



ID: 491288

Sample Name:

nDHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe

Cookbook: default.jbs

Time: 12:42:54

Date: 27/09/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report	
nDHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Threatname: GuLoader	3
Yara Overview	3
Memory Dumps	3
Sigma Overview	3
Jbx Signature Overview	4
AV Detection:	4
Networking:	4
System Summary:	4
Data Obfuscation:	4
Anti Debugging:	4
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	6
Initial Sample	6
Dropped Files	6
Unpacked PE Files	6
Domains	6
URLs	6
Domains and IPs	7
Contacted Domains	7
Contacted URLs	7
Contacted IPs	7
General Information	7
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	8
IPs	8
Domains	8
ASN	8
JA3 Fingerprints	8
Dropped Files	8
Created / dropped Files	8
Static File Info	8
General	8
File Icon	8
Static PE Info	9
General	9
Entrypoint Preview	9
Data Directories	9
Sections	9
Resources	9
Imports	9
Version Infos	9
Possible Origin	9
Network Behavior	9
Network Port Distribution	9
UDP Packets	10
Code Manipulations	10
Statistics	10
System Behavior	10
Analysis Process: nDHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe PID: 4880 Parent PID: 620	10
General	10
Disassembly	10
Code Analysis	10

Windows Analysis Report nDHL_Shipment_Notification...

Overview

General Information

Sample Name:

nDHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe

Analysis ID:

491288

MD5:

cd65994e4f53363.

SHA1:

241dda06961d32..

SHA256:

634115d5eb9122..

Tags:

DHL

exe

GuLoader

Infos:

Most interesting Screenshot:

Process-Tree

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

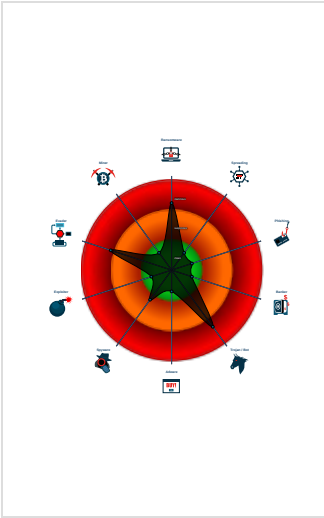
GuLoader

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Potential malicious icon found
- Multi AV Scanner detection for subm...
- Yara detected GuLoader
- Found potential dummy code loops (...)
- Machine Learning detection for samp...
- C2 URLs / IPs found in malware con...
- Creates a DirectInput object (often fo...
- Uses 32bit PE files
- Sample file is different than original ...
- PE file contains strange resources
- Program does not show much activi...

Classification



- System is w10x64
- nDHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe (PID: 4880 cmdline: 'C:\Users\user\Desktop\nDHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe' MD5: CD65994E4F53363527E3651759103759)
- cleanup

Malware Configuration

Threatname: GuLoader

```
{  
  "Payload URL": "http://178.32.63.50/moss/nancata_Rbk"  
}
```

Yara Overview


Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.822232989.0000000000063 0000.00000040.00000001.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:



Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:



C2 URLs / IPs found in malware configuration

System Summary:



Potential malicious icon found

Data Obfuscation:



Yara detected GuLoader

Anti Debugging:

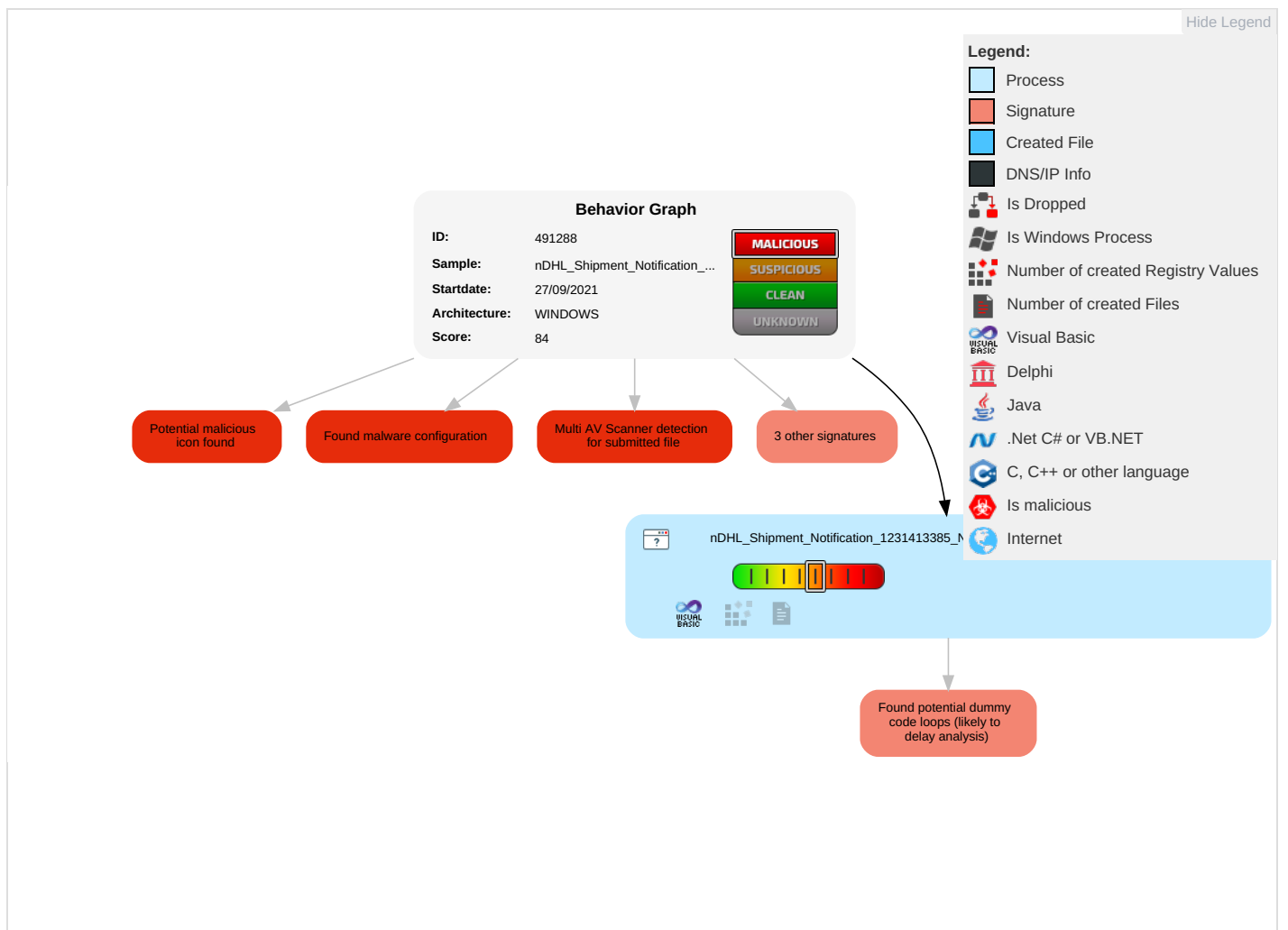


Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Reputation
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	Input Capture 1	Security Software Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Application Layer Protocol 1	Eavesdrop on Insecure Network Communication	Reputation
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Virtualization/Sandbox Evasion 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Reputation
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Reputation
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	Reputation

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
nDHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe	29%	Virustotal		Browse
nDHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe	13%	ReversingLabs	Win32.Trojan.Mucc	
nDHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://178.32.63.50/moss/nancata_Rbk	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://178.32.63.50/moss/nancata_Rbk	true	<ul style="list-style-type: none">Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491288
Start date:	27.09.2021
Start time:	12:42:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 0s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	nDHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	21
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:	<ul style="list-style-type: none">HCA enabledEGA enabledHDC enabledAMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal84.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	<ul style="list-style-type: none">Successful, ratio: 5.3% (good quality ratio 4.7%)Quality average: 54.6%Quality standard deviation: 22.3%
HCA Information:	Failed
Cookbook Comments:	<ul style="list-style-type: none">Adjust boot timeEnable AMSIFound application associated with file extension: .exeOverride analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.7049263215720325
TrID:	<ul style="list-style-type: none">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:	nDHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe
File size:	94208
MD5:	cd65994e4f53363527e3651759103759
SHA1:	241dda06961d323299c19c1f558168864867169e
SHA256:	634115d5eb91226011678443a96617cb0bcc1831621b418a0e16860b79502de7
SHA512:	077473c0b90b1f41f2775a144909ca6c4edd1c1a03df92ece1de2637124d5e3ed903bb6073e81e486906fe2b00b472f2da75e40d5ddcfbe2dfd016d3d2d1583
SSDEEP:	768:L/nxsMCmcp1FaKWg49kg8cf3hVFwal+HZL+J0d937yH38o5pjZ4vLJTX8HjIF8uj:znxUH49NNf3hMDkeyX8qpjZc9oX8M
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode....\$.SM..S M..SM...Q..RM...o..uM..ek..RM..RichSM.....PE..L.....S.....@...@.....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:	0x53BB158E [Mon Jul 7 21:47:58 2014 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	0x136d0	0x14000	False	0.483056640625	data	6.11514265963	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x15000	0x205c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x18000	0x8f4	0x1000	False	0.1708984375	data	1.95064287814	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
Chinese	Taiwan	

Network Behavior

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

System Behavior

Analysis Process:

nDHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe

PID: 4880 Parent PID: 620

General

Start time:	12:43:53
Start date:	27/09/2021
Path:	C:\Users\user\Desktop\InDHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\InDHL_Shipment_Notification_1231413385_Notification_1231413385_september2021.exe'
Imagebase:	0x400000
File size:	94208 bytes
MD5 hash:	CD65994E4F53363527E3651759103759
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	<ul style="list-style-type: none">Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.822232989.0000000000630000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis