ID: 755357
Sample Name: PO No. 3200005919.exe
Cookbook: default.jbs
Time: 16:13:12
Date: 28/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

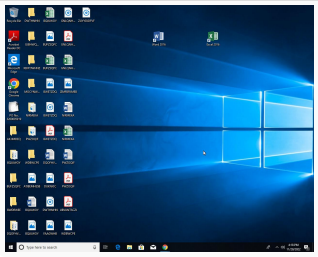
Windows Analysis Report

PO No. 3200005919.exe

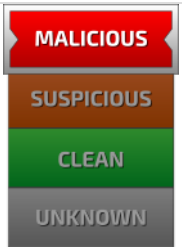
Overview

General Information

Sample Name:	PO No. 3200005919.exe
Analysis ID:	755357
MD5:	9453cdcf822134…
SHA1:	c35a23cdc61eb4..
SHA256:	7490acc48d1659..
Tags:	exe
Infos:	



Detection



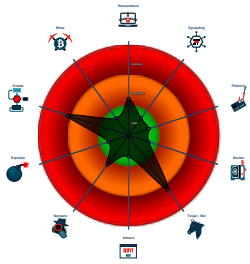
GuLoader

Score:	60
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Tries to detect virtualization through…
- Uses 32bit PE files
- Sample file is different than original …
- Drops PE files
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- Creates files inside the system direc…
- PE file contains sections with non-s…
- Detected potential crypto function
- Found dropped PE file which has no…

Classification



Process Tree

- **System is w10x64**
- PO No. 3200005919.exe (PID: 3308 cmdline: C:\Users\user\Desktop\PO No. 3200005919.exe MD5: 9453CDCF8221341D06BAC47B8AB3AA19)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.761070766.0000000004020000.00000040.00001000.00020000.00000000.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

Multi AV Scanner detection for submitted file

Data Obfuscation

Yara detected GuLoader

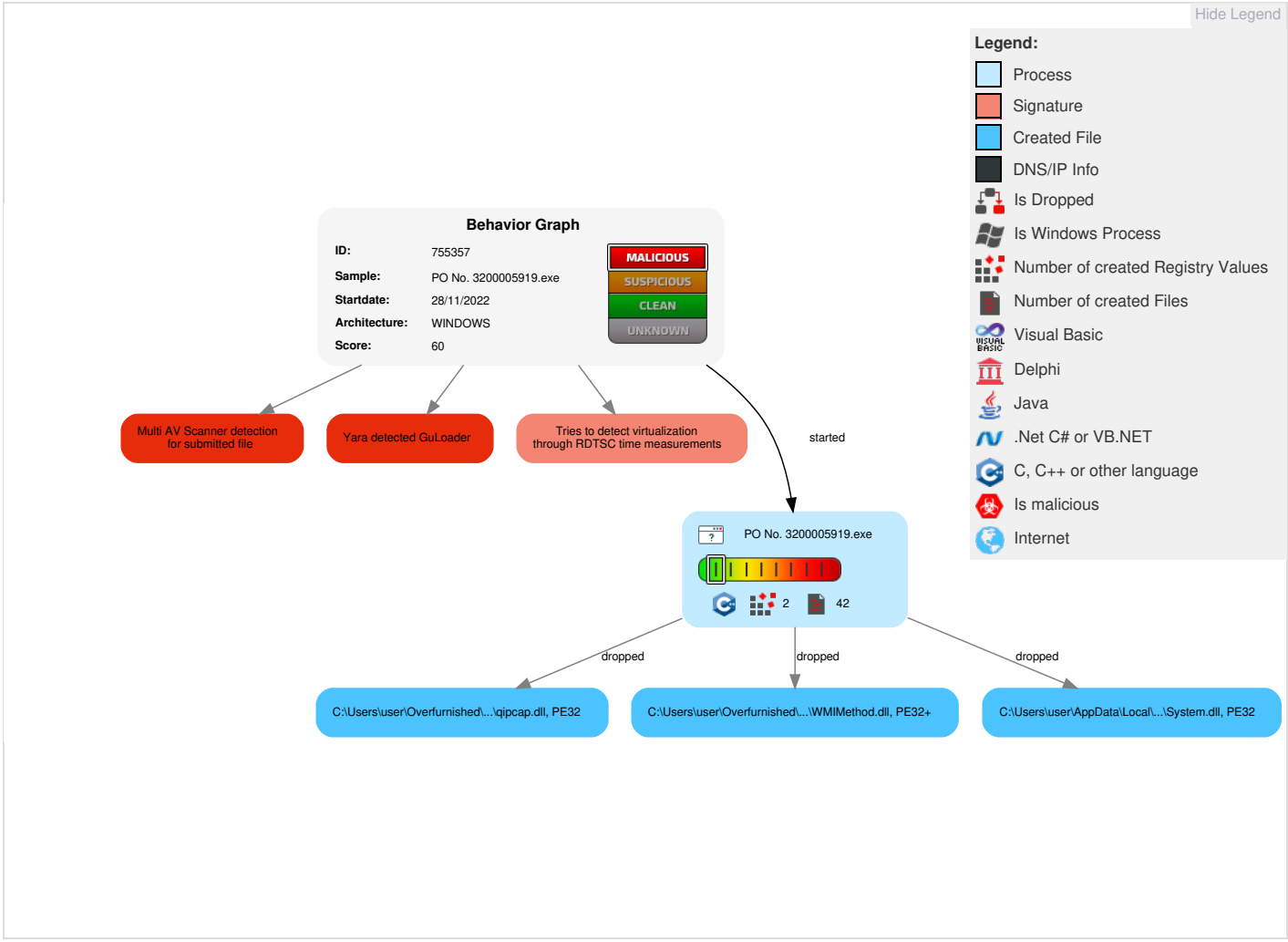
Malware Analysis System Evasion

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	Windows Management Instrumentation	Path Interception	1 Access Token Manipulation	1 1 Masquerading	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 Access Token Manipulation	LSASS Memory	3 File and Directory Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 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

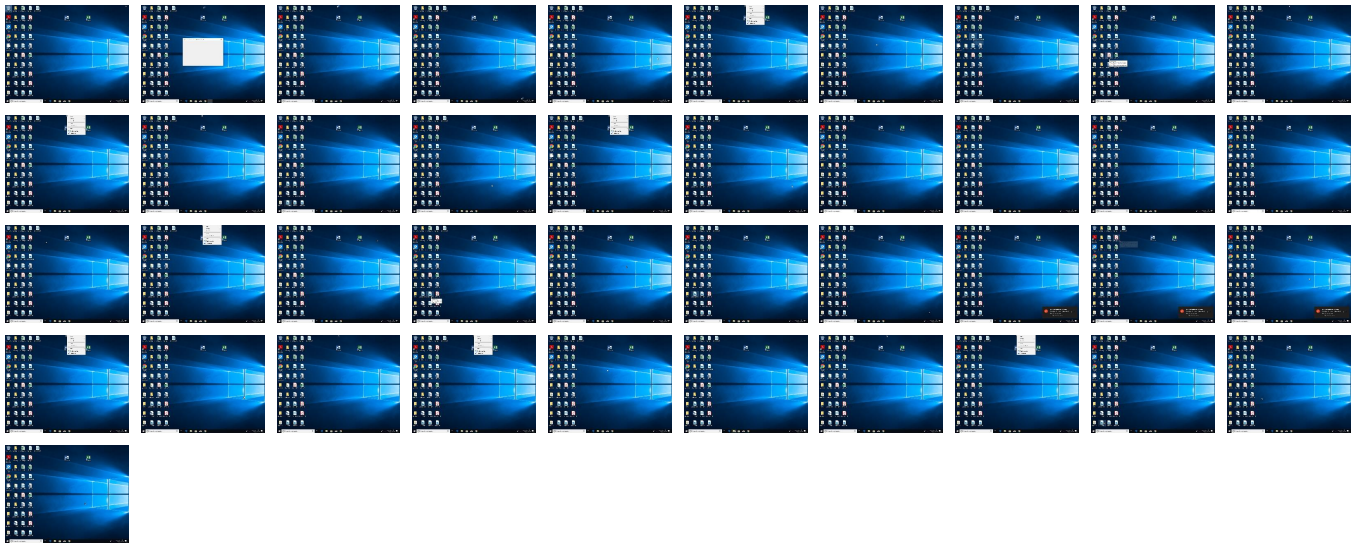
Behavior Graph



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
PO No. 3200005919.exe	47%	Virustotal		Browse
PO No. 3200005919.exe	62%	ReversingLabs	Win32.Trojan.Leonem	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nskA46.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nskA46.tmp\System.dll	1%	Virustotal		Browse
C:\Users\user\Overfurnished\Tuberculisation\Woodwose\Circularizations126\Iltningernes\Mellivorous\WMIMethod.dll	0%	ReversingLabs		
C:\Users\user\Overfurnished\Tuberculisation\Woodwose\Circularizations126\Iltningernes\Mellivorous\WMIMethod.dll	0%	Virustotal		Browse
C:\Users\user\Overfurnished\Tuberculisation\Woodwose\Circularizations126\Iltningernes\Mellivorous\qipcap.dll	0%	ReversingLabs		
C:\Users\user\Overfurnished\Tuberculisation\Woodwose\Circularizations126\Iltningernes\Mellivorous\qipcap.dll	0%	Virustotal		Browse

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://mozilla.org0	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://nsis.sf.net/NSIS_ErrorError	PO No. 3200005919.exe	false		high
http://https://mozilla.org0	PO No. 3200005919.exe, 00000000.00000002.760167646.000000000040A000.00000004.00000001.01000000.00000003.sdmp, PO No. 3200005919.exe, 00000000.00000002.760693342.0000000002859000.00000004.00000800.00020000.00000000.sdmp, qipcap.dll.0.dr	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	755357
Start date and time:	2022-11-28 16:13:12 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO No. 3200005919.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	11
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:	mal60.troj.evad.winEXE@1/7@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 86.2% (good quality ratio 85%) • Quality average: 88% • Quality standard deviation: 21%

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 • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

No simulations

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\nskA46.tmp\System.dll

Process:	C:\Users\user\Desktop\PO No. 3200005919.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	11776
Entropy (8bit):	5.659384359264642
Encrypted:	false
SSDEEP:	192:ex24sihno00Wfl97nH6BenXwWobpWBTtvShJ5omi7dJWjOlESlS:h8QII972eXqlWBFSt273YOlEz
MD5:	8B3830B9DBF87F84DDD3B26645FED3A0
SHA1:	223BEF1F19E644A610A0877D01EADC9E28299509
SHA-256:	F004C568D305CD95EDBD704166FCD2849D395B595DFF814BCC2012693527AC37

SHA-512:	D13CFD98DB5CA8DC9C15723EEE0E7454975078A776BCE26247228BE4603A0217E166058EBADC68090AFE988862B7514CB8CB84DE13B3DE35737412A6F0A8AC3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 1%, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...u.u.u...s.u.a....r.!..q....t....t.Richu.....PE..L.....uY.. ....'.....0.....`.....2.....0..P.....P.....0..X.....text..... ..... ..... ..`.rdata..S....0.....$.....@..@.data...x....@.....(.....@....reloc..`....P.....*.....@..B..... .....

C:\Users\user\Overfurnished\Tuberculisation\Woodwose\Afskede\Hitherunto\Sale\Swedish.ini

Process:	C:\Users\user\Desktop\PO No. 3200005919.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	dropped
Size (bytes):	3296
Entropy (8bit):	3.4113461059426067
Encrypted:	false
SSDEEP:	96:rLAi578zFA1TbATYHGzrSClCl2Pih5A9EE9EaiFy:fP57nlATYHyrSV5S5AfZ
MD5:	419178A0AA370FC69EFC1A54202CBFAC
SHA1:	BCACA6EB056D92BF2E4ABACCA16ACD80CA055BE6
SHA-256:	9C5948468DD8ADA15A36D7A1F7F5BC9563B7C7602A9BFB3CDC1B70F40C67DE36
SHA-512:	93FFD54400BBECD18D7EE69116364DDC2075E34294B9769880C53DB6DF3B0837A3E0590B0584EB3B79882BD66D8D9451E9014D33D8AD61C246E1EFDA65971B8
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	..[.T.r.a.n.s.l.a.t.i.o.n.s.].....R.O.G. .X.G. .M.o.b.i.l.e. .p.l.u.g.g.e.d.-.i.n. .=.R.O.G. .X.G. .M.o.b.i.l.e. ...r. .a.n.s.l.u.t.e.n.....P.u.s.h. .t.h.e. .".U.n.l.o.c.k. .S.w.i.t.c.h.". .o.n. .t.o.p. .o.f. .t.h.e. .p.l.u.g. .t.o. .l.o.c.k. .y.o.u.r. .c.a.b.l.e. .i.n. .p.l.a.c.e...=.T.r.y.c.k. .p... .l...s.k.n.a.p.p.e.n. .o.v.a.n.f...r. .k.o.n.t.a.k.t.e.n. .f...r. .a.t.t. .l...s.a. .f.a.s.t. .k.a.b.e.l.n. .....D.o.n.'.t. .s.h.o.w. .t.h.i.s. .m.e.s.s.a.g.e. .a.g.a.i.n.=.V.i.s.a. .i.n.t.e. .d.e.t. .h...r. .m.e.d.d.e.l.a.n.d.e.t. .i.g.e.n.....O.K.=.O.K.....C.a.n.c.e.l.=.A.v.b.r.y.t.....A.c.t.i.v.a.t.e. . t.h.e. .R.O.G. .X.G. .M.o.b.i.l.e.=.A.k.t.i.v.e.r.a. .R.O.G. .X.G. .M.o.b.i.l.e....D.e.a.c.t.i.v.a.t.e. .t.h.e. .R.O.G. .X.G. .M.o.b.i.l.e.=.I.n.a.k.t.i.v.e.r.a. .R.O.G. .X.G. .M.o.b.i.l.e. ....C.l.i.c.k. .O.K. .t.o. .s.w.i.t.c.h. .t.o. .t.h.e. .R.O.G. .X.G. .M.o.b.i.l.e...=.K.l.i.c.k.a. .p... .O.K. .f...r. .a.t.t. .b.y.t.a. .t.i.l.l. .R.O.G. .X.G. .M.o.b.i.l.e.....C.l.i.c.k. .O.K. .t.

