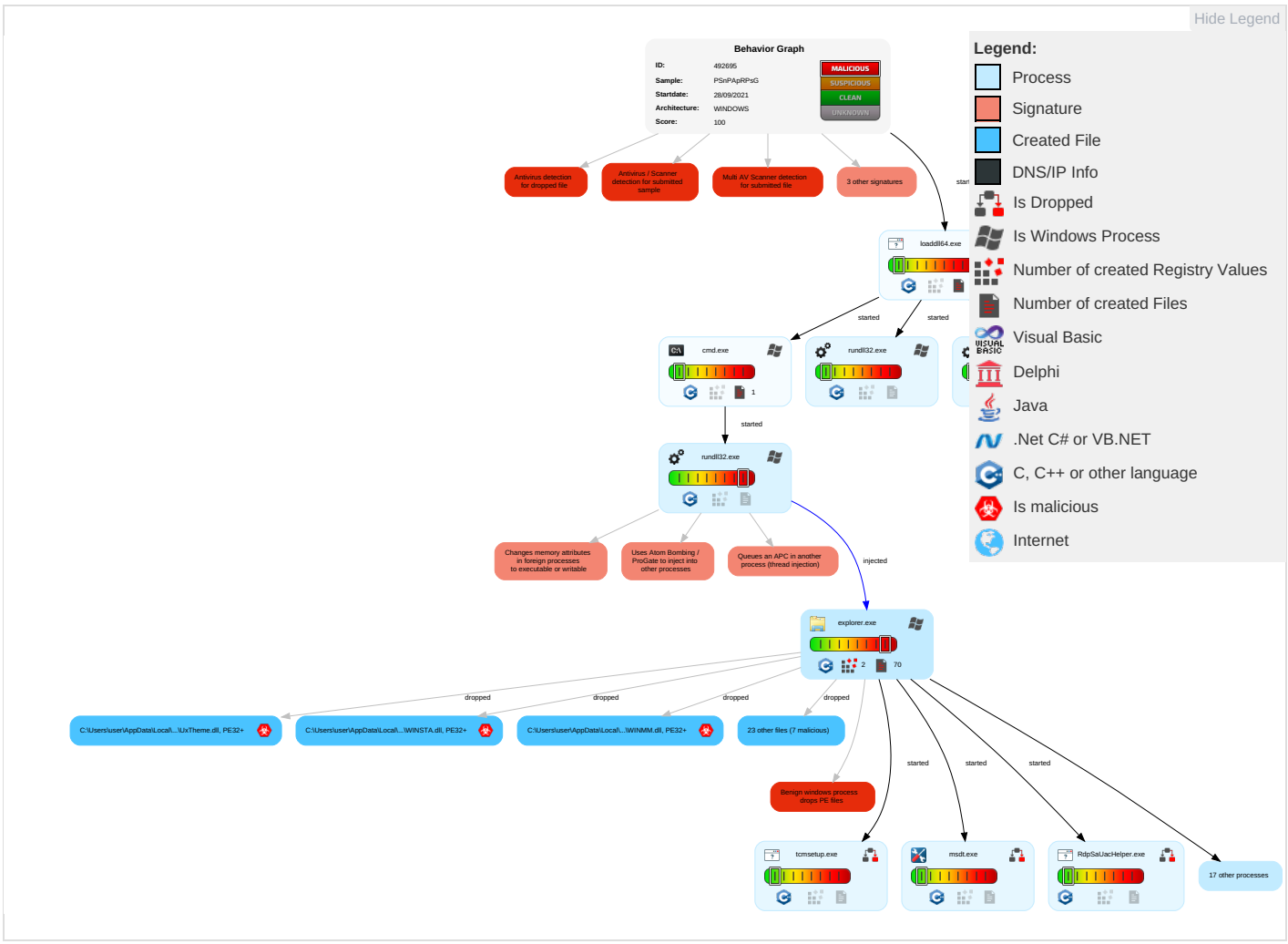
Queues an APC in another process (thread injection)

Uses Atom Bombing / ProGate to inject into other processes

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Command and Scripting Interpreter 2	Windows Service 1	Exploitation for Privilege Escalation 1	Masquerading 1	OS Credential Dumping	System Time Discovery 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop Insecure Network Communic
Default Accounts	Service Execution 2	Boot or Logon Initialization Scripts	Access Token Manipulation 1	Virtualization/Sandbox Evasion 1	LSASS Memory	Security Software Discovery 3 1	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Junk Data	Exploit SS Redirect P Calls/SMS
Domain Accounts	Exploitation for Client Execution 1	Logon Script (Windows)	Windows Service 1	Access Token Manipulation 1	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS Track Dev Location
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 3 1 3	Process Injection 3 1 3	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
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	Manipulate Device Communic
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	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Rundll32 1	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi Access Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 2	Proc Filesystem	System Information Discovery 2 5	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrad Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	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	Rogue Cel Base Stati

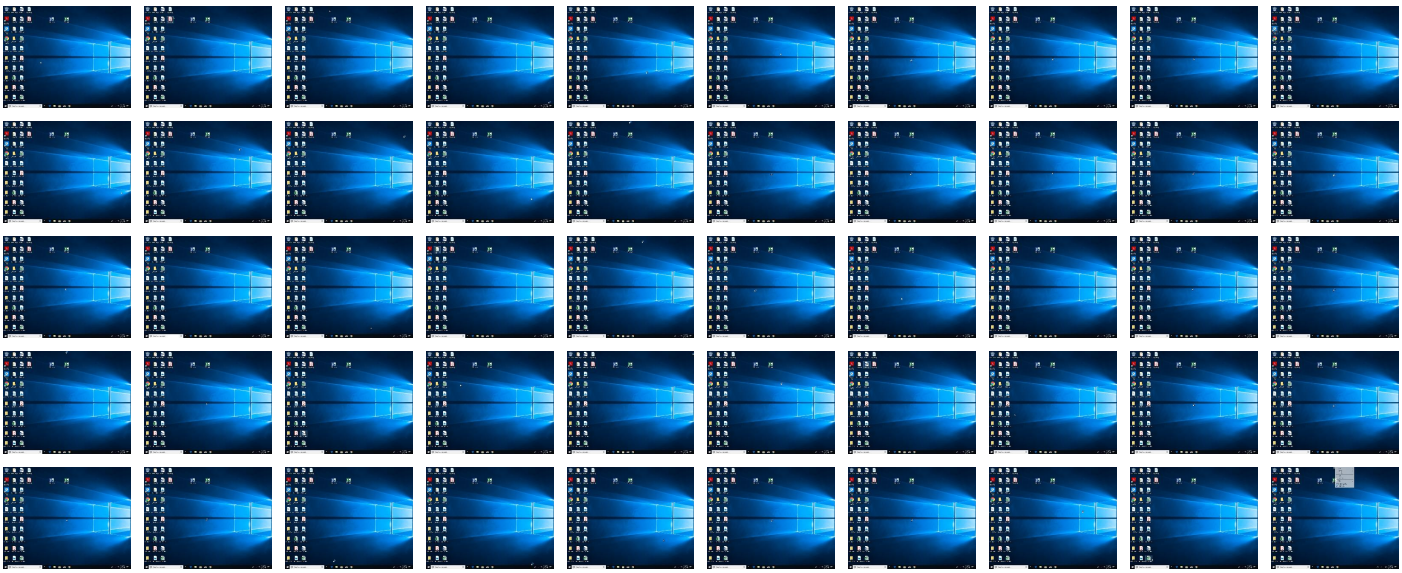
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PSnPApRPsG.dll	80%	ReversingLabs	Win64.Infostealer.Dridex	
PSnPApRPsG.dll	100%	Avira	HEUR/AGEN.1114452	
PSnPApRPsG.dll	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\a5Q9CELTE\VERSION.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\br5u0t\WINMM.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\PVSXo\DUI70.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\YaR\MFC42u.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\Tp5KLY\XmlLite.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\TQbOBk\DUser.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\a5Q9CELTE\VERSION.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\PVSXo\DUI70.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\72PXeqK\TAPI32.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\nmYaGulOu\UxTheme.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\PVSXo\DUI70.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\HtmF\credui.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\hUhx9Ta\WINSTA.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\a5Q9CELTE\VERSION.dll	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\br5u0t\WINMM.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\PVSXo\DUI70.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\YaR\MFC42u.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Tp5KLY\XmlLite.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\TQbOBk\DUser.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\a5Q9CELTE\VERSION.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\PVSXo\DUI70.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\72PXeqK\TAPI32.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\nmYaGulOu\UxTheme.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\PVSXo\DUI70.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\HtmF\credui.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\hUhx9Ta\WINSTA.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\72PXeqK\tcmsetup.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\72PXeqK\tcmsetup.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\HtmF\perfmon.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\HtmF\perfmon.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\PVSXo\wlrmdr.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\PVSXo\wlrmdr.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\RjGeORx\bdechangepin.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\RjGeORx\bdechangepin.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
20.2.RdpSaUacHelper.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
18.2.tcmsetup.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
33.2.psr.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
5.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
38.2.DevicePairingWizard.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
23.2.msdt.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
36.2.wlrmdr.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
29.2.ProximityUxHost.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
40.2.PresentationSettings.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
31.2.psr.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
26.2.bdechangepin.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

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	492695
Start date:	28.09.2021
Start time:	23:00:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 49s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PSnPApRPsG (renamed file extension from none to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@57/27@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 42.1% (good quality ratio 27.9%) • Quality average: 49.4% • Quality standard deviation: 42.2%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32 • Stop behavior analysis, all processes terminated
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\72PXeqK\TAPI32.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1527808
Entropy (8bit):	4.693391564888678
Encrypted:	false
SSDEEP:	12288:SVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:PfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	4441DC6E13ED55823A6FE19061C57785
SHA1:	D2EDA84980357BB70998B4393C17C4B5F3EA7763
SHA-256:	4174BFCA405A1249B2FCE8453F648FE1BFF887B35BBB752C3D178B0C442A8A8A
SHA-512:	04651D77D34B35959F5AAEFEC08AAE2391A9F2F468856C481BC07FCD8A2664511DD4A70F07DCCBE564B0001900092866E25D040B68D2587108576F1BBEFB0558
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....$.....\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.(..DN^....." .....0.....p.....@.....P.....@\|x}..b.....0..V....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\72PXeqK\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: 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\HtmF\credui.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1523712
Entropy (8bit):	4.673043182665197
Encrypted:	false
SSDEEP:	12288:KVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:XfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	94EEF4660920EB34F50F20810A44AB86
SHA1:	7CD1FF09EA7B63AE4FA9E191EF4653B6BEE24960
SHA-256:	B8E2D3215B26CD75C322EF81C74AFA5F535180F140B440B57FDB0F46F25955F5
SHA-512:	2556ED8B3D9DE1F8F47C4DD4B4AEF58DA34D9DC30E706391EEA68C614374EA72E6BF78F4AFFFF509B417F78BEA9CC623824960A3905540874EF0A927E40295A

C:\Users\user\AppData\Local\HtmF\credui.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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.(..DN^....." ....p.....@.....@.....@lx}..b.....0.....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\HtmF\perfmon.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	175616
Entropy (8bit):	6.895507339523819
Encrypted:	false
SSDEEP:	3072:uVt2h5auVl9cMHFO+ZyGghtYIo9piswTogiqQKy349:uVMzVIOMHFhyhqIo9s37iTK24
MD5:	BD9ABDEA680B56534CE7627E39270A7C
SHA1:	24FCF3E615F5E7F434244D90AE5C4EB90F7C5EB5
SHA-256:	EB9FF0CDA3E15147BB0FE00984B75C5F7B04644957CCAC135996AC18C1FD3EED
SHA-512:	CEFA87534CB62E705EEE00CE5FA7C73083562A6B97E5D9D0106A3BCB3499A1F7FE997376DB22F73BB4F19DA66E6CE65FE85E2DF1FD06051CC19C006B590824 7
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....$.....H....f..f..f.c...f.c...f.c...f.c...f..f..f.c...f.c. ..f.c...f.Rich.f.....PE..d.....i6.....".....$.....P.....@.....9....`..... .....D.....@.....0.....p...T.....`.....`.....t ext..... ..`.rdata..:x.....z.....@..@.data..... .....@....pdata.....0.....@..@.rsrc.....@.....@..@.reloc..... ...@..B..... .....

C:\Users\user\AppData\Local\PVSXo\DUI70.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1806336
Entropy (8bit):	5.1466425775068245
Encrypted:	false
SSDEEP:	12288:2VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1AcX4Yc:rfP7fWsK5z9A+WGAW+V5SB6Ct4bnbNI
MD5:	EB43F254B0FCC1FA10EC0C59130C442A
SHA1:	5002A9D37F594E84379581DA8479C0783A9B1957
SHA-256:	E326F8DA2BCB694C8F56272C5F8741F1722A38D877788CB6C234ECB5BDE23D2E
SHA-512:	552C148AFF9F8224A2DE3133322A3F18014EDE46E0116749167F5642B15D2B4CB3A1DA994925C837AF5453B1F95006693E28E1D963373B4FAE8BFEC09E07F432
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.(..DN^....." .....p.....p.....@.....@lx}..b.....0..dQ...c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\PVSXo\wlrmdr.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	65704
Entropy (8bit):	5.834154867756865
Encrypted:	false
SSDEEP:	1536:B14+6gGQ7ubZiQ+KytHlyObsvqr9PxDt8PcPs:QgGIu1iFtHJLu9ZDt8kU

C:\Users\user\AppData\Local\PVSXo\wlrmdr.exe	
MD5:	4849E997AF1274DD145672A2F9BC0827
SHA1:	D24E9C6079A20D1AED8C1C409C3FC8E1C63628F3
SHA-256:	B43FC043A61BDBCF290929666A62959C8AD2C8C121C7A3F36436D61BBD011C9D
SHA-512:	FB9227F0B758496DE1F1D7CEB3B7A5E847C6846ADD360754CFB900358A71422994C4904333AD51852DC169113ACE4FF3349520C816E7EE796E0FBE6106255AEF
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....$.....j.s... ... ... .s\ ... .o.!... .o.!... .o.!... .o.!... ... t.. .o.!... .o0 ... .o.!... Rich ... .PE..d....2....."....4.....:.....@.....@.....b.....P.....xg.....$...0.....y..T.....f.....g..x. .....text....3.....4..... ..`.imrsiv.....P.....rdata..J2...`...4...8.....@..@.data...h.....l.....@....pdata.....n.....@..@.rsr c...xg.....h...r.....@..@.reloc.....0.....@..B..... .....

C:\Users\user\AppData\Local\RjGeORx\DUI70.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1806336
Entropy (8bit):	5.146430269158369
Encrypted:	false
SSDEEP:	24576:BfP7fWsK5z9A+WGAW+V5SB6Ct4bnbN2I:BDW/e+WG0Vo6CtSnZf
MD5:	D2FE5DD6B761D5620B46087FF94F6EC8
SHA1:	6569BA8D06760494A3559B70DA8CB5BC76C8269B
SHA-256:	F11F70DD4CE14021A3F9A298EEEA6BA62824F8FFBB154C9022864563259ACD15
SHA-512:	BF9949C76E1B6F9DD67EF324338412A546C61B6FBF9804169FD63DA4A7C779A8C0E42A0F21830191A299113B569EA857FF2FC52D5E1A5BE48EBEB5C0D76AF19
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.(..DN^....." .....p.....p.....@.....@lx}..b.....0..dQ...c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\RjGeORx\bdechangepin.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	369664
Entropy (8bit):	6.503464732962775
Encrypted:	false
SSDEEP:	6144:so87gEZlHVxHEVHHHQVb1kHVqHVqHQQbTuTRTHTfTEHVf2XTQT6TITQT+VyW1727:1H+S+
MD5:	013D00A367D851B0EC869F209337754E
SHA1:	240B731FAA42E170511C1D0676B3ADE76712451B
SHA-256:	3D0BFED2F2A17FA8246634FDA7162A1BE56DDB3080519BCEFEAFD69FBC7F2FE1
SHA-512:	BD55925D3EC097FDD713A6847F69005C7B1007DBFAEAAFD02B0B23567F81C5721B4BFAF6A87DB1E94F4D71D6CC5E23AA31C443FD9030BD2D630489E9E736062
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....$.....j..9..9..9.8..9.8..9.8..9.8..9..9..9.8..9.8..9.k9..9.8..9Rich..9..... .....PE..d...l..`.....".....r...4.....0t.....@.....`..... .....T...4.....@..X....0..|.....T..... .....text....q.....r..... ..`.rdata..v.....v.....@..@.data..... .....@....pdata..|....0.....@..@.rsrc...X....@.....@. .@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\TQbOBk\DUser.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1527808
Entropy (8bit):	4.678124390083214
Encrypted:	false
SSDEEP:	12288:0VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:xfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	45F2082293D80022AF480E926ADA97DE

C:\Users\user\AppData\Local\TQbOBk\DUser.dll	
SHA1:	1D1849B46676B49A58F8044CD33E96B938D087C9
SHA-256:	5CF647A594E50F7E4C0BF294E76BBCD092C4CEE00AB7A6F90724AA25A05D3249
SHA-512:	01A4A18E7BD9D1572A2ABCB3C82DF9E327BCE9D91BD887FD2EFD52B29AB4F056ED8668EBA324CD91AAD23670019889D785EA94CD3D8651D174DDB19DA0CA F00
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.(..DN^....." .....0.....p.....@.....P.....@lx}..b.....0.....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\TQbOBk\EaseOfAccessDialog.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	304640
Entropy (8bit):	6.843015704242449
Encrypted:	false
SSDEEP:	6144:E/Odkrq1AlGra6uFz2LJGRg4kLNnei36cw:As5+FCdUc
MD5:	F87F2E5EBF3FFBA39DF1621B5F8689B5
SHA1:	B4E358BF1BE0DF6D341CA1BC949867D94F13EC07
SHA-256:	06780477637707BEA6317AE81D059A4D75B101542ADFA6DC855287EAEDFC822A
SHA-512:	6E8D60C17396260791898A2914422AFFF2921A4C3D924F56C83ED117B683D3F3AEFB15E234600F3B5375A47C0C6A13F6160B0638CA91663D29DC56067EB5E5B7
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....)..8m..km..km..kd.Hki..k...jn..k...j{..k...j`..k...jv..km..k3..k...jx..k ..$kl..k...jl..kRichm..k.....PE..d...1.(i....."....@.....L}...`..... .....(0.,.....5.....X.....T..... .....text..... ..`.rdata.....@..@.data...0....p.....X.....@....pdata.....b.....@..@.rsrc....5.... ....6...l.....@..@.reloc..X.....@..B.....

C:\Users\user\AppData\Local\Tp5KLY\XmlLite.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1523712
Entropy (8bit):	4.669713032094796
Encrypted:	false
SSDEEP:	12288:QVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:VfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	E1B6631ED63495598724E765533854EC
SHA1:	DEB955764D6C692B34385D043F9251C3900DEF13
SHA-256:	71D8FD1B0D8EFEC04B8E44EE6892F6852EE77AC32D3548DB37D997E895338B0E
SHA-512:	56ACCEF1B329CC5D1380F214135BC887DB3B3AAB95D1F0FD722A4D1DE30469F884878984A6B189A3DD71F56741DE1989544A333B6998DF3FBD701109AFA5999
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.(..DN^....." ....p.....@.....@.....@lx}..b.....0.....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\Tp5KLY\psr.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	600576
Entropy (8bit):	6.4861677167766665
Encrypted:	false
SSDEEP:	12288:B2mS50ICmAX+ASa8wd9Nkmw6cD8pellpco//EH1:B2mlmeFSa8wd9NStApeCoXEH
MD5:	3B8262EB45E790BF7FA648CEE2CCCB7B
SHA1:	EDDD81D1B3FD2EE99E42A43B25BD74D39BB850BC

C:\Users\user\AppData\Local\Tp5KLY\psr.exe	
SHA-256:	D1225E9FD2834BD2EF84EADAA4126020D20F4A0F50321440190C3896E69BD5D8
SHA-512:	A3709D39372CDB6D9C9E58932144CE8BA437C2134EFC9BCD2531708C1515CBAEA5929C220DF25D76785F7594BC5F8541E6ED5330EA3CA12E87C4DA5A2171C45
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....}.....x.....x.....x.....x...x.....x.....xR.....x.....Rich..... ....PE..d....S.....".....`.....@.....h....`..... .....7..,.....L.....D.....T..... .....X...8....7..@. .....text...5..... ..`.rdata.....@..@.data....m...`.....H.....@....pdata..L.....T.....@..@.didat.....j.....@....rsrc..... .....I.....@..@.reloc..D.....&.....@..B.....

C:\Users\user\AppData\Local\YaR\DevicePairingWizard.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	92160
Entropy (8bit):	5.664138088677901
Encrypted:	false
SSDEEP:	1536:D/BmrFjio5/vzDSPwiEKi3xGyibqZ3qOT3:9mp5SwiEKWZiTo3
MD5:	E23643C785D498FF73B5C9D7EA173C3D
SHA1:	56296F1D29FC2DCBFAA1D991C87B10968C6D3882
SHA-256:	40F423488FC0C13DED29109F8CC1C0D2CCE52ECB1BD01939EF774FE31014E0F4
SHA-512:	22E29A06F19E2DA941A707B8DA7115E0F5962617295CC36395A8E9B2A98F0239B6519B4BF4AB1DC671DEF8CD558E8F59F4E50C63130D392D1E085BBF6B710914
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%...a...a...a...h...o.....b.....r.....i.....j...a.....c.....j.`.....`...Richa..... .....PE..d....x.1".....".....\.....b.....@.....H....`..... .....|..T.....`r.....`s..8 .....text....[.....\..... ..`.rdata...-...p.....`.....@..@.data... .....@....pdata.....@..@.rsrc.....@..@.re loc.....f.....@..B.....

C:\Users\user\AppData\Local\YaR\MFC42u.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1548288
Entropy (8bit):	4.704719914724775
Encrypted:	false
SSDEEP:	12288:sVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:ZfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	9A038C371A16C9B3C62D29B74F52FEDF
SHA1:	A842D1B72E1A5549E711BA134F9B2ADED1BBC93A
SHA-256:	CD123ED5259A5A2213E159906F8DB937BCCA1667C0A3469B92576C83452E3372
SHA-512:	67782A30361ADE3F9777D49A89C67250C5DA2FFDC215EB897ED1C2E72545DD2E34C938786FCF6BED2868B67DA8812CA3B6C0A6FAD52EE9E2320D1794E375C38
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....$.....|...|...|....K.#}...'...}.....{}....X.#}....f..|....g..}..*...a|.....}....N..}..*... E}..[.I.E|...'..U}....N.+}..[.K.P|..[.K./}...I.h}..u.Y.k|.....|..W"...|..b.L.t|...|...}.....N|..2%...|..Rich.|.....PE..d.(..DN^..... .....p.....@.....@lx}..b.....0...l...c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\a5Q9CELTE\VERSION.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1523712
Entropy (8bit):	4.67079382802602
Encrypted:	false
SSDEEP:	12288:XVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:efP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	ED571DF99ACEF5ACC34ABB7B905915D5
SHA1:	484AE4125B91CD8EE87CE9E604D3667DBA97A167
SHA-256:	845EAA492DC7F66D7C1FFC14BA0620BC0E6A324DD151120420AD7B027F5D0B4A

C:\Users\user\AppData\Local\a5Q9CELTE\VERSION.dll	
SHA-512:	1FF7C353F05E92478C13060365F14D5335A4C6765158BF969EDCAC1C0BB838622839C28EB2BA814CEB31B628BF5FABAC2579C3E8353821A7BE5DBC4E5F98E67A
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.(..DN^....." ....p.....@.....@.....@lx}..b.....0..+....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\a5Q9CELTE\ie4uinit.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	221184
Entropy (8bit):	6.1390918249618585
Encrypted:	false
SSDEEP:	6144:RgDsww9O7gTBdbl6vxiBEByyrZKLeXOQPIx5mZ:0zlgfIvBjyrZwUJF
MD5:	9DD77F0F421AA9A70383210706ECA529
SHA1:	1EBEFD2674716D6302EC9AE88349CBDE52A18686
SHA-256:	8E8C4A1402E0AF960AB1FF23C8925BBC35B0F015537056CE5C51658519DE41BB
SHA-512:	17875904D790A56A08216732B60E1317F7B916258C903C24313188ECA5D948A6566F558C8F8ECE89BEB18F67B8730F98D7428EC14381C13C212BF8169EC768D5
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....7Uj.s4..s4..s4...P..p4...P..h4...P..w4...P..Z4..s4..J6...P...4...P..r4...P..r4..Richs4.....PE..d....."......6...0.....8.....@.....`..... .....|.....`...`..... ...T.....c..(....b.....c..x.....@.....text....4.....6..... ..`.rdata.....P.....:.....@..@.data.....@..... .....@....pdata.....`.....(.....@..@.didat..(.....B.....@....rsrc...`.....D.....@..@.reloc.....Z.....@..B.....

C:\Users\user\AppData\Local\br5u0t\PresentationSettings.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	222208
Entropy (8bit):	6.618425906220987
Encrypted:	false
SSDEEP:	3072:dklO/b97taQPr5pT8as3lJwvkAarSvDZpFB+2xmh0QSoKKBlKxyAZEHA:Oo/b1txPlh8I+rUts2xmhfGKraEH
MD5:	76086DD04B6760277A2B897345A0B457
SHA1:	DC65093DB601FE7AA2F4C0C400D18F43DA92DCFA
SHA-256:	BF492302281E3CD4F023FB54E101D8C3BD00FFEAFF75B5D7FE0C1CA43F291A81
SHA-512:	6528C86BA0272274A907F8559DFD79C55D1A6BAF3A4545EF3F6CDC4C790CC9FBDB7A3A8A2E72D0ED39651975DF5967608111448D1351BDC659E8F0F5E8C7244
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....._.".>.q.>.q.>.q.F~q.>.q.Z.p.>.q.Z.p.>.q.Z.p.>.q.Z.p.>.q.>.q/>.q.Z.p.>.q.Z.q.>.q.Z.p.>.qRich.>.q.....PE..d... ..8....."....J... ..... O.....@.....9....`..... .....x.....T.....a.....b.....text....H.....J..... ..`.rdata...]...`...^...N.....@..@.data...H.....@....pdata..x.....@..@.rsrc.....@..@.reloc.....b.....@..B.....

C:\Users\user\AppData\Local\br5u0t\WINMM.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1527808
Entropy (8bit):	4.679438633254575
Encrypted:	false
SSDEEP:	12288:MVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:5fP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	1A21CFA5BCFAD80861AB99E593F0B9CD
SHA1:	14083E0AD3D66E58D3BBE6BBCC58502A5454C47F
SHA-256:	5C8D6C9C0B0FF0020E27DF2E223DDB31458563D937054495A53A5E46B32458B6
SHA-512:	614C8565F28FCB52B7A48C15922CF27E34ACCE88BB704D19D499662CED45B82DDD60E3233C1169C8DE18744CF115025E5AB29BA9ACA1C650AA65B0B165AA1C6

C:\Users\user\AppData\Local\br5u0t\WINMM.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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.(..DN^....." .....0.....p.....@.....P.....@lx}..b.....0..h....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\hUhx9Ta\RdpSaUacHelper.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	29184
Entropy (8bit):	5.483991269470949
Encrypted:	false
SSDEEP:	384:x1i6wkbsVQCy+MmItEV3DAOnKjXxyWzyWpaTeinj7qHk9FyMWagW:x1TwgsmCRMmIcTRnKbQW/kj7uk2U
MD5:	DA88A7B872B1A52F2465D12CFBA4EDAB
SHA1:	8421C2A12DFF33B827E8A6F942C2C87082D933DB
SHA-256:	6A97CF791352C68EFFEFCBE3BB23357A76D93CB51D08543ED993210C56782627
SHA-512:	CA96D8D423235E013B228D05961ED5AA347D25736F8DFC4C7FEB81BFA5A1193D013CD29AA027E1793D6835E52F6557B3491520D56DE7C09F0165F1D5C8FD9ED
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....& ..bA..bA..bA..k9..`A...%..cA...%..`A...%..pA...%..uA..bA...A ...%..hA...%p.cA...%..cA..RichbA.....PE..d...?.1V....."....6...>..... =.....@.....f....`..... .....4k.....f.. T.....U.....V.....text....4.....6..... ..`.rdata...'...P...(...:.....@..@.data.....b.....@....pdata.....d..... ..@..@.rsrc.....f.....@..@.reloc.....p.....@..B.....

C:\Users\user\AppData\Local\hUhx9Ta\WINSTA.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1527808
Entropy (8bit):	4.689164819327771
Encrypted:	false
SSDEEP:	12288:9VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:kfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	6153AAE0E62E602E994A951F792A307F
SHA1:	B731C0D74529F0A0DF0CCB445D715ADAECD5642E
SHA-256:	A5CBA571E031F0E3B62F3D115A6B0BC386FCA1527A30B0ED6F92C755F4C77B50
SHA-512:	3CE2FADE0001F3C4CF17440FEBDDAB7E73F305506F879E87E77D0A37697E04C7059D3511A2071710A7153D98823D619CCA2F31B939B37BD90079ABF4A09CB86
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.(..DN^....." .....0.....p.....@.....P.....@lx}..b.....0..m....c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\ifnj9zHVv\VERSION.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1523712
Entropy (8bit):	4.670799396744364
Encrypted:	false
SSDEEP:	12288:6VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:nfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	860353B8B3E177786D05F2A2FEAD2FF9
SHA1:	E0D5FA5BEE5DF61560116CE8AACA33AE13391872
SHA-256:	6A58D432E4687914A23E76A9EFD962D6942DC154617F615CEB6FE6EBF0054088
SHA-512:	D11E9A554F5A736F57CE17A1EE13496768CDD686BEA253CCE64072D772A7FE0C636DAC118827F8C74EC1650AF0107FA074B53F984F636BDA5B33455A763BB56
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\ifnj9zHVv\VERSION.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.(..DN^....." ....p.....@.....@.....@lx}..b.....0..+....c.....h.....$#..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\ifnj9zHVv\psr.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	600576
Entropy (8bit):	6.4861677167766665
Encrypted:	false
SSDEEP:	12288:B2mS50lCmAX+ASa8wd9Nkmw6cD8pellpco//EH1:B2mlmeFSa8wd9NStApeCoXEH
MD5:	3B8262EB45E790BF7FA648CEE2CCCB7B
SHA1:	EDDD81D1B3FD2EE99E42A43B25BD74D39BB850BC
SHA-256:	D1225E9FD2834BD2EF84EADAA4126020D20F4A0F50321440190C3896E69BD5D8
SHA-512:	A3709D39372CDB6D9C9E58932144CE8BA437C2134EFC9BCD2531708C1515CBAEA5929C220DF25D76785F7594BC5F8541E6ED5330EA3CA12E87C4DA5A2171C45
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....}.....x.....x.....x.....x...x.....x.....xR.....x.....Rich.....PE..d....S.....".....`.....@.....h....`..... .....7.....L.....D.....T..... .....X...8....7..@.....text...5..... ..`.rdata.....@..@.data....m...`.....H.....@....pdata..L.....T.....@..@.didat.....j.....@....rsrc.....l.....@..@.reloc..D.....&.....@..B.....

C:\Users\user\AppData\Local\nmYaGulOu\UxTheme.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1523712
Entropy (8bit):	4.681960328473459
Encrypted:	false
SSDEEP:	12288:nVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:OfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	7F6034B455EE3B99B1A95AD8A809A85A
SHA1:	4C10BA2334C8AD676A5E1C863040309B0197FF18
SHA-256:	B504AD194233C476E7CDC5E16294C664036BB00F915228568C1716D8274366FD
SHA-512:	4507B6C43262C1C5D6034F610D46BBD8A9E91FBB18E3255778FD8ED876DED7BE97398B35C046C58C517F022E6E31070A261D7BA8586E01F9AB80790598ACA40
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....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.(..DN^....." ....p.....@.....@.....@lx}..b.....0.....c.....h.....$#..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\nmYaGulOu\msdt.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1560576
Entropy (8bit):	6.10038070749878
Encrypted:	false
SSDEEP:	24576:tnPfp054tZwxDl6XH4qvIReK1odddGdBnyE0k26kVZnBm:VC4tAqNK7utRB
MD5:	8BE43BAF1F37DA5AB31A53CA1C07EE0C
SHA1:	F2C9EB38775B91C4DE45AA25CDDDB86F5F056BF5
SHA-256:	BD59B4362F8590C5009B28830FF11B339B37FF142FB873204368905A9C843A08
SHA-512:	B30BDD7C3B71D58140F642196D5E44ED4C8B11A35DB65D37414C49F7FE64DD0C63DDEE4A0FDF5E75BB0BEB69FE0AA1D609C252F05D5661E7DCD4B6A427415C7
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\nmYaGulOu\msdt.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....+..eo..6o..6o..6...7m..6...7q..6...7@..6o..6...6...7\..6...7k..6..X6n..6 ...7n..6Richo..6.....PE..d...4....."....b...r.....]....@...._....`..... ..P....."....^..T..... .....text...`.....b..... ..`.rdata...^.....`...f.....@..@.data...p.....@....pdata..."....$.....@..@.rsrc...P.... ....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\yC4r\DUI70.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1806336
Entropy (8bit):	5.146677664163729
Encrypted:	false
SSDEEP:	12288:SVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1MX4Yc:PfP7fWsK5z9A+WGAW+V5SB6Ct4bnbMI
MD5:	35FD10B6FCDE5D28D95CDCF5404D3FC9
SHA1:	3882017D7113AD36EDDAEED7D03A7EC5D1E43952
SHA-256:	5AF3534EFB5F306B7F0F0A6BAB9E3BD6CE0A02F569FF983509A0C837B2A672AF
SHA-512:	F532A36385B91B5D02AC1197ED30FD5D2BC496357BB9CC1676621F13D6850B5C104D65CAEF6694BDE745F45DD9225EA25BE1CF9EFDF257FBA2858D18783941A
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.(..DN^....." .....p.....p.....@.....@lx}..b.....0..dQ...c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\yC4r\ProximityUxHost.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	264480
Entropy (8bit):	6.478365286411354
Encrypted:	false
SSDEEP:	6144:xSt+s2GFGbqEuzhJONjx9UVuCuHpwqr/vt9r+ULJBaBpcIFz:xStzFGbGhoPgMHpwqrHthUB6IF
MD5:	E7F0E9B3779E54CD271959C600A2A531
SHA1:	8006E2D1AA91798E48D8BFDE1EBF94A2D6BA6C0A
SHA-256:	155CE33E0E145314FE9D8911BE69B8CBBD2AC09B7B6D98363F9BAA277C71954E
SHA-512:	E10C3FD9C5F34260323CEC9E8EEDF2290F40254F0FFDCA582DB57D113B32871793CDFFF03D55941EF5E79FA8141803AB353BA4938357A4555233F2D090045338
Malicious:	false
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B..B..B..K.`.&..-..A..-...U..-...K..-..U..B..t..-...]..-...C..-..C..RichB..... .....PE..d...;.*Q....."....@..... .....&..... .....H.....T..... +.....Pa..T.....p3..(...p2.....3. .....text..... ..`.imrsiv.....rdata..... .....@..@.data...x.....@....pdata..T.....@..@. rsrc...H.....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\bc49718863ee53e026d805ec372039e9_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	4442
Entropy (8bit):	5.463883728651604
Encrypted:	false
SSDEEP:	48:jpibUB5EI/126dFX1UYvScd0BFc4rjpibUBzoXA346zDExxCVjouPUBsRwA:juo5EILdnUYv+F3uoEkJDcCVTAi
MD5:	BDF7DAB20DD2985C56270F410E71A5F3
SHA1:	3BF6E1C4EEC5CAFB952D52529FA8EF07D81C040C
SHA-256:	9F6CCFE39CDBBD3379EFE2F5B10EA7693EECE1A291EC18BE2121C17C26E5D27F
SHA-512:	9796BA0533E0A821073A139CED69AF5681B58C95C3182A9714B031697F5C4F78F3D2C7A073E4776EB28DB3135E7C98FBF768782312653E0547FD3A901E367D8B
Malicious:	false
Reputation:	unknown
Preview:	.....user.....user.....RSA1.....].....W.6.*..f..bdy+..>._WT.,K.e-..p.m...>1....4'.....u.f]...u.dJ)....3c.>T....1.5l.m. ....B..WJs.....ce.....M.7.....z..O.....A...0C..>GXc.....,...C.r.y.p.t.o.A.P.I. .P.r.i.v.a.t.e. .K.e.y....f..... .....'g.T.H..9.|.....d..... ...O.q.y..y.qK..\G.D....x.8. N.....B.yw1.R].z..S.0/...|.n....3..w..i.W.....M...?U..E.+yhro7.Q...g..n..aX..~{..... ../..=.....%y...w.@...97...pU.Qj..H-:..D.#.,V..|-.j.H._...1|.a.[.c..@.....a..zo..[.j].c.c2.od..... ..*.e$..}.C.>.3.$|.....%.C.u5.Tb...X..Z^o.....g.I.....A..X.x..J|.E.K.}...I...E..bs6j.O+. o..nc4.l.Z....[$2..*h..mB.%.....dp....D9..hv..U.q#;.;<..V.6p|..|;g4..z,.<LV0...&bWS..A]....D..P..Q. <.)...l..Q.19.|.B.n'..k>.....-.....2...],....Y(.._7.P.A...X.....v1.f.d..W_.k.F..;.....z.(.M.9p..St.R.s.....I.S...)..I...Qu{j....

Static File Info

General

File type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Entropy (8bit):	5.873565632129989
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:	PSnPApRPsG.dll
File size:	1519616
MD5:	ed37656551984cf5c1196d88c282e4aa
SHA1:	1475e0b8fd14a3a13160dc8ab28d228f3027c8b9
SHA256:	4bbd6db4f6bdad3bbcb134c53fb0886197c2880f9e9dd7a630707dbf333623f4
SHA512:	71c2f7bc62fbc229d8b73e76cd216d34215af55f609b5040024d0674cd6cbe6b25f807ba98f0fa1cecca3e990ba34b7641bf0b6d99d200bee6b455e6801d6515
SSDEEP:	12288:gVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1o:FfP7fWsK5z9A+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
.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
.nhglos	0x11a000	0x1af	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.itzo	0x11b000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.nmsaom	0x11c000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rvhi	0x11d000	0x1af	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ucrzce	0x11e000	0x389	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
.ijc	0x11f000	0xbf6	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ohvs	0x120000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rlvrc	0x121000	0x1ee	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.yjv	0x122000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.clbcyy	0x123000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.xcyn	0x124000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.boqx	0x125000	0x389	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rnlia	0x126000	0x389	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ctip	0x127000	0x5a7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.fkv	0x128000	0x1124	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pczrv	0x12a000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ibglr	0x12b000	0x3fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.uirkq	0x12c000	0x3ba	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.nzhxgg	0x12d000	0x451c2	0x46000	False	0.218607003348	data	5.76576859256	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: 7012 Parent PID: 5300

General

Start time:	23:01:25
Start date:	28/09/2021
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe 'C:\Users\user\Desktop\PSnPApRPsG.dll'
Imagebase:	0x7ff7b3380000
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: 00000001.00000002.698738573.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 7056 Parent PID: 7012

General

Start time:	23:01:26
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\PSnPApRPsG.dll',#1
Imagebase:	0x7ff622070000
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: 7092 Parent PID: 7056

General

Start time:	23:01:26
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe 'C:\Users\user\Desktop\PSnPApRPsG.dll',#1
Imagebase:	0x7ff7f3d00000
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: 00000004.00000002.761772602.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 7120 Parent PID: 7012

General

Start time:	23:01:27
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\PSnPApRPsG.dll,??0?$PatternProvider@VExpandCollapseProvider@DirectUI@@UIExpandCollapseProvider@@$00@DirectUI@@QEAA@XZ
Imagebase:	0x7ff7f3d00000
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: 00000005.00000002.677061553.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 7092

General

Start time:	23:01:28
Start date:	28/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000
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: 4388 Parent PID: 7012

General

Start time:	23:01:30
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\PSnPApRPsG.dll,??0?$PatternProvider@VGridItemProvider@DirectUI@@UIGridItemProvider@@$01@DirectUI@@QEAA@XZ
Imagebase:	0x7ff7f3d00000
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: 00000008.00000002.684710947.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 6328 Parent PID: 7012

General

Start time:	23:01:33
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\PSnPApRPsG.dll,??0?$PatternProvider@VGridProvider@DirectUI@@UIGridProvider@@$02@DirectUI@@QEAA@XZ
Imagebase:	0x7ff7f3d00000
File size:	69632 bytes

MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000009.00000002.691449064.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: tcmsetup.exe PID: 6868 Parent PID: 3424

General

Start time:	23:02:09
Start date:	28/09/2021
Path:	C:\Windows\System32\tcmsetup.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\tcmsetup.exe
Imagebase:	0x7ff65b780000
File size:	16384 bytes
MD5 hash:	0DDA495155D552D024593C4B3246C8FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: tcmsetup.exe PID: 6980 Parent PID: 3424

General

Start time:	23:02:11
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\72PXeqK\tcmsetup.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\72PXeqK\tcmsetup.exe
Imagebase:	0x7ff708130000
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: 00000012.00000002.791585057.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: RdpSaUacHelper.exe PID: 5052 Parent PID: 3424

General

Start time:	23:02:22
Start date:	28/09/2021
Path:	C:\Windows\System32\RdpSaUacHelper.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\RdpSaUacHelper.exe
Imagebase:	0x7ff79a8d0000
File size:	29184 bytes
MD5 hash:	DA88A7B872B1A52F2465D12CFBA4EDAB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: RdpSaUacHelper.exe PID: 6204 Parent PID: 3424

