ID: 492663
Sample Name: 2qTIaOLW2o
Cookbook: default.jbs
Time: 22:15:13
Date: 28/09/2021
Version: 33.0.0 White Diamond

Table of Contents

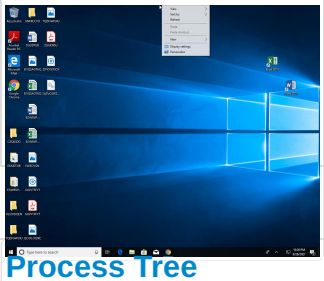
Windows Analysis Report 2qTIaOLW2o

Overview

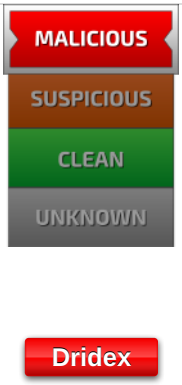
General Information

Sample Name:	2qTIaOLW2o (renamed file extension from none to dll)
Analysis ID:	492663
MD5:	8ad564b939e5a7..
SHA1:	8cd069a890ab23..
SHA256:	1fa221f1d5a2c00..
Tags:	Dridex exe
Infos:	

Most interesting Screenshot:



Detection

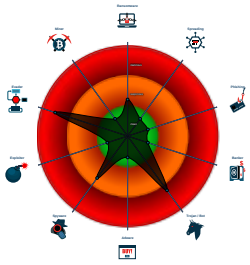


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- Contains functionality to hide window…
- Queues an APC in another process …
- Machine Learning detection for dropp…
- Contains functionality to automate e…
- Uses Atom Bombing / ProGate to in…
- Queries the volume information (nam…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 5360 cmdline: loaddll64.exe 'C:\Users\user\Desktop\2qTIaOLW2o.dll' MD5: E0CC9D126C39A9D2FA1CAD5027EBBD18)
  - cmd.exe (PID: 5532 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\2qTIaOLW2o.dll',#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 5612 cmdline: rundll32.exe 'C:\Users\user\Desktop\2qTIaOLW2o.dll',#1 MD5: 73C519F050C20580F8A62C849D49215A)
      - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
        - SndVol.exe (PID: 2540 cmdline: C:\Windows\system32\SndVol.exe MD5: CDD7C7DF2D0859AC3F4088423D11BD08)
        - SndVol.exe (PID: 4928 cmdline: C:\Users\user\AppData\Local\cAlXLQGkN\SndVol.exe MD5: CDD7C7DF2D0859AC3F4088423D11BD08)
        - tabcal.exe (PID: 1488 cmdline: C:\Windows\system32\tabcal.exe MD5: F04F239BA5FED275E652372222D1BE00)
        - tabcal.exe (PID: 6012 cmdline: C:\Users\user\AppData\Local\CsJaRZ\tabcal.exe MD5: F04F239BA5FED275E652372222D1BE00)
        - ProximityUxHost.exe (PID: 4660 cmdline: C:\Windows\system32\ProximityUxHost.exe MD5: E7F0E9B3779E54CD271959C600A2A531)
        - ProximityUxHost.exe (PID: 1692 cmdline: C:\Users\user\AppData\Local\rPj\ProximityUxHost.exe MD5: E7F0E9B3779E54CD271959C600A2A531)
        - msinfo32.exe (PID: 3060 cmdline: C:\Windows\system32\msinfo32.exe MD5: C471C6B06F47EA1C66E5FAA8DFCEF108)
        - msinfo32.exe (PID: 2616 cmdline: C:\Users\user\AppData\Local\52smNq1W\msinfo32.exe MD5: C471C6B06F47EA1C66E5FAA8DFCEF108)
        - dpapimig.exe (PID: 5972 cmdline: C:\Windows\system32\dpapimig.exe MD5: EE7DB7B615B48D8F9F08FAE70CAF46D7)
        - dpapimig.exe (PID: 4628 cmdline: C:\Users\user\AppData\Local\famGrLP\dpapimig.exe MD5: EE7DB7B615B48D8F9F08FAE70CAF46D7)
        - dpapimig.exe (PID: 3104 cmdline: C:\Windows\system32\dpapimig.exe MD5: EE7DB7B615B48D8F9F08FAE70CAF46D7)
        - dpapimig.exe (PID: 1576 cmdline: C:\Users\user\AppData\Local\y7FgRNmA\dpapimig.exe MD5: EE7DB7B615B48D8F9F08FAE70CAF46D7)
        - SystemPropertiesPerformance.exe (PID: 5336 cmdline: C:\Windows\system32\SystemPropertiesPerformance.exe MD5: F325976CDC0F7E9C680B51B35D24D23A)
        - SystemPropertiesPerformance.exe (PID: 612 cmdline: C:\Users\user\AppData\Local\hbyq\SystemPropertiesPerformance.exe MD5: F325976CDC0F7E9C680B51B35D24D23A)
  - rundll32.exe (PID: 240 cmdline: rundll32.exe C:\Users\user\Desktop\2qTIaOLW2o.dll,??0?$PatternProvider@VExpandCollapseProvider@DirectUI@@UIExpandCollapseProvider@@$00@DirectUI@@QEAA@XZ MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 2920 cmdline: rundll32.exe C:\Users\user\Desktop\2qTIaOLW2o.dll,??0?$PatternProvider@VGridItemProvider@DirectUI@@UIGridItemProvider@@$01@DirectUI@@QEAA@XZ MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5156 cmdline: rundll32.exe C:\Users\user\Desktop\2qTIaOLW2o.dll,??0?$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
00000002.00000002.322869708.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
0000001C.00000002.412511294.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000021.00000002.441901323.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000008.00000002.253887228.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000004.00000002.245204685.0000000140001000.00000020.00020000.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
Click to see the 7 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Machine Learning detection for dropped file

E-Banking Fraud:

Yara detected Dridex unpacked file

Protection of GUI:

Contains functionality to hide windows to a different desktop

HIPS / PFW / Operating System Protection Evasion:

Benign windows process drops PE files

Changes memory attributes in foreign processes to executable or writable

Queues an APC in another process (thread injection)

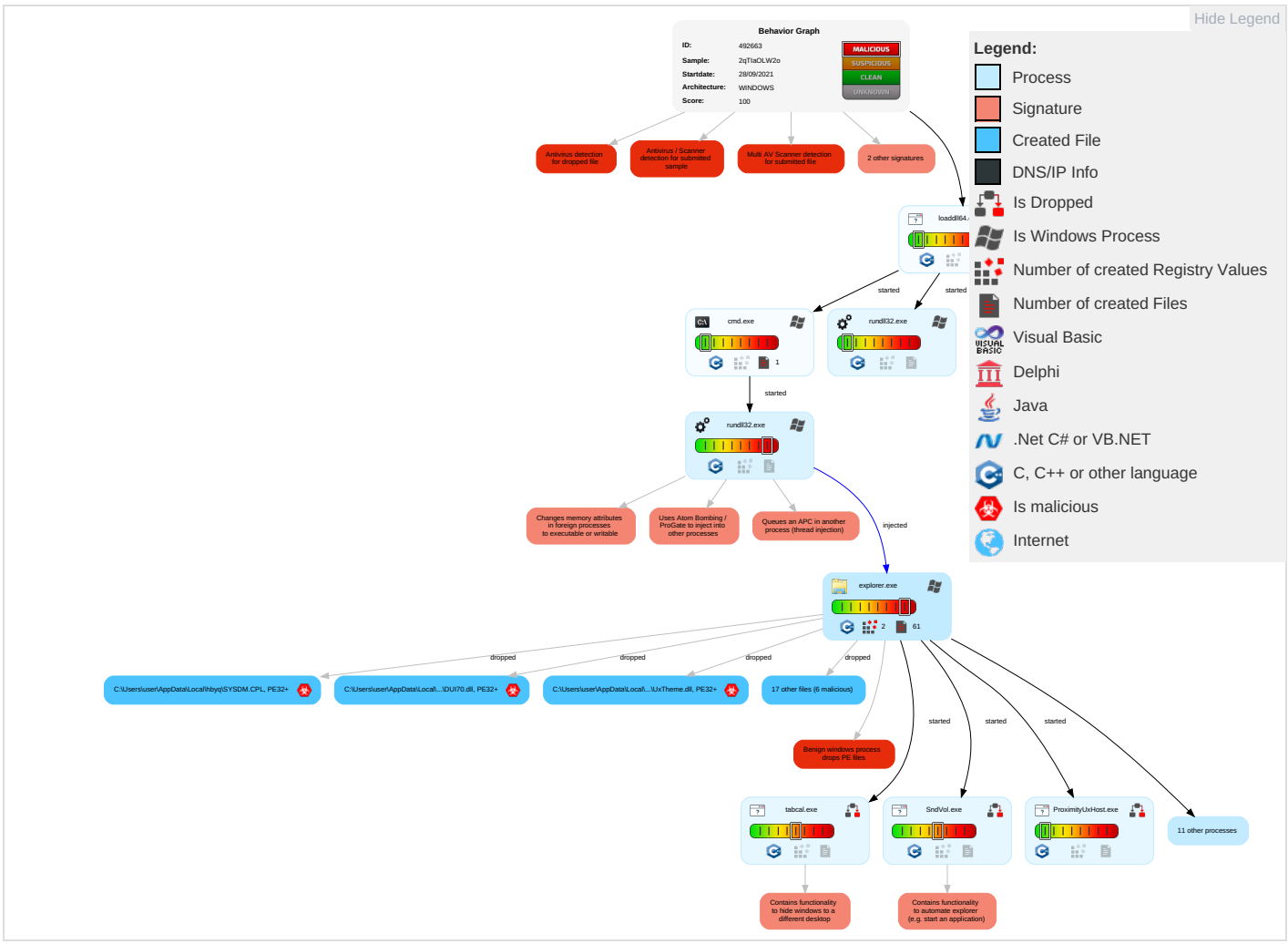
Contains functionality to automate explorer (e.g. start an application)

Uses Atom Bombing / ProGate to inject into other processes

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Commar and Con
Valid Accounts	Exploitation for Client Execution 1	Create Account 1	Exploitation for Privilege Escalation 1	Masquerading 1 1	Input Capture 1 1	System Time Discovery 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypte Channel
Default Accounts	Scheduled Task/Job	Registry Run Keys / Startup Folder 1	Process Injection 3 1 2	Virtualization/Sandbox Evasion 1	LSASS Memory	Security Software Discovery 2 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Junk Dat
Domain Accounts	At (Linux)	DLL Side-Loading 1	Registry Run Keys / Startup Folder 1	Process Injection 3 1 2	Security Account Manager	Virtualization/Sandbox Evasion 1	SMB/Windows Admin Shares	Clipboard Data 2	Automated Exfiltration	Steganog
Local Accounts	At (Windows)	Logon Script (Mac)	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Imperson
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Window 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	System Information Discovery 3 5	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Commun
External Remote Services	Scheduled Task	Startup Items	Startup Items	Rundll32 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Common Used Por
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicatio Layer Pro
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 Prot
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	DLL Side-Loading 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Trans Protocols

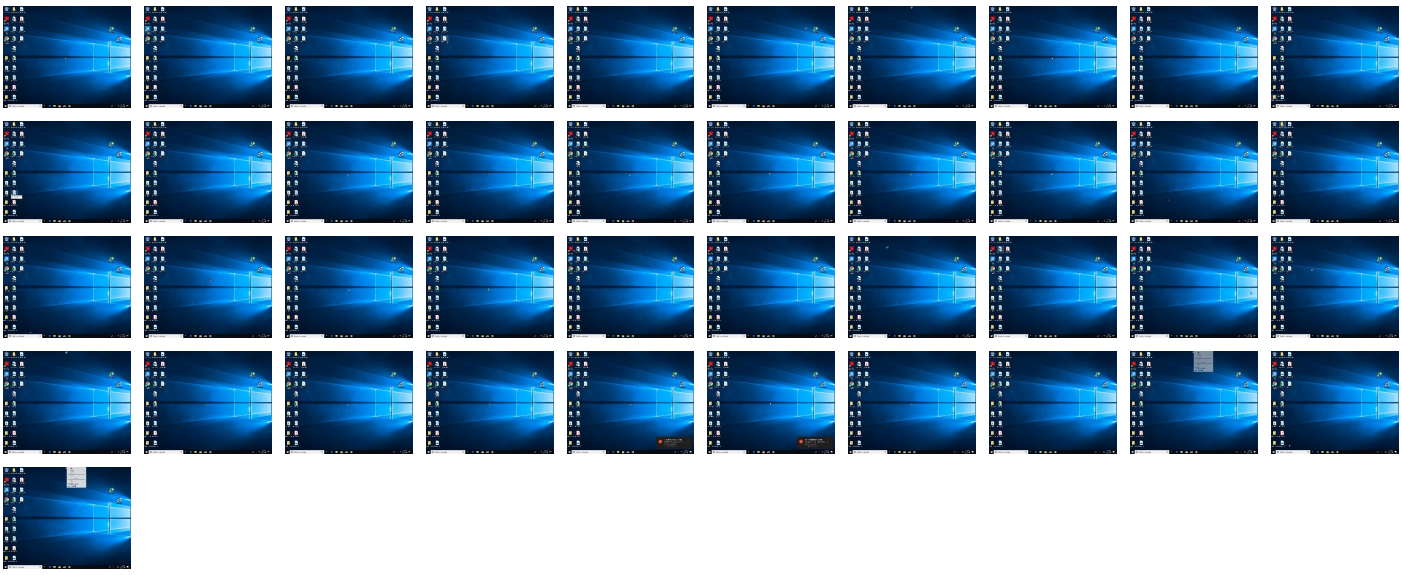
Behavior Graph



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
2qTIaOLW2o.dll	68%	Virustotal		Browse
2qTIaOLW2o.dll	76%	ReversingLabs	Win64.Infostealer.Dridex	
2qTIaOLW2o.dll	100%	Avira	HEUR/AGEN.1114452	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\ScS40sYu\dwmapi.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\cAIXLQGkN\UxTheme.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\CsJaRZ\HID.DLL	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\famGrLP\DUI70.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\famGrLP\DUI70.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\ScS40sYu\dwmapi.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\N52IORg\WTSAPI32.dll	100%	Avira	TR/Crypt.ZPACK.Gen	
C:\Users\user\AppData\Local\52smNq1W\SLC.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\hbyq\SYSDM.CPL	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\famGrLP\DUI70.dll	100%	Avira	HEUR/AGEN.1114452	
C:\Users\user\AppData\Local\ScS40sYu\dwmapi.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\cAIXLQGkN\UxTheme.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\CsJaRZ\HID.DLL	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\famGrLP\DUI70.dll	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\famGrLP\DUI70.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\ScS40sYu\dwmapi.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\N52IORg\WTSAPI32.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\52smNq1W\SLC.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\hbyq\SYSDM.CPL	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\famGrLP\DUI70.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\52smNq1W\msinfo32.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\52smNq1W\msinfo32.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\CsJaRZ\tabcal.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\CsJaRZ\tabcal.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\N52IORg\rdpinit.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\N52IORg\rdpinit.exe	2%	ReversingLabs		
C:\Users\user\AppData\Local\ScS40sYu\GamePanel.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\ScS40sYu\GamePanel.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
38.2.dpapimig.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
24.2.tabcal.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
35.2.dpapimig.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
22.2.SndVol.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
28.2.ProximityUxHost.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.loaddll64.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
40.2.SystemPropertiesPerformance.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.2.rundll32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
33.2.msinfo32.exe.140000000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

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

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	492663
Start date:	28.09.2021
Start time:	22:15:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	2qTIaOLW2o (renamed file extension from none to dll)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	41
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@45/21@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 22.4% (good quality ratio 12.7%) • Quality average: 41.3% • Quality standard deviation: 42.3%
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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\52smNq1W\msinfo32.exe	HGFrrT5cBg.dll	Get hash	malicious	Browse	
	wKfbxvfLA7.dll	Get hash	malicious	Browse	
	YZz3lg22hZ.dll	Get hash	malicious	Browse	
	gSrnekbzWz.dll	Get hash	malicious	Browse	
	CKkP707sai.dll	Get hash	malicious	Browse	
	D5v1a7JiAH.dll	Get hash	malicious	Browse	
	rJyP5pxSI7.dll	Get hash	malicious	Browse	
	88BSEM1lkN.dll	Get hash	malicious	Browse	
	vZj1JjJAy2.dll	Get hash	malicious	Browse	
	eQXkEkSQhL.dll	Get hash	malicious	Browse	
	YO7iRsM7tG.dll	Get hash	malicious	Browse	
	l7ytx2QXnx.dll	Get hash	malicious	Browse	
	QWgClRWFNy.dll	Get hash	malicious	Browse	
	470DeIOhtD.dll	Get hash	malicious	Browse	
	Us23xitkTH.dll	Get hash	malicious	Browse	
	Zb6sV9ey4t.dll	Get hash	malicious	Browse	
	l8r3L9j0OV.dll	Get hash	malicious	Browse	
	t7jfSji774.dll	Get hash	malicious	Browse	
	oCyvFsS0pj.dll	Get hash	malicious	Browse	
	Hc3Lunec1q.dll	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\52smNq1W\SLC.dll

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1507328
Entropy (8bit):	4.714933571001978
Encrypted:	false
SSDEEP:	12288:9VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1/1:kfP7fWsK5z9A+WGAW+V5SB6Ct4bnb/1
MD5:	931F07A0FF47CF3564D15E608659ED58
SHA1:	1015C7CCD1235FE1F983EE7644FDE582389FB000
SHA-256:	588D87F044D8503B5467BBA8C3007164F14BAE891DE3D4D59A221991CB1F4AFE
SHA-512:	25BEFE8EF97D40D2260C362A8A0E944B2D49A4AD5EFDE8AF8C816049865252BCB7FF6AB26DF8C2A06C954324678B50CEF638E28FB72A1B26A3F47CF3B081CAAB
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.#..DN^....." .....p.....@.....@lx}..b.....3....c.....h.....$#..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\52smNq1W\msinfo32.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	370176
Entropy (8bit):	6.448503897594857
Encrypted:	false
SSDEEP:	6144:Uca2EiZg+uTUbSFWjSJilOKZXcmg3GexhxiZEOHHrpm1XUZLxEZEOHHrpm1XUZLx:UB2PsUbSFWWAkZXcmkVx+tLpm1EwtLpr
MD5:	C471C6B06F47EA1C66E5FAA8DFCEF108
SHA1:	F8672A2B3B32956CBC948A954CEF236581045B78
SHA-256:	E2255751C1CF58596C8FE70C3093E099F8D71ED89580CFD0156FFCF0FED32861
SHA-512:	F7A2A31910CD4694B58FFCED83A2CCF633B5594859F178AFB9F67C02E3E664DA72701E7E45AA5590C4F1E1C99C82B665F0C0B80401506F0DFA49B61A8EEBD6EA
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Users\user\AppData\Local\52smNq1W\msinfo32.exe

Joe Sandbox View:	• Filename: HGFrrT5cBg.dll, Detection: malicious, Browse • Filename: wKfbxvfLA7.dll, Detection: malicious, Browse • Filename: YZz3lg22hZ.dll, Detection: malicious, Browse • Filename: gSrnekbzWz.dll, Detection: malicious, Browse • Filename: CKkP707sai.dll, Detection: malicious, Browse • Filename: D5v1a7JiAH.dll, Detection: malicious, Browse • Filename: rJyP5pxSI7.dll, Detection: malicious, Browse • Filename: 88BSEM1IkN.dll, Detection: malicious, Browse • Filename: vZj1JjJAy2.dll, Detection: malicious, Browse • Filename: eQXkEkSQhL.dll, Detection: malicious, Browse • Filename: YO7iRsM7tG.dll, Detection: malicious, Browse • Filename: l7ytx2QXnx.dll, Detection: malicious, Browse • Filename: QWgClRWFNy.dll, Detection: malicious, Browse • Filename: 470DelOhtD.dll, Detection: malicious, Browse • Filename: Us23xitkTH.dll, Detection: malicious, Browse • Filename: Zb6sV9ey4t.dll, Detection: malicious, Browse • Filename: l8r3L9j0OV.dll, Detection: malicious, Browse • Filename: t7jfSji774.dll, Detection: malicious, Browse • Filename: oCyvFsS0pj.dll, Detection: malicious, Browse • Filename: Hc3Lunec1q.dll, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|....y...y...y..yz...y..y}...y..y\|...y..yx...y...x...y..yp...y..y....y..y{...y.Rich..y.....PE..d....a....."....@.....0.....`..... .....$...h.....xJ.....(..... .. ...P...T.....P..... ....P... .....text..... ..`.rdata..H*.....,.....@..@.data....k...@.....(.....@....pdata..(.....D.....@..@.rsrc...xJ.....L...V..... ..@..@.reloc.. ....@..B..... .....

C:\Users\user\AppData\Local\CsJaRZ\HID.DLL

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1507328
Entropy (8bit):	4.715367229885423
Encrypted:	false
SSDEEP:	12288:EVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:hfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	1B5413AD9E40CC700FF62DE89BAF56BE
SHA1:	1D7D75FC0645F2FD05DAF0FF475169DF707E5CCF
SHA-256:	5CA62F2EF0BF9E37DAF51EAD56EC7BCB3BA7F2B5CB55AD2023A2040C40C00C7A
SHA-512:	773133FDCFF1D9746B019B52125F501ADAF86DF362829F91A49E80C2B51C795D7793E35C9CCC766B662CF15411CCD5BE34071304BE4458C5D33ABF0F9EB789B
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
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\CsJaRZ\tabcal.exe

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	82944
Entropy (8bit):	5.705817452511626
Encrypted:	false
SSDEEP:	1536:Q77RYSqLmKbndnBRdv2RWUUTtj11VM0bJDrdfW2jbJK:QuxLmKbndDdv2WUczVMKrdfZbs
MD5:	F04F239BA5FED275E652372222D1BE00
SHA1:	883C7915ADD2B47D1012E52321D670A4A29ABB53
SHA-256:	CE81E5BFF4C0A646EFD86791DB938A7F5E148666F518990B156FE208F8454423
SHA-512:	61B80BC6E68057C425C624DC4FC8A551F60F6E4DA60A7F5A6D6520FE92E0B61D1B63B16DF70A5019C3F0AFFE8064CD072BBADC3C69E1DB8833E1E3ABA9C455 29
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....d.. ... ...).`.>...O..."...O...2...O...&...O...7... ...$...O...)...O...!...O.. .!...Rich .....PE..d...r.T,....."....@.....&.....`..... .....0..@r.....|...p...T..... .....text...J..... ..`.rdata..f4.....6.....@..@.data....!.....@....pdata.....@..@.didat..P.... ....@....rsrc...@r...0...t.....@..@.reloc..|.....B.....@..B..... .....

C:\Users\user\AppData\Local\N52IORg\WTSAPI32.dll

Process:	C:\Windows\explorer.exe

C:\Users\user\AppData\Local\N52IORg\WTSAPI32.dll	
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1507328
Entropy (8bit):	4.719488777601788
Encrypted:	false
SSDEEP:	12288:JVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:ofP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	977F0FAC6FBFF743D7F33651AAE2FAE7
SHA1:	B1011C13AC6088B70FB838D62F360894871CCCF1
SHA-256:	2A9205980480DFA5839343742120B4AFE90EA0C23BD6BEB95F62AADDF81D0E5C
SHA-512:	798865671A7F428DFF7D65D969E8AD2AD591180C1EA599943FA43F6B3FBCCC9EA0507F4EBC20643FFA60649417E5DEFED446024EC810B1649624C684D4C3ABE E
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
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\N52IORg\rdpinit.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	327168
Entropy (8bit):	6.414070673036673
Encrypted:	false
SSDEEP:	6144:fOzsB7eGjsO+VxyQ/qY4gCJkxkVPXqdzVxNwK3S3drxhUS4eMZfCZc/o:fOzsB7eGjb+VxynJkxkZ6dzV63drxhlF
MD5:	EF7C9CF6EA5B8B9C5C8320990714C35D
SHA1:	9CBD44DE4761F9383F2E0352035D52B86ECE80C2
SHA-256:	0FD9B6C366E042ED83BFC53C5EA1AAF43F13F53D97F220B5571681BB766C33FA
SHA-512:	C2F5E902DF725BC05F03052042767635689A35226CA1C3436ADF4835C57666B3E815FD386B80517734AC3B71F2FB15E48CE2F6739D669B5F68F4A8989713E8FC
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 2%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s.....S...S...S.j.S...S.v.R...S.v.R...S.v.R...S.v.R...S...S...S.v.R...S .vmS...S.v.R...SRich...S.....PE..d...q....."....."....f..... .....@.....p.....+..... .....@....@.....d .....`..x.....T..... .....text...<..... ..`.imrsiv.....rdata.....@..@.data....:.....@....pdata..d ..... ".....@..@.rsrc.....@.....@..@.reloc..x....`.....@..B..... .....

C:\Users\user\AppData\Local\ScS40sYu\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:	0494166D4AE6BB7925E4F57BB6DFAC629C95AE9E03DFC925F82328932 36BD982
SHA-512:	C122CD7A245EF6A6A7B7DECAB6500BDC11E4C57B8E35F8462CC0615E44E54071E6BF79B69BB8519470ACBAF0D2E62ABC45C38CBF0606261792EDB4A84790E 61
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
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\ScS40sYu\dwmapi.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows

C:\Users\user\AppData\Local\ScS40sYu\dwmapi.dll	
Category:	dropped
Size (bytes):	1507328
Entropy (8bit):	4.7172480760765225
Encrypted:	false
SSDEEP:	12288:QVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:VfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	F0C1C0EFA6B7AA1310B6396A0C7792B8
SHA1:	70EBE0CDC6B1B58E63DEC768585E43A61CC04104
SHA-256:	FBD29EC92724DA370034AE036C4BA84B1E5950E6610195E1F67A2F79F939D3F8
SHA-512:	06F5B9FF6300097D4D4BE0FD38159FDBA325A9910856925851EF7ADE5ED2FC3F2CA52995A1FC48C8C345ABEDF59536DC11E8B24D41DE41BEE05FE7AA8C7D9F E9
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
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\cAIXLQGkN\SndVol.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	259904
Entropy (8bit):	5.955701055747905
Encrypted:	false
SSDEEP:	3072:UfYIZJbRydnidilSnGvLqeD358rwW39nuyHjVozZcxSHfcBL1ljbEyB7HbIa+:Uf9JonidFnqLV358rNnJqcRcy10/
MD5:	CDD7C7DF2D0859AC3F4088423D11BD08
SHA1:	128789A2EA904F684B5DF2384BA6EEF4EB60FB8E
SHA-256:	D98DB8339EB1B93A7345EECAC2B7290FA7156E3E12B7632D876BD0FD1F31EC66
SHA-512:	A093BF3C40C880A80164F2CAA87DF76DCD854375C5216D761E60F3770DFA04F4B02EC0CA6313C32413AC99A3EBDC081CF915A7B468EE3CED80F9B1ECF4B498 4
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....<.BL]..L]..L]..E%...]..#9..O]..#9..U]..#9..F]..#9..W]..L]...\..#9..o].. #9k.M]..#9..M]..RichL].....PE..d...wJSn.....".....@.....@..... ....p.... ..@.....@+...0..... ..U..T.....p&..(...p%.....&.....P.....text..... ..`.imrsiv.....rdata..... .....@..@.data.....@.. ..pdata.....@..@.didat.....@....rsrc...@.... .....@..@.reloc.....0.....@..B..... .....

C:\Users\user\AppData\Local\cAIXLQGkN\UxTheme.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1507328
Entropy (8bit):	4.722422114873919
Encrypted:	false
SSDEEP:	12288:7VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:afP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	68DE2990C8FE0CE0A8E8D7FC6D5476F7
SHA1:	DA109B2BD225C4A8684EC6180597721B3A59D218
SHA-256:	660AB33F14DF750EFCB35D432C96636CDDC072934C49E66BFE5414BEDBD4FF3C
SHA-512:	7E69341AA3D59EBF67E0C83858BE75BE4BB0498A5B2CFF6CB227F30430D6DED9402DC649D7246FA440DE97691352B9E12839825343B85ED4483B13F885BF9533
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
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\famGrLP\DUI70.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1789952

C:\Users\user\AppData\Local\famGrLP\DUI70.dll	
Entropy (8bit):	5.183242701242126
Encrypted:	false
SSDEEP:	12288:rVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1Zy:qfP7fWsK5z9A+WGAW+V5SB6Ct4bnbZ
MD5:	C7F2912674EC4F16E8BB5950E583BD8C
SHA1:	F6E8E4206F69AC4E7D6CE7D5CA6BEF04A14AEE98
SHA-256:	98A46C671364D336B6EED344EF0ECBD4E4D534E2754F8EA281305D66B87F7773
SHA-512:	291A48B6F3BA34F0F4DCB8E040C94C3D9341FBCF5DBEA46C46B6DBC1917F8B7258C650DA579DDAA01645988A68BED29ED8DFB63521A0544C3182174D77F7E79
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%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*...E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.#..DN^....." .....0.....p.....@.....P.....@\|x}..b.....dQ...c.....h.....$#..... .....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata.,.....A..@.rsrc.....@..@.reloc..$#....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\famGrLP\dpapimig.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	76800
Entropy (8bit):	5.908989367752963
Encrypted:	false
SSDEEP:	1536:CzbG9gXEurcYIZh800l3uU1HIED1fCbWpygzU:obezur2hrSJj16bE
MD5:	EE7DB7B615B48D8F9F08FAE70CAF46D7
SHA1:	FB5021297FDF24000ADD478164EEC8048871B335
SHA-256:	7999B821F8A673B0528C8F5F72A68A61393BEF78785FC1B4A0B3938D8CDD14B8
SHA-512:	F2292577166A330409813215DD49F2A276739AB51621316FBD418A377F4FD2476E50720A88F3069D16146E5C57DF47B21D800089EE48B28158BCBCFE3B6776AB
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....nx..nx..nx.....nx...{..nx...|..nx...}..nx...y..nx..ny..nx...q..nx.....nx...z..nx.Rich.nx.....PE..d...Y.....".....".....@'.....@.....+....`..... .....L.....@.....p..P....H..T.....@.....A.....text.... .....".....  ..`.rdata... ...@..."...&.....@..@.data.....p.....H.....@....pdata.....J.....@..@.rsrc...@.....L.....@..@.reloc..P....p.....*.....@..B.....

C:\Users\user\AppData\Local\hbyq\SYSDM.CPL	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1507328
Entropy (8bit):	4.710638800025406
Encrypted:	false
SSDEEP:	12288:8VI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:JfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	68DF43064563A92810B1367FF511759D
SHA1:	D09AF560BA699A11552E885A11D855B6233D194D
SHA-256:	365C3153CB477FF992F9E21BF6CB1F6A4C9C61E8219980B4B311C6B61D639345
SHA-512:	BFC3FD937C7D1F16236B88F24A4F5C915DB82FCBBC2C7B941D96A4E32F7156E5A1AABC81AEBE5B9317558A3DE7855EEC18DA5E4A5F776B665886D45E795598E5
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
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\hbyq\SystemPropertiesPerformance.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	83968

C:\Users\user\AppData\Local\hbyq\SystemPropertiesPerformance.exe	
Entropy (8bit):	7.071848641739436
Encrypted:	false
SSDEEP:	1536:5MVEZnXtREC/rMcgEPJV+G57ThjEC0kzJP+V5J9:3XzECTMpuDhjRVJGf
MD5:	F325976CDC0F7E9C680B51B35D24D23A
SHA1:	8BA00280B451378802DD2A06BB139B8BEA78C90C
SHA-256:	E24A61B15FD191DDC8A2CA82E22A759609E6099A832ADE0B5C0C6E0F1ABB05FE
SHA-512:	9D65A154758B5C38C09AACA1BB51E53FE6E8DEA374EAD88AEA33AB41525B3BB180211D6F6C93CA112197F7455842228960699DF471F47EE83DBC6CA59A5166EC
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....E.v..c...c...c.....c..n....c..n....c..n....c..n...c..c.."c..n....c..n...c..n.. ..c..Rich.c.....PE..d...0....."..... >.....@.....s...`..... .....<&.....P..P'...@..... ....#..T..... .....!..H.....text..... ..`.rdata..... .....@..@.data.....0.....@....pdata.....@.....@..@.rsrc...P'...P...(..... .....@..@.reloc.. .....F.....@..B..... .....

C:\Users\user\AppData\Local\rPj\DUI70.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1789952
Entropy (8bit):	5.18332372992189
Encrypted:	false
SSDEEP:	12288:IVI0W/TtlPLfJCm3WIYxJ9yK5lQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1Ry:dfP7fWsK5z9A+WGAW+V5SB6Ct4bnbR
MD5:	10B3C5DF9285A3ECF64198911AC01974
SHA1:	D4A99A0992F267974BF4463A35990DFAE443BA36
SHA-256:	94670AEE3C795FF8FC8D0829B626D2D02B516259F875CF6C7CA1E6B709EA99A1
SHA-512:	53DC073092979D1E2D3F7F89AD0A4A6DF1285A28A74DEA66AE7EEF9D398AA82E6FF486A2CD514DCFD5314177F777C91C10A1A94963B1C0B707919DBFE8867B2
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.# ..DN^....." .....0.....p.....@.....P.....@lx}..b.....dQ...c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\rPj\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
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B..B..B..K.`.&..-..A..-...U..-...K..-..U..B..t..-...]..-...C..-..C..RichB..... .....PE..d...;.*Q....."..... .....@..... .....&..... .....H.....T..... +.....Pa..T.....p3..(...p2.....3. .....text..... ..`.imrsiv.....rdata..... .....@..@.data...x.....@....pdata..T.....@..@. rsrc...H.....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Local\xOu8\LockScreenContentServer.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	47600
Entropy (8bit):	6.182394161787695
Encrypted:	false
SSDEEP:	768:0SD9dkiWX/i7Ek29r9Hu53ldEkUZGYP7loL1Prco:pVKFudldlUZGYP7loPwo
MD5:	45E51238434FAF543D66E17EF3783413
SHA1:	1CE0BA884E5C2ADA74A34D10F32A5E7431C66411
SHA-256:	DAFF63C2C374463E0CF476B5CBADF2D58D0DADE0BB0C29DDAE543A69BA34FB93

C:\Users\user\AppData\Local\xOu8\LockScreenContentServer.exe	
SHA-512:	353467F3477B136909C1AD0206A3E9CA84AC9104B386529345BBEBABFCA1B3239F6C0B387C2C1018B937885144D43ACAADA264EB4D266B815A632A3DFEDEB33 1
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....4E..gE..gE..gL.4gg..g*..fG..g*..fQ..g*..fB..g*..fT..gE..g...g*..fC..g *.XgD..g*..fD..gRichE..g.....PE..d...|dV.....".....>...Z.....@.....@.....` ..... .....h..... .....#.....L....a..T. .....U..(....T.....U.....text....<.....>..... ..`.rdata..`@...P...B...B.....@..@.data.....@....pdata..... @..@.rsrc... .....@..@.reloc..L.....@..B.....

C:\Users\user\AppData\Local\xOu8\dwmapi.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1507328
Entropy (8bit):	4.717208456102618
Encrypted:	false
SSDEEP:	12288:IVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1:dfP7fWsK5z9A+WGAW+V5SB6Ct4bnb
MD5:	ED1EC4C1EFFCC510E3B9663B916CEE94
SHA1:	A5D5CDE05C3D219B38D2478154BDD2303400E4B3
SHA-256:	E928425FDDD9EF3FBF255CD067DB453417ABACDB1BC9B50473A36CD655E804FC
SHA-512:	B4E4D48CF37D2463E67FFE62467BBA163FA33AA26ABB475D80076A04006560A225137D8D7F4B36B50D608EB52C437B04A1BC31928EC6EEBA11000F51A284B6F9
Malicious:	false
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\y7FgRNmA\DUI70.dll	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1789952
Entropy (8bit):	5.18319370146472
Encrypted:	false
SSDEEP:	12288:PVI0W/TtlPLfJCm3WIYxJ9yK5IQ9PElOlidGAWilgm5Qq0nB6wtt4AenZ1mrGy:mfP7fWsK5z9A+WGAW+V5SB6Ct4bnbmy
MD5:	F00DC6D1F73547993C34EFBDB69108E2
SHA1:	3AF5EB57D1D583986B1E77D18208423F236316FA
SHA-256:	8384EAFCD2DE1D1275528DE3114E3A0A643233C9F5F10F65D2A235FB836BF26C
SHA-512:	A5ACA81A6E905F71E5F19CD9550C346027FD02EF4F660CB87D2A4F7639939092CF7DFC137290448774AD26A2823E003FEB5B501C1BD425EA6746B90281A647AC
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....\|...\|...\|....K.#}...'...}.....{}....X.#}....f..\|....g..}..*...a\|.....}....N..}..*... E}..[.I.E\|...'..U}....N.+}..[.K.P\|..[.K./}...I.h}..u.Y.k\|.....\|..W"...\|..b.L.t\|...\|...}.....N\|..2%...\|..Rich.\|.....PE..d.# ..DN^....." .....0.....p.....@.....P.....@lx}..b.....dQ...c.....h.....$#..... ....text..... ..`.rdata...O... ...P... .....@..@.data....x...p.....p.....@....pdata..,.....A..@.rsrc.....@..@.reloc..$#... ....0.....@..B.qkm....J....@.....@.....@..@.cvjb...f...

C:\Users\user\AppData\Local\y7FgRNmA\dpapimig.exe	
Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	76800
Entropy (8bit):	5.908989367752963
Encrypted:	false
SSDEEP:	1536:CzbG9gXEurcYIZh800l3uU1HIED1fCbWpygzU:obezur2hrSJj16bE
MD5:	EE7DB7B615B48D8F9F08FAE70CAF46D7
SHA1:	FB5021297FDF24000ADD478164EEC8048871B335
SHA-256:	7999B821F8A673B0528C8F5F72A68A61393BEF78785FC1B4A0B3938D8CDD14B8
SHA-512:	F2292577166A330409813215DD49F2A276739AB51621316FBD418A377F4FD2476E50720A88F3069D16146E5C57DF47B21D800089EE48B28158BCBCFE3B6776AB
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....nx..nx..nx.....nx...{..nx...|..nx...}..nx...y..nx..ny..nx...q..nx.....nx... z..nx.Rich.nx.....PE..d...Y.....".....".....@'.....@.....+....` ..... .....L.....@.....p..P....H..T..... .....@.....A.....text.... .....".....  ..`.rdata... ...@..."...&.....@..@.data.....p.....H.....@....pdata.....J.....@..@.rsrc...@..... .....L.....@..@.reloc..P....p.....*.....@..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):	5.462775166120593
Encrypted:	false
SSDEEP:	48:JfSr3rUT4mr/exe2enZ6bIQTVlofSr3rUTUi/Cjy76ziFDEXfQk3g8Tduoq:JfoWyM2eFfo1i/wtzLvQk3Huoq
MD5:	143CF11BF139B3754CAA7FE5CBC79A38
SHA1:	0825B6D02AAC1B9494B0F9AE7AEBA321E12B4025
SHA-256:	DFED9C74937B0C99C8B8E1F742BDC22EA1EC3F6D09A8FF96DB342905B2766794
SHA-512:	8CC1EE998E11AFB2F0468B2502477425D61D273B4D39ED832212A49CE33481C61D2BD0C90B15A7AF8B3B707326D7251086E20D54C640A83C29D1017F7CAF5152
Malicious:	false
Preview:	.....user.....user.....RSA1.....3Ot...y.~.*.1..4..5.]. ...t:..0.|...5...#..l...:.R|6.._a.^.`a..w..h..h0.n.w.../;..}{....S...Nc.hp.~^..6..2....y.....z..O.....{R.uH.....,...C.r.y.p.t.o.A.P.I. .P.r.i.v.a.t.e. .K.e.y....f..... ....h~...D..Y...{....[{{...O.P..... ...;..X..n.C.Z"v.W.....\....2r.=.....Va.!....a.[.D...|....h.....:t.h.:T.X!...N.p...e...l..*x.....r..N0....*jV...u.Q.>..u.#...B.....F.....S,.0.G.[.!....n..O<.wQ.....X?.....@k.[.....<.~.%0..e...b.....1.'.....f).o....U....H...[p..5.....g..lr...B...&X.....P....b..Y...=....S.u.. i.....5. T..2Hz.L.c..c.a/H2#..n..k./.DP.`(.,..U.o.Z.B....a..t..Y.].....8...[...Lq./....l.o...X.....!Y...M.-.g..Lo.y.h.....mL'P...x.I.+.|...&2W.M.....r GsOn....%."P.bb.e..A..=..>...?.tKn;.....#.....w..Q.b.0....^..?.L..H..x.....#.A.pz...s9..O..k.Y0Qu(.

Static File Info

General

File type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Entropy (8bit):	5.920279505250315
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:	2qTIaOLW2o.dll
File size:	1503232
MD5:	8ad564b939e5a713e39154c7e566adc6
SHA1:	8cd069a890ab232fca75a17e324de60c426f3115
SHA256:	1fa221f1d5a2c006943c6986babc756890b79c2b3838040 3789e54f467e1a84c
SHA512:	d23b0ca458cc91756ac7bc15934a040c71ac4a270676ff4 2bd9e20e1675736084bd9820f6456bf4da784a4cf5d7556 df16be07af770a19d931349c003e9ca46f
SSDEEP:	24576:wfP7fWsK5z9A+WGAW+V5SB6Ct4bnb2Gw:MDW/e+WG0Vo6CtSn3
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]

General

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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.hzrd	0x117000	0x1124	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.gfrpb	0x119000	0x389	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ymlijr	0x11a000	0x1f7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tntrb	0x11b000	0x389	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rmvhl	0x11c000	0x128f	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ukcyi	0x11e000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.knmra	0x11f000	0x1f7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.wtn	0x120000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.kjnw	0x121000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.okpgp	0x122000	0x1f2a	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.oxbitk	0x124000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.dplkzo	0x125000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.psnue	0x126000	0x543	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.lida	0x127000	0x9cd	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.arovjd	0x128000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.xsnm	0x129000	0x45174	0x46000	False	0.218526785714	data	5.75845428978	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: 5360 Parent PID: 5352

General

Start time:	22:16:09
Start date:	28/09/2021
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe 'C:\Users\user\Desktop\2qTIaOLW2o.dll'
Imagebase:	0x7ff616e00000
File size:	1136128 bytes
MD5 hash:	E0CC9D126C39A9D2FA1CAD5027EBBD18
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000000.00000002.266558177.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 5532 Parent PID: 5360

General

Start time:	22:16:10
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\2qTIaOLW2o.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: 5612 Parent PID: 5532

General

Start time:	22:16:10
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe 'C:\Users\user\Desktop\2qTIaOLW2o.dll',#1
Imagebase:	0x7ff657810000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000002.00000002.322869708.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 240 Parent PID: 5360