C:\Users\user\Overfurnished\Tuberculisation\Woodwose\Airward.Sav

Process:	C:\Users\user\Desktop\PO No. 3200005919.exe
File Type:	Java JCE KeyStore
Category:	dropped
Size (bytes):	163026
Entropy (8bit):	6.663116548350503
Encrypted:	false
SSDEEP:	3072:i33VZ54T8JgMEU0pR3e6aahDHuP0IXt0dQ4SUy:OVZ54HMJCRO6RFFNL9y
MD5:	DD964C96ACC8FC51404B2205E7E740BD
SHA1:	81396D8F7BC367620BB127671CC324F63730B05F
SHA-256:	B42CF7F21B859E1C5D2ACE876913738A979DBF5FE9D4F5BAFFDFF60A0577FCE3
SHA-512:	6554D0BB128D204FD434D7E04C23DCEE55DD4DA8EE08433D54B8DF7690C9F3A8FF284A7F7023F889ABA798582BFC665E612958DD2D85374F37D3F82FF73C765E
Malicious:	false
Reputation:	low
Preview:	....

C:\Users\user\Overfurnished\Tuberculisation\Woodwose\Circularizations126\Iltningernes\Mellivorous\Oncosis.syl

Process:	C:\Users\user\Desktop\PO No. 3200005919.exe
File Type:	data
Category:	dropped
Size (bytes):	100097
Entropy (8bit):	**7.998148981940183**
Encrypted:	**true**
SSDEEP:	1536:iHaaOtGX0NzHwQMkIhF5kPtF/c2xo10IKCxvEYiCOw3u3ASAlNs9LHLpKvnO8:pryszHOhbWplCOE0uGLHLcm8
MD5:	115DDC0D007BC8ACA7678133CDF5B024
SHA1:	EED3949E406842152A374530E8971C52CB68ED8A
SHA-256:	17EABBA40E488BE3A65E30F5ABFA82F4C1E119C3EF484C2C39E9C95E993CA248

SHA-512:	622B9CD498B1AE71457CFC3094667077A5281BC1FEAA04789FC8F2B3FE641EF3F205D6DBE900E18C9A555866DD1FD00A6080827653225FA45AE9C1300C66244(
Malicious:	false
Reputation:	low
Preview:	2=..g.e.S.....2..H>m.....k.....)_.q.6.R..B....~:....Eh.7.8q."..CE.5..)e.e"..^.Z..d8#..n0...7....K.....)Z.8."..L...9.b.KQ?.)U.8.euF.....&...../...bQ.N...0.t.,....YT...?0...H..E. .v.po.+....{.U.E..#.....@7\.(.[+...K1...#....|.....b.@../l7...S.....X...2.dx.l..:..xtR...h..|9.+e..&....0...l8-..!....Gw;0l...j.L`..L.^.%..G..U....e.Y..t.7.X...4^k.G....'S..?..7.&.,...j...<r..OU G.A=.`.h.~....)..1..o..|.Y.X...:...A.}...1.[{.]S...y....sE.:....c..~.Z&6V.....`...%..)gm.fc.`...8.!.."._.Q....Rmrw*&..V..~.p.:..0.....AF...U..%*=>S]{....8..o.9.a.....0_.a.b.X....{....=m....k ....._M.....0..JG...r.._+3h....B..ECC.Q..0.....e...6.8.....o{!.....P'g..WZx.....2GC!k._..p}:..1l.?mX..iP<=..Z.d..7.3.X..... *`.H.9.....@yY..Q'..|H3..q.....-....].....C../..s..|... ....h.z.E....IA...URZ.*.=..H.;..+#....g.....$...y..EN}.@...Q.Y#.0GL..U)F6..`.(...+.O.....e%....h..V...5..s.D.|p:.....i.W.;.x....?..,.....lv*\.a....|.G..."..K..!P.n..

C:\Users\user\Overfurnished\Tuberculisation\Woodwose\Circularizations126\Iltningernes\Mellivorous\WMIMethod.dll

Process:	C:\Users\user\Desktop\PO No. 3200005919.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	106536
Entropy (8bit):	6.014036571306393
Encrypted:	false
SSDEEP:	1536:Uu0DxbI1QwdCVQiZSGMwd1v9gL2ZJeIAsW1IEd09dlIZ05PD/tbXZJ+NPE1H:URxIawUGiZ7M6VgLMII4JM50PbXiNPMH
MD5:	93FBA0E88958082664890BA74C8463E3
SHA1:	11C4F155494FB93232719AF3BA173EAC6F781CD8
SHA-256:	5C8B1D73B57905CB0024B6B00136363BEEF051ED8E1F0EFC7BC72F565AF06175
SHA-512:	6A13C83F5176FF78E16E98CFD155C5263CD2E1CFD1E00FABF13B8E85D426A4437F92D17559691FE149CDD7376AEF8573E0167B1BDECF999E31FC665412A86B2 0
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....y.k.*.k.*.k.*...+.k.*...+.k.*...+%k.*...+.k.*...+.k.*...+.k.*...+.k.* .k.*.k.*...+.k.*...+.k.*..i*.k.*.k.*.k.*...+.k.*Rich.k.*.....PE..d....8.a....." .....`.....[..|....\..(..... .....4....~..("..  ....X...XF..p.....F..8.....(.....text..... ..`.rdata..n.....@..@.data...h....p.....R.....@....pdata..4.....^ .....@..@_RDATA.....n.....@..@.rsrc... .....p.....@..@.reloc..X.....v.....@..B..... .....

