ID: 829392
Sample Name: Rechung-R1663322504.exe
Cookbook: default.jbs
Time: 05:25:10
Date: 18/03/2023
Version: 37.0.0 Beryl

Table of Contents

Table of Contents 2
Windows Analysis Report Rechung-R1663322504.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Threat Intel 4
Malware Configuration 4
Yara Signatures 5
Memory Dumps 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Data Obfuscation 5
Malware Analysis System Evasion 5
Mitre Att&ck Matrix 5
Behavior Graph 5
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 7
URLs 8
Domains and IPs 8
Contacted Domains 8
URLs from Memory and Binaries 8
World Map of Contacted IPs 8
General Information 8
Warnings 9
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASNs 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
C:\Users\user\AppData\Local\Temp\nsw3E4B.tmp\AdvSplash.dll 9
C:\Users\user\AppData\Local\Temp\nsw3E4B.tmp\System.dll 10
C:\Users\user\Separationerne.lnk 10
C:\Users\user\Socialdirektrer\Fornices\Vingummis\Flannelled\Yndighed\Adventure_20.bmp 10
C:\Users\user\Socialdirektrer\Fornices\Vingummis\Flannelled\Yndighed\Dialektforskningen134.Luk 11
C:\Users\user\Socialdirektrer\Vandspildets.Shi37 11
C:\Users\user\Socialdirektrer\media-floppy-symbolic.symbolic.png 11
C:\Users\user\Socialdirektrer\mk.txt 12
Static File Info 12
General 12
File Icon 12
Static PE Info 12
General 12
Authenticode Signature 13
Entrypoint Preview 13
Rich Headers 14
Data Directories 14
Sections 14
Resources 15
Imports 15
Possible Origin 16
Network Behavior 16
Statistics 16
System Behavior 16
Analysis Process: Rechung-R1663322504.exePID: 3332, Parent PID: 3452 16
General 16
File Activities 16
File Created 16
File Deleted 18
File Written 19

File Read 21
Registry Activities 21
Key Created 21
Key Value Created 22
Disassembly 22

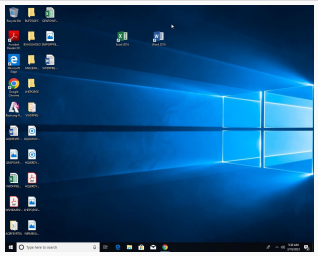
Windows Analysis Report

Rechung-R1663322504.exe

Overview

General Information

Sample Name:	Rechung-R1663322504.exe
Analysis ID:	829392
MD5:	11b5b208de7a…
SHA1:	c578bc317e66…
SHA256:	0a80ba418f561..
Tags:	DEU exe geo signed SnakeKeylogger
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

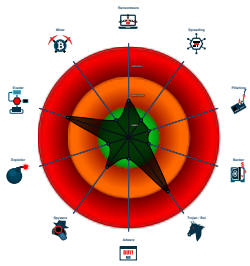
GuLoader

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
- Drops PE files
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- Creates files inside the system direc…
- Detected potential crypto function
- PE / OLE file has an invalid certifica…
- Contains functionality to dynamicall…
- Abnormal high CPU Usage

Classification



Process Tree

- **System is w10x64**
- Rechung-R1663322504.exe (PID: 3332 cmdline: C:\Users\user\Desktop\Rechung-R1663322504.exe MD5: 11B5B208DE7A85B46104A0597C5DA7DC)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
CloudEyE, GuLoader	CloudEyE (initially named GuLoader) is a small VB5/6 downloader. It typically downloads RATs/Stealers, such as Agent Tesla, Arkei/Vidar, Formbook, Lokibot, Netwire and Remcos, often but not always from Google Drive. The downloaded payload is xored.	No Attribution	http://https://0x00sec.org/t/analyzing-modern-malware-techniques-part-3/18943https://blog.malwarebytes.com/scams/2020/08/sba-phishing-scams-from-malware-to-advanced-social-engineering/https://blog.morphisec.com/guloader-the-rat-downloaderhttps://blog.vincss.net/2020/05/re014-guloader-antivm-techniques.htmlhttps://cert-agid.gov.it/news/malware/tecniche-per-semplificare-lanalisi-del-malware-guloader/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.cloudeye

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.774741365.00000000064AB000.00000040.00001000.00020000.00000000.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

