ID: 527846
Sample Name: Statement from QNB.exe
Cookbook: default.jbs
Time: 14:05:13
Date: 24/11/2021
Version: 34.0.0 Boulder Opal
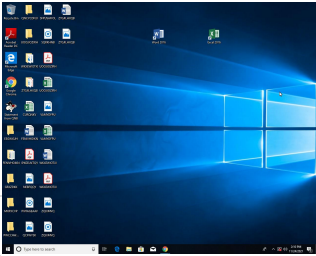
Table of Contents

Windows Analysis Report Statement from QNB.exe

Overview

General Information

Sample Name:	Statement from QNB.exe
Analysis ID:	527846
MD5:	9c8b626668e14a..
SHA1:	554069b1fb3a80a.
SHA256:	d63ed0450efe28d.
Tags:	exe
Infos:	

Most interesting Screenshot:

Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

GuLoader

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Found malware configuration

Yara detected GuLoader

Found potential dummy code loops (…

Tries to detect virtualization through…

C2 URLs / IPs found in malware con…

Uses 32bit PE files

Contains functionality to call native f…

Sample file is different than original …

Contains functionality to read the PEB

Program does not show much activi…

Uses code obfuscation techniques (…

Contains functionality for execution …

Classification

Process Tree

- **System is w10x64**
  - Statement from QNB.exe (PID: 6836 cmdline: "C:\Users\user\Desktop\Statement from QNB.exe" MD5: 9C8B626668E14AEB4355EA39D1520E33)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
    "Payload URL": "https://drive.google.com/uc?export=download&id=1y{\\"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.866154306.00000000021F0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

AV Detection:

Found malware configuration

Networking:

C2 URLs / IPs found in malware configuration

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

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	R… S… E…
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	R… T… W… A…
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	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	R… W… W… A…
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	O… D… C… B…
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

Behavior Graph

Behavior Graph

ID: 527846
Sample: Statement from QNB.exe
Startdate: 24/11/2021
Architecture: WINDOWS
Score: 68

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

Legend:
- Process
- Signature
- Created File
- DNS/IP Info
- Is Dropped
- Is Windows Process
- Number of created Registry Values
- Number of created Files
- Visual Basic
- Delphi
- Java
- .Net C# or VB.NET
- C, C++ or other language
- Is malicious
- Internet

Found malware configuration

Yara detected GuLoader

C2 URLs / IPs found in malware configuration

2 othe

Statement from QNB.exe

1

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
Statement from QNB.exe	7%	ReversingLabs	Win32.Worm.Wbvb	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	527846
Start date:	24.11.2021
Start time:	14:05:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 35s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Statement from QNB.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:	6
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:	mal68.troj.evad.winEXE@1/1@0/0
EGA Information:	Failed
HDC Information:	- Successful, ratio: 29.7% (good quality ratio 21.7%) - Quality average: 42% - Quality standard deviation: 31.9%
HCA Information:	Failed
Cookbook Comments:	- Adjust boot time - Enable AMSI - Found application associated with file extension: .exe - Override 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

C:\Users\user\AppData\Local\Temp\~DF9449C0319C5371E6.TMP	
Process:	C:\Users\user\Desktop\Statement from QNB.exe
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	16384
Entropy (8bit):	0.9277305547216628
Encrypted:	false
SSDEEP:	48:rJSq2Upu8metqPrIXHimU7zdvP1vncU7pCr8P:VSKUpACLFcUVCrG
MD5:	19809EDD1FF00A1D7C105BC58A97CD02
SHA1:	26FB6D339CF2A7474DE6F785166163FA9B2ADBB1
SHA-256:	4745D04A4BB99D70866D722394D9E71F3FAE597AA84E229A1E3B40F31521594C
SHA-512:	434722936006B56B042FB5C72CAB98D8B7615A5A0E48EE6746DD6839BE029029E3BCECF7EFA49DDC8A9DB016FA472FB9EE1CE75126C13E06D66EAA12166A38 7
Malicious:	false
Reputation:	low
Preview:	......................>.. ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	4.787310245899602
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:	Statement from QNB.exe
File size:	135168
MD5:	9c8b626668e14aeb4355ea39d1520e33
SHA1:	554069b1fb3a80a02840158d31c6c2826812cb40
SHA256:	d63ed0450efe28d525954d84556394f21df1c2d882e74b4 891492fefab00dd79

General

SHA512:	7a6d99ab3be3a6f43eeabacc4eb70ccd7d88f0dded718ed c3fbabb9522e4b3b82009a0edf95a6b4909af90fe9e6828 66e6459a43a709831cc93732a8e3ff69db
SSDEEP:	1536:tGDSlb6oBiIOhMk98Riy6NaXuknILxq+o7g8r8A0H iD:tGAtO198yNa/SoXIA4i
File Content Preview:	MZ....................@...............................!..L.!Th is program cannot be run in DOS mode....$........i............ ....*..............Rich....................PE..L....f.O................. ...0...................@........

File Icon

Icon Hash:	981dca909cee36b0

Static PE Info

General

Entrypoint:	0x4013b4
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:	0x4FBF669F [Fri May 25 11:01:51 2012 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:	d77040f4614bccfda7b8aa2e04863738

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x1d31c	0x1e000	False	0.349731445312	data	4.97110902784	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1f000	0x141c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DA TA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x21000	0xf58	0x1000	False	0.339111328125	data	3.26223123132	IMAGE_SCN_CNT_INITIALIZED_DA TA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Language of compilation system	Country where language is spoken	Map
Turkmen	Turkmenistan	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: Statement from QNB.exe PID: 6836 Parent PID: 5704

General

Start time:	14:06:10
Start date:	24/11/2021
Path:	C:\Users\user\Desktop\Statement from QNB.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Statement from QNB.exe"
Imagebase:	0x400000
File size:	135168 bytes
MD5 hash:	9C8B626668E14AEB4355EA39D1520E33
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.866154306.00000000021F0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities   Show Windows behavior

Disassembly

Code Analysis

Joe Sandbox Cloud Basic 34.0.0 Boulder Opal