ID: 755464
Sample Name: documentos DHL.exe
Cookbook: default.jbs
Time: 19:00:32
Date: 28/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

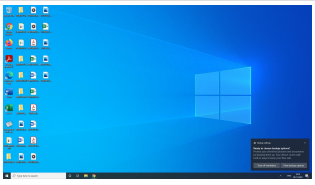
Windows Analysis Report

documentos DHL.exe

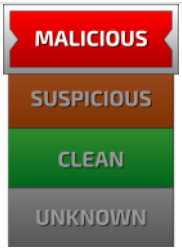
Overview

General Information

Sample Name:	documentos DHL.exe
Analysis ID:	755464
MD5:	ca1cd0656568af…
SHA1:	1fde05eb6e5870..
SHA256:	6931d5a8ac6e00..
Infos:	



Detection



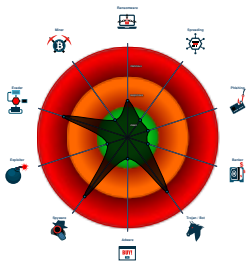
GuLoader

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Tries to steal Mail credentials (via fi…
- Initial sample is a PE file and has a…
- Found stalling execution ending in A…
- Tries to harvest and steal Putty / W…
- Tries to detect Any.run
- Tries to harvest and steal ftp login c…
- Executable has a suspicious name …
- Tries to harvest and steal browser in…
- Uses 32bit PE files
- Contains functionality to shutdown /…

Classification



Process Tree

- **System is w10x64native**
- documentos DHL.exe (PID: 7424 cmdline: C:\Users\user\Desktop\documentos DHL.exe MD5: CA1CD0656568AF4F58AA28E61A3E3EDB)
  - ieinstal.exe (PID: 8576 cmdline: C:\Users\user\Desktop\documentos DHL.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
  - ieinstal.exe (PID: 8584 cmdline: C:\Users\user\Desktop\documentos DHL.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
  - ieinstal.exe (PID: 8596 cmdline: C:\Users\user\Desktop\documentos DHL.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
  - ieinstal.exe (PID: 8604 cmdline: C:\Users\user\Desktop\documentos DHL.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
  - ieinstal.exe (PID: 8612 cmdline: C:\Users\user\Desktop\documentos DHL.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
  - ieinstal.exe (PID: 8620 cmdline: C:\Users\user\Desktop\documentos DHL.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
  - ieinstal.exe (PID: 8628 cmdline: C:\Users\user\Desktop\documentos DHL.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
  - ieinstal.exe (PID: 8640 cmdline: C:\Users\user\Desktop\documentos DHL.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
  - ieinstal.exe (PID: 8648 cmdline: C:\Users\user\Desktop\documentos DHL.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
  - ieinstal.exe (PID: 8672 cmdline: C:\Users\user\Desktop\documentos DHL.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
  - ieinstal.exe (PID: 8680 cmdline: C:\Users\user\Desktop\documentos DHL.exe MD5: 7871873BABCEA94FBA13900B561C7C55)
  - ielowutil.exe (PID: 8688 cmdline: C:\Users\user\Desktop\documentos DHL.exe MD5: 650FE7460630188008BF8C8153526CEB)
  - ielowutil.exe (PID: 8696 cmdline: C:\Users\user\Desktop\documentos DHL.exe MD5: 650FE7460630188008BF8C8153526CEB)
  - ielowutil.exe (PID: 8704 cmdline: C:\Users\user\Desktop\documentos DHL.exe MD5: 650FE7460630188008BF8C8153526CEB)
  - ielowutil.exe (PID: 8712 cmdline: C:\Users\user\Desktop\documentos DHL.exe MD5: 650FE7460630188008BF8C8153526CEB)
  - ielowutil.exe (PID: 8720 cmdline: C:\Users\user\Desktop\documentos DHL.exe MD5: 650FE7460630188008BF8C8153526CEB)
  - ielowutil.exe (PID: 8728 cmdline: C:\Users\user\Desktop\documentos DHL.exe MD5: 650FE7460630188008BF8C8153526CEB)
  - ielowutil.exe (PID: 8736 cmdline: C:\Users\user\Desktop\documentos DHL.exe MD5: 650FE7460630188008BF8C8153526CEB)
  - ielowutil.exe (PID: 8748 cmdline: C:\Users\user\Desktop\documentos DHL.exe MD5: 650FE7460630188008BF8C8153526CEB)
  - ielowutil.exe (PID: 8760 cmdline: C:\Users\user\Desktop\documentos DHL.exe MD5: 650FE7460630188008BF8C8153526CEB)
  - ielowutil.exe (PID: 8776 cmdline: C:\Users\user\Desktop\documentos DHL.exe MD5: 650FE7460630188008BF8C8153526CEB)
  - ExtExport.exe (PID: 8784 cmdline: C:\Users\user\Desktop\documentos DHL.exe MD5: 3253FD643C51C133C3489A146781913B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000025.00000002.1820565807.0000000002A00000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000025.00000000.1618126975.0000000002A00000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000002.00000002.1824658615.0000000003370000.00000040.00001000.00020000.00000000.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

Multi AV Scanner detection for submitted file

System Summary

Initial sample is a PE file and has a suspicious name

Executable has a suspicious name (potential lure to open the executable)