C:\Users\user\Overfurnished\Tuberculisation\Woodwose\Circularizations126\Iltningernes\Mellivorous\qipcap.dll

Process:	C:\Users\user\Desktop\PO No. 3200005919.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	16824
Entropy (8bit):	6.421949257045276
Encrypted:	false
SSDEEP:	192:fvcU3c5wjYguwJba7RXAQV01eSKMP7x0KDWpH4AAANa3JZHSVMyMt:fvVkeYpwJKRn61jKMNvDG/GhqMys
MD5:	2D75C46C8030F312DFC2F56A0E016692
SHA1:	F95F12C987AF20A69BA05088B2F9E4F4BEC445AE
SHA-256:	AADD6DE734D7585D23833BA5C303313ED2273B2BD3D1B4B7BA55ABC1366FD8DD
SHA-512:	C0F0F07E6BA4A6676B753EC3613AC388DE88F32D508CB1B9BD8521FBF192889232B4722756DDC72A46B0AC4A4BFB48F26E06651E64CF3D31EB8F82134A5D367 1
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Reputation:	moderate, very likely benign file
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L...&.#b....."!.....P.....p.....g ....@A.....(!..P....P.....".....`..4.... .....!..h.....text..... ..`.rdata..$.... .....@..@.d ata.....0.....@....00cfg.....@.....@..@.rsrc.....P.....@..@.reloc..4....`..... .....@..B..... ....

C:\Windows\leprousness.lnk

Process:	C:\Users\user\Desktop\PO No. 3200005919.exe
File Type:	MS Windows shortcut, Item id list present, Has Relative path, Has Working directory, ctime=Sun Dec 31 23:06:32 1600, mtime=Sun Dec 31 23:06:32 1600, atime=Sun Dec 31 23:06:32 1600, length=0, window=hide
Category:	dropped
Size (bytes):	844
Entropy (8bit):	3.341138906905135
Encrypted:	false
SSDEEP:	12:8wl01Rm/3BVkUnDyXdICRDufdXPu7dl5ST5D0TL6CNbw4t2Y+xIBjK:8S/BTD3YDuiI50B2bI7aB

MD5:	113F0C5E3EE1E38568EDBE3A02B34900
SHA1:	2614DC469A25BB5EE1CD7EF1DCFC5EF3731E6B15
SHA-256:	71FAA8993B5ED93D7C418794BAE50BBA4E1B78F3A2EE74CAEEF07F82561BD4E5
SHA-512:	61672429CDC9CDA7BB6587457B11DD93275EB53898785CE53FAF94BAC2151F078DE4FA55A44C6F6967952E5C44D36EB928DBFA4ADB994CFFFE7EEFBD56282E A1
Malicious:	false
Preview:	L.....F.....=....P.O. .:i.....+00.../C:\.....V.1.....Windows.@.....W.i.n.d.o.w.s.....P.1.....Fonts.<. .....F.o.n.t.s.....h.2.....Tolknings.Fin.L.....T.o.l.k.n.i.n.g.s...F.i.n.....\.F.o.n.t.s.\.T.o.l.k.n.i.n.g.s...F.i.n.e.C.:.\.U.s.e. r.s.\.e.n.g.i.n.e.e.r.\.O.v.e.r.f.u.r.n.i.s.h.e.d.\.T.u.b.e.r.c.u.l.i.s.a.t.i.o.n.\.W.o.o.d.w.o.s.e.\.C.i.r.c.u.l.a.r.i.z.a.t.i.o.n.s.1.2.6.\.I.l.l.t.n.i.n.g.e.r.n.e.s.\.M.e.l.l.i.v.o.r.o.u.s.....$. .....C..B..g..(.#.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.575298268219731
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:	PO No. 3200005919.exe
File size:	373461
MD5:	9453cdcf8221341d06bac47b8ab3aa19
SHA1:	c35a23cdc61eb42594e1a39a23ccae06399263c0
SHA256:	7490acc48d1659234d61c1716c0d549880a98375f502502b60dcc71b49f7f14f
SHA512:	d37774b11400256fb4fe21b1e298f90274b0c83f2b0f90bc7c5d2a6ed3e0edb276bc49df8f65b0099f1d0ce6c4abac277805adf590971e277d1c1e15fd1190cd
SSDEEP:	6144:8Iw37uc96d+riI5FhrmKugnyj/wFW+hy88BSFz0PALceeozAs9k:pld6f5Ftgayj/kW+hyRYBVce3k5
TLSH:	2F84BF2F711D505ED917353266AEF0AA2B597C8B2B71E8164BA37DDF94F07200A0FB02
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.....uY.....d...*.....

File Icon

Icon Hash:	e0f0f0d0d8c0f81e

Static PE Info

General

Entrypoint:	0x403489
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x5975952E [Mon Jul 24 06:35:26 2017 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:	1f23f452093b5c1ff091a2f9fb4fa3e9

Entrypoint Preview

Instruction
sub esp, 000002D4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+14h], ebx
mov dword ptr [esp+10h], 0040A230h
mov dword ptr [esp+1Ch], ebx
call dword ptr [004080ACh]
call dword ptr [004080A8h]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [0042A24Ch], eax
je 00007F22E4D5A543h
push ebx
call 00007F22E4D5D7F1h
cmp eax, ebx
je 00007F22E4D5A539h
push 00000C00h
call eax
mov esi, 004082B0h
push esi
call 00007F22E4D5D76Bh
push esi
call dword ptr [00408150h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], 00000000h
jne 00007F22E4D5A51Ch
push 0000000Ah
call 00007F22E4D5D7C4h
push 00000008h
call 00007F22E4D5D7BDh
push 00000006h
mov dword ptr [0042A244h], eax
call 00007F22E4D5D7B1h
cmp eax, ebx
je 00007F22E4D5A541h
push 0000001Eh
call eax
test eax, eax
je 00007F22E4D5A539h
or byte ptr [0042A24Fh], 00000040h
push ebp
call dword ptr [00408044h]
push ebx
call dword ptr [004082A0h]
mov dword ptr [0042A318h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 000002B4h
push eax
push ebx
push 004216E8h
call dword ptr [00408188h]
push 0040A384h

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	0x84fc	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x60000	0x10890	.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	0x63d1	0x6400	False	0.66515625	data	6.479451209065	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x138e	0x1400	False	0.45	data	5.143831732151552	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20358	0x600	False	0.501953125	data	4.000739070159718	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x2b000	0x35000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x60000	0x10890	0x10a00	False	0.19385867011278196	data	3.7626047476334135	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x603e8	0x368	Device independent bitmap graphic, 96 x 16 x 4, image size 768	English	United States
RT_ICON	0x60750	0x5488	Device independent bitmap graphic, 72 x 144 x 32, image size 21600	English	United States
RT_ICON	0x65bd8	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16896	English	United States
RT_ICON	0x69e00	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	English	United States
RT_ICON	0x6c3a8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	English	United States
RT_ICON	0x6d450	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 2304, 256 important colors	English	United States
RT_ICON	0x6e2f8	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400	English	United States
RT_ICON	0x6ec80	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 1024, 256 important colors	English	United States
RT_ICON	0x6f528	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 256, 256 important colors	English	United States
RT_ICON	0x6fa90	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	English	United States
RT_DIALOG	0x6fef8	0x144	data	English	United States
RT_DIALOG	0x70040	0x13c	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0x70180	0x100	data	English	United States
RT_DIALOG	0x70280	0x11c	data	English	United States
RT_DIALOG	0x703a0	0xc4	data	English	United States
RT_DIALOG	0x70468	0x60	data	English	United States
RT_GROUP_ICON	0x704c8	0x84	data	English	United States
RT_MANIFEST	0x70550	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States

Imports

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

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: PO No. 3200005919.exe PID: **3308**, Parent PID: **3452**

General

Target ID:	0
Start time:	16:14:05
Start date:	28/11/2022
Path:	C:\Users\user\Desktop\PO No. 3200005919.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PO No. 3200005919.exe
Imagebase:	0x400000
File size:	373461 bytes
MD5 hash:	9453CDCF8221341D06BAC47B8AB3AA19
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: 00000000.00000002.761070766.0000000004020000.00000040.00001000.00020000.00000000.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	40596C	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsyEC5C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405F10	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nssEC8B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405F10	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	3	40596C	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	3	40596C	CreateDirectoryW
C:\Users\user\Overfurnished	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40596C	CreateDirectoryW
C:\Users\user\Overfurnished\Tuberculisation	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40596C	CreateDirectoryW
C:\Users\user\Overfurnished\Tuberculisation\Woodwose	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40596C	CreateDirectoryW
C:\Users\user\Overfurnished\Tuberculisation\Woodwose\Airward.Sav	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405ECE	CreateFileW
C:\Users\user\Overfurnished	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	40596C	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Overfurnished\Tuberculisation	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	40596C	CreateDirectoryW
C:\Users\user\Overfurnished\Tuberculisation\Woodwose	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	40596C	CreateDirectoryW
C:\Users\user\Overfurnished\Tuberculisation\Woodwose\Afskede	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40596C	CreateDirectoryW
C:\Users\user\Overfurnished\Tuberculisation\Woodwose\Afskede\Hitherunto	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40596C	CreateDirectoryW
C:\Users\user\Overfurnished\Tuberculisation\Woodwose\Afskede\Hitherunto\Sale	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40596C	CreateDirectoryW
C:\Users\user\Overfurnished\Tuberculisation\Woodwose\Afskede\Hitherunto\Sale\Swedish.ini	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405ECE	CreateFileW
C:\Users\user\Overfurnished\Tuberculisation\Woodwose\Circularizations126	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40596C	CreateDirectoryW
C:\Users\user\Overfurnished\Tuberculisation\Woodwose\Circularizations126\Iltningernes	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40596C	CreateDirectoryW
C:\Users\user\Overfurnished\Tuberculisation\Woodwose\Circularizations126\Iltningernes\Mellivorous	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40596C	CreateDirectoryW
C:\Users\user\Overfurnished\Tuberculisation\Woodwose\Circularizations126\Iltningernes\Mellivorous\Oncosis.syl	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405ECE	CreateFileW
C:\Users\user\Overfurnished\Tuberculisation\Woodwose\Circularizations126\Iltningernes\Mellivorous\WMIMethod.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405ECE	CreateFileW
C:\Users\user\Overfurnished\Tuberculisation\Woodwose\Circularizations126\Iltningernes\Mellivorous\qipcap.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405ECE	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	5066	40596C	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	5066	40596C	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	5066	40596C	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	5066	40596C	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	5065	40596C	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\Windows	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	5065	40596C	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	5065	40596C	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Fejltagelsernes	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40596C	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Fejltagelsernes\Finansudvalgenes	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40596C	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Fejltagelsernes\Finansudvalgenes\Tarlatanen	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40596C	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Fejltagelsernes	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	5064	40596C	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Fejltagelsernes\Finansudvalgenes	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	5064	40596C	CreateDirectoryW
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Fejltagelsernes\Finansudvalgenes\Tarlatanen	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	5064	40596C	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nskA46.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405F10	GetTempFileNameW
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	40596C	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nskA46.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	40592C	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nskA46.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405ECE	CreateFileW
C:\Users\user\AppData\Local\Temp\nskA46.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	4	405ECE	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsyEC5C.tmp	success or wait	1	40373A	DeleteFileW
C:\Users\user\AppData\Local\Temp\nskA46.tmp	success or wait	1	405AED	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	405F6E	WriteFile
unknown	45406	23838	75 6e 6b 6e 6f 77 6e	unknown	success or wait	18	405F6E	WriteFile
C:\Users\user\Overfurnished\Tuberculisation\Woodwose\Airward.Sav	0	16384	fd fd		success or wait	10	405F6E	WriteFile
C:\Users\user\Overfurnished\Tuberculisation\Woodwose\Afskede\Hitherunto\Sale\Swedish.ini	0	3296	fd fd 5b 00 54 00 72 00 61 00 6e 00 73 00 6c 00 61 00 74 00 69 00 6f 00 6e 00 73 00 5d 00 0d 00 0a 00 52 00 4f 00 47 00 20 00 58 00 47 00 20 00 4d 00 6f 00 62 00 69 00 6c 00 65 00 20 00 70 00 6c 00 75 00 67 00 67 00 65 00 64 00 2d 00 69 00 6e 00 20 00 3d 00 52 00 4f 00 47 00 20 00 58 00 47 00 20 00 4d 00 6f 00 62 00 69 00 6c 00 65 00 20 00 fd 00 72 00 20 00 61 00 6e 00 73 00 6c 00 75 00 74 00 65 00 6e 00 0d 00 0a 00 50 00 75 00 73 00 68 00 20 00 74 00 68 00 65 00 20 00 22 00 55 00 6e 00 6c 00 6f 00 63 00 6b 00 20 00 53 00 77 00 69 00 74 00 63 00 68 00 22 00 20 00 6f 00 6e 00 20 00 74 00 6f 00 70 00 20 00 6f 00 66 00 20 00 74 00 68 00 65 00 20 00 70 00 6c 00 75 00 67 00 20 00 74 00 6f 00 20 00 6c 00 6f 00 63 00 6b 00 20 00 79 00 6f 00 75 00 72 00 20 00 63	[Translations]ROG XG Mobile plugged-in =ROG XG Mobile r ansl utenPush the "Unlock Switch" on top of the plug to lock your c	success or wait	1	405F6E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Overfurnished\Tuberculisation\Woodwose\Circularizations126\Iltningernes\Mellivorous\Oncosis.syl	0	16384	32 3d fd 2e 67 fd 65 fd 53 17 fd 0e fd fd fd 32 fd fd 48 3e 6d fd 18 fd fd fd 04 11 fd 6b a3 fd fd fd fd fd fd fd 29 5f fd 71 fd 36 fd 52 fd 05 42 fd fd 1b fd 7e 3a fd fd fd 00 45 68 fd 37 fd 38 71 f1 22 fd fd 43 45 fd 35 11 fd 29 65 02 65 22 0b fd 5e fd 5a fd fd 64 38 23 fd fd 6e 30 fd fd fd 37 fd 1b fd fd 4b 84 1e fd fd 01 2e 29 5a fd 38 fd 22 fd fd 4c 06 fd 18 39 fd 62 1a 4b 51 3f 0f 29 55 fd 38 fd 65 75 46 fd fd fd fd fd 26 91 0e fd fd fd 1f 17 58 fd 2f fd fd fd 62 51 fd 4e fd 17 fd 30 fd 74 00 2c fd fd fd fd 1d 59 54 fd fd fd 3f 30 fd fd fd 48 fd fd 45 fd 20 fd 76 10 70 6f fd 2b fd fd 1b 10 7b fd 55 fd 45 fd fd 23 fd fd fd fd fd fd 40 37 5c fd 28 20 5b 2b fd fd 4b 31 fd fd 1e 23 fd fd cf fd 7c fd fd fd fd fd fd 0f 62 fd	2=.geS2H>mk)_q6RB~:Eh78q"CE5)ee"^Zd8#n07K.)Z8"L9bKQ?)U8euF&/bQN0t,YT?0HE vpo+{UE#@7\([+K1#|b	success or wait	7	405F6E	WriteFile
C:\Users\user\Overfurnished\Tuberculisation\Woodwose\Circularizations126\Iltningernes\Mellivorous\WMIMethod.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 08 01 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 0a fd 79 fd 6b fd 2a fd 6b fd 2a fd 6b fd 2a fd 00 fd 2b fd 6b fd 2a fd 00 fd 2b fd 6b fd 2a fd 00 fd 2b 25 6b fd 2a fd 1e fd 2b fd 6b fd 2a fd 1e fd 2b fd 6b fd 2a fd 1e fd 2b fd 6b fd 2a fd 00 fd 2b fd 6b fd 2a fd 6b fd 2a fd 6b fd 2a fd 1e fd 2b fd 6b fd 2a fd 1e fd 2b fd 6b fd 2a fd 1e 69 2a fd 6b fd 2a fd 6b 01 2a fd 6b fd 2a fd 1e fd 2b fd 6b fd 2a 52 69 63 68 fd 6b fd	MZ@!L!This program cannot be run in DOS mode.$yk*k*k*+k*+k*+%k*+k*+k*+k*+k*k*k*+k*+k*i*k*k*k*+k*Richk	success or wait	7	405F6E	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Overfurnished\Tuberculisation\Woodwose\Circularizations126\Iltningernes\Mellivorous\qipcap.dll	0	16384	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 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 78 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 24 00 00 50 45 00 00 4c 01 06 00 26 fd 23 62 00 00 00 00 00 00 00 00 fd 00 22 21 0b 01 0e 00 00 0e 00 00 00 10 00 00 00 00 00 00 50 13 00 00 00 10 00 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 01 00 00 00 00 00 06 00 01 00 00 00 00 00 00 70 00 00 00 04 00 00 fd 67 00 00 02 00 40 41 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 28 21 00 00 50 00 00	MZx@x!L!This program cannot be run in DOS mode.$PEL&#b"!Ppg@A(!P	success or wait	2	405F6E	WriteFile
C:\Users\user\AppData\Local\Temp\nskA46.tmp\System.dll	0	11776	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 31 fd fd fd 75 fd 75 fd 75 fd fd bd 73 fd 75 fd 61 b3 76 fd fd 72 fd 21 4c fd 71 fd 16 16 fd 74 b3 4a b8 fd 74 fd 52 69 63 68 75 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 50 45 00 00 4c 01 04 00 0e fd 75 59 00 00 00 00 00 00 00 00 fd 00 0e 21 0b 01 06 00 00 20 00	MZ@!L!This program cannot be run in DOS mode.$1uuusuar!qttRichuPELuY!	success or wait	1	405F6E	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PO No. 3200005919.exe	unknown	512	success or wait	209	405F3F	ReadFile
C:\Users\user\Desktop\PO No. 3200005919.exe	unknown	16384	success or wait	1	405F3F	ReadFile
C:\Users\user\AppData\Local\Temp\nssEC8B.tmp	unknown	4	success or wait	1	405F3F	ReadFile
C:\Users\user\AppData\Local\Temp\nssEC8B.tmp	unknown	18552	success or wait	1	4032A8	ReadFile
C:\Users\user\AppData\Local\Temp\nssEC8B.tmp	unknown	4	success or wait	5	405F3F	ReadFile
C:\Users\user\Desktop\PO No. 3200005919.exe	unknown	16384	success or wait	16	405F3F	ReadFile
C:\Users\user\AppData\Local\Temp\nssEC8B.tmp	unknown	16384	success or wait	27	405F3F	ReadFile
C:\Users\user\Overfurnished\Tuberculisation\Woodwose\Circularizations126\Iltningernes\Mellivorous\Oncosis.syl	unknown	2	success or wait	277	4026B6	ReadFile
C:\Users\user\AppData\Local\Temp\nssEC8B.tmp	unknown	4	success or wait	1	405F3F	ReadFile
C:\Users\user\Overfurnished\Tuberculisation\Woodwose\Airward.Sav	unknown	1052672	success or wait	1	1000295D	ReadFile

Registry Activities

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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly