ID: 491982
Sample Name:
ilnQNBU7NA.exe
Cookbook: default.jbs
Time: 08:42:00
Date: 28/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report ilnQNBU7NA.exe 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Malware Configuration 3
Yara Overview 3
Sigma Overview 3
Jbx Signature Overview 3
AV Detection: 3
Mitre Att&ck Matrix 4
Behavior Graph 4
Screenshots 4
Thumbnails 4
Antivirus, Machine Learning and Genetic Malware Detection 5
Initial Sample 5
Dropped Files 5
Unpacked PE Files 5
Domains 5
URLs 5
Domains and IPs 6
Contacted Domains 6
URLs from Memory and Binaries 6
Contacted IPs 6
General Information 6
Simulations 6
Behavior and APIs 6
Joe Sandbox View / Context 7
IPs 7
Domains 7
ASN 7
JA3 Fingerprints 7
Dropped Files 7
Created / dropped Files 7
Static File Info 7
General 7
File Icon 7
Static PE Info 7
General 8
Entrypoint Preview 8
Rich Headers 8
Data Directories 8
Sections 8
Resources 8
Imports 8
Version Infos 8
Possible Origin 8
Network Behavior 8
Network Port Distribution 8
UDP Packets 8
Code Manipulations 9
Statistics 9
System Behavior 9
Analysis Process: ilnQNBU7NA.exe PID: 6316 Parent PID: 1324 9
General 9
File Activities 9
File Created 9
File Deleted 9
File Read 9
Disassembly 9
Code Analysis 9

Copyright Joe Security LLC 2021

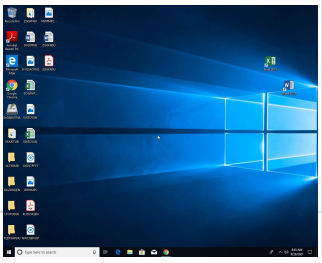
Windows Analysis Report ilnQNBU7NA.exe

Overview

General Information

Sample Name:	ilnQNBU7NA.exe
Analysis ID:	491982
MD5:	76449275538d70..
SHA1:	6dc592eb5c639f7..
SHA256:	bb47883b9a0e02..
Tags:	exe
Infos:	

Most interesting Screenshot:



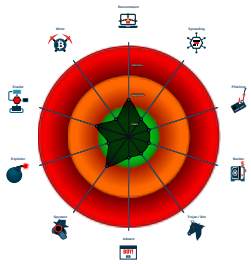
Detection

Score:	24
Range:	0 - 100
Whitelisted:	false
Confidence:	80%

Signatures

- Machine Learning detection for samp…
- Uses 32bit PE files
- Sample file is different than original …
- PE file contains an invalid checksum
- PE file contains strange resources
- Contains functionality to shutdown / …
- Detected potential crypto function
- Program does not show much activi…
- Contains functionality for read data f…

Classification



Process Tree

- **System is w10x64**
- ilnQNBU7NA.exe (PID: 6316 cmdline: 'C:\Users\user\Desktop\ilnQNBU7NA.exe' MD5: 76449275538D7041BEBEEEDF2AB75B1D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

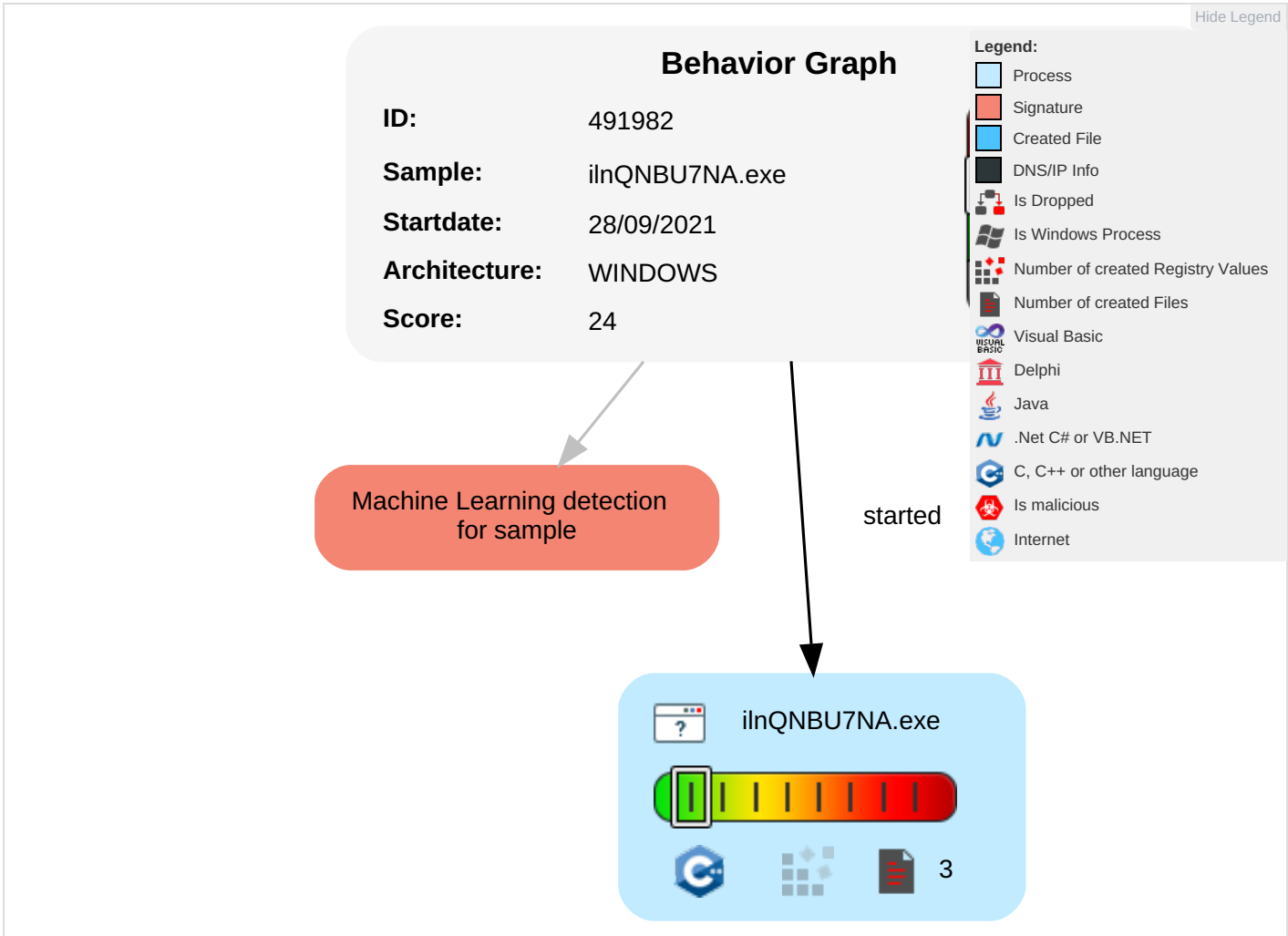
Click to jump to signature section

AV Detection:

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Access Token Manipulation 1	Access Token Manipulation 1	OS Credential Dumping	File and Directory Discovery 2	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	System Shutdo
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	System Information Discovery 4	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Copyright Joe Security LLC 2021

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
ilnQNBU7NA.exe	9%	ReversingLabs		
ilnQNBU7NA.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.ilnQNBU7NA.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
1.0.ilnQNBU7NA.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Copyright Joe Security LLC 2021

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491982
Start date:	28.09.2021
Start time:	08:42:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ilnQNBU7NA.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:	22
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:	SUS
Classification:	sus24.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 100% (good quality ratio 96.5%) • Quality average: 83.3% • Quality standard deviation: 25%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
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, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.982776725752498
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:	ilnQNBU7NA.exe
File size:	3333764
MD5:	76449275538d7041bebeeedf2ab75b1d
SHA1:	6dc592eb5c639f79e67d7e1d45b03d15c703ea08
SHA256:	bb47883b9a0e02bc3f3df2605176307900ea804ffa9698e35f93ea4909b28dbe
SHA512:	935df085c9cc9f04bb7f81051c9f23dbf6614d6a29f8fd13943caac046a3410c562bbad99bdaec50ca7cb1198ce81a9eddbedad7528793e4fb5f58ba18ce5bdc
SSDEEP:	98304:MNwTt3NIxtu9rEjll7HTelXboTTTncIcTqHSgr+i:zxdInu5EOHTgrmPcIcGygr9
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG..sw..PG..VA..PG.Rich.PG.....PE..L...".$_.....f.....H3.....@

File Icon

Icon Hash:	eccce4d6d2f0a7a3

Static PE Info

General

Entrypoint:	0x403348
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:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5F24D722 [Sat Aug 1 02:44:50 2020 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:	ced282d9b261d1462772017fe2f6972b

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6457	0x6600	False	0.66823682598	data	6.43498570321	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1380	0x1400	False	0.4625	data	5.26100389731	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x25538	0x600	False	0.463541666667	data	4.133728555	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x30000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x38000	0x19b44	0x19c00	False	0.330040200243	data	5.57673300046	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
English	United States	

Network Behavior

Network Port Distribution

UDP Packets

Code Manipulations

Statistics

System Behavior

Analysis Process: ilnQNBU7NA.exe PID: 6316 Parent PID: 1324

General

Start time:	08:42:58
Start date:	28/09/2021
Path:	C:\Users\user\Desktop\ilnQNBU7NA.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ilnQNBU7NA.exe'
Imagebase:	0x400000
File size:	3333764 bytes
MD5 hash:	76449275538D7041BEBEEEDF2AB75B1D
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 Deleted

File Read

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021