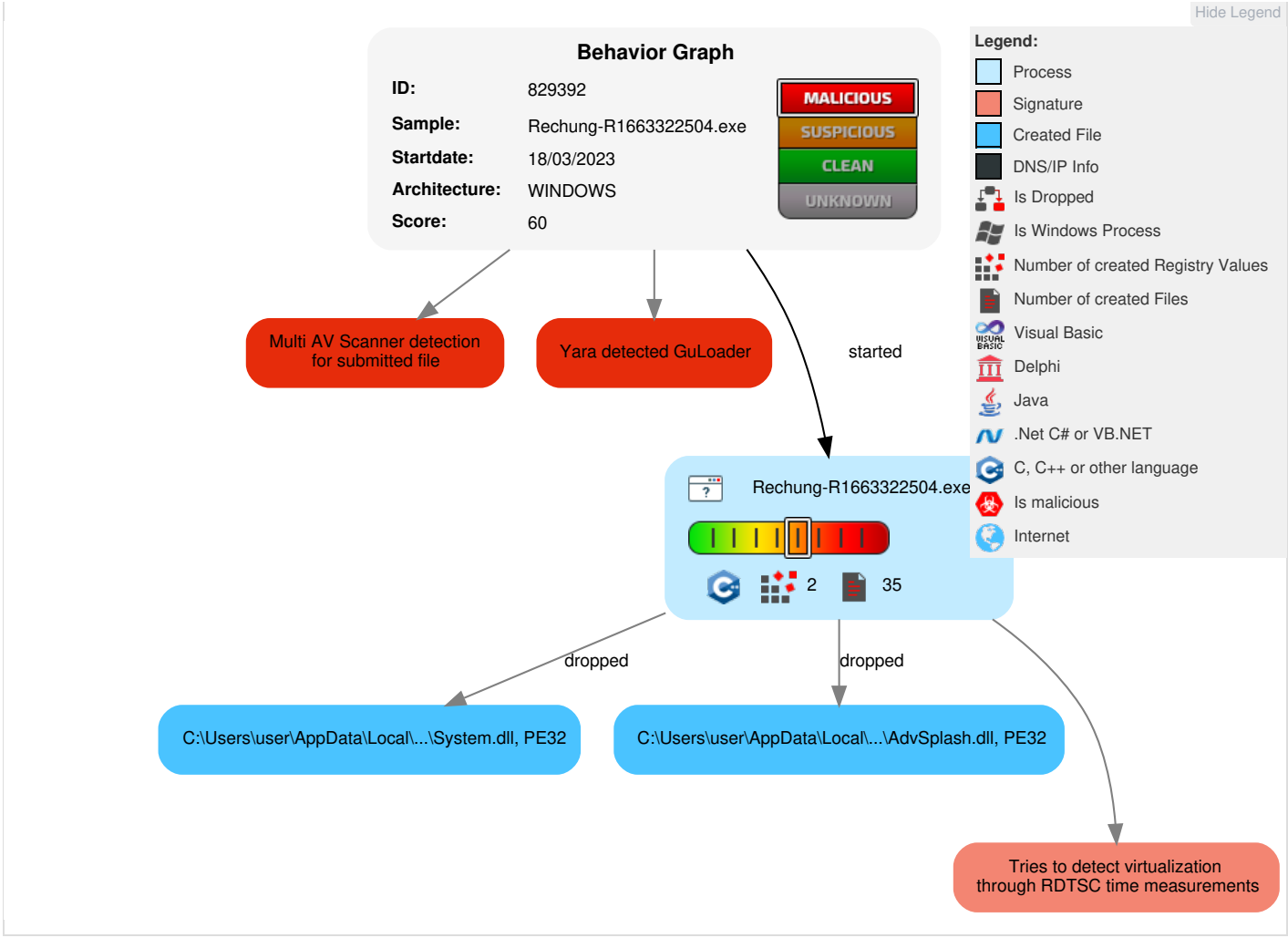
Malware Analysis System Evasion

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	1 Native API	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
Rechung-R1663322504.exe	31%	ReversingLabs	Win32.Trojan.Tnega	
Rechung-R1663322504.exe	38%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsw3E4B.tmp\AdvSplash.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsw3E4B.tmp\AdvSplash.dll	3%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nsw3E4B.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsw3E4B.tmp\System.dll	1%	Virustotal		Browse

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://subca.ocsp-certum.com05	0%	URL Reputation	safe	
http://subca.ocsp-certum.com02	0%	URL Reputation	safe	
http://subca.ocsp-certum.com01	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://crl.certum.pl/ctnca2.crl0l	Rechung-R1663322504.exe	false		high
http://repository.certum.pl/ctnca2.cer09	Rechung-R1663322504.exe	false		high
http://crl.certum.pl/ctsca2021.crl0o	Rechung-R1663322504.exe	false		high
http://repository.certum.pl/ctnca.cer09	Rechung-R1663322504.exe	false		high
http://nsis.sf.net/NSIS_ErrorError	Rechung-R1663322504.exe	false		high
http://repository.certum.pl/ctsca2021.cer0	Rechung-R1663322504.exe	false		high
http://crl.certum.pl/ctnca.crl0k	Rechung-R1663322504.exe	false		high
http://subca.ocsp-certum.com05	Rechung-R1663322504.exe	false	• URL Reputation: safe	unknown
http://www.certum.pl/CPS0	Rechung-R1663322504.exe	false		high
http://subca.ocsp-certum.com02	Rechung-R1663322504.exe	false	• URL Reputation: safe	unknown
http://subca.ocsp-certum.com01	Rechung-R1663322504.exe	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	829392
Start date and time:	2023-03-18 05:25:10 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
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:	15
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
Sample file name:	Rechung-R1663322504.exe
Detection:	MAL
Classification:	mal60.troj.evad.winEXE@1/8@0/0

EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 62.5% (good quality ratio 61%) • Quality average: 88% • Quality standard deviation: 22%
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, audiodg.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- 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\nsw3E4B.tmp\AdvSplash.dll

Process:	C:\Users\user\Desktop\Rechung-R1663322504.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	6144
Entropy (8bit):	4.496995234059773
Encrypted:	false
SSDEEP:	96:1IUNaXnnXyEIPtXvZhr5RwiULuxDtJ1+wolpE:1Ix3XyEwXvZh1RwnLUDtf+I
MD5:	E8B67A37FB41D54A7EDA453309D45D97

SHA1:	96BE9BF7A988D9CEA06150D57CD1DE19F1FEC19E
SHA-256:	2AD232BCCF4CA06CF13475AF87B510C5788AA790785FD50509BE483AFC0E0BCF
SHA-512:	20EFFAE18EEBB2DF90D3186A281FA9233A97998F226F7ADEAD0784FBC787FEEE419973962F8369D8822C1BBCDFB6E7948D9CA6086C9CF90190C8AB3EC97F4C38
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 3%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....+.Y.o.7Eo.7Eo.7Eo.6EF.7E..jEf.7E;..Em.7E..3En.7ERicho.7E..... ..PE..L.....uY.....!.....`..... .....P.....`$..E.... ..d.....@..$..... ..... .text..... ..`.rdata..... .....@..@.data.....0.....@....reloc.....@.....@..B..... ....

C:\Users\user\AppData\Local\Temp\nsw3E4B.tmp\System.dll

Process:	C:\Users\user\Desktop\Rechung-R1663322504.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	11776
Entropy (8bit):	5.659384359264642
Encrypted:	false
SSDEEP:	192:ex24sihno00Wfl97nH6BenXwWobpWBTtvShJ5omi7dJWjOlESlS:h8Qll972eXqlWBFSt273YOlEz
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\Separationerne.lnk

Process:	C:\Users\user\Desktop\Rechung-R1663322504.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):	1274
Entropy (8bit):	3.128346526396717
Encrypted:	false
SSDEEP:	24:8Cf4eWLgD4/BV02De69kqy+pepAFpd7aB:8JXgDszheOTpeeHwB
MD5:	E3BDEAA5B7F272426C9B086E815EF5B8
SHA1:	3789A45941BF4410EBB314C46BBD6DC33AB0D7A5
SHA-256:	41AEE8966E4BBC0AF245942852F14EAF81BAFDD67DC2F512DED93F569FE9A7B1
SHA-512:	ED5D406C653590590015CF3DCFC60F1E014DD132551116CE4F79BFFB181F52F81168E621FF661AA9C5E04B3207ADF3EB71A6CF8013C49E7E7FD21BF28BC5961A
Malicious:	false
Reputation:	low
Preview:	L.....F.....P.O. .:i.....+00.../C:\.....P.1.....Users.<.....U.s.e.r.s.....P.1.....user.<..... .....h.a.r.d.z.....V.1.....AppData.@.....A.p.p.D.a.t.a.....V.1.....Roaming.@.....R.o.a.m.i.n.g.....\.1..... ....Microsoft.D.....M.i.c.r.o.s.o.f.t.....V.1.....Windows.@.....W.i.n.d.o.w.s.....t.1.....Printer Shortcuts.T..... .....P.r.i.n.t.e.r. .S.h.o.r.t.c.u.t.s... .t.2.....Genoptagelsen.Phi.T.....G.e.n.o.p.t.a.g.e.l.s.e.n...P.h.i... ...G...\.A.p.p.D.a.t.a.\.R.o.a.m.i.n.g.\.M.i.c.r.o.s.o.f.t.\.W.i.n.d.o.w.s.\.P.r.i.n.t.e.r. .S.h.o.r.t.c.u.t.s.\.G.e.n.o.p.t.a.g.e.l.s.e

C:\Users\user\Socialdirektrer\Fornices\Vingummis\Flannelled\Yndighed\Adventure_20.bmp

Process:	C:\Users\user\Desktop\Rechung-R1663322504.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 100x100, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=3], baseline, precision 8, 110x110, components 3
Category:	dropped
Size (bytes):	10534

Entropy (8bit):	7.884822059718216
Encrypted:	false
SSDEEP:	192:oXRZxdt62XpqRigPYtY0CfKTQlh5NKW6F5oJxfskCjGmXa6Pbplv26Zzkq:KRfdt62X+XoElh/KW6ifskEGeaIp9zkq
MD5:	A4530760E13B17372AE0D8CB48F66D0D
SHA1:	AA21564FA3A847E59402B62D3F600DDA5046A926
SHA-256:	F37F7A75DC27903EA88D1A3912DFB9123CA217E2467EB6D5DC966F60DC7F9DB7
SHA-512:	E42C32B412CD4AA560EFED98050F4B2F858190EA8BF56A81311F24C6F0751E2E397F624777E759BC80B1D34BF0AA9ECF6356E26D553D22E503A53CEF76797D4
Malicious:	false
Reputation:	low
Preview:	......JFIF.....d.d.....:Exif..MM.*.....Q.....Q.....Q.....aQ.....a.....C.....C.....n.n.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....(..9...k....X.....&.2.Z.....k~I.....e...J...}..<..M..8.....".../...O.u.....5.h...71]ZZ.....v..Yc...<.i'..m2_..>..#...K...,.qq.^<2\|D.V...j..ae.0Mu.^K..#k..3<."F V$HV.)..vmG..H.....z.\..#.....3_..Wo.g.>.o.....|...V.}.Ho.]...q#..W667Z`..)..I._E'.....+\.w..K....O.o..5.....4O..~.

C:\Users\user\Socialdirektrer\Fornices\Vingummis\Flannelled\Yndighed\Dialektforskningen134.Luk

Process:	C:\Users\user\Desktop\Rechung-R1663322504.exe
File Type:	ASCII text, with very long lines (35012), with no line terminators
Category:	dropped
Size (bytes):	35012
Entropy (8bit):	2.713079331895783
Encrypted:	false
SSDEEP:	768:YOYEtjBKsUje7ciMsO9Z/mAXEEEJu+am7luxsr6mPpHOEEEEESW0ymwpTiq:d4/98AEMRNPpHrViq
MD5:	F75A78EE11492D9F9146075023D485D3
SHA1:	772AE864C11AE2C45834F681EFDF662BBD28268B
SHA-256:	5916C8773319EA24B225C76FE361D360360CE03E1F61E2E86387514A185BDAF9
SHA-512:	BB2D74E9F7D7F02E682E302B115C280C886F4E99789F4E5A198E7B2E973FFBE788559140CC2625EE8F754831497E67038CA327196EC14370968B47828863BD0D
Malicious:	false
Reputation:	low
Preview:	0000000000000F00007200F400C000D900DDDD00009D005D5D5D000E0E0E0E00C20000005F5F5F00E4E4E400000000009B0013000026262600A90000 8C006D0032320036000000171700870 0C600B4B400007900B0B0B0B0000000006F6F004C4C00590000003F000041414100004C00C1C1C10000004A4A00000000AA AA0000000000F10039390000000043000 0AC00F6000093002600C5C5C5000000029000067000020000000AE0000006700010000000004D005D5D5D0000E0E00046 46464600C90000202000D8000086005700BDBD00007000212100FC0006060606000800680000000000D8D800A7000060600092 00A4004600D000CCCC00E9E90000 005700F600888888002700CCCC00000000006F6F00D9003D3D3D009F000000000000DDDDDD0000B2000000001B0000CD003D3D00060606005D5D0000 B5B5B5B5009898007100DE000F000000F0F0F000BDBD000000000012121200000004800E1003A3A3A005656560000000 00B60000000001300272727 00E90000000096 96004B00770078000000A8000000DCDC0007070700C8005959595959000D000000840000740000EAEA00D9D9D9D900000000A70000B70000828282820000780082 8200000000000000515151007878000022220 08E0000DB00001E0000DD006C00FA00000000AAAA000000950000002500CF00000000A000

C:\Users\user\Socialdirektrer\Vandspildets.Shi37

Process:	C:\Users\user\Desktop\Rechung-R1663322504.exe
File Type:	data
Category:	dropped
Size (bytes):	225168
Entropy (8bit):	7.3676127973119225
Encrypted:	false
SSDEEP:	3072:NOUzxidFkCI6+rXNfJEow2a5KTa49D1bdzeDZ/7SkPtnWpA2Or1/nD9kS/fmi:s9dFrl6ifJLwV0/9Jd4RSYtWpBanD9kG
MD5:	BAFC11E1543369B58D7852857D986EFA
SHA1:	A00AD13ECA7F98C1CBBC7AE32151D3878DD2BBB0
SHA-256:	F8D1014289006D2ACCAB3D5A1C36CD867B4D6BEC50781365175B4FF8323A5E81
SHA-512:	69883FDF36A90C35625D74BF7FE5808AFD1F88314EF60FAB7785C443BD992F72656BB727E3E44503266BECC28A48E0BAF7DF70A6C5CAA10D2B2DFED28C07AA 02
Malicious:	false
Reputation:	low
Preview:	.....t..cc.....dd.@@.rr..ZZ.====.....vvvvv.""...i..SS.....((.v.....dd.....K.....m.....OO.....@@.....00._..... ...XX...EE..$$.HHHHHH.....m.....nn.....oo.....hhh.....__.....^.7.....#.....1..-.....H...J.....???.....|..>.^.W..... .....H..^^^^^..???.CCC..n.....nnn.xx.....;.....E.....&&&&.....hhh....W.....?.ss....B.b....III.....#.....q.....Q.s...#... .....%...nn.EE.....||.....___.....p.....R.88.....$.....LL.....k.....I...".pp.....:.aa.....].....&.....jj..`.JJ.....//.... e...^^^^^^^^^^....2.p.....I.....$.....oo.....E.....

C:\Users\user\Socialdirektrer\media-floppy-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\Rechung-R1663322504.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	183

Entropy (8bit):	6.337608034945541
Encrypted:	false
SSDEEP:	3:yionv//thPl9vt3lAnsrtxBllTV00EDgZ1uP6he3LFIY8roNQh/e9OuTB+Mg1J7d:6v/lhPysY0EeDyLiRroCh/0B+v1MC1jp
MD5:	293D1D4F18C3A918A44FAD289715E950
SHA1:	BD92A45835DD693FE8D0B72F296FE0134D46B876
SHA-256:	553F673950BE4DE71377A297050888D0BE5A997DB334781994C3265EDA30C7B3
SHA-512:	E62D45E30997EB18EB3C45BC1574C75462DC4CC36144D4E529F917B6091ADD14F91779F5C428458CEA129EF37B27FDDBBCEA8E5005563DC2AABCB370BEDF2E8C
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d....nIDAT8.....0...wp(.....,...J.A[.O....i.4..x d..F.(.N.$ .su.w.C.~..XyZ.|.....k....z`../..aA.<.>....j.. ...=....z....IEND.B`.

C:\Users\user\Socialdirektrer\mk.txt

Process:	C:\Users\user\Desktop\Rechung-R1663322504.exe
File Type:	Unicode text, UTF-8 (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	8934
Entropy (8bit):	4.259244159879149
Encrypted:	false
SSDEEP:	192:ia3g0F7SHayJ5vKVEB3Bxg5GteGIxpWNMll39oWvt/i4drxJ4MrZEXSW:iWg0zyJlKVEB3A6SM2mWvt/i4dtJ4MNO
MD5:	71D42ABE45803AC9C3DA5FCACF9CC59C
SHA1:	98A1049906972ABB480ABAF1F5658C1B8C10F27C
SHA-256:	78F5CB9345AB258CF745EAA90D44C7A7A73D3FE06EA182B1298A989135FFA11F
SHA-512:	A0096575D6F911CC2600DAC93D6FD7AA8D9E2F9F71A92571A76996FB4C47BDB714BBA453C862B3F42CC5F4BAAF2AED1DFF3C9D6F84A3E2053FF2037C56AB85A5
Malicious:	false
Preview:	.;!@Lang2@!UTF-8!..; 4.09 : Gabriel Stojanoski..;.;.;.;.;.;.;.;.;.;.;..0..7-Zip..Macedonian.....401.....&....&....&.....&.....440.... &..... .&..... .....&.....&.....&..... ....?..500..&.....&.....&.....&.....&.....&.....540..&..... &..... &.....&.....&.....&.....&..... .....&. ....&.....&..... .....&..... .....&.....&..... ....&.....600..... &..... ...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.1116261135004395
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:	Rechung-R1663322504.exe
File size:	416280
MD5:	11b5b208de7a85b46104a0597c5da7dc
SHA1:	c578bc317e666159cbfc191cb4e50de2de03ab79
SHA256:	0a80ba418f561098477e18cc42ddfc31796b2be3166ff6c99967b98388fe4826
SHA512:	c79e0deeb1686edc5bfe2db026f423277740fe816a674a3111fb36fd4813825a080048b44d03e92310db526a8c791259684778f8dea0861cd9b26e2f5f0b5d23
SSDEEP:	6144:16bAcJtT+SdoujpZM5DMJ+VGM1IMwJ1OPH7USLahNcfM9rQ09j3V/PySssz:2APSbyDMOJrOPH7UfnpCSD
TLSH:	B694BFA0F620D0DADCB417F16C9FD9211AE76EECE4E0220F65A73259AD736D3051F24A
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!`G.@...@...@../OQ..@...@..I@../OS..@...c>..@..+F...@..Rich.@.....PE..L.....uY.....d....'....

File Icon

Icon Hash:	f169e8e4e4ccca88

Static PE Info

General

Entrypoint:	0x403350
Entrypoint Section:	.text

Digitally signed:	true
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:	0x59759518 [Mon Jul 24 06:35:04 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:	b34f154ec913d2d2c435cbd644e91687

Authenticode Signature	
Signature Valid:	**false**
Signature Issuer:	E=Departmentalizations@Trisulphide193.Lok, OU="Pasteuriseringens Eternellerne ", O=Stikprvestandardafvigelsernes, L=Dividing Creek, S=New Jersey, C=US
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 12/27/2022 3:19:02 AM 12/26/2025 3:19:02 AM
Subject Chain	• E=Departmentalizations@Trisulphide193.Lok, OU="Pasteuriseringens Eternellerne ", O=Stikprvestandardafvigelsernes, L=Dividing Creek, S=New Jersey, C=US
Version:	3
Thumbprint MD5:	1F7F4BF42A830708AC95921509004FCC
Thumbprint SHA-1:	54B3D870C522C1CA544E3D38597EEC9DC6D3C3A0
Thumbprint SHA-256:	ED0BD8E407BDD2EB9D4B7BDFEC49D761B0F85D212BDFDC1A3F9981BBA4AD638B
Serial:	4122AFC051A99F02AE188FBC961AC5C36F876297

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], 0040A2E0h
mov dword ptr [esp+1Ch], ebx
call dword ptr [004080A8h]
call dword ptr [004080A4h]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [007A8A2Ch], eax
je 00007FB134BEE563h
push ebx
call 00007FB134BF17F9h
cmp eax, ebx
je 00007FB134BEE559h
push 00000C00h
call eax
mov esi, 004082B0h
push esi
call 00007FB134BF1773h
push esi

Instruction
call dword ptr [00408150h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], 00000000h
jne 00007FB134BEE53Ch
push 0000000Ah
call 00007FB134BF17CCh
push 00000008h
call 00007FB134BF17C5h
push 00000006h
mov dword ptr [007A8A24h], eax
call 00007FB134BF17B9h
cmp eax, ebx
je 00007FB134BEE561h
push 0000001Eh
call eax
test eax, eax
je 00007FB134BEE559h
or byte ptr [007A8A2Fh], 00000040h
push ebp
call dword ptr [00408044h]
push ebx
call dword ptr [004082A0h]
mov dword ptr [007A8AF8h], eax
push ebx
lea eax, dword ptr [esp+34h]
push 000002B4h
push eax
push ebx
push 0079FEE0h
call dword ptr [00408188h]
push 0040A2C8h

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	0x3d3000	0x281f0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x63778	0x22a0	.data
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	0x63c8	0x6400	False	0.6766015625	data	6.504099201068482	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rdata	0x8000	0x138e	0x1400	False	0.4509765625	data	5.146454805063938	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x39eb38	0x600	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x3a9000	0x2a000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x3d3000	0x281f0	0x28200	False	0.35579731308411217	data	5.085440369030725	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3d3310	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 65536	English	United States
RT_ICON	0x3e3b38	0x94a8	Device independent bitmap graphic, 96 x 192 x 32, image size 36864	English	United States
RT_ICON	0x3ecfe0	0x5488	Device independent bitmap graphic, 72 x 144 x 32, image size 20736	English	United States
RT_ICON	0x3f2468	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16384	English	United States
RT_ICON	0x3f6690	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216	English	United States
RT_ICON	0x3f8c38	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096	English	United States
RT_ICON	0x3f9ce0	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2304	English	United States
RT_ICON	0x3fa668	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1024	English	United States
RT_DIALOG	0x3faad0	0x120	data	English	United States
RT_DIALOG	0x3fabf0	0x11c	data	English	United States
RT_DIALOG	0x3fad10	0xc4	data	English	United States
RT_DIALOG	0x3fadd8	0x60	data	English	United States
RT_GROUP_ICON	0x3fae38	0x76	data	English	United States
RT_MANIFEST	0x3faeb0	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States

Imports

DLL	Import
KERNEL32.dll	SetEnvironmentVariableW, SetFileAttributesW, Sleep, GetTickCount, GetFileSize, GetModuleFileNameW, GetCurrentProcess, CopyFileW, SetCurrentDirectoryW, GetFileAttributesW, GetWindowsDirectoryW, GetTempPathW, GetCommandLineW, GetVersion, SetErrorMode, lstrlenW, lstrcpynW, GetDiskFreeSpaceW, ExitProcess, GetShortPathNameW, CreateThread, GetLastError, CreateDirectoryW, CreateProcessW, RemoveDirectoryW, lstrcmpiA, CreateFileW, GetTempFileNameW, WriteFile, lstrcpyA, MoveFileExW, lstrcatW, GetSystemDirectoryW, GetProcAddress, GetModuleHandleA, GetExitCodeProcess, WaitForSingleObject, lstrcmpiW, MoveFileW, GetFullPathNameW, SetFileTime, SearchPathW, CompareFileTime, lstrcmpW, CloseHandle, ExpandEnvironmentStringsW, GlobalFree, GlobalLock, GlobalUnlock, 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

Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.

Statistics

No statistics

System Behavior

Analysis Process: Rechung-R1663322504.exe PID: 3332, Parent PID: 3452

General

Target ID:	0
Start time:	05:26:04
Start date:	18/03/2023
Path:	C:\Users\user\Desktop\Rechung-R1663322504.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Rechung-R1663322504.exe
Imagebase:	0x400000
File size:	416280 bytes
MD5 hash:	11B5B208DE7A85B46104A0597C5DA7DC
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: 00000000.00000002.774741365.00000000064AB000.00000040.00001000.00020000.00000000.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	40581B	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsv3DAD.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405DBF	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsw3E4B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405DBF	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	40581B	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	40581B	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	40581B	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	40581B	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	40581B	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsw3E4B.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	4057DB	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsw3E4B.tmp\AdvSplash.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D7D	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	3	40581B	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	40581B	CreateDirectoryW
C:\Users\user\Socialdirektrer	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40581B	CreateDirectoryW
C:\Users\user\Socialdirektrer\Vandspildets.Shi37	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D7D	CreateFileW
C:\Users\user\Socialdirektrer	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	2	40581B	CreateDirectoryW
C:\Users\user\Socialdirektrer\Fornices	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40581B	CreateDirectoryW
C:\Users\user\Socialdirektrer\Fornices\Vingummis	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40581B	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Socialdirektrer\Fornices\Vingummis\Flannelled	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40581B	CreateDirectoryW
C:\Users\user\Socialdirektrer\Fornices\Vingummis\Flannelled\Yndighed	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40581B	CreateDirectoryW
C:\Users\user\Socialdirektrer\Fornices\Vingummis\Flannelled\Yndighed\Adventure_20.bmp	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D7D	CreateFileW
C:\Users\user\Socialdirektrer\Fornices\Vingummis\Flannelled\Yndighed\Dialektforskningen134.Luk	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D7D	CreateFileW
C:\Users\user\Socialdirektrer\media-floppy-symbolic.symbolic.png	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D7D	CreateFileW
C:\Users\user\Socialdirektrer\mk.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D7D	CreateFileW
C:\Users\user\AppData\Local\Temp\nsw3E4B.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405D7D	CreateFileW
C:\Windows	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	4	40581B	CreateDirectoryW
C:\Windows\SysWOW64	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	4	40581B	CreateDirectoryW
C:\Windows\SysWOW64\Arbejdsglderne	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40581B	CreateDirectoryW
C:\Windows\SysWOW64\Arbejdsglderne\Baal	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40581B	CreateDirectoryW
C:\Windows\SysWOW64\Arbejdsglderne\Baal\Cashboxes122	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40581B	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsw3E4B.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	4	405D7D	CreateFileW
C:\Windows\SysWOW64\Arbejdsglderne	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	40581B	CreateDirectoryW
C:\Windows\SysWOW64\Arbejdsglderne\Baal	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	40581B	CreateDirectoryW
C:\Windows\SysWOW64\Arbejdsglderne\Baal\Cashboxes122	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	3	40581B	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsv3DAD.tmp	success or wait	1	403601	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsw3E4B.tmp	success or wait	1	40599C	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsw3E4B.tmp\AdvSplash.dll	0	6144	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 2b fd 59 16 6f fd 37 45 6f fd 37 45 6f fd 37 45 6f fd 36 45 46 fd 37 45 fd fd 6a 45 66 fd 37 45 3b fd 07 45 6d fd 37 45 fd fd 33 45 6e fd 37 45 52 69 63 68 6f fd 37 45 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 08 fd 75 59 00 00 00 00 00 00 00 00 fd 00 0e 21 0b 01 06 00 00 0a 00 00 00 0a 00 00 00 00 00 00 60 11 00 00 00 10 00 00 00 20 00 00 00 00 00 10 00 10 00 00 00 02 00	MZ@!L!This program cannot be run in DOS mode.$+Yo7Eo7Eo7Eo6E F7EjEf7E;Em7E3En7ERicho7EPELuY!`	success or wait	1	405E1D	WriteFile
C:\Users\user\Socialdirektrer\Vandspildets.Shi37	0	32768	00 00 00 00 00 00 00 fd 00 07 00 00 08 08 08 08 00 00 00 fd fd fd fd 00 00 fd fd 00 fd fd 00 00 00 74 00 00 63 63 00 00 1f 00 00 fd 00 fd 00 00 fd fd 00 fd fd fd 00 00 64 64 00 40 40 00 72 72 00 00 5a 5a 00 3d 3d 3d 3d 00 1b 1b 00 00 00 fd 00 76 76 76 76 76 00 22 22 00 00 00 69 00 00 53 53 00 fd 00 00 13 13 13 00 fd fd 00 28 28 00 76 00 11 11 00 00 fd fd 00 64 64 00 00 fd 00 00 00 00 fd fd 00 fd 00 00 00 00 4b 00 fd 00 00 fd fd 00 00 fd 00 00 12 00 00 00 02 00 6d 00 00 00 00 00 00 15 00 fd 00 00 00 00 fd fd 00 00 4f 4f 00 00 1f 00 00 fd 00 fd 00 00 40 40 00 02 00 fd fd 00 00 00 fd 00 14 14 14 00 00 00 00 fd 00 30 30 00 5f 00 0a 0a 00 00 00 00 00 fd fd 00 00 00 58 58 00 00 00 45 45 00 00 24 24 00 48 48 48 48 48 48 00 00 fd 00 fd fd fd fd 00 00 00 fd 00 00	tccdd@@rrZZ====vvvvv ""iSS((vdd KmOO@@00_XXEE$$HHHHHH	success or wait	7	405E1D	WriteFile

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\Socialdirektrer\Fornices\Vingummis\Flannelled\Yndighed\Adventure_20.bmp</td><td>0</td><td>10534</td><td>fd fd fd fd 00 10 4a 46 49 46 00 01 01 01 00 64 00 64 00 00 fd fd 00 3a 45 78 69 66 00 00 4d 4d 00 2a 00 00 00 08 00 03 51 10 00 01 00 00 00 01 01 00 00 00 51 11 00 04 00 00 00 01 00 00 0f 61 51 12 00 04 00 00 00 01 00 00 0f 61 00 00 00 00 fd fd 00 43 00 02 01 01 01 01 01 02 01 01 01 02 02 02 02 02 04 03 02 02 02 02 05 04 04 03 04 06 05 06 06 06 05 06 06 06 07 09 08 06 07 09 07 06 06 08 0b 08 09 0a 0a 0a 0a 0a 06 08 0b 0c 0b 0a 0c 09 0a 0a 0a fd fd 00 43 01 02 02 02 02 02 02 05 03 03 05 0a 07 06 07 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a 0a fd fd 00 11 08 00 6e 00 6e 03 01 22 00 02 11 01 03 11 01 fd fd 00 1f 00 00 01 05 01 01 01 01 01 01 00 00 00 00</td><td>JFIFdd:ExifMM*QQaQaC
Cnn"</td><td>success or wait</td><td>1</td><td>405E1D</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\Socialdirektrer\Fornices\Vingummis\Flannelled\Yndighed\Dialektforskningen134.Luk</td><td>0</td><td>32768</td><td>30 30 30 30 30 30 30 30 30 30 30 30 30 46 30 30 30 30 37 32 30 30 46 34 30 30 43 30 30 30 44 39 30 30 44 44 44 44 30 30 30 30 39 44 30 30 35 44 35 44 35 44 30 30 30 45 30 45 30 45 30 45 30 30 43 32 30 30 30 30 30 30 35 46 35 46 35 46 30 30 45 34 45 34 45 34 30 30 30 30 30 30 30 30 30 30 39 42 30 30 31 33 30 30 30 30 32 36 32 36 32 36 30 30 41 39 30 30 30 30 38 43 30 30 36 44 30 30 33 32 33 32 30 30 33 36 30 30 30 30 30 30 31 37 31 37 30 30 38 37 30 30 43 36 30 30 42 34 42 34 30 30 30 30 37 39 30 30 42 30 42 30 42 30 42 30 30 30 30 30 30 30 30 30 36 46 36 46 30 30 34 43 34 43 30 30 35 39 30 30 30 30 30 30 33 46 30 30 30 30 34 31 34 31 34 31 30 30 30 30 34 43 30 30 43 31 43 31 43 31 30 30 30 30 30 30 34 41 34 41 30 30 30 30 30 30 30 30 41 41 41 41 30 30 30</td><td>0000000000000F0000720
0F400C000
D900DDDD00009D005D5
D5D000E0E0E
0E00C20000005F5F5F00
E4E4E40000
0000009B001300002626
2600A90000
8C006D00323200360000
0017170087
00C600B4B400007900B0
B0B0B00000
00006F6F004C4C005900
00003F0000
41414100004C00C1C1C1
0000004A4A
00000000AAAA000</td><td>success or wait</td><td>2</td><td>405E1D</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\Socialdirektrer\media-floppy-symbolic.symbolic.png</td><td>0</td><td>183</td><td>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 6e 49 44 41 54 38 fd fd fd 09 fd 30 0c 05 0f 77 70 28 6d fd 05 fd 09 2c fd fd fd fd 4a fd 41 5b fd 4f 1f 04 90 1c 69 1e 34 fd 04 78 20 64 fd 07 46 09 28 19 4e fd 24 20 15 73 75 fd 77 05 43 fd 7e fd 0d 58 79 5a fd 7c fd fd fd fd fd 6b fd fd f8 c2 7a 60 fd fd 2f fd fd 61 41 fd 3c fd 3e fd 00 0e 18 6a fd 06 20 02 fd fd 3d fd fd fd fd 7a 00 00 00 00 49 45 4e 44 fd 42 60 fd</td><td>PNGIHDRasBIT|dnIDAT8
0wp(,JA[Oi4x dF(N$
suwC~XyZ|kz`/aA<>j =z<br>IENDB`</td><td>success or wait</td><td>1</td><td>405E1D</td><td>WriteFile</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Socialdirektrer\mk.txt	0	8934	ff 3b 21 40 4c 61 6e 67 32 40 21 55 54 46 2d 38 21 0d 0a 3b 20 20 34 2e 30 39 20 3a 20 47 61 62 72 69 65 6c 20 53 74 6f 6a 61 6e 6f 73 6b 69 0d 0a 3b 0d 0a 3b 0d 0a 3b 0d 0a 3b 0d 0a 3b 0d 0a 3b 0d 0a 3b 0d 0a 3b 0d 0a 3b 0d 0a 3b 0d 0a 30 0d 0a 37 2d 5a 69 70 0d 0a 4d 61 63 65 64 6f 6e 69 61 6e 0d 0a 1c 30 3a 35 34 3e 3d 41 3a 38 0d 0a 34 30 31 0d 0a 1e 3a 0d 0a 1e 42 3a 30 36 38 0d 0a 0d 0a 0d 0a 0d 0a 26 14 30 0d 0a 26 1d 35 0d 0a 26 17 30 42 32 3e 40 38 0d 0a 1f 3e 3c 3e 48 0d 0a 0d 0a 1f 26 40 3e 34 3e 3b 36 38 0d 0a 34 34 30 0d 0a 14 30 20 26 21 38 42 35 0d 0a 1d 35 20 1d 26 38 35 34	;!@Lang2@!UTF-8!; 4.09 : Gabriel Stojanoski;;;;;;;;;;07-Zip Macedonian401&&&&440 & &	success or wait	1	405E1D	WriteFile
C:\Users\user\AppData\Local\Temp\nsw3E4B.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 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 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	405E1D	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Rechung-R1663322504.exe	unknown	512	success or wait	395	405DEE	ReadFile
C:\Users\user\Desktop\Rechung-R1663322504.exe	unknown	4	success or wait	2	405DEE	ReadFile
C:\Users\user\Desktop\Rechung-R1663322504.exe	unknown	4	success or wait	22	405DEE	ReadFile
C:\Users\user\Socialdirektrer\Fornices\Vingummis\Flannelled\Yndighed\Dialektforskningen134.Luk	unknown	2	success or wait	1023	4026B6	ReadFile
C:\Users\user\Desktop\Rechung-R1663322504.exe	unknown	4	success or wait	2	405DEE	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\InstallDir32	success or wait	1	406129	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Aminosyrefordelingen	success or wait	1	406129	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Aminosyrefordelingen\Hyperesthete	success or wait	1	406129	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Aminosyrefordelingen\Hyperesthete\Pyemias	success or wait	1	406129	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Aminosyrefordelingen\Hyperesthete\Pyemias\hydrophidae	success or wait	1	406129	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\InstallDir32	Path	unicode	256	success or wait	1	40246F	RegSetValueExW
HKEY_CURRENT_USER\Software\Ami nosyrefordelingen\Hyperesthete\Pyemias\hydrophidae	Opinionsdannendes	expand unicode	%Stngningers%\Overdebate.For	success or wait	1	40246F	RegSetValueExW

Disassembly

No disassembly