ID: 385245
Sample Name:
NTS_eTaxInvoice#U00a004-08-2021#U00b7pdf.exe
Cookbook: default.jbs
Time: 08:57:32
Date: 12/04/2021
Version: 31.0.0 Emerald

Table of Contents

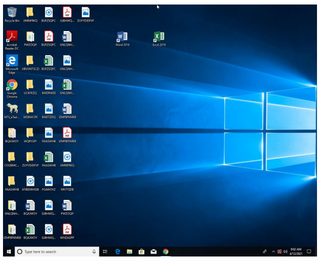
Analysis Report NTS_eTaxInvoice#U00a004-08-2021#U0…

Overview

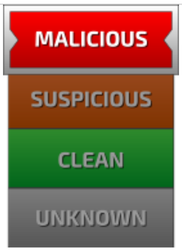
General Information

Sample Name:	NTS_eTaxInvoice#U00a004-08-2021#U00b7pdf.exe
Analysis ID:	385245
MD5:	69273783da83c9..
SHA1:	c1f879d4c66d53a..
SHA256:	81980be7abe0eb..
Infos:	

Most interesting Screenshot:



Detection



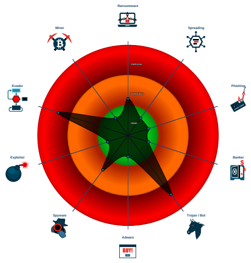
GuLoader

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Detected RDTSC dummy instruction…
- Executable has a suspicious name (…
- Found potential dummy code loops (…
- Initial sample is a PE file and has a …
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Yara detected VB6 Downloader Gen…
- Abnormal high CPU Usage
- Contains functionality for execution …

Classification



Startup

- **System is w10x64**
- NTS_eTaxInvoice#U00a004-08-2021#U00b7pdf.exe (PID: 7100 cmdline: 'C:\Users\user\Desktop\NTS_eTaxInvoice#U00a004-08-2021#U00b7pdf.exe' MD5: 69273783DA83C97FF021E1002243DD8B)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=1vOQNsh0Cmxl5hty4ZPc18pGNKUD5RTVY"
}
```

Yara Overview

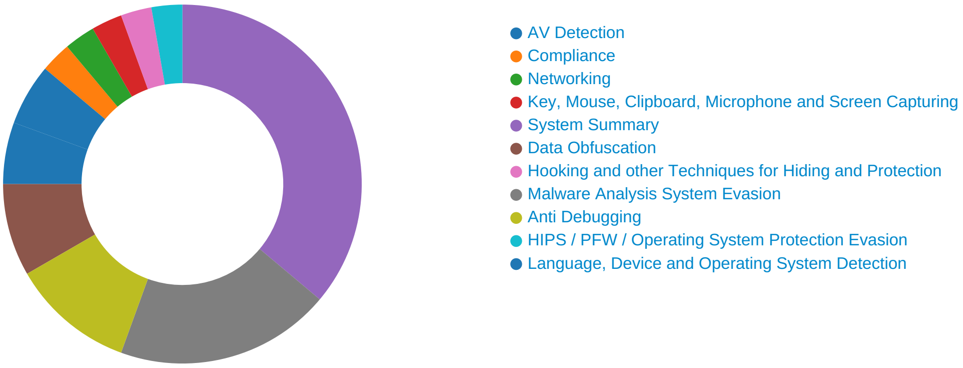
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: NTS_eTaxInvoice#U00a004-08-2021#U00b7pdf.exe PID: 7100	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: NTS_eTaxInvoice#U00a004-08-2021#U00b7pdf.exe PID: 7100	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

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

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

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

Tries to detect virtualization through RDTSC time measurements

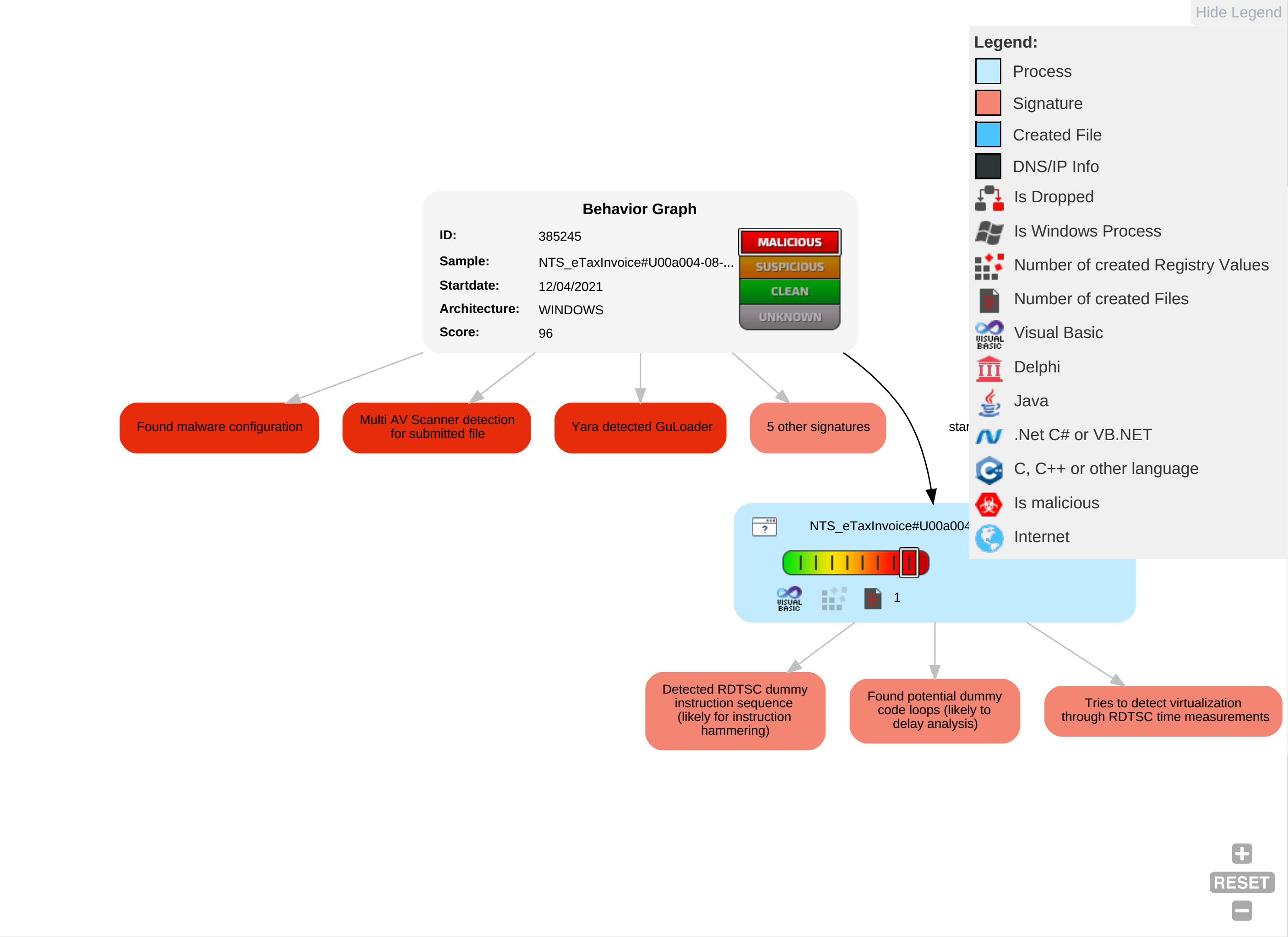
Anti Debugging:

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	Re Se Ef
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 4 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Re Tr W Au
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	Clipboard Data 1	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Re W W Au
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	Ol De Cl Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Information Discovery 2 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

Behavior Graph



ID: 385245
Sample: NTS_eTaxInvoice#U00a004-08-...
Startdate: 12/04/2021
Architecture: WINDOWS
Score: 96

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
NTS_eTaxInvoice#U00a004-08-2021#U00b7pdf.exe	61%	Virustotal		Browse
NTS_eTaxInvoice#U00a004-08-2021#U00b7pdf.exe	32%	Metadefender		Browse
NTS_eTaxInvoice#U00a004-08-2021#U00b7pdf.exe	60%	ReversingLabs	Win32.Trojan.Guloader	

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:	31.0.0 Emerald
Analysis ID:	385245
Start date:	12.04.2021
Start time:	08:57:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NTS_eTaxInvoice#U00a004-08-2021#U00b7pdf.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:	17
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:	mal96.troj.evad.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 6.4% (good quality ratio 6.4%) • Quality average: 55.8% • Quality standard deviation: 12%
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 • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe

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):	5.7345833661144345
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:	NTS_eTaxInvoice#U00a004-08-2021#U00b7pdf.exe
File size:	131072
MD5:	69273783da83c97ff021e1002243dd8b
SHA1:	c1f879d4c66d53ae682b870f3e9e0e016929e220
SHA256:	81980be7abe0eb985644d9c867fe8ad4820d9d6a2c9538 011d67251dd9378170
SHA512:	6bf65db5a6798bfe67e935351357d99f9fc531f9a3d94aec 4b20b67fed94135d51f948a4f2a3ed7d53e922d5da808ea 3a6f18cfc18f1021313ce3420e73f1837
SSDEEP:	1536:P2GouBbBuyXebN6nGZ+yIbpklD0o/WlQgWs6Wc pvihGo:+GZBb9nttbpvQ7s8pvihG

General

File Content Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......u...1...1...1.......0...~...0.......0...Rich1...........PE..L...-.!M.....................`....................@................

File Icon

Icon Hash:	0ccea09899191898

Static PE Info

General

Entrypoint:	0x4016bc
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:	0x4D21FF2D [Mon Jan 3 16:54:05 2011 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:	b99d75676bd131a32dd8593967e4443d

Entrypoint Preview

Instruction
push 00410D34h
call 00007F9D58BCA873h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
cmp byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
retn 3C04h
pop ebp
retn 78C8h
dec ebx
xchg eax, ebx
popfd
add byte ptr [edi+3A915898h], ah
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
jo 00007F9D58BCA8A2h
and byte ptr [eax], ah
and byte ptr [eax], ah
push ebx
je 00007F9D58BCA8E7h
outsb

Instruction
bound edi, dword ptr [eax]
add byte ptr [eax], ah
add byte ptr [eax], al
add byte ptr [eax], al
dec esp
xor dword ptr [eax], eax
sub byte ptr [eax-1Fh], ah
shr dword ptr [ebx], cl
push cs
push ds
dec ebx
inc esp
mov dh, BCh
cwde
adc byte ptr [ebp+5Fh], dh
cwde
out CCh, al
les esp, eax
and eax, 46E3687Bh
movsb
jp 00007F9D58BCA86Bh
mov bl, 32h
call 00007F9DA7F78877h
lodsd
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
dec esi
cmc
add byte ptr [eax], al
rol dword ptr [eax+eax+00h], 1
add byte ptr [eax+eax], al
dec ebp
outsb
jnc 00007F9D58BCA882h
or eax, 50000601h
outsd
jnc 00007F9D58BCA8F6h
je 00007F9D58BCA8B3h
add byte ptr [ecx], bl
add dword ptr [eax], eax
inc edx
add byte ptr [edx], ah
add byte ptr [ebx], ah

Instruction
mov es, word ptr [eax+eax+00h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x18b64	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1b000	0x485e	.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	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x160	.text
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	0x180e8	0x19000	False	0.39478515625	data	6.26229031411	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x1a000	0xaf4	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1b000	0x485e	0x5000	False	0.4140625	data	4.36108868789	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1d2b6	0x25a8	data		
RT_ICON	0x1c20e	0x10a8	data		
RT_ICON	0x1b886	0x988	data		
RT_ICON	0x1b41e	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x1b3e0	0x3e	data		
RT_VERSION	0x1b180	0x260	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaFreeVar, __vbaStrVarMove, __vbaFreeVarList, __vbaEnd, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaSetSystemError, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryVar, __vbaAryDestruct, __vbaVarForInit, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, _adj_fdivr_m16i, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, DllFunctionCall, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, __vbaStrVarVal, _CIlog, __vbaNew2, __vbaR8Str, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaI4Str, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarAdd, __vbaVarDup, __vbaStrToAnsi, __vbaFpI4, _CIatan, __vbaStrMove, __vbaCastObj, __vbaAryCopy, _allmul, __vbaLateIdSt, _CItan, __vbaFPInt, __vbaVarForNext, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x0409 0x04b0
InternalName	Stringet3
FileVersion	3.00
CompanyName	Salty
Comments	Salty
ProductName	Salty
ProductVersion	3.00
FileDescription	Salty
OriginalFilename	Stringet3.exe

Possible Origin

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

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: NTS_eTaxInvoice#U00a004-08-2021#U00b7pdf.exe PID: 7100 Parent PID: 5944

General

Start time:	08:58:18
Start date:	12/04/2021
Path:	C:\Users\user\Desktop\NTS_eTaxInvoice#U00a004-08-2021#U00b7pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\NTS_eTaxInvoice#U00a004-08-2021#U00b7pdf.exe'
Imagebase:	0x400000
File size:	131072 bytes
MD5 hash:	69273783DA83C97FF021E1002243DD8B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis