ID: 628420
Sample Name: QT_0948765446-NMPMUST-9876563783.exe
Cookbook: default.jbs
Time: 16:39:40
Date: 17/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

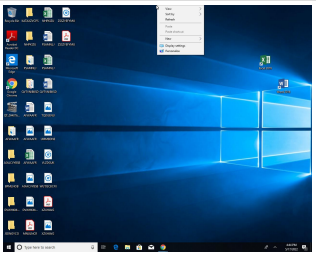
Windows Analysis Report

QT_0948765446-NMPMUST-9876563783.exe

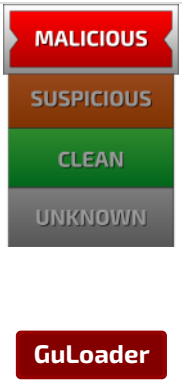
Overview

General Information

Sample Name:	QT_0948765446-NMPMUST-9876563783.exe
Analysis ID:	628420
MD5:	155a8b146f63fce..
SHA1:	7abaf8a0df564b8.
SHA256:	361deb3d9ef665..
Infos:	



Detection



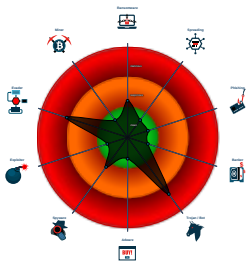
GuLoader

Score:	64
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected GuLoader
- Tries to detect virtualization through…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- PE file does not import any functions
- PE file contains strange resources
- Drops PE files
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- PE file contains sections with non-s…
- Detected potential crypto function

Classification



Process Tree

- **System is w10x64**
- QT_0948765446-NMPMUST-9876563783.exe (PID: 6972 cmdline: "C:\Users\user\Desktop\QT_0948765446-NMPMUST-9876563783.exe" MD5: 155A8B146F63FCECC360CC1162974373)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=15pFGBWcJey0L1ljJmoCXsS1qG0k_QM5X"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.957100646.0000000003370000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Networking

C2 URLs / IPs found in malware configuration

Data Obfuscation

Yara detected GuLoader

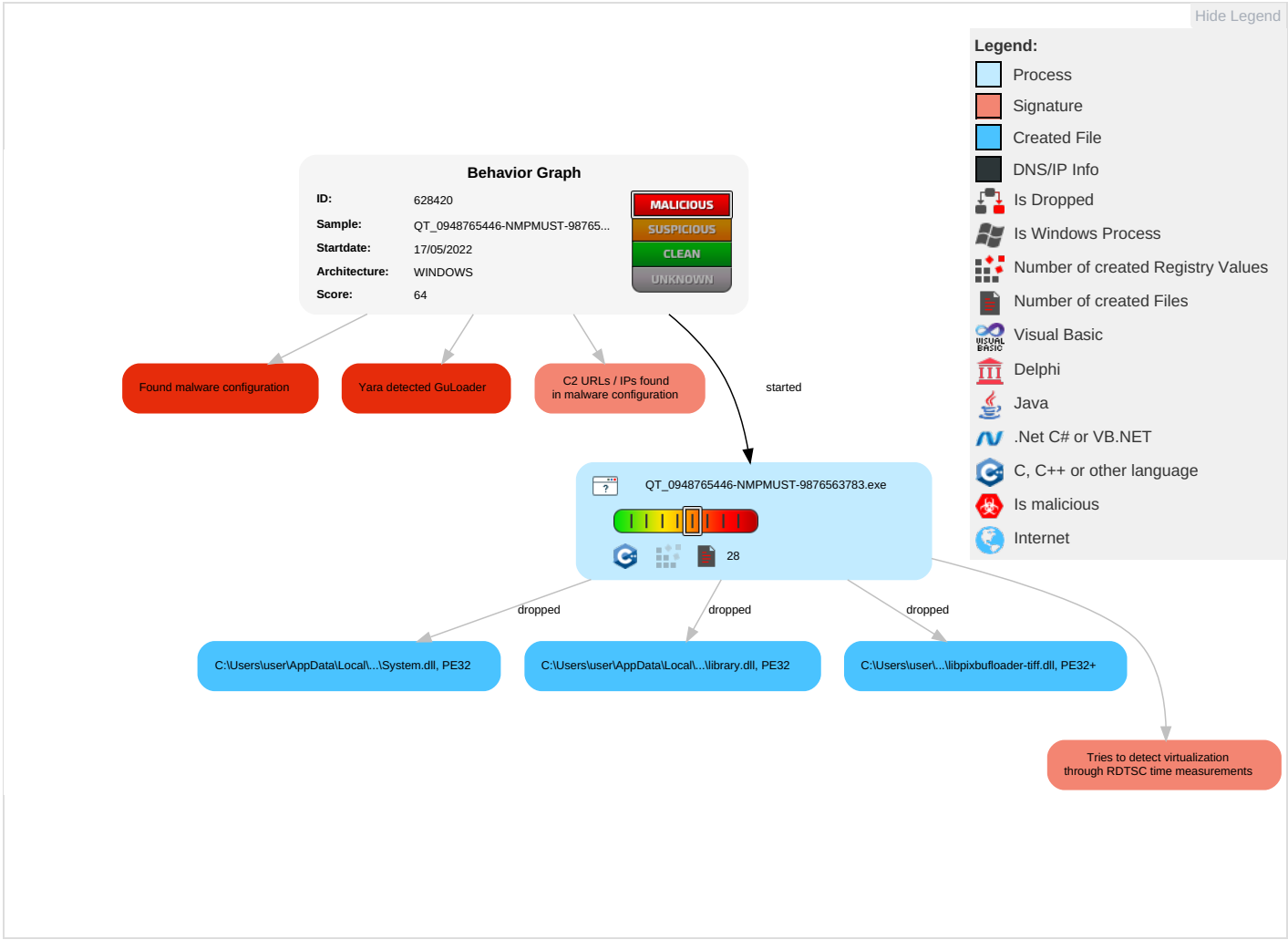
Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

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 Native API	Path Interception	1 Access Token Manipulation	1 Access Token Manipulation	OS Credential Dumping	1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Obfuscated Files or Information	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	1 3 System Information 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

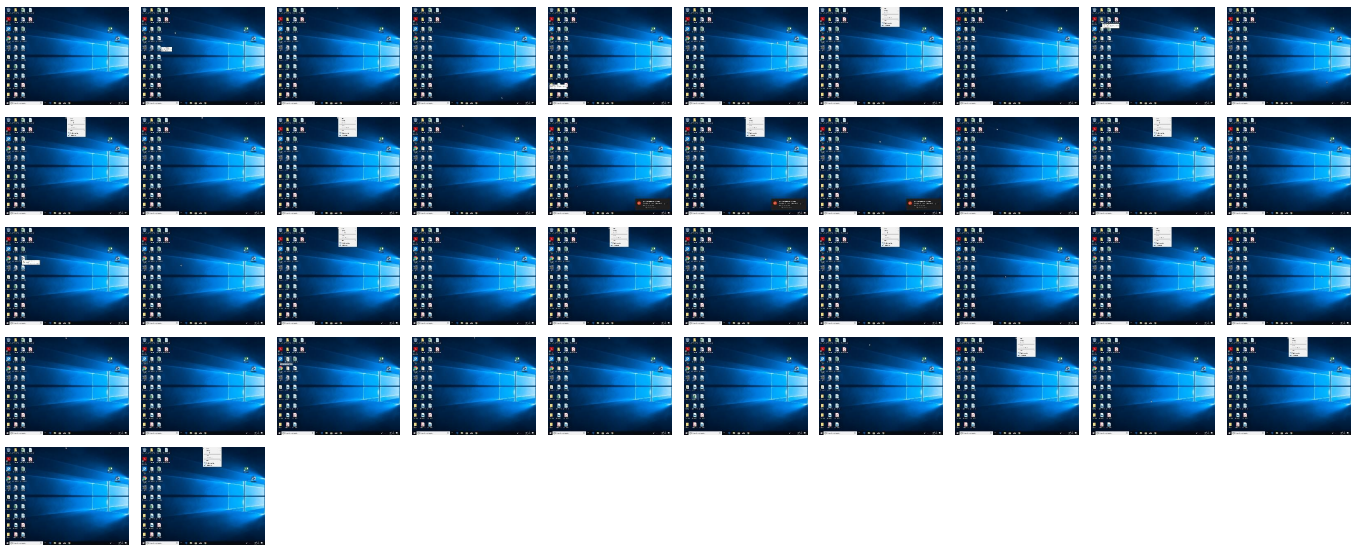
Behavior Graph



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
QT_0948765446-NMPMUST-9876563783.exe	2%	ReversingLabs	Win32.Trojan.Shelsy	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\libpixbufloader-tiff.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\libpixbufloader-tiff.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\libpixbufloader-tiff.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\library.dll	3%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\library.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\library.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsmF740.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsmF740.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://nsis.sf.net/NSIS_ErrorError	QT_0948765446-NMPMUST-9876563783.exe	false		high

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	628420
Start date and time: 17/05/202216:39:40	2022-05-17 16:39:40 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	QT_0948765446-NMPMUST-9876563783.exe
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:	9
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:	mal64.troj.evad.winEXE@1/11@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 86% (good quality ratio 84.7%) • Quality average: 87.8% • Quality standard deviation: 21.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, ctldl.windowsupdate.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com

Simulations

Behavior and APIs

Time	Type	Description
16:40:59	API Interceptor	1x Sleep call for process: QT_0948765446-NMPMUST-9876563783.exe modified

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\ArtDeco_green_22.bmp

Process:	C:\Users\user\Desktop\QT_0948765446-NMPMUST-9876563783.exe
File Type:	PNG image data, 110 x 110, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	6849
Entropy (8bit):	7.964410103086909
Encrypted:	false
SSDEEP:	192:84tawNmazDkzm194nzoleRkBVth1GHnClTPfiu3P713O+WZQC:vJLkm16nzRknth1GHCl7iuf9rWZQC
MD5:	C9E51CDC81D062234E363D135F53D582
SHA1:	BBF061CB6C6E6C85A0FBEC058F2DC27DE7A56BC9
SHA-256:	599388CC93E8D2AE04325F6A692B31E6CBCFEE9D11FEA4A22E8FE31E1FF89AA2
SHA-512:	ABDF90AF83C2555F5675BD85F525672ADDFFAC965FBF349E2B1020E613E82377417646F1956A9EBD17B947B209655A721101AF4FF70970845DFC53FF7E8072C8
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR...n...n.....I9.....pHYs...a...a..?.i...sIDATx..].[.7..O./1..."q0./tu..^&.%y.yI&o.lbg.7....w.#.:R..p.]_.|Ew.J:...R...c...{..|.z.r.....n.pn.....z...,B...\.}...,f...`...~..]8...`%.. ..A...Y.<...H...".F.J.v%`.~.m..w..pQ.z....Hz.%.....{h.#=..^....7.S`.....3.....Q..X...[W....._.o....I..g>.3I:.....a.*^ (.....,P6.."N4.....<.i.H..1..z._.P@..=k7.....L.v.3.x.=;@..(:. =P.'4P2...h.Z ("...lY.{q1.....$..Y.:...9hU.....<z....E..08TM/.}../.M..M...4D..+...Bd._K.....2...L...A..^.$.:*^..5;-4...p4 .@...t0.....6z....LH.....f..b...SA.M....HZo.!X.3...a#!|..... 5.....t4i...Uh....6.x*.y....S.l..t-.I...p...~..A.....W.....h.o^.ex...bn8so(:Oy.=r.YTj.sz.*%.]..8...9.A.."A.....O.....h.Q.+.v.v...9..md.Aa....7a.....]...!..v.?.9...\.....l.HI..(h ....O_...wF6.....C7..+2N.x@z'G.8..hoO...+m...N.....Jza.#.....T..Sk..?.1....=..=..>..5...2#F.wm<,z.....!..O...n`H.%.@D(.4\FrX.[.'.}~.HZ.7.....x..0.5LM. .b....

C:\Users\user\AppData\Local\Temp\applications-engineering.png

Process:	C:\Users\user\Desktop\QT_0948765446-NMPMUST-9876563783.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	495
Entropy (8bit):	7.413794533078799
Encrypted:	false
SSDEEP:	12:6v/7lgK+7rivq3U5TPrJlMjyFp25GxlaPaBkgGiYbmgaEwPF:s/kkhrEjyFp25GxlaPaKg3pdF
MD5:	DA02560CE065ED9F812FC23B6AF4E2C6
SHA1:	1A05DEAA45D137500AE2279C5EB608FD8F77B1F8
SHA-256:	2BEC36AB11AA5A8328257C4A9D1F268805451983D5AAC657E098C9FC386574F6
SHA-512:	EF3CDAF6F39C9EFC309DE851F798840DAA475F6263FCC23E590DB40D98640B3481053720FBF0015D83BAFB6F0CACE7CBF09131EE0498C7C4CF1AD34472E800B
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....a....IDATx...E..`...^.....Kd|..k$.....[K..H-.L..=OY.....P.n..iW..z.0.{...j....%..W.D0{...QQ...S..9/^>K.k.....EH$..y.....h.3.....v .....u...g.86.{."Ti*H9..ii...p?.B $I.k....~.....E.....P.6.9G.-P->\|z....9.>x.`...m).hvn.(.._...Jf4.....-'E.....^?.....C#.....?.....=...w.t...i>.....&^.~..76.c.T...nAb.....3NP..'&....b..`tl8$...."..f.....$.H.....7o].7o^a-i.....C||...H.`k./..'1.! ...D..E...]0...j9....IEND.B`.

C:\Users\user\AppData\Local\Temp\document-print-preview-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\QT_0948765446-NMPMUST-9876563783.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	290
Entropy (8bit):	6.970419229774679
Encrypted:	false
SSDEEP:	6:6v/lhPys1jeVXJA4VdfgDp3/wrnyVNS5hhll0IdXEVnyBaJa6jp:6v/7VjQ10OTGgL0zVyBaQ6N
MD5:	0D79E9D00775B587F7DDC07F85581167
SHA1:	E094329B29C52656965AF26D944CBC8B753B831A
SHA-256:	3A431205D5999B6CE43AFE3E3F553BEB46C95B40F202880E8B6A404593A138B5
SHA-512:	46724C6B562D9D5161971599302114EE8B66D163FDAB8EE4625E489DBE765734CA283C9289C92BBD183444368974D17B2DC143204D6C0AA805F5D2A92DF686A
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8...J.Q.../..,....7.\..^.L+.V....S...V. .....M..Eq..Y..f5..>v.O.....6.....E...+la..p...2....-.)6....f....'..Y7.(.....%...&.T^.D9.n..X/K.B.A.....Z...E.u.....~...Cl.....1....[!./.#S.....IEND.B`.

C:\Users\user\AppData\Local\Temp\flugters.GLA

Process:	C:\Users\user\Desktop\QT_0948765446-NMPMUST-9876563783.exe
File Type:	data
Category:	dropped
Size (bytes):	94761
Entropy (8bit):	7.147038765629842
Encrypted:	false
SSDEEP:	1536:2XNlqvDX7cKj1l6vX42bW/9eSn3pPi+4mad2LIVfWUXX290zHBsSBbe6kf:iNlaDLcY4X4D/Ln3p6qad06e0HH3Fkf
MD5:	DB1F8338E32AEA828E5F3BC1E479EA4D
SHA1:	D0EC5F2CC0A8A865F7420C5185F39D406DA0523C
SHA-256:	847653D9662EB47618CADA712604EFAD95A9093844A40C60546F97D7604208F9
SHA-512:	E4A647449E22428D3B3DBD1BED29290B61E8DA8D6CCAA4E53B78699ABC4CED3D46E09C23C62AC5C7321F01F2A8CCF807801E8F7B18B3EC1861856121295BE728
Malicious:	false
Reputation:	low
Preview:	...<.....B.....V.....:<#...<j....B....9.....Y<..L.....<...<...$..(..(_....7.....)...../.....<.<-..(.....1..I....i....z.....N..I..W<....<U.....7..h..i.....v.....c..-.4.j.....<.....!.....~..H.....a.....<..z.....t..u.....{..4....K.....<.....m..o..N....9..c..n..-..w.....X..j.R..G.....H.....>6..%Ex-(..9.y.Y.P..q..Hu.B...OGohJ....sA).C.s.b.....Q...nb..b".:.|. eLN.....n...Ww..\.8e..R.b.r..SV...E(.@H..T...4c=.....%.."u../*..*..}..!D..v.....c<.....B.Z....M.!.cr...f....7...<.X..i2...GC.....4.....:.I.....n.....R}.....7N-.I....G.....k.....a..-.i1..