Data Obfuscation

Yara detected GuLoader

Malware Analysis System Evasion

Found stalling execution ending in API Sleep call

Tries to detect Any.run

Stealing of Sensitive Information

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

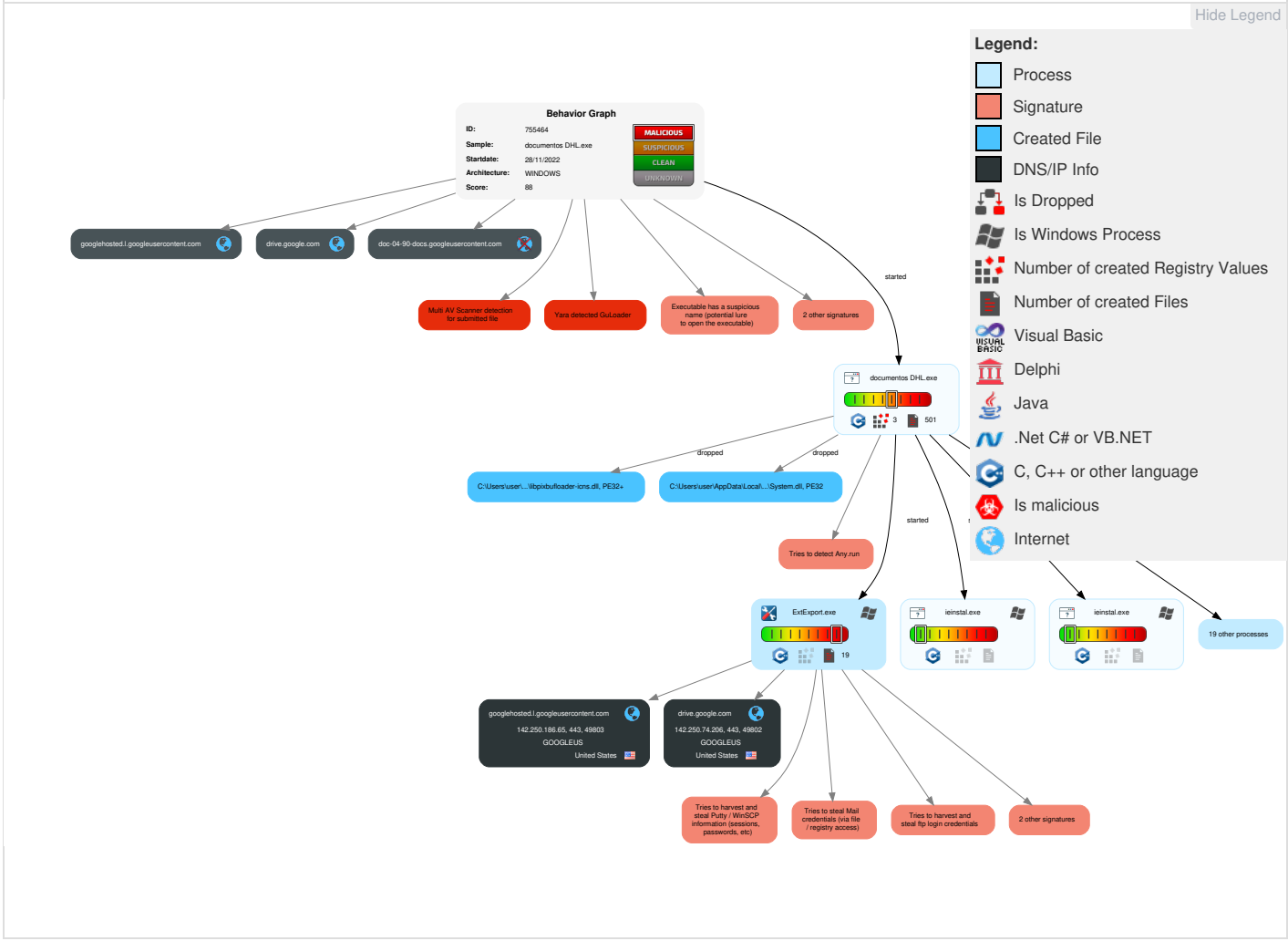
Tries to harvest and steal ftp login credentials

Tries to harvest and steal browser information (history, passwords, etc)

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	1 DLL Side-Loading	1 Access Token Manipulation	1 Masquerading	2 OS Credential Dumping	1 2 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 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	1 1 Process Injection	1 1 Virtualization/Sandbox Evasion	1 Credentials in Registry	1 1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 DLL Side-Loading	1 Access Token Manipulation	Security Account Manager	4 File and Directory Discovery	SMB/Windows Admin Shares	2 Data from Local System	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Process Injection	NTDS	6 System Information Discovery	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 DLL Side-Loading	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

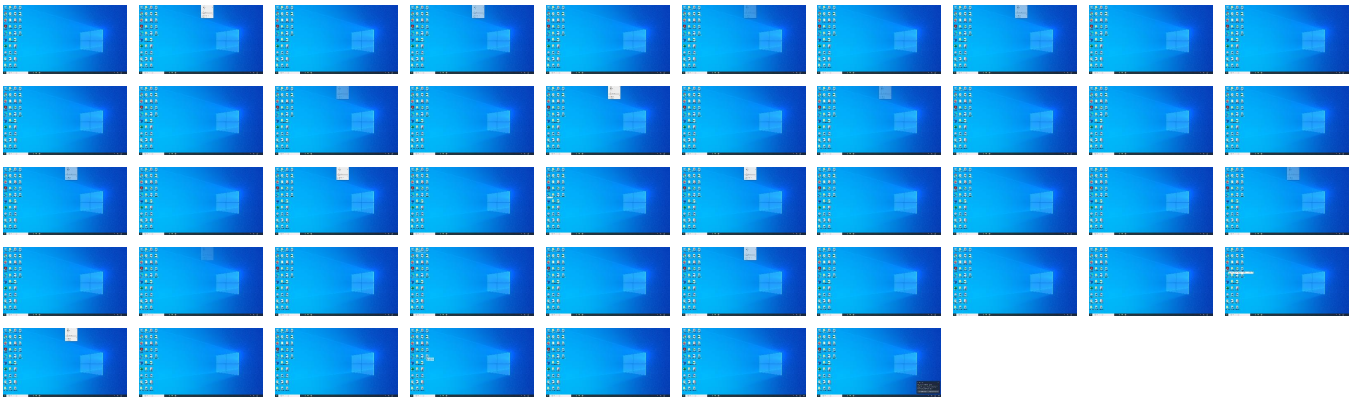
Behavior Graph

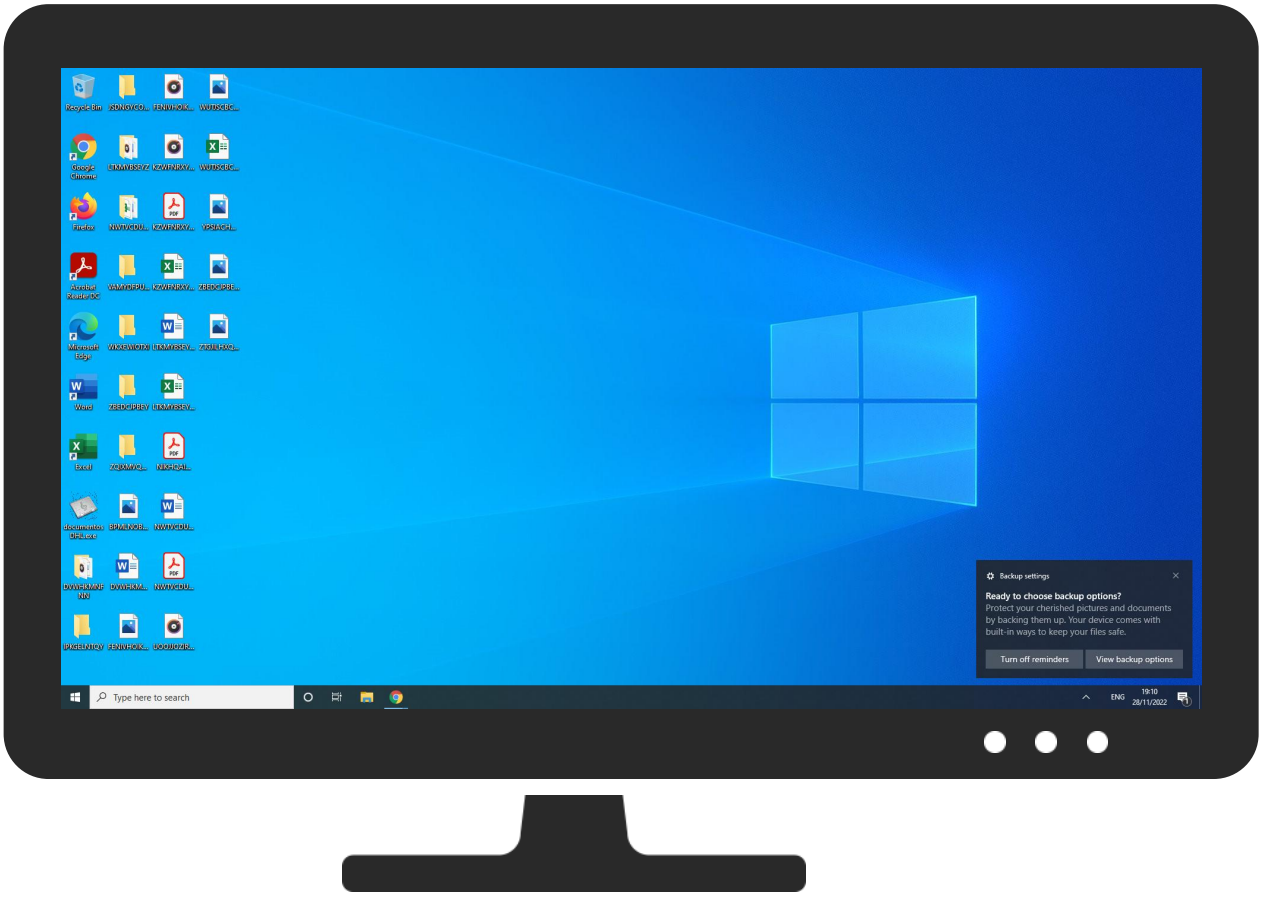


Screenshots

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
documentos DHL.exe	18%	ReversingLabs	Win32.Downloader.Minix	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsw5DC6.tmp\System.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsw5DC6.tmp\System.dll	1%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\Zorillinae\Skaalpundet\Inkbslistes\Tset\Demodulationen\Iagttagerposition\libpixbufloader-icns.dll	0%	ReversingLabs		
C:\Users\user\Zorillinae\Skaalpundet\Inkbslistes\Tset\Demodulationen\Iagttagerposition\libpixbufloader-icns.dll	0%	Virustotal		Browse

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://csp.withgoogle.com/csp/report-to/DriveUntrustedContentHttp/external	0%	Avira URL Cloud	safe	
http://https://csp.withgoogle.com/csp/report-to/DriveUntrustedContentHttp/external	0%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
drive.google.com	142.250.74.206	true	false		high
googlehosted.l.googleusercontent.com	142.250.186.65	true	false		high
doc-04-90-docs.googleusercontent.com	unknown	unknown	false		high

Contacted URLs

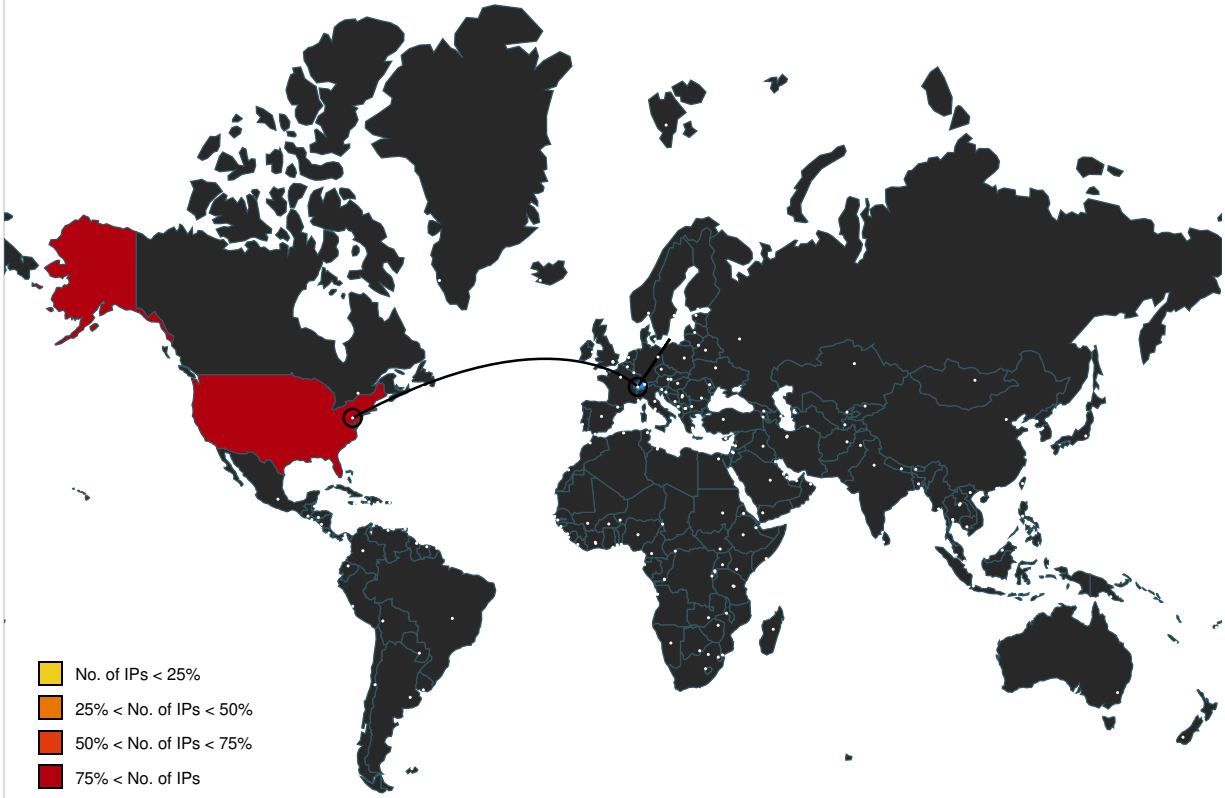
Name	Malicious	Antivirus Detection	Reputation
http://https://doc-04-90-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/cus72g9uti9p4sqam1k45t4h3de3hhkd/1669658550000/01268323115933183181/*/1lmBjkmJX2WixZUvaKmoyB8cex-DCePE2?e=download&uuid=e0f4c7f4-041c-4571-801a-cda7ca0f1ae2	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://doc-04-90-docs.googleusercontent.com/docs/securesc/ha0ro937gcuc7l7deffksulhg5h7mbp1/cus72g9u	ExtExport.exe, 00000025.00000002.1822822611.0000000002E46000.00000004.00000020.00020000.00000000.sdmp, ExtExport.exe, 00000025.00000003.1809581126.0000000002E0A000.00000004.00000020.00020000.00000000.sdmp, ExtExport.exe, 00000025.00000003.1802976587.0000000002E0A000.00000004.00000020.00020000.00000000.sdmp, ExtExport.exe, 00000025.00000002.1821975252.0000000002DD7000.00000004.00000020.00020000.00000000.sdmp, ExtExport.exe, 00000025.00000003.1803583412.0000000002E0A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://nsis.sf.net/NSIS_ErrorError	documentos DHL.exe	false		high
http://https://doc-04-90-docs.googleusercontent.com/	ExtExport.exe, 00000025.00000003.1809581126.0000000002E0A000.00000004.00000020.00020000.00000000.sdmp, ExtExport.exe, 00000025.00000002.1822393701.0000000002E0A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://doc-04-90-docs.googleusercontent.com/:	ExtExport.exe, 00000025.00000003.1809581126.0000000002E0A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://drive.google.com/	ExtExport.exe, 00000025.00000002.1821244010.0000000002D78000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://drive.google.com/d	ExtExport.exe, 00000025.00000002.1821244010.0000000002D78000.00000004.00000020.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://doc-04-90-docs.googleusercontent.com/=	ExtExport.exe, 00000025.00000003.1809581126.0000000002E0A000.00000004.00000020.00020000.00000000.sdmp, ExtExport.exe, 00000025.00000002.1822393701.0000000002E0A000.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://csp.withgoogle.com/csp/report-to/DriveUntrustedContentHttp/external	ExtExport.exe, 00000025.00000003.1802976587.0000000002E0A000.00000004.00000020.00020000.00000000.sdmp, ExtExport.exe, 00000025.00000003.1803583412.0000000002E0A000.00000004.00000020.00020000.00000000.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.74.206	drive.google.com	United States		15169	GOOGLEUS	false
142.250.186.65	googlehosted.l.googleusercontent.com	United States		15169	GOOGLEUS	false

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	755464
Start date and time:	2022-11-28 19:00:32 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	documentos DHL.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	40
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:	mal88.troj.spyw.evad.winEXE@45/6@2/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 21.5% (good quality ratio 21.1%) • Quality average: 88.5% • Quality standard deviation: 21.7%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Sleeps bigger than 100000000ms are automatically reduced to 1000ms

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WMIADAP.exe, SIHClient.exe, backgroundTaskHost.exe, SgrmBroker.exe, MoUsoCoreWorker.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): spclient.wg.spotify.com, wdcpalt.microsoft.com, client.wns.windows.com, login.live.com, slscr.update.microsoft.com, ctldl.windowsupdate.com, settings-win.data.microsoft.com, wdcp.microsoft.com, fe3cr.delivery.mp.microsoft.com
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile 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\nsw5DC6.tmp\System.dll

Process:	C:\Users\user\Desktop\documentos DHL.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
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\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3425316567-2969588382-3778222414-1001\1b1d0082738e9f9011266f86ab9723d2_11389406-0377-47ed-98c7-d564e683c6eb

Process:	C:\Program Files (x86)\Internet Explorer\ExtExport.exe
File Type:	data
Category:	dropped
Size (bytes):	47
Entropy (8bit):	1.1262763721961973
Encrypted:	false
SSDEEP:	3:/lSlIIEXln:AWE1
MD5:	D69FB7CE74DAC48982B69816C3772E4E
SHA1:	B1C04CDB2567DC2B50D903B0E1D0D3211191E065
SHA-256:	8CC6CA5CA4D0FA03842A60D90A6141F0B8D64969E830FC899DBA60ACB4905396
SHA-512:	7E4EC58DA8335E43A4542E0F6E05FA2D15393E83634BE973AA3E758A870577BA0BA136F6E831907C4B30D587B8E6EEAFA2A4B8142F49714101BA50ECC294DDB0
Malicious:	false
Preview:	.....user.

C:\Users\user\Zorillinae\Skaalpundet\Inkbslistes\Tset\Demodulationen\Iagttagerposition\Americanly.Unc

Process:	C:\Users\user\Desktop\documentos DHL.exe
File Type:	ASCII text, with very long lines (41286), with no line terminators
Category:	dropped
Size (bytes):	41286
Entropy (8bit):	3.9996729388074086
Encrypted:	false
SSDEEP:	768:7QFBt4/f3V9yKs85GMDkPo5jwtKrqfKOrd/t1GfhfzAa08RtCdIc:7QGf3V1siGM/5jEKrqyOrdl+hrZRQr
MD5:	9B8C8C90EE802C398079F4AF57961D8B
SHA1:	644AA417B2BC3B61BC2966CB4F732304B6229655
SHA-256:	A0B1E5CAC30130A40C239EB24DC2EEFE148B78310D1A550A580E1EBE0FCEEE74
SHA-512:	7640ACDF2F4B38E18FC7F633BEA98FFAA7CC5137CCDBEB108529F2C92027A3241CEF942FA511A5E028E056FF2F97779886C7F8CBD69CE31D6C31D951CDB60EF2
Malicious:	false

Preview:	C089DEEE2F80F894D8CBCAC903AB13EAC24FB93D53429CC2C6616687919B015FAA04E2F0BE0D98B80F07DEB3ED384DC5CC6C3BA629AE650595DF0601 DB2EE4DD9AE8CFDE80A1D7654162110360D3AB982B82270DCEE3FC808955B6F679823F99DBAA0C0F3E32822D500A45EDB7520148BE33E06F34B63DD8 C015A6DEA3AE12F22E096BED860F1BC954127D6474140237C63259E2F631647C50BD25671C3415E72ACBCA78ECA905C3E9A1E49775CE31B542CBF59F CFB34011A5732FCD5D4DA7FBD63CD845581795F251CC1698A2154BFE0ECDAE654CD0AC07496EB565AB5BD8B792B032F2AB7BBB48D24C4D517442BED5 6E04D7816FFE1E05673F622F9D66330D5FF86FABFF9CFE0A90B2F4EC6DB66AEACCE6E3D82E93296888BC80F6892F9215F1BBB49894B3ABFC46481822 C132E84B9A2DCC8C6700C7225BE56C81339D37252D584772F5774F94F90C6AA3FD0C64845D9641B4DFF60D7F957BCC90EB6CE94A6AD6511BBDA4CD76 70DE769CFD8BBEAA9ACC7BF1C77123A9EE35E323281877BE2BDB8D230B235C5C80C3C753E91D61731B47905A8EF9A1295B6000FCC3F8E930BAE3A761 C2C2D0EC9C5AB9047A6DE6343F5CD2058FD508B1E654DA845F2F48E4DD0B1189979BE314B1D99FDA992D8101AEFBEBB862ECC07F10E1DA299D23C689 53FA5D227ADF643F111211C4AC24CEA9C3961A78

C:\Users\user\Zorillinae\Skaalpundet\Inkbslistes\Tset\Demodulationen\Iagttagerposition\Strukturerne.Pom

Process:	C:\Users\user\Desktop\documentos DHL.exe
File Type:	OpenPGP Public Key
Category:	dropped
Size (bytes):	158847
Entropy (8bit):	6.98796457235067
Encrypted:	false
SSDEEP:	3072:tGYqJRr8sNY/ryIAYmvZ535mkL9bebIbws3CMppUy3V:FqJRr8UY/Bgvr35mkJ0Y9I
MD5:	7C98821952212D7D1554D45AF77DED1E
SHA1:	41DBCCEFDC520F60122AF9A6FEBDF452AC65DE10
SHA-256:	387C91D05A65764ED93EB897E5D68465E251811A5D09EAB2EA23BB7F26740A8E
SHA-512:	0E8B46122DEE44C2BE98A747A4F508FD8E2E41631D68C361D95AB701ECDB2C2D18923E7047DA6A74E93B0B43C6F553FD61FC1AF452D2404C259346D68431D12 E
Malicious:	false
Preview:	.....

C:\Users\user\Zorillinae\Skaalpundet\Inkbslistes\Tset\Demodulationen\Iagttagerposition\libpixbufloader-icns.dll

Process:	C:\Users\user\Desktop\documentos DHL.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	19856
Entropy (8bit):	4.96426410091434
Encrypted:	false
SSDEEP:	384:GNe90VEZnTALI8BHHJOpA6nHPrrNUgNGcRr:Gg90WAI8BnJ1KTRr
MD5:	7DEA5DAB23582505C0EB671EF816C927
SHA1:	CBB8443E8511DF1A6CDBD5AB6D1A8982B881B52E
SHA-256:	C655C545DE5F07D85F588599043D8429CC7682FFA9E1DC55FD5275308ABCA20E
SHA-512:	BA054DF0AEDB086F2300AE5E3E2BB705256BFDDFC6BD24D37638A502B6B37150C6FCA1ACF28237B8BCCB95EE2D87633539E60D813EFC9C7C5EE49E36249B6 361
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0% • Antivirus: Virustotal, Detection: 0%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....D..>.....&"...%.....@.....P..... .....P....`... .....k.....P.....h.....B..(.....0.....text...(.....`..`.data.....0.....".... .....@....rdata.....@.....$.....@..@.pdata.....P.....,.....@..@.xdata.....`.....0.....@..@.bss.....p.....edata..k.....2.....@. .@.idata.....4.....@....CRT....X.....>.....@....tls.....@.....@....reloc..h.....B.....@..B. .....

C:\Windows\Resources\0409\Transcriptive.ini

Process:	C:\Users\user\Desktop\documentos DHL.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	34
Entropy (8bit):	4.253212018409155
Encrypted:	false
SSDEEP:	3:uyl6sJQ7n:uyeC7n
MD5:	7A4C132CE54889252F5A733BBC39C097
SHA1:	B235DE8CA2A3E8667B283AED77E3518C21925BE0
SHA-256:	FF5E7709D11246A22FD9D7532BD01A7E2BF640713521E9B5539C9B38D09A9433
SHA-512:	C9EFBD99C4C3930AD311DD761952902E93D38AC988BFC3959CE490B41B475E167AF865C63922606D7A7A0A79DFA44C348215356602E6E6AA4241FA033AA2C75
Malicious:	false

Preview:	[Reproached222]..teenie=Firklang..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	6.448537030186477
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:	documentos DHL.exe
File size:	339276
MD5:	ca1cd0656568af4f58aa28e61a3e3edb
SHA1:	1fde05eb6e587047d8a47950bcb2efdb53409b42
SHA256:	6931d5a8ac6e00c855139d9da394b7895d83a9a18a8974c0b2381c5a28e68678
SHA512:	bfd4b3dfe4a78d2e1a4c94a78c633ba5dcef7ad9abe209fce6dbe123538b3bdbcf9c5e2de4a35d24237a663188ed6475810f9f686b9429f782bb16a819febc7a
SSDEEP:	6144:YIw3Q/ld1TZuGuUbWNTarTP6oJgZqI5wyqYVyQH:TQPYG/WZaXP6oN2wJ27
TLSH:	7974C0462360D13BFDBE0770B82710937995AC1675BCC0AAF29CB69D67F31620B2A771
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:	8660f0e68af8388d

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

Instruction
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 00007F7CDCCE8193h
push ebx
call 00007F7CDCCEB441h
cmp eax, ebx
je 00007F7CDCCE8189h
push 00000C00h
call eax
mov esi, 004082B0h
push esi
call 00007F7CDCCEB3BBh
push esi
call dword ptr [00408150h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], 00000000h
jne 00007F7CDCCE816Ch
push 0000000Ah
call 00007F7CDCCEB414h
push 00000008h
call 00007F7CDCCEB40Dh
push 00000006h
mov dword ptr [0042A244h], eax
call 00007F7CDCCEB401h
cmp eax, ebx
je 00007F7CDCCE8191h
push 0000001Eh
call eax
test eax, eax
je 00007F7CDCCE8189h
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

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x5e000	0x28868	.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	0x33000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x5e000	0x28868	0x28a00	False	0.28479567307692305	data	4.106888119561181	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x5e3b8	0x368	Device independent bitmap graphic, 96 x 16 x 4, image size 768	English	United States
RT_ICON	0x5e720	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 67584	English	United States
RT_ICON	0x6ef48	0x94a8	Device independent bitmap graphic, 96 x 192 x 32, image size 38016	English	United States
RT_ICON	0x783f0	0x5488	Device independent bitmap graphic, 72 x 144 x 32, image size 21600	English	United States
RT_ICON	0x7d878	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16896	English	United States
RT_ICON	0x81aa0	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	English	United States
RT_ICON	0x84048	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	English	United States
RT_ICON	0x850f0	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400	English	United States
RT_ICON	0x85a78	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	English	United States
RT_DIALOG	0x85ee0	0x144	data	English	United States
RT_DIALOG	0x86028	0x13c	data	English	United States
RT_DIALOG	0x86168	0x100	data	English	United States
RT_DIALOG	0x86268	0x11c	data	English	United States
RT_DIALOG	0x86388	0xc4	data	English	United States
RT_DIALOG	0x86450	0x60	data	English	United States
RT_GROUP_ICON	0x864b0	0x76	data	English	United States
RT_MANIFEST	0x86528	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States

Imports

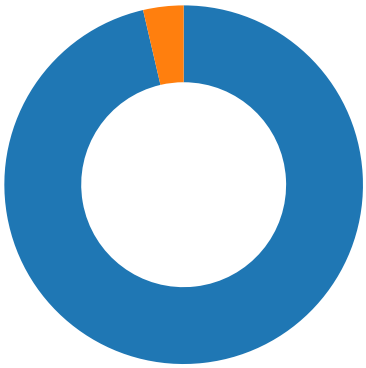
DLL	Import
KERNEL32.dll	ExitProcess, SetFileAttributesW, Sleep, GetTickCount, CreateFileW, GetFileSize, GetModuleFileNameW, GetCurrentProcess, SetCurrentDirectoryW, GetFileAttributesW, SetEnvironmentVariableW, GetWindowsDirectoryW, GetTempPathW, GetCommandLineW, GetVersion, SetErrorMode, lstrlenW, lstrcpynW, 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

Network Port Distribution



Total Packets: 55

- 53 (DNS)
- 443 (HTTPS)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2022 19:03:18.615021944 CET	49802	443	192.168.11.20	142.250.74.206
Nov 28, 2022 19:03:18.615070105 CET	443	49802	142.250.74.206	192.168.11.20
Nov 28, 2022 19:03:18.615206957 CET	49802	443	192.168.11.20	142.250.74.206

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2022 19:03:18.639564991 CET	49802	443	192.168.11.20	142.250.74.206
Nov 28, 2022 19:03:18.639585018 CET	443	49802	142.250.74.206	192.168.11.20
Nov 28, 2022 19:03:18.677011967 CET	443	49802	142.250.74.206	192.168.11.20
Nov 28, 2022 19:03:18.677251101 CET	49802	443	192.168.11.20	142.250.74.206
Nov 28, 2022 19:03:18.677993059 CET	443	49802	142.250.74.206	192.168.11.20
Nov 28, 2022 19:03:18.678250074 CET	49802	443	192.168.11.20	142.250.74.206
Nov 28, 2022 19:03:18.913369894 CET	49802	443	192.168.11.20	142.250.74.206
Nov 28, 2022 19:03:18.913429976 CET	443	49802	142.250.74.206	192.168.11.20
Nov 28, 2022 19:03:18.914542913 CET	443	49802	142.250.74.206	192.168.11.20
Nov 28, 2022 19:03:18.914834023 CET	49802	443	192.168.11.20	142.250.74.206
Nov 28, 2022 19:03:18.933219910 CET	49802	443	192.168.11.20	142.250.74.206
Nov 28, 2022 19:03:18.980402946 CET	443	49802	142.250.74.206	192.168.11.20
Nov 28, 2022 19:03:19.381166935 CET	443	49802	142.250.74.206	192.168.11.20
Nov 28, 2022 19:03:19.381335974 CET	49802	443	192.168.11.20	142.250.74.206
Nov 28, 2022 19:03:19.381417036 CET	443	49802	142.250.74.206	192.168.11.20
Nov 28, 2022 19:03:19.381680965 CET	49802	443	192.168.11.20	142.250.74.206
Nov 28, 2022 19:03:19.381733894 CET	49802	443	192.168.11.20	142.250.74.206
Nov 28, 2022 19:03:19.381897926 CET	443	49802	142.250.74.206	192.168.11.20
Nov 28, 2022 19:03:19.382034063 CET	49802	443	192.168.11.20	142.250.74.206
Nov 28, 2022 19:03:19.382050991 CET	443	49802	142.250.74.206	192.168.11.20
Nov 28, 2022 19:03:19.382185936 CET	49802	443	192.168.11.20	142.250.74.206
Nov 28, 2022 19:03:19.544370890 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:19.544482946 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:19.544661045 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:19.545027018 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:19.545068026 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:19.601592064 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:19.601780891 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:19.601839066 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:19.602772951 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:19.603266001 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:19.606729031 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:19.606743097 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:19.607040882 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:19.607247114 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:19.607765913 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:19.648458004 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:20.017338037 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:20.017560959 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:20.017635107 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:20.017712116 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:20.017822981 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:20.017864943 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:20.017889977 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:20.018009901 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:20.019331932 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:20.019500017 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:20.019557953 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:20.020034075 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:20.020205021 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:20.020205975 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:20.020286083 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:20.020354033 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:20.020477057 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:20.020766973 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:20.021039963 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:20.021116972 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:20.021365881 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:20.021579981 CET	443	49803	142.250.186.65	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2022 19:03:20.021781921 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:20.028414011 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:20.028592110 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:20.028697968 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:20.028853893 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:20.028918028 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:20.029164076 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:20.029230118 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:20.029441118 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:20.029491901 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:20.029648066 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:20.029702902 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:20.029735088 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:20.029911041 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:20.029911995 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:20.029992104 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:20.030206919 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:20.030698061 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:20.030905962 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:20.030972958 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:20.031176090 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:20.031251907 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:20.031435966 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:20.031749964 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:20.032052040 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:20.032118082 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:20.032354116 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:20.032409906 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:20.032641888 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:20.032717943 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:20.032777071 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:20.032818079 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:20.033026934 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:20.033077002 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:20.033278942 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:20.033329010 CET	443	49803	142.250.186.65	192.168.11.20
Nov 28, 2022 19:03:20.033663034 CET	49803	443	192.168.11.20	142.250.186.65
Nov 28, 2022 19:03:20.033716917 CET	443	49803	142.250.186.65	192.168.11.20

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 28, 2022 19:03:18.583724976 CET	54443	53	192.168.11.20	1.1.1.1
Nov 28, 2022 19:03:18.594630003 CET	53	54443	1.1.1.1	192.168.11.20
Nov 28, 2022 19:03:19.510133982 CET	60672	53	192.168.11.20	1.1.1.1
Nov 28, 2022 19:03:19.541562080 CET	53	60672	1.1.1.1	192.168.11.20

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 28, 2022 19:03:18.583724976 CET	192.168.11.20	1.1.1.1	0xbc76	Standard query (0)	drive.google.com	A (IP address)	IN (0x0001)	false
Nov 28, 2022 19:03:19.510133982 CET	192.168.11.20	1.1.1.1	0xa3a7	Standard query (0)	doc-04-90-docs.googleusercontent.com	A (IP address)	IN (0x0001)	false

DNS Answers

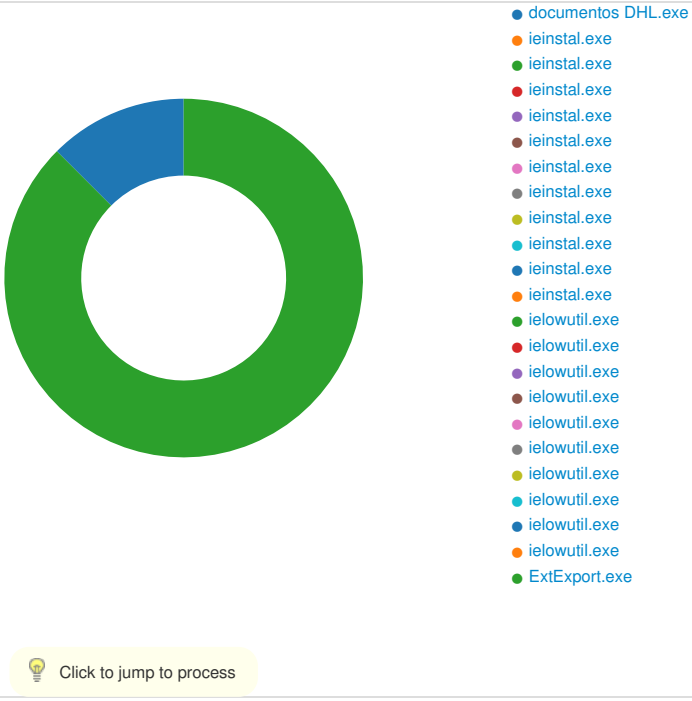
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 28, 2022 19:03:18.594630003 CET	1.1.1.1	192.168.11.20	0xbc76	No error (0)	drive.google.com		142.250.74.206	A (IP address)	IN (0x0001)	false
Nov 28, 2022 19:03:19.541562080 CET	1.1.1.1	192.168.11.20	0xa3a7	No error (0)	doc-04-90-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 28, 2022 19:03:19.541562080 CET	1.1.1.1	192.168.11.20	0xa3a7	No error (0)	googlehosted.l.googleusercontent.com		142.250.186.65	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- drive.google.com
- doc-04-90-docs.googleusercontent.com

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: documentos DHL.exe PID: **7424**, Parent PID: **4684**

General

Target ID:	2
Start time:	19:02:24
Start date:	28/11/2022
Path:	C:\Users\user\Desktop\documentos DHL.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\documentos DHL.exe
Imagebase:	0x400000

File size:	339276 bytes
MD5 hash:	CA1CD0656568AF4F58AA28E61A3E3EDB
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: 00000002.00000002.1824658615.0000000003370000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Zorillinae\Skaalpundet\Inkbslistes\Tset\Demodulationen\lagttagerposition\Strukturerne.Pom	unknown	1048576	success or wait	1	1000295D	ReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: ieinstal.exe PID: 8576, Parent PID: 7424

General

Target ID:	16
Start time:	19:02:53
Start date:	28/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\documentos DHL.exe
Imagebase:	0x4b0000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: 8584, Parent PID: 7424

General

Target ID:	17
Start time:	19:02:53
Start date:	28/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\documentos DHL.exe
Imagebase:	0x4b0000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: **8596**, Parent PID: **7424**

General	
Target ID:	18
Start time:	19:02:53
Start date:	28/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\documentos DHL.exe
Imagebase:	0x4b0000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: **8604**, Parent PID: **7424**

General	
Target ID:	19
Start time:	19:02:54
Start date:	28/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\documentos DHL.exe
Imagebase:	0x4b0000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: **8612**, Parent PID: **7424**

General	
Target ID:	20
Start time:	19:02:54
Start date:	28/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\documentos DHL.exe
Imagebase:	0x4b0000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: **8620**, Parent PID: **7424**

General	
Target ID:	21
Start time:	19:02:54
Start date:	28/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\documentos DHL.exe
Imagebase:	0x4b0000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: **8628**, Parent PID: **7424**

General	
Target ID:	22
Start time:	19:02:55
Start date:	28/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\documentos DHL.exe
Imagebase:	0x4b0000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: ieinstal.exe PID: **8640**, Parent PID: **7424**

General	
Target ID:	23
Start time:	19:02:55
Start date:	28/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\documentos DHL.exe
Imagebase:	0x4b0000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: **8648**, Parent PID: **7424**

General	
Target ID:	24
Start time:	19:02:55

Start date:	28/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\documentos DHL.exe
Imagebase:	0x4b0000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: **8672**, Parent PID: **7424**

General	
Target ID:	25
Start time:	19:02:55
Start date:	28/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\documentos DHL.exe
Imagebase:	0x4b0000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ieinstal.exe PID: **8680**, Parent PID: **7424**

General	
Target ID:	26
Start time:	19:02:56
Start date:	28/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\documentos DHL.exe
Imagebase:	0x4b0000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ielowutil.exe PID: **8688**, Parent PID: **7424**

General	
Target ID:	27
Start time:	19:02:56
Start date:	28/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ielowutil.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\documentos DHL.exe
Imagebase:	0x3e0000
File size:	221696 bytes
MD5 hash:	650FE7460630188008BF8C8153526CEB
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ielowutil.exe PID: **8696**, Parent PID: **7424**

General	
Target ID:	28
Start time:	19:02:56
Start date:	28/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ielowutil.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\documentos DHL.exe
Imagebase:	0x3e0000
File size:	221696 bytes
MD5 hash:	650FE7460630188008BF8C8153526CEB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ielowutil.exe PID: **8704**, Parent PID: **7424**

General	
Target ID:	29
Start time:	19:02:57
Start date:	28/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ielowutil.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\documentos DHL.exe
Imagebase:	0x3e0000
File size:	221696 bytes
MD5 hash:	650FE7460630188008BF8C8153526CEB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ielowutil.exe PID: **8712**, Parent PID: **7424**

General	
Target ID:	30
Start time:	19:02:57
Start date:	28/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ielowutil.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\documentos DHL.exe
Imagebase:	0x3e0000
File size:	221696 bytes
MD5 hash:	650FE7460630188008BF8C8153526CEB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ielowutil.exe PID: **8720**, Parent PID: **7424**

General	
Target ID:	31

Start time:	19:02:57
Start date:	28/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ielowutil.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\documentos DHL.exe
Imagebase:	0x3e0000
File size:	221696 bytes
MD5 hash:	650FE7460630188008BF8C8153526CEB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ielowutil.exe PID: **8728**, Parent PID: **7424**

General

Target ID:	32
Start time:	19:02:58
Start date:	28/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ielowutil.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\documentos DHL.exe
Imagebase:	0x3e0000
File size:	221696 bytes
MD5 hash:	650FE7460630188008BF8C8153526CEB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ielowutil.exe PID: **8736**, Parent PID: **7424**

General

Target ID:	33
Start time:	19:02:58
Start date:	28/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ielowutil.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\documentos DHL.exe
Imagebase:	0x3e0000
File size:	221696 bytes
MD5 hash:	650FE7460630188008BF8C8153526CEB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ielowutil.exe PID: **8748**, Parent PID: **7424**

General

Target ID:	34
Start time:	19:02:58
Start date:	28/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ielowutil.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\documentos DHL.exe
Imagebase:	0x3e0000
File size:	221696 bytes
MD5 hash:	650FE7460630188008BF8C8153526CEB

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ielowutil.exe PID: **8760**, Parent PID: **7424**

General	
Target ID:	35
Start time:	19:02:59
Start date:	28/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ielowutil.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\documentos DHL.exe
Imagebase:	0x3e0000
File size:	221696 bytes
MD5 hash:	650FE7460630188008BF8C8153526CEB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ielowutil.exe PID: **8776**, Parent PID: **7424**

General	
Target ID:	36
Start time:	19:02:59
Start date:	28/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ielowutil.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\documentos DHL.exe
Imagebase:	0x3e0000
File size:	221696 bytes
MD5 hash:	650FE7460630188008BF8C8153526CEB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: ExtExport.exe PID: **8784**, Parent PID: **7424**

General	
Target ID:	37
Start time:	19:02:59
Start date:	28/11/2022
Path:	C:\Program Files (x86)\Internet Explorer\ExtExport.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\documentos DHL.exe
Imagebase:	0x190000
File size:	45056 bytes
MD5 hash:	3253FD643C51C133C3489A146781913B
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: 00000025.00000002.1820565807.0000000002A00000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000025.00000000.1618126975.0000000002A00000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	2A20051	InternetOpenUrlA
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	2A20051	InternetOpenUrlA
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	1	2A20051	InternetOpenUrlA
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	2A20051	InternetOpenUrlA
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	2A20051	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	2A20051	InternetOpenUrlA

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	45056	success or wait	1	40415C	ReadFile

Disassembly

No disassembly