General

Start time:	23:02:23
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\hUhx9Ta\RdpSaUacHelper.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\hUhx9Ta\RdpSaUacHelper.exe
Imagebase:	0x7ff677470000
File size:	29184 bytes
MD5 hash:	DA88A7B872B1A52F2465D12CFBA4EDAB
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: 00000014.00000002.818480177.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Read

Analysis Process: msdt.exe PID: 1568 Parent PID: 3424

General

Start time:	23:02:35
Start date:	28/09/2021
Path:	C:\Windows\System32\msdt.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msdt.exe
Imagebase:	0x7ff7544e0000
File size:	1560576 bytes
MD5 hash:	8BE43BAF1F37DA5AB31A53CA1C07EE0C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: msdt.exe PID: 5628 Parent PID: 3424

General

Start time:	23:02:36

Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\nmYaGulOu\msdt.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\nmYaGulOu\msdt.exe
Imagebase:	0x7ff6edaf0000
File size:	1560576 bytes
MD5 hash:	8BE43BAF1F37DA5AB31A53CA1C07EE0C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000017.00000002.846583663.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities Show Windows behavior

File Read

Analysis Process: bdechangepin.exe PID: 6688 Parent PID: 3424

General

Start time:	23:02:49
Start date:	28/09/2021
Path:	C:\Windows\System32\bdechangepin.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\bdechangepin.exe
Imagebase:	0x7ff79fd40000
File size:	369664 bytes
MD5 hash:	013D00A367D851B0EC869F209337754E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: bdechangepin.exe PID: 6608 Parent PID: 3424

General

Start time:	23:02:54
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\RjGeORx\bdechangepin.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\RjGeORx\bdechangepin.exe
Imagebase:	0x7ff7a2af0000
File size:	369664 bytes
MD5 hash:	013D00A367D851B0EC869F209337754E
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.00000002.885485800.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: ProximityUxHost.exe PID: 4584 Parent PID: 3424

General

Start time:	23:03:06
Start date:	28/09/2021
Path:	C:\Windows\System32\ProximityUxHost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\ProximityUxHost.exe
Imagebase:	0x7ff6e9370000
File size:	264480 bytes
MD5 hash:	E7F0E9B3779E54CD271959C600A2A531
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ProximityUxHost.exe PID: 5376 Parent PID: 3424

General

Start time:	23:03:13
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\yC4r\ProximityUxHost.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\yC4r\ProximityUxHost.exe
Imagebase:	0x7ff70c010000
File size:	264480 bytes
MD5 hash:	E7F0E9B3779E54CD271959C600A2A531
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000001D.00000002.924400956.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: psr.exe PID: 3064 Parent PID: 3424

General

Start time:	23:03:24
Start date:	28/09/2021
Path:	C:\Windows\System32\psr.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\psr.exe
Imagebase:	0x7ff6aeb80000
File size:	600576 bytes
MD5 hash:	3B8262EB45E790BF7FA648CEE2CCCB7B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: psr.exe PID: 5152 Parent PID: 3424

General

Start time:	23:03:26
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\Tp5KLY\psr.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\Tp5KLY\psr.exe
Imagebase:	0x7ff631db0000
File size:	600576 bytes
MD5 hash:	3B8262EB45E790BF7FA648CEE2CCCB7B

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000001F.00000002.955848713.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: psr.exe PID: 1716 Parent PID: 3424

General

Start time:	23:03:39
Start date:	28/09/2021
Path:	C:\Windows\System32\psr.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\psr.exe
Imagebase:	0x7ff6aeb80000
File size:	600576 bytes
MD5 hash:	3B8262EB45E790BF7FA648CEE2CCCB7B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: psr.exe PID: 5520 Parent PID: 3424

General

Start time:	23:03:40
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\ifnj9zHVv\psr.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\ifnj9zHVv\psr.exe
Imagebase:	0x7ff6a2d70000
File size:	600576 bytes
MD5 hash:	3B8262EB45E790BF7FA648CEE2CCCB7B
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: 00000021.00000002.982719749.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: wlrmdr.exe PID: 5688 Parent PID: 3424

General

Start time:	23:03:52
Start date:	28/09/2021
Path:	C:\Windows\System32\wlrmdr.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\wlrmdr.exe
Imagebase:	0x7ff60a940000
File size:	65704 bytes
MD5 hash:	4849E997AF1274DD145672A2F9BC0827
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: wlrmdr.exe PID: 5696 Parent PID: 3424

General

Start time:	23:03:56
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\PVSXo\wlrmdr.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\PVSXo\wlrmdr.exe
Imagebase:	0x7ff70e3f0000
File size:	65704 bytes
MD5 hash:	4849E997AF1274DD145672A2F9BC0827
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: 00000024.00000002.1017398501.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: DevicePairingWizard.exe PID: 5468 Parent PID: 3424

General

Start time:	23:04:08
Start date:	28/09/2021
Path:	C:\Windows\System32\DevicePairingWizard.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\DevicePairingWizard.exe
Imagebase:	0x7ff684110000
File size:	92160 bytes
MD5 hash:	E23643C785D498FF73B5C9D7EA173C3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: DevicePairingWizard.exe PID: 2832 Parent PID: 3424

General

Start time:	23:04:14
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\YaR\DevicePairingWizard.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\YaR\DevicePairingWizard.exe
Imagebase:	0x7ff621230000
File size:	92160 bytes
MD5 hash:	E23643C785D498FF73B5C9D7EA173C3D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000026.00000002.1056321571.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: PresentationSettings.exe PID: 2108 Parent PID: 3424

General

Start time:	23:04:26
Start date:	28/09/2021
Path:	C:\Windows\System32\PresentationSettings.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\PresentationSettings.exe
Imagebase:	0x7ff63db90000
File size:	222208 bytes
MD5 hash:	76086DD04B6760277A2B897345A0B457
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: PresentationSettings.exe PID: 1072 Parent PID: 3424

General

Start time:	23:04:27
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\br5u0t\PresentationSettings.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\br5u0t\PresentationSettings.exe
Imagebase:	0x7ff7b1f30000
File size:	222208 bytes
MD5 hash:	76086DD04B6760277A2B897345A0B457
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: 00000028.00000002.1082755771.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Disassembly

Code Analysis