C:\Users\user\AppData\Local\Temp\libpixbufloader-tiff.dll

Process:	C:\Users\user\Desktop\QT_0948765446-NMPMUST-9876563783.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows

Category:	dropped
Size (bytes):	28353
Entropy (8bit):	5.247530837724658
Encrypted:	false
SSDEEP:	384:iRGqs9qVGO2LHItNcLIHJOJF9yX8EzQrwEl6/p9ekFCCq:iu9qk3o0LIHJ4LycFFq
MD5:	9174157F50762DD5D6E160C7E0DDADF1
SHA1:	D9E0BA6AA58B561D25C5A122A842A7B5DE1D47A4
SHA-256:	80495E26F7ACE00DDE275B5C96292C7C31AF65AC7732D42D4E626EDE68F8C7F8
SHA-512:	9A8A32B1A6648CFFFE2EE44DFC8BD95500738766AC14F13D967006DF35745FCAB18C7D4CB67EEEA2EAC0A2FCC343B2D670B20A67960589236300E522EC2014A
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....b..T.....&"...%.2...^.....P.....~B..... .....!....`.. .....k.....p.....p.....e..(.....`.....text....0.....2.....`..`.data.....P.....6..... .....@....rdata..@....`.....8.....@..@.pdata.....p.....F.....@..@.xdata..0.....J.....@..@.bss.....edata..k.....N.....@.. @.idata.....P.....@....CRT....X.....\.....@....tls.....^.....@....reloc..p.....`.....@..B..... .....

C:\Users\user\AppData\Local\Temp\library.dll

Process:	C:\Users\user\Desktop\QT_0948765446-NMPMUST-9876563783.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	528
Entropy (8bit):	2.454669672012672
Encrypted:	false
SSDEEP:	3:WlWUqt/vllXl+YZcFTS9gXeF+X32Zp9XojoW2mnKt3MGHlXml/4XSkVlXllXl/l5:idq2Vg3F+X32RojB5nKKZ4i
MD5:	56D41F7E91B9DCD5E8AF747A13C6004B
SHA1:	C59F6AE0DE9D72F3046293E9CEE3A8E5077A3F58
SHA-256:	9B84941527243130 33EE4A2C2112212816F9C11AB5DEF42D3325617ADFF6DE49
SHA-512:	CB28A005BFE866102538AF218606269018D7B433DA559E3496C21A63815D439A397A1B9281C4DDEB1D575BC0645D4C0F8D6156171611534F9CA8F6124CB21CA5
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 3%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....)...m.o.m.o.m.o...i.l.o.2.e.l.o.Richm.o.....PE..L.....:..... .....@.....rsrc.....@..@..... .....

C:\Users\user\AppData\Local\Temp\mail-attachment-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\QT_0948765446-NMPMUST-9876563783.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	337
Entropy (8bit):	7.0965599412000255
Encrypted:	false
SSDEEP:	6:6v/lhPys2zWtl1SjYx4LeRiaTJBeWiqIWODcmaq0LsOHmjknp:6v/7W11M3LekaTJkiO9hXOykp
MD5:	659220014DDED044AE048DE1F707787D
SHA1:	32D7305C1A0315A59B7B6F12A652D409F1E53077
SHA-256:	3C7677231B2B2E41865F2772B97F2ED21235A6D3377A5C18A66D66ABB5F289C5
SHA-512:	C577E4688BCB1B98CF559062EB9A158E82FA2FE408A89D53E7C3E857796211166FEB17958001DC397BA04C303C42A6B4E5481BC0434CA58BB3512F4A72C5AE1
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8...JCQ.../.....F....b..0...o.EZE.X...,6.BHkk....D&.....3._3{.....5..?*.A.....m@.8.5~#..d..{..H&...V..;Fs..}l.....'x.uT..*t../. #..Q[A7j..=.Z'.,E...XC/j...ji.!\.".O.x.{|.b.2|7.....ij.W.Fo'....N....M.'Q-m...q...k...,..0.s.F.E..&...M.?L9.....6).....g...__*.@.*....IEND.B`.

C:\Users\user\AppData\Local\Temp\mail-forward.png

Process:	C:\Users\user\Desktop\QT_0948765446-NMPMUST-9876563783.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced

Category:	dropped
Size (bytes):	358
Entropy (8bit):	7.110934101486144
Encrypted:	false
SSDEEP:	6:6v/lhPWbD+rdtFtN6aho0HHOGaB7YrI1QJYB+rCiYb3FoiiiI99r9Bp:6v/7TrbN7lnOGuY8iJg+eiG1odr9v
MD5:	3D4B275979C1C90F8802E34E1AE6BB03
SHA1:	13596B93FB14BE97D6275CCE43969935DEA3762C
SHA-256:	2D547F84EA8DF35ECAAF5F4CDB92CA50488514174CF77A2B955D7CD4E0660B9F
SHA-512:	77F5F9C39A1C9133682BFCE4BD41FB58D04C226973C86EDD2A12DACD9D2BD06D4A1F3278620A7CAD658EE90D33AD5513EDFBF5AB0B035E6301E97BA4E9006E44
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....a...-IDATx.c...?E.z...Z.\..X.....}.8I6 ..`.....-..X.....Y..$u...e6..p/.py....C..>6I]....i>z...|.....g...^s.y..Y.%@b{/.....+.!..H[.w....A.j..6.+.....-?x.?0.@.@..x.....}.C0..:.=.w.....z...m.....].b.q.LV.!..:.|.....+D....CW.../..z..(L.....X.....J.....0.....IEND.B`.

C:\Users\user\AppData\Local\Temp\mail-reply-all-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\QT_0948765446-NMPMUST-9876563783.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	244
Entropy (8bit):	6.758520539988057
Encrypted:	false
SSDEEP:	6:6v/lhPys81g2WMTrmv2GxdaTKUWdXhcorhOZXd5bvn0LGp:6v/7c1ZWarYvDa+UWdxcor87bv0g
MD5:	4FD7AA500BD09F4AE3D4D0951D56B095
SHA1:	215730E32EE69DBA4A8CCF190D16903C51803C3C
SHA-256:	B34B352C04C4578B1130C979A3571DBF058BC939CDC45723E479BCE27D80B7A5
SHA-512:	B4EEA2408A0A717EE79DB3BD66DFDA455A67058CF707F5638DF786DADFFEBE0E9DFF508DA6ED235AE5AD73EE82656C1338590910850A046B66ECB82AEE19B036
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8...?jBA.....)...!<....y..a.T.H .....g.<X.....[|3.3...1.'..oe..(...V.....]~..U.4.....2.\..^....S.....<9.OL.c..K|s.S.Wy.1..|..U..j^i.{(.. ..J..5..E4.V.....2...t.....IEND.B`.

C:\Users\user\AppData\Local\Temp\network-cellular-disabled-symbolic.svg

Process:	C:\Users\user\Desktop\QT_0948765446-NMPMUST-9876563783.exe
File Type:	SVG Scalable Vector Graphics image
Category:	modified
Size (bytes):	845
Entropy (8bit):	5.12125030062822
Encrypted:	false
SSDEEP:	12:t4C8glnfnjdiYJCX+iCydrkeYRAerAFhLtHLAmVAcZ3AGdK5UMtz4y7jXvNM:t4CjlfhZJCX0yKbRAecFhBrN3AGMaM7O
MD5:	5CD531D175E59C4A36AC0025E613F689
SHA1:	62F4DF65A5F6E3DE4A89774953F9C41FA9A0A4AA
SHA-256:	41B4A84FD5B41F294B59E4CB4D9B76C6ACF4E5066C6AB9E458BEFEF116525B0C
SHA-512:	6F2A2241BEC4DA98D1D9949343FBE01B0431C80CC378915B1A62D3CF3F34C3240C35AAA3CE7799A91D9FBAE89203CCAF05C149F45564FCB1C5103AB6722297 3
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16">. <g fill="#2e3436">. <path d="M12.016 1v10.586l3 3V1zm-4 3v3.586l3 3V4zm-4 3v8h3V9.414L4.6 7zm-4 3v5h3v-5zm8 .414V15h3v-1.586zm4 4V15h.585z" style="line-height:normal;font-variant-ligatures:normal;font-variant-position:normal;font-variant-caps:normal;font-variant-numeric:normal;font-variant-alternates:normal;font-feature-settings:normal;text-indent:0;text-align:start;text-decoration-line:none;text-decoration-style:solid;text-decoration-color:#000;text-transform:none;text-orientation:mixed;white-space:normal;shape-padding:0;isolation:auto;mix-blend-mode:normal;solid-color:#000;solid-opacity:1" color="#000" font-weight="400" font-family="sans-serif" overflow="visible" fill-rule="evenodd"/>. <path d="M1.53.47L.469 1.53l14 14 1.062-1.061z"/>. </g>.</svg>.

C:\Users\user\AppData\Local\Temp\nsmF740.tmp\System.dll

Process:	C:\Users\user\Desktop\QT_0948765446-NMPMUST-9876563783.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2

SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4. D.Rich5.D.....PE..L.....Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@..X. .....text.... ....."..... ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.569756741108006
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	QT_0948765446-NMPMUST-9876563783.exe
File size:	260733
MD5:	155a8b146f63fcecc360cc1162974373
SHA1:	7abaf8a0df564b853227fdb8a614e7f8ba3edd15
SHA256:	361deb3d9ef665902441a554d099bd5e43266cd6320ef84facacdee256d325bd
SHA512:	fd424da3119cb0b13337a867278bec2418b0e9b4e5d7ba7799db15157d1a040a77c71fc585a9d9582980657bdb483d1124f8cfa83745702efdab6e0bc7d416e4
SSDEEP:	6144:UYa6ZtKR5Z0v2uTcWdq+LKimLlF21W0PLpxYwX:UY3Y5Z0eGJq+LuxF2sL0
TLSH:	8344F09576E0C863D9A50674EE35C9F65BF4BE22C8B50A0737E43F5C397A222D80C362
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L.....Oa.....h...*.....

File Icon

Icon Hash:	84f68684c4c33fc0

Static PE Info

General

Entrypoint:	0x403640
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9B1F [Sat Sep 25 21:56:47 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	61259b55b8912888e90f516ca08dc514

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A230h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080C8h]
mov esi, dword ptr [004080CCh]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007F4324DDDBEAh
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007F4324DDDBBAh
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A318h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x6c000	0x1f320	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	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	0x8000	0x2b0	.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	0x6676	0x6800	False	0.656813401442	data	6.41745998719	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.4498046875	data	5.14106681717	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20378	0x600	False	0.509765625	data	4.11058212765	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x2b000	0x41000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x6c000	0x1f320	0x1f400	False	0.7696953125	data	7.24749238687	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x6c448	0x93bf	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x75808	0x66ac	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x7beb8	0x4c28	dBase IV DBT, blocks size 0, block length 18432, next free block index 40, next free block 0, next used block 4279173120	English	United States
RT_ICON	0x80ae0	0x3c12	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x846f8	0x25a8	data	English	United States
RT_ICON	0x86ca0	0x10a8	data	English	United States
RT_ICON	0x87d48	0xea8	data	English	United States
RT_ICON	0x88bf0	0x8a8	data	English	United States
RT_ICON	0x89498	0x668	dBase IV DBT of `.DBF, block length 1536, next free block index 40, next free block 251658488, next used block 65535	English	United States
RT_ICON	0x89b00	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x8a068	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_ICON	0x8a4d0	0x2e8	data	English	United States
RT_ICON	0x8a7b8	0x128	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x8a8e0	0x100	data	English	United States
RT_DIALOG	0x8a9e0	0x11c	data	English	United States
RT_DIALOG	0x8ab00	0xc4	data	English	United States
RT_DIALOG	0x8abc8	0x60	data	English	United States
RT_GROUP_ICON	0x8ac28	0xbc	data	English	United States
RT_VERSION	0x8ace8	0x2f4	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x8afe0	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, CreateFileW, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Version Infos

Description	Data
LegalCopyright	Xamasoft
FileVersion	32.24.11
CompanyName	1995-2013 Stellar Information Systems Ltd.
LegalTrademarks	Advanced Micro Devices, Inc.
Comments	Coca-Cola Co.
ProductName	Bausch & Lomb Incorporated
FileDescription	IT Group Inc.
Translation	0x0409 0x04b0

Possible Origin

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

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: QT_0948765446-NMPMUST-9876563783.exe PID: 6972, Parent PID: 632

General

Target ID:	0
Start time:	16:40:54
Start date:	17/05/2022
Path:	C:\Users\user\Desktop\QT_0948765446-NMPMUST-9876563783.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\QT_0948765446-NMPMUST-9876563783.exe"
Imagebase:	0x400000
File size:	260733 bytes
MD5 hash:	155A8B146F63FCECC360CC1162974373
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.957100646.0000000003370000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsvF5A7.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsbF616.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsmF740.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsmF740.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405BE2	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsmF740.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\nsmF740.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	14	406184	CreateFileW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\flugters.GLA	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\ArtDeco_green_22.bmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\applications-engineering.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\document-print-preview-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\libpixbufloader-tiff.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\library.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\mail-attachment-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\mail-forward.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\mail-reply-all-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\network-cellular-disabled-symbolic.svg	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsvF5A7.tmp	success or wait	1	403988	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsmF740.tmp	success or wait	1	405DA3	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
unknown	0	32768	75 6e 6b 6e 6f 77 6e	unknown	success or wait	2	406224	WriteFile
C:\Users\user\AppData\Local\Temp\nsmF740.tmp\System.dll	0	12288	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 71 72 2a fd 35 13 44 fd 35 13 44 fd 35 13 44 fd fd 0f 4a fd 32 13 44 fd 35 13 45 fd 21 13 44 fd fd 1c 19 fd 32 13 44 fd 61 30 74 fd 31 13 44 fd 56 31 6e fd 34 13 44 fd fd 33 40 fd 34 13 44 fd 52 69 63 68 35 13 44 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 19 fd 4f 61 00 00 00 00 00 00 00 00 fd 00 2e 21 0b 01 06 00 00 22 00 00 00 0a 00 00 00 00 00 00 7f 2a 00 00 00 10 00	MZ@!L!This program cannot be run in DOS mode.$qr*5D5D5DJ2D5E!D2Da0t1DV1n4D3@4DRich5DPELOa.!"*	success or wait	1	406224	WriteFile
unknown	33641	21588	75 6e 6b 6e 6f 77 6e	unknown	success or wait	7	406224	WriteFile
C:\Users\user\AppData\Local\Temp\flugters.GLA	0	16384	fd fd fd 3c fd fd 04 fd fd 42 fd fd fd fd fd fd fd fd 56 fd fd fd fd fd 3a 3c 23 fd fd fd 3c 6a fd fd fd fd 42 fd fd 07 fd 39 01 00 00 fd fd 59 3c 00 fd 4c fd fd 14 fd fd fd fd fd fd fd fd 09 fd fd 80 fd 13 3c fd fd fd 3c fd fd fd 24 fd fd 28 fd fd 28 5f fd fd fd fd 37 fd fd fd fd fd 29 fd fd fd fd fd fd fd fd fd fd 2f fd fd fd fd fd fd 3c fd 3c 2d fd fd 28 fd fd fd fd fd 1f fd fd 1b 31 80 fd 6c fd fd fd fd fd 69 fd fd fd fd 7a fd fd 12 fd fd 4e fd fd 49 fd fd 57 3c fd fd fd fd 3c 55 fd fd fd fd fd c0 fd fd fd fd fd fd 37 fd fd 68 fd fd 69 fd fd fd fd fd 76 fd fd fd fd fd 63 fd fd 2d fd 34 17 6a fd 07 00 fd 17 fd fd fd 3c fd fd fd fd fd fd 21 fd fd fd fd fd fd fd 7e fd fd 48 fd fd c0 fd fd fd 80 fd 61 fd fd	<BV:<#<jB9Y<L<<$((_7)/<<-(1lizNIW<<U7hivc-4j<!~Ha	success or wait	6	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ArtDeco_green_22.bmp	0	6849	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 6e 00 00 00 6e 08 02 00 00 00 49 39 fd fd 00 00 00 09 70 48 59 73 00 00 0f 61 00 00 0f 61 01 fd 3f fd 69 00 00 1a 73 49 44 41 54 78 fd fd 5d 09 5b 1c 37 fd fd 4f 05 2f 31 fd fd a0 22 71 30 18 2f 74 75 fd fd 5e 26 fd 25 79 fd 79 49 26 6f fd 49 62 67 fd 37 fd fd fd fd 77 fd 23 fd 3a 52 15 18 70 03 5d 5f 7f 7c 45 77 fd 4a 3a fd fd fd 52 7d fd fd 63 fd fd fd 7b fd 7f 5c 7c fd 7a fd 72 fd fd fd fd fd fd 5d fd 6e fd 70 6e fd fd fd fd 7a fd fd 01 2c 42 fd 0f fd 5c fd 7d 05 fd 2c fd 66 7f fd fd 60 fd fd fd 7e 19 fd 5d 38 fd fd fd 60 25 fd fd fd 15 41 04 16 fd 59 3c 3c 38 02 fd 48 fd fd fd 22 fd 46 fd 4a fd 76 25 60 fd 7e fd 6d fd 1e 77 78 fd 70 51 fd 7a 1e 0f fd fd 48 7a	PNGIHDRnnI9pHYsaa? isIDATx][7O/ 1"q0/tu^&%yyI&oIbg7w#: Rp]_|EwJ :Rc{|zrnpnz,B\},f`~]8`%A Y<H"FJv%`~mwpQzHz	success or wait	1	406224	WriteFile
C:\Users\user\AppData\Local\Temp\applications-engineering.png	0	495	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 01 fd 49 44 41 54 78 01 fd fd 45 fd fd 60 10 fd fd 5e fd 13 fd 1b fd fd fd 1e 0e 00 4b 64 7c fd 09 6b 24 fd fd fd fd fd fd fd 5b 4b fd fd 48 2d fd 4c fd fd 3d 4f 59 fd fd fd 15 fd 50 fd 6e fd ad 69 57 fd fd 7a fd 30 fd 7b fd fd fd 6a fd fd fd 0d 25 fd fd 57 fd 44 30 7b fd fd fd 51 51 19 fd fd 53 fd fd 39 2f 5e 3e 4b fd 6b fd fd fd fd 1c fd fd fd 45 48 24 13 fd 79 1e fd fd 1f 06 fd 68 12 33 0d fd fd fd fd 76 20 11 fd 03 09 fd 75 fd fd fd 67 fd 38 36 39 7b 13 22 54 69 2a 48 39 1c 85 69 69 fd fd fd 70 3f 1a 42 20 24 49 05 6b ea fd 18 fd 7e fd 1c 06 fd fd fd 03 45 fd 0c fd fd fd fd 50 fd 36 fd 39 47 fd 2d 50 2d 3e 7c 7a 13 fd 0f 1d 39	PNGIHDRaIDATxE`^Kd|k $[KH-L=OYP niWz0{j%WD0{QQS9/^> KkEH$yh3v u g86{"Ti*H9iip?B $Ik~EP69G-P->|z9	success or wait	1	406224	WriteFile
C:\Users\user\AppData\Local\Temp\document-print-preview-symbolic.symbolic.png	0	290	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 fd 00 00 00 fd 49 44 41 54 38 fd fd fb 4a fd 51 10 04 fd 2f fd 15 2c fd 05 fd fd 37 fd 5c fd fd 5e fd 4c 2b 82 56 86 10 fd fd 53 fd fd fd 56 fd 20 fd 68 fd fd 1f fd 04 07 06 0e fd fd fd fd 2e fd 7f fd 04 4d fd fd 45 71 fd 60 59 a0 fd 66 35 0c fd 3e 76 fd 4f fd fd fd 5f fd fd fd fd 36 fd b0 fd 1e fd 45 fd fd fd 2b 6c 61 fd fd 70 fd fd fd 32 fd fd 08 fd 2d fd 29 36 fd fd 1a fd 66 fd 0d 0d 1d fd 27 fd fd 59 37 17 28 fd 09 0f fd fd fd 25 1e fd fd 26 fd 54 5e fd 44 39 fd 6e fd fd 58 2f 4b fd 42 fd 41 fd fd fd 06 fd 0b 5a fd 16 fd 45 fd 75 fd fd 0a d8 fd fd fd fd 7e fd fd	PNGIHDRasBIT|dIDAT8J Q/,7\^L+VSV .MEqYf5>vO6E+lap2-)6f'Y7(%&T ^D9nX/KBAZEu~	success or wait	1	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\libpixbufloader-tiff.dll	0	16384	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 50 45 00 00 64 fd 0b 00 00 00 00 00 00 62 00 00 54 00 00 00 fd 00 26 22 0b 02 02 25 00 32 00 00 00 5e 00 00 00 02 00 00 50 13 00 00 00 10 00 00 00 00 7e 42 02 00 00 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 05 00 02 00 00 00 00 00 00 fd 00 00 00 04 00 00 fd 21 01 00 03 00 60 01 00 00 20 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEdbT&"%2^P~B!`	success or wait	2	406224	WriteFile
C:\Users\user\AppData\Local\Temp\library.dll	0	528	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 29 fd 01 fd 6d fd 6f fd 6d fd 6f fd 6d fd 6f fd fd fd 69 fd 6c fd 6f fd 32 fd 65 fd 6c fd 6f fd 52 69 63 68 6d fd 6f fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 01 00 0c fd fd 3a 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 02 00 00 00 00 40 00 10 00 00 00 10 00 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$)momomoilo2eloRichmoPEL:@	success or wait	1	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\mail-attachment-symbolic.symbolic.png	0	337	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 fd 00 00 01 08 49 44 41 54 38 fd fd fb 4a 43 51 10 fd fd 2f fd fd fd 01 fd fd fd fd 46 fd fd fd fd 62 fd 07 30 fd fd fd 6f fd 45 5a 45 fd 58 fd 0d fd 2c 36 fd 42 48 6b 6b fd 0d fd fd 44 26 fd fd 06 06 0e 33 fd 5f 33 7b fd 0f fd fd 00 1d fd fd 35 fd fd 3f 2a fd 41 fd fd fd bc fd 6d 40 fd 38 fd 35 7e 23 fd fd 64 fd 0b 7b fd fd 48 26 fd fd fd 56 fd fd 3b 46 73 16 06 7d 6c fd fd fd 01 7f 27 78 19 75 54 fd fd 2a 74 fd 0c 2f fd 23 1a fd 51 5b 41 37 6a fd fd 3d fd 5a 27 1b 2c 45 fd 0d fd 58 43 2f 6a fd fd 04 6a 69 fd 21 5c fd 22 fd 4f fd 78 fd 7b 7c fd 62 fd 32 7c 37 fd fd 13 09 1b 69 6a fd 57 fd 46 6f 27 fd	PNGIHDRasBIT|dIDAT8JCQ/Fb0oEZEX,6BHkkD&3_3{5?*Am@85~#d{H&V;Fs}l'xuT*t/#Q[A7j=Z',EXC/jji\"Ox{|b2|7ijWFo'	success or wait	1	406224	WriteFile
C:\Users\user\AppData\Local\Temp\mail-forward.png	0	358	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 01 2d 49 44 41 54 78 01 63 fd fd fd 3f 45 fd 7a 06 fd fd 5a fd 5c fd fd 58 fd fd fd 0e fd 7d fd 38 49 36 20 fd fd 60 74 1d fd fd fd fd 2d fd fd 58 fd 00 12 fd fd 59 fd fd 24 75 fd 7f fd 65 36 04 0d 70 2f fd 70 79 fd fd 07 fd 43 1b fd 3e 36 49 5d fd 07 12 03 69 3e 7a fd fd 7f 7c fd fd 09 fd fd 67 fd fd fd 5e 73 fd 79 b2 e6 59 fd 25 40 62 7b 2f fd fd 7f fd fd 2b fd 21 fd 0d 48 5b fd 77 fd fd fd fd 41 fd 6a 89 fd 36 fd 2b fd fd fd 00 1b fd fd fd 03 fd fd fd 19 16 fd fd fd 2d 3f 78 fd 3f 30 1c 40 1a 40 1a fd 78 fd fd fd fd fd fd fd fd 7d 14 43 30 0c 00 3a fd 3d fd 77 fd fd fd fd fd fd fd fd fd 57 fd fd 2e	PNGIHDRa-IDATxc?EzZ\X}8l6 `-XY$ue6p/pyC>6I]i>z|g^syY%@b{/+!H[wAj6+-?x?0@@x}C0:=w.	success or wait	1	406224	WriteFile
C:\Users\user\AppData\Local\Temp\mail-reply-all-symbolic.symbolic.png	0	244	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 fd 00 00 00 fd 49 44 41 54 38 fd fd fd 3f 6a 42 41 10 fd fd 10 fd 14 29 c0 0a fd 21 3c fd fd fd 0b 79 0a 0f 61 fd 54 09 48 20 fd fd 1b fd fd fd fd fd 67 fd 3c 58 fd fd 1e fd fd 07 5b 7c 33 fd 33 fd fd fd 31 fd 27 fd 06 6f 65 fd fd 28 fd fd fd 56 fd fd fd fd 03 7f fd 5d 7e fd 09 55 fd 34 fd fd fd fd fd 32 fd 5c fd fd 5e fd 05 fd fd 53 fd fd fd 16 fd 3c 39 fd 4f 4c fd 63 fd fd 4b 7c 73 fd 53 fd 57 79 fd 31 fd fd 7c fd fd 55 fd fd 6a 5e 69 12 7b 28 1b fd fd fd 4a fd fd 35 fd 0b 45 34 fd 56 fd f9 01 fd fd 32 fd fd fd 74 11 00 00 00 00 49 45 4e 44 fd 42 60 fd	PNGIHDRasBIT|dIDAT8?jBA)!<yaTHg<X[|331'oe(V]~U42\^S<9OLcK|sSWy1|Uj^i{(J5E4V2tIENDB`	success or wait	1	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\network-cellular-disabled-symbolic.svg	0	845	3c 73 76 67 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 73 76 67 22 20 77 69 64 74 68 3d 22 31 36 22 20 68 65 69 67 68 74 3d 22 31 36 22 3e 0a 20 20 20 20 3c 67 20 66 69 6c 6c 3d 22 23 32 65 33 34 33 36 22 3e 0a 20 20 20 20 20 20 20 3c 70 61 74 68 20 64 3d 22 4d 31 32 2e 30 31 36 20 31 76 31 30 2e 35 38 36 6c 33 20 33 56 31 7a 6d 2d 34 20 33 76 33 2e 35 38 36 6c 33 20 33 56 34 7a 6d 2d 34 20 33 76 38 68 33 56 39 2e 34 31 34 4c 34 2e 36 20 37 7a 6d 2d 34 20 33 76 35 68 33 76 2d 35 7a 6d 38 20 2e 34 31 34 56 31 35 68 33 76 2d 31 2e 35 38 36 7a 6d 34 20 34 56 31 35 68 2e 35 38 35 7a 22 20 73 74 79 6c 65 3d 22 6c 69 6e 65 2d 68 65 69 67 68 74 3a 6e 6f 72 6d 61 6c 3b 66 6f 6e 74 2d 76 61 72 69 61 6e 74 2d 6c	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"> <g fill="#2e3436"> <path d="M12.016 1v10.586l3 3V1zm-4 3v3.586l3 3V4zm-4 3v8h3V9.414L4.6 7zm-4 3v5h3v-5zm8 .414V15h3v-1.586zm4 4V15h.585z" style="line-height:normal;font-variant-l	success or wait	1	406224	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\QT_0948765446-NMPMUST-9876563783.exe	unknown	512	success or wait	322	4061F5	ReadFile
C:\Users\user\Desktop\QT_0948765446-NMPMUST-9876563783.exe	unknown	16384	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsbF616.tmp	unknown	4	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsbF616.tmp	unknown	11940	success or wait	1	40345F	ReadFile
C:\Users\user\AppData\Local\Temp\nsbF616.tmp	unknown	4	success or wait	11	4061F5	ReadFile
C:\Users\user\Desktop\QT_0948765446-NMPMUST-9876563783.exe	unknown	16384	success or wait	6	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\flugters.GLA	unknown	94761	success or wait	1	739B2C59	ReadFile

Disassembly

No disassembly