General

Start time:	22:16:11
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\2qTIaOLW2o.dll,??0?$PatternProvider@VExpandCollapseProvider@DirectUI@@UIExpandCollapseProvider@@$00@DirectUI@@QEAA@XZ
Imagebase:	0x7ff657810000
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: 00000004.00000002.245204685.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3472 Parent PID: 5612

General

Start time:	22:16:12
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: 2920 Parent PID: 5360

General

Start time:	22:16:14
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\2qTIaOLW2o.dll,??0?$PatternProvider@VGridItem Provider@DirectUI@@UIGridItemProvider@@$01@DirectUI@@QEAA@XZ
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: 00000008.00000002.253887228.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: rundll32.exe PID: 5156 Parent PID: 5360

General

Start time:	22:16:18
Start date:	28/09/2021
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false

Commandline:	rundll32.exe C:\Users\user\Desktop\2qTIaOLW2o.dll,??0?$PatternProvider@VGridProvider@DirectUI@@UIGridProvider@@$02@DirectUI@@QEAA@XZ
Imagebase:	0x7ff657810000
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: 00000009.00000002.261001867.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: SndVol.exe PID: 2540 Parent PID: 3472

General

Start time:	22:16:50
Start date:	28/09/2021
Path:	C:\Windows\System32\SndVol.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SndVol.exe
Imagebase:	0x7ff65a090000
File size:	259904 bytes
MD5 hash:	CDD7C7DF2D0859AC3F4088423D11BD08
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: SndVol.exe PID: 4928 Parent PID: 3472

General

Start time:	22:16:51
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\cAIXLQGkN\SndVol.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\cAIXLQGkN\SndVol.exe
Imagebase:	0x7ff6153d0000
File size:	259904 bytes
MD5 hash:	CDD7C7DF2D0859AC3F4088423D11BD08
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000016.00000002.352259211.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities Show Windows behavior

File Read

Analysis Process: tabcal.exe PID: 1488 Parent PID: 3472

General

Start time:	22:17:03
Start date:	28/09/2021
Path:	C:\Windows\System32\tabcal.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\tabcal.exe
Imagebase:	0x7ff7522b0000
File size:	82944 bytes
MD5 hash:	F04F239BA5FED275E652372222D1BE00
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: tabcal.exe PID: 6012 Parent PID: 3472

General

Start time:	22:17:03
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\CsJaRZ\tabcal.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\CsJaRZ\tabcal.exe
Imagebase:	0x7ff6fb150000
File size:	82944 bytes
MD5 hash:	F04F239BA5FED275E652372222D1BE00
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: 00000018.00000002.379949090.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

File Activities

Show Windows behavior

File Read

Analysis Process: ProximityUxHost.exe PID: 4660 Parent PID: 3472

General

Start time:	22:17:16
Start date:	28/09/2021
Path:	C:\Windows\System32\ProximityUxHost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\ProximityUxHost.exe
Imagebase:	0x7ff7c6a70000
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: 1692 Parent PID: 3472

General

Start time:	22:17:20
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\rPj\ProximityUxHost.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\rPj\ProximityUxHost.exe
Imagebase:	0x7ff6a5690000
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: 0000001C.00000002.412511294.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

File Activities

Show Windows behavior

File Read

Analysis Process: msinfo32.exe PID: 3060 Parent PID: 3472

General

Start time:	22:17:33
Start date:	28/09/2021
Path:	C:\Windows\System32\msinfo32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\msinfo32.exe
Imagebase:	0x7ff6e1410000
File size:	370176 bytes
MD5 hash:	C471C6B06F47EA1C66E5FAA8DFCEF108
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: msinfo32.exe PID: 2616 Parent PID: 3472

General

Start time:	22:17:33
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\52smNq1W\msinfo32.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\52smNq1W\msinfo32.exe
Imagebase:	0x7ff7b2450000
File size:	370176 bytes
MD5 hash:	C471C6B06F47EA1C66E5FAA8DFCEF108
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: 00000021.00000002.441901323.0000000140001000.00000020.00020000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: dpapimig.exe PID: 5972 Parent PID: 3472

General

Start time:	22:17:45
Start date:	28/09/2021
Path:	C:\Windows\System32\dpapimig.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\dpapimig.exe
Imagebase:	0x7ff758cd0000
File size:	76800 bytes
MD5 hash:	EE7DB7B615B48D8F9F08FAE70CAF46D7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dpapimig.exe PID: 4628 Parent PID: 3472

General

Start time:	22:17:50
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\famGrLP\dpapimig.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\famGrLP\dpapimig.exe
Imagebase:	0x7ff6882c0000
File size:	76800 bytes
MD5 hash:	EE7DB7B615B48D8F9F08FAE70CAF46D7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000023.00000002.478548185.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: dpapimig.exe PID: 3104 Parent PID: 3472

General

Start time:	22:18:02
Start date:	28/09/2021
Path:	C:\Windows\System32\dpapimig.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\dpapimig.exe
Imagebase:	0x7ff758cd0000
File size:	76800 bytes
MD5 hash:	EE7DB7B615B48D8F9F08FAE70CAF46D7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dpapimig.exe PID: 1576 Parent PID: 3472

General

Start time:	22:18:05
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\y7FgRNmA\dpapimig.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\y7FgRNmA\dpapimig.exe
Imagebase:	0x7ff675100000
File size:	76800 bytes
MD5 hash:	EE7DB7B615B48D8F9F08FAE70CAF46D7

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: 00000026.00000002.511156934.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Analysis Process: SystemPropertiesPerformance.exe PID: 5336 Parent PID: 3472

General

Start time:	22:18:17
Start date:	28/09/2021
Path:	C:\Windows\System32\SystemPropertiesPerformance.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SystemPropertiesPerformance.exe
Imagebase:	0x7ff7d0cd0000
File size:	83968 bytes
MD5 hash:	F325976CDC0F7E9C680B51B35D24D23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: SystemPropertiesPerformance.exe PID: 612 Parent PID: 3472

General

Start time:	22:18:18
Start date:	28/09/2021
Path:	C:\Users\user\AppData\Local\hbyq\SystemPropertiesPerformance.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Local\hbyq\SystemPropertiesPerformance.exe
Imagebase:	0x7ff605250000
File size:	83968 bytes
MD5 hash:	F325976CDC0F7E9C680B51B35D24D23A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000028.00000002.536952423.0000000140001000.00000020.00020000.sdmp, Author: Joe Security

Disassembly

Code Analysis