ID: 358491
Sample Name:
TNTNumber1062324.PDF.exe
Cookbook: default.jbs
Time: 17:45:48
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

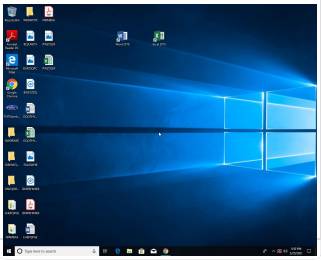
Analysis Report TNTNumber1062324.PDF.exe

Overview

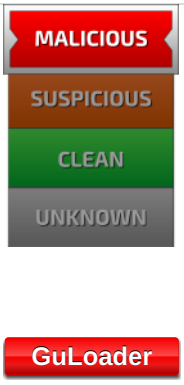
General Information

Sample Name:	TNTNumber1062324.PDF.exe
Analysis ID:	358491
MD5:	90524c4f4816eb2.
SHA1:	b10d499c6aedcc...
SHA256:	adea37317bf08b2.
Infos:	

Most interesting Screenshot:



Detection



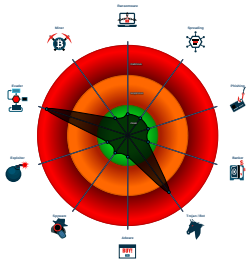
GuLoader

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

Signatures

- Multi AV Scanner detection for subm…
- Sigma detected: Suspicious Double …
- Yara detected GuLoader
- Contains functionality to detect hard…
- Detected RDTSC dummy instruction…
- Found potential dummy code loops (…
- Hides threads from debuggers
- Initial sample is a PE file and has a …
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Uses an obfuscated file name to hid…

Classification



Startup

- **System is w10x64**
- TNTNumber1062324.PDF.exe (PID: 7092 cmdline: 'C:\Users\user\Desktop\TNTNumber1062324.PDF.exe' MD5: 90524C4F4816EB22693E92212B8CAB6C)
  - TNTNumber1062324.PDF.exe (PID: 6072 cmdline: 'C:\Users\user\Desktop\TNTNumber1062324.PDF.exe' MD5: 90524C4F4816EB22693E92212B8CAB6C)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

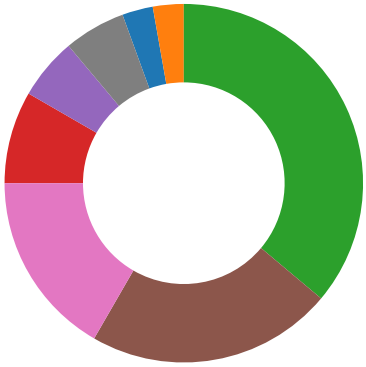
Source	Rule	Description	Author	Strings
Process Memory Space: TNTNumber1062324.PDF.exe PID: 6072	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: TNTNumber1062324.PDF.exe PID: 6072	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Suspicious Double Extension

Signature Overview



- AV Detection
- Compliance
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Compliance:

Uses 32bit PE files

System Summary:

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Hooking and other Techniques for Hiding and Protection:

Uses an obfuscated file name to hide its real file extension (double extension)

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect Any.run

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:

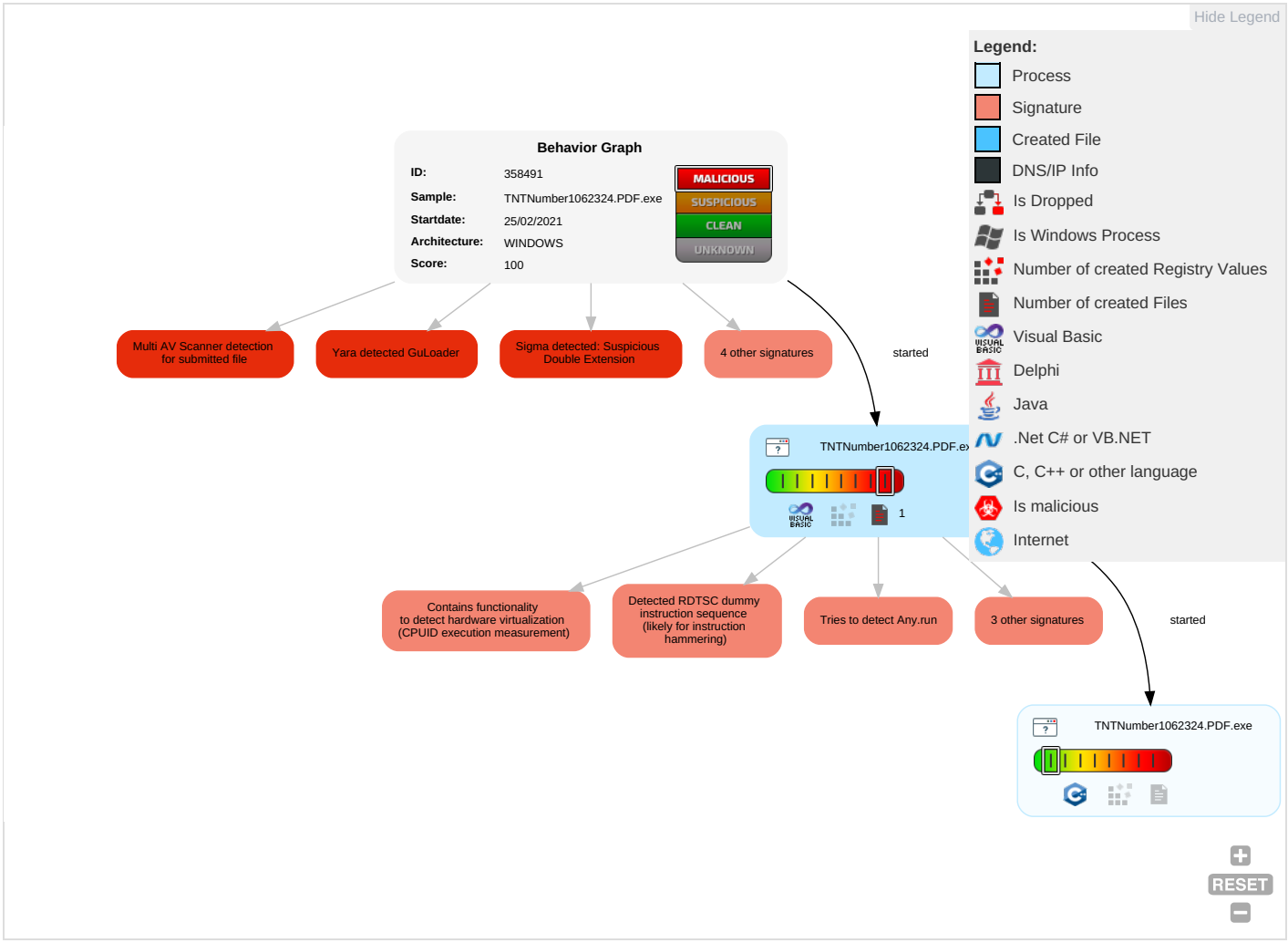
Found potential dummy code loops (likely to delay analysis)

Hides threads from debuggers

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 7 2 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 3 1 1	LSASS Memory	Virtualization/Sandbox Evasion 3 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1 1	NTDS	System Information Discovery 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap

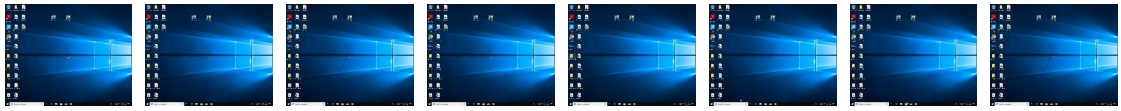
Behavior Graph



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
TNTNumber1062324.PDF.exe	42%	Virustotal		Browse
TNTNumber1062324.PDF.exe	32%	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:	358491
Start date:	25.02.2021
Start time:	17:45:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TNTNumber1062324.PDF.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:	mal100.troj.evad.winEXE@3/0@0/0
EGA Information:	Failed
HDC Information:	Failed
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 • Execution Graph export aborted for target TNTNumber1062324.PDF.exe, PID 6072 because there are no executed function • Report size getting too big, too many NtAllocateVirtualMemory calls found.

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):	4.84338309214011
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:	TNTNumber1062324.PDF.exe
File size:	135168
MD5:	90524c4f4816eb22693e92212b8cab6c
SHA1:	b10d499c6aedcc0c0a3cf728a609466824a73d19
SHA256:	adea37317bf08b2dbb86164c609b0ee2eec3ccd6ef0e82c1c46d8447623e5899
SHA512:	676d45524b435f4736ea7f42945c196f27226f0428214c0616626a6c8fe74cb6e803549dd31b2125b2eda7d95643b9e5ab8c896cdae04646a3bab7e974510e41
SSDEEP:	3072:i4wVUPBu0Mxbf+rr3AfKDeQVXrbGQqwV:i4wVUPgxbf+rr3AfKSQVXrqQqwV

General

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

File Icon

Icon Hash:	01d292796dda0080

Static PE Info

General

Entrypoint:	0x4013dc
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:	0x512282FE [Mon Feb 18 19:37:34 2013 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:	cc882d101998a701353b40b0cd8c341a

Entrypoint Preview

Instruction
push 00412ED0h
call 00007F0CB4E2DD63h
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
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax+198A3DB9h], ah
sub byte ptr [eax], ah
inc esp
mov al, byte ptr [F9C22134h]
xor eax, 0000BFC7h
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
jc 00007F0CB4E2DD7Fh
or al, byte ptr [edx+6Fh]
jc 00007F0CB4E2DDC6h
push edx
inc ecx
push eax
inc ecx
inc ebx
inc ebp

Instruction
dec edi
push ebp
push ebx
add byte ptr [edx], dh
or eax, 0061430Ah
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax
add al, B6h
fisub word ptr [edi-44h]
and dl, byte ptr [C59A4D6Ch]
pop esi
mov esp, dword ptr [ebp+23h]
or al, D3h
test eax, 3FC1CD10h
jc 00007F0CB4E2DDB9h
sub byte ptr [esi-7D7ED3EBh], 00000009h
sar dword ptr [edx], 4Fh
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
add byte ptr [eax], al
add byte ptr [eax], al
sbb dword ptr [ecx], eax
add byte ptr [edi+edi*2+0D000000h], ah
add byte ptr [ebx+65h], dl
imul esi, dword ptr [esi+65h], 6Eh
jnc 00007F0CB4E2DDE0h
jne 00007F0CB4E2DDDFh
insd
jc 00007F0CB4E2DD73h
or eax, 49000C01h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x160c4	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x18000	0x83de	.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	

Name	Virtual Address	Virtual Size	Is in Section
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	0xe0	.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	0x154f4	0x16000	False	0.397283380682	data	5.49793705448	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x17000	0xa18	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x18000	0x83de	0x9000	False	0.340304904514	data	3.5303201949	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x202b6	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0x1ec8e	0x1628	dBase IV DBT of \200.DBF, blocks size 0, block length 4608, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x1cfe6	0x1ca8	data		
RT_ICON	0x1c33e	0xca8	data		
RT_ICON	0x1bfd6	0x368	GLS_BINARY_LSB_FIRST		
RT_ICON	0x19a2e	0x25a8	data		
RT_ICON	0x18986	0x10a8	data		
RT_ICON	0x1851e	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x184a8	0x76	data		
RT_VERSION	0x18240	0x268	MS Windows COFF Motorola 68000 object file		

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaFreeVar, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaGenerateBoundsError, __vbaStrCmp, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaNew2, __vbaInStr, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaLateMemCall, __vbaVarDup, _CIatan, __vbaStrMove, _allmul, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x0000 0x04b0
InternalName	SEMICHORIC
FileVersion	1.00
CompanyName	Sinth Radio
ProductName	Sinth Radio
ProductVersion	1.00
FileDescription	Sinth Radio
OriginalFilename	SEMICHORIC.exe

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

System Behavior

Analysis Process: TNTNumber1062324.PDF.exe PID: 7092 Parent PID: 5876

General

Start time:	17:46:30
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\TNTNumber1062324.PDF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\TNTNumber1062324.PDF.exe'
Imagebase:	0x400000
File size:	135168 bytes
MD5 hash:	90524C4F4816EB22693E92212B8CAB6C
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

Analysis Process: TNTNumber1062324.PDF.exe PID: 6072 Parent PID: 7092

General

Start time:	17:49:09
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\TNTNumber1062324.PDF.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\user\Desktop\TNTNumber1062324.PDF.exe'
Imagebase:	0x400000
File size:	135168 bytes
MD5 hash:	90524C4F4816EB22693E92212B8CAB6C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis