ID: 528770
Sample Name: TNT
Documents.exe
Cookbook: default.jbs
Time: 18:49:10
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

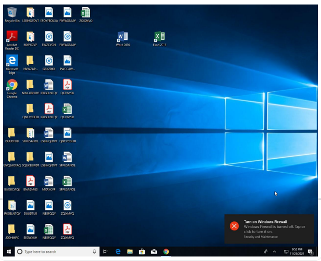
Windows Analysis Report TNT Documents.exe

Overview

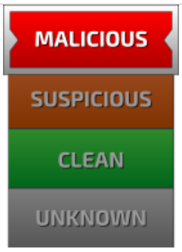
General Information

Sample Name:	TNT Documents.exe
Analysis ID:	528770
MD5:	53213cdc9809c6..
SHA1:	2383fe2e296a1f2..
SHA256:	f49a87b9fa0e2e8..
Tags:	exe Formbook TNT
Infos:	

Most interesting Screenshot:



Detection



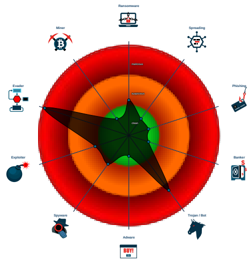
FormBook

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Initial sample is a PE file and has a …
- Tries to detect sandboxes and other…
- Machine Learning detection for samp…
- Self deletion via cmd delete
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- TNT Documents.exe (PID: 6612 cmdline: "C:\Users\user\Desktop\TNT Documents.exe" MD5: 53213CDC9809C6DEBEBE6400A4D1A891)
  - TNT Documents.exe (PID: 6040 cmdline: {path} MD5: 53213CDC9809C6DEBEBE6400A4D1A891)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
    - autoconv.exe (PID: 6884 cmdline: C:\Windows\SysWOW64\autoconv.exe MD5: 4506BE56787EDCD771A351C10B5AE3B7)
    - msdt.exe (PID: 6076 cmdline: C:\Windows\SysWOW64\msdt.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
      - cmd.exe (PID: 5964 cmdline: /c del "C:\Users\user\Desktop\TNT Documents.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6684 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - explorer.exe (PID: 3240 cmdline: "C:\Windows\explorer.exe" /LOADSAVEDWINDOWS MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.floridanratraining.com/how6/"
  ],
  "decoy": [
    "wealthcabana.com",
    "fourfortyfourcreations.com",
    "cqqcsy.com",
    "bhwzjd.com",
    "niftyfashionrewards.com",
    "andersongiftemporium.com",
    "smarttradingcoin.com",
    "ilarealty.com",
    "sherrywine.net",
    "fsecg.info",
    "xoti.top",
    "pirosconsulting.com",
    "fundapie.com",
    "bbgm4egda.xyz",
    "legalfortmyers.com",
    "improvizy.com",
    "yxdyhs.com",
    "lucky2balls.com",
    "panelmall.com",
    "davenportkartway.com",
    "springfieldlottery.com",
    "pentagonpublishers.com",
    "icanmakeyoufamous.com",
    "40m2k.com",
    "projectcentered.com",
    "webfactory.agency",
    "metronixmedical.com",
    "dalingtao.xyz",
    "functionalsoft.com",
    "klopert77.com",
    "cortepuroiberico.com",
    "viavelleiloes.online",
    "bamedia.online",
    "skolicalunjo.com",
    "kayhardy.com",
    "excellentappraisers.com",
    "sademakale.com",
    "zbycsb.com",
    "empirejewelss.com",
    "coached.info",
    "20215414.online",
    "dazzlehide.com",
    "swickstyle.com",
    "specialtyplastics.online",
    "noordinarysenior.com",
    "bluinfo.digital",
    "chuxiaoxin.xyz",
    "adwin-estate.com",
    "girlwithaglow.com",
    "auctions.email",
    "topekasecurestorage.com",
    "mountain-chicken.com",
    "lhdtrj.com",
    "mhtqph.club",
    "solatopotato.com",
    "mecitiris.com",
    "hotrodathangtrungquoc.com",
    "gapteknews.com",
    "mantraexchange.online",
    "cinematiccarpenter.com",
    "wozka.xyz",
    "car-tech.tech",
    "jssatchell.media",
    "joyokanji-cheer.com"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.798434648.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000002.798434648.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	- 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC - 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC - 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 - 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 - 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F - 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 - 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 - 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 - 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D - 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 - 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000004.00000002.798434648.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	- 0x16ae9:$sqlite3step: 68 34 1C 7B E1 - 0x16bfc:$sqlite3step: 68 34 1C 7B E1 - 0x16b18:$sqlite3text: 68 38 2A 90 C5 - 0x16c3d:$sqlite3text: 68 38 2A 90 C5 - 0x16b2b:$sqlite3blob: 68 53 D8 7F 8C - 0x16c53:$sqlite3blob: 68 53 D8 7F 8C
0000000B.00000002.962732138.0000000004670000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000B.00000002.962732138.0000000004670000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	- 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC - 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC - 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 - 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 - 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F - 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 - 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 - 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 - 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D - 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 - 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.0.TNT Documents.exe.400000.8.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.0.TNT Documents.exe.400000.8.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	- 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC - 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC - 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 - 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 - 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F - 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 - 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 - 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 - 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D - 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 - 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
4.0.TNT Documents.exe.400000.8.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	- 0x16ae9:$sqlite3step: 68 34 1C 7B E1 - 0x16bfc:$sqlite3step: 68 34 1C 7B E1 - 0x16b18:$sqlite3text: 68 38 2A 90 C5 - 0x16c3d:$sqlite3text: 68 38 2A 90 C5 - 0x16b2b:$sqlite3blob: 68 53 D8 7F 8C - 0x16c53:$sqlite3blob: 68 53 D8 7F 8C
4.2.TNT Documents.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.TNT Documents.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	- 0x7818:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC - 0x7bb2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC - 0x138c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 - 0x133b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 - 0x139c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F - 0x13b3f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 - 0x85ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 - 0x1262c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 - 0x9342:$sequence_7: 66 89 0C 02 5B 8B E5 5D - 0x18db7:$sequence_8: 3C 54 74 04 3C 74 75 F4 - 0x19e5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

Sigma Overview

System Summary:

Sigma detected: Possible Applocker Bypass

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

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

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

Self deletion via cmd delete

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information:

Yara detected FormBook

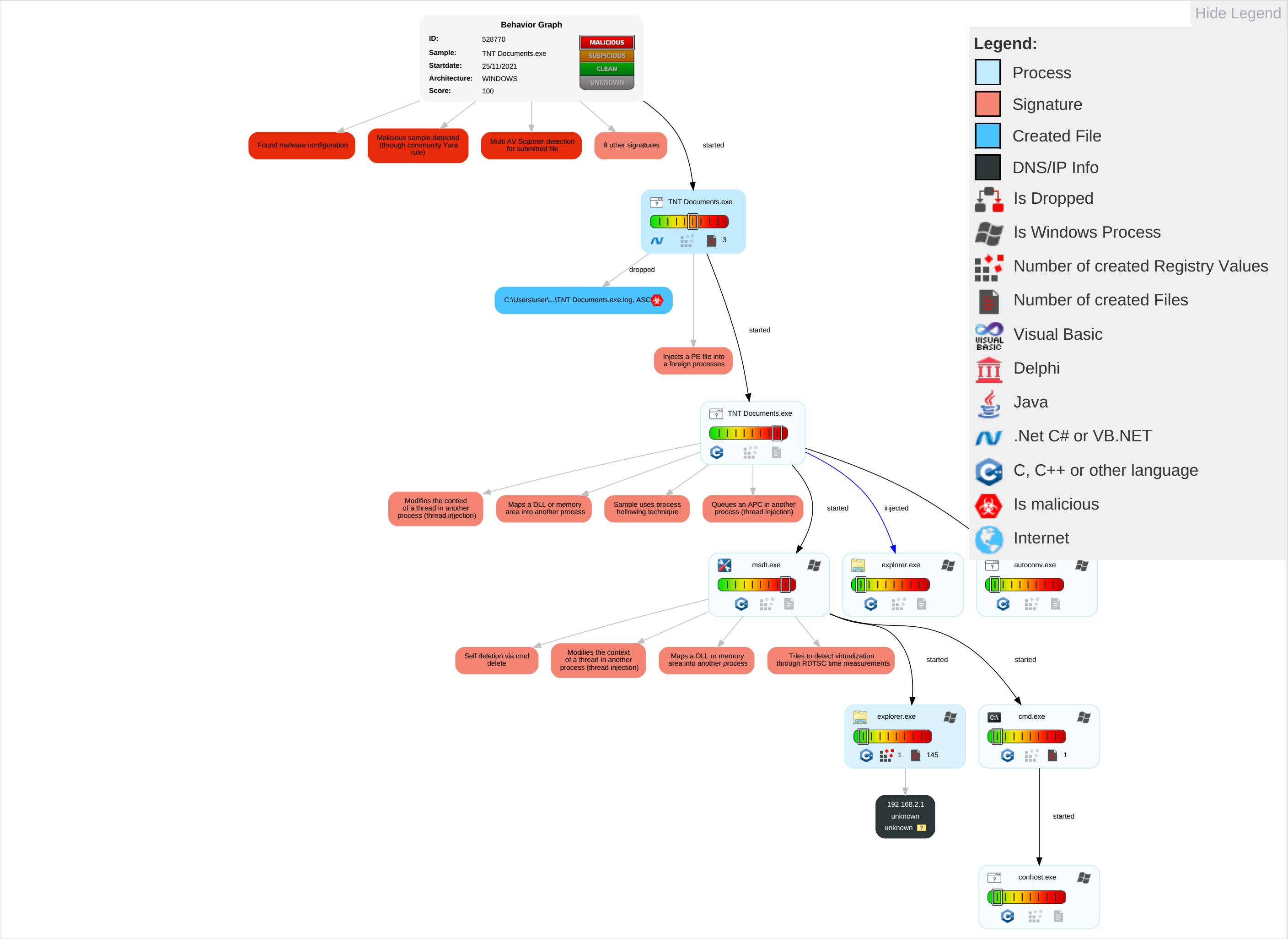
Remote Access Functionality:

Yara detected FormBook

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	Shared Modules 1	Path Interception	Process Injection 5 1 2	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop c Insecure Network Communicat
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 2 3 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 4 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 1 2	NTDS	Virtualization/Sandbox Evasion 4 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Information Discovery 1 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	File Deletion 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

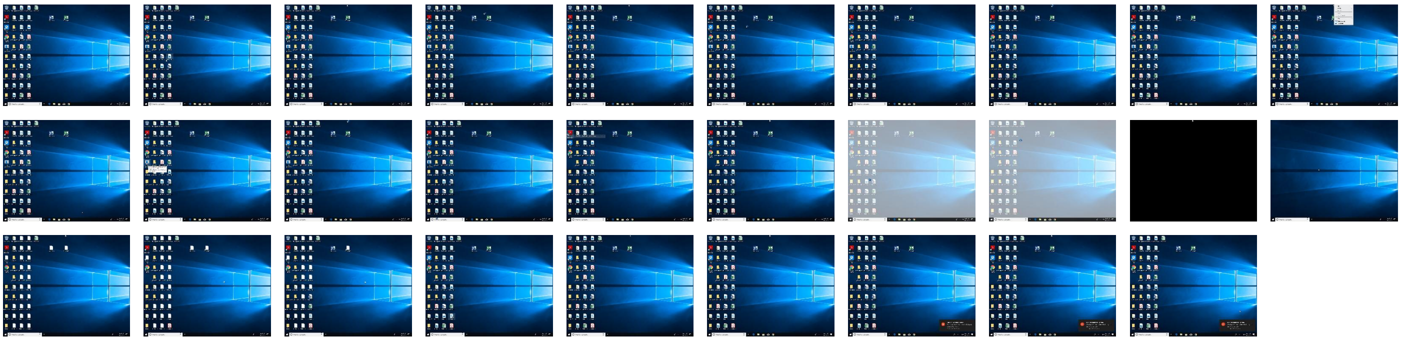
Behavior Graph

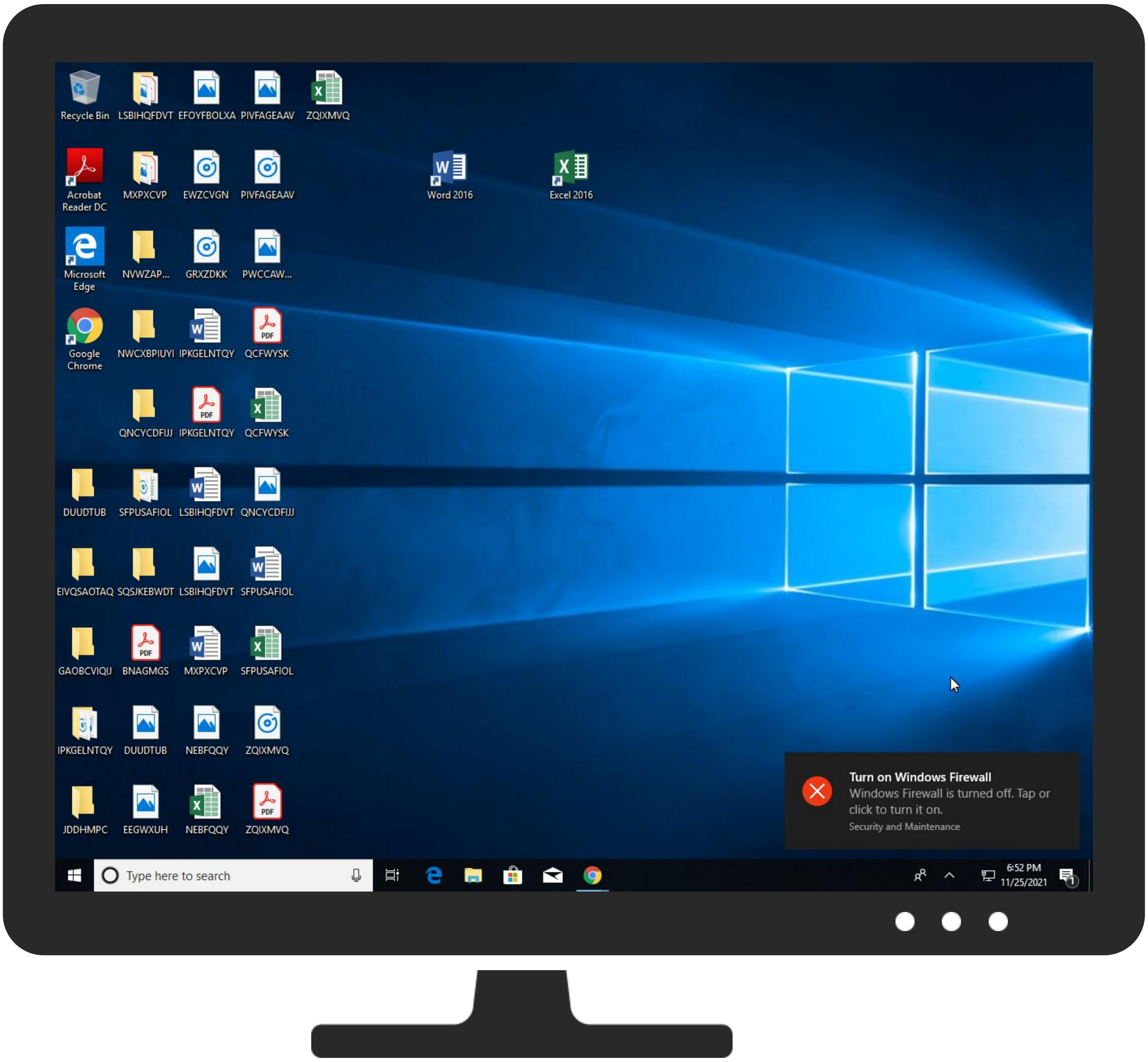

Hide Legend
Behavior Graph
ID: 528770
Sample: TNT Documents.exe
Startdate: 25/11/2021
Architecture: WINDOWS
Score: 100
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Found malware configuration
Malicious sample detected (through community Yara rule)
Multi AV Scanner detection for submitted file
9 other signatures
started
TNT Documents.exe
3
dropped
C:\Users\user\...\TNT Documents.exe.log, ASCII
Injects a PE file into a foreign processes
started
TNT Documents.exe
Modifies the context of a thread in another process (thread injection)
Maps a DLL or memory area into another process
Sample uses process hollowing technique
Queues an APC in another process (thread injection)
started
injected
msdt.exe
explorer.exe
autoconv.exe
Self deletion via cmd delete
Modifies the context of a thread in another process (thread injection)
Maps a DLL or memory area into another process
Tries to detect virtualization through RDTSC time measurements
started
started
explorer.exe
1
145
cmd.exe
1
192.168.2.1
unknown
unknown
started
conhost.exe
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

Screenshots

Thumbnails

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





Turn on Windows Firewall
Windows Firewall is turned off. Tap or click to turn it on.
Security and Maintenance

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
TNT Documents.exe	49%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
TNT Documents.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.TNT Documents.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.0.TNT Documents.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.0.TNT Documents.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.0.TNT Documents.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
www.floridanratraining.com/how6/	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://ns.adobp	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.floridanratraining.com/how6/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528770
Start date:	25.11.2021
Start time:	18:49:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 22s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TNT Documents.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:	27
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@11/1@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 11.6% (good quality ratio 10.6%) • Quality average: 74.9% • Quality standard deviation: 30.2%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
18:50:19	API Interceptor	1x Sleep call for process: TNT Documents.exe modified
18:51:48	API Interceptor	76x Sleep call for process: explorer.exe modified

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\Microsoft\CLR_v4.0_32\UsageLogs\TNT Documents.exe.log

Process:	C:\Users\user\Desktop\TNT Documents.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F8
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.955416061350034
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	TNT Documents.exe
File size:	390656
MD5:	53213cdc9809c6debebe6400a4d1a891
SHA1:	2383fe2e296a1f28deb600cfeadb0a3fa18856f3
SHA256:	f49a87b9fa0e2e84273ad690ffe6d7548d7ed13a595fd4ad df7c6211b0eb5108
SHA512:	7dd498aeaeaa092c37adad278b2847d2b7712635aedcde c1c4ecd8789523ba4b9995dc14b7e5c1bf5130f55edba5e 611d8e78f621a38c7bba11bf379d3a6f6de
SSDEEP:	6144:tdu3v3Ur+0zBbMStodHnsU/IvlLhGj+bTmHlBfJ5HCoTPtUm84YMfN:tdu3Pm+0zRopB8Gj+b0trioTXfN
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L......a................................. ... .@.. ....`............@................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x460b0e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui

General

Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x619EEFA3 [Thu Nov 25 02:06:27 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x5eb14	0x5ec00	False	0.962746330805	SysEx File - AKG	7.96472261238	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x62000	0x580	0x600	False	0.419270833333	data	4.43335713516	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x64000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: TNT Documents.exe PID: 6612 Parent PID: 5444

General

Start time:	18:50:10
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\TNT Documents.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\TNT Documents.exe"
Imagebase:	0xb40000
File size:	390656 bytes
MD5 hash:	53213CDC9809C6DEBEBE6400A4D1A891
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.703985087.0000000003206000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.707439158.0000000003F39000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.707439158.0000000003F39000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.707439158.0000000003F39000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: TNT Documents.exe PID: 6040 Parent PID: 6612

General

Start time:	18:50:21
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\TNT Documents.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x890000
File size:	390656 bytes
MD5 hash:	53213CDC9809C6DEBEBE6400A4D1A891
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.798434648.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.798434648.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.798434648.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.698679096.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.698679096.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.698679096.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.799493056.00000000015D0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.799493056.00000000015D0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.799493056.00000000015D0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.798798288.0000000000E30000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.798798288.0000000000E30000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.798798288.0000000000E30000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.699262494.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.699262494.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.699262494.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 6040

General

Start time:	18:50:24
Start date:	25/11/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	- Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.756647993.000000000E4CE000.00000040.00020000.sdmp, Author: Joe Security - Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.756647993.000000000E4CE000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com - Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.756647993.000000000E4CE000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group - Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.735741697.000000000E4CE000.00000040.00020000.sdmp, Author: Joe Security - Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.735741697.000000000E4CE000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com - Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.735741697.000000000E4CE000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: autoconv.exe PID: 6884 Parent PID: 6040

General

Start time:	18:51:04
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\autoconv.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autoconv.exe
Imagebase:	0x960000
File size:	851968 bytes
MD5 hash:	4506BE56787EDCD771A351C10B5AE3B7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: msdt.exe PID: 6076 Parent PID: 6040

General

Start time:	18:51:06
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msdt.exe
Imagebase:	0xaf0000
File size:	1508352 bytes
MD5 hash:	7F0C51DBA69B9DE5DDF6AA04CE3A69F4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.962732138.0000000004670000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.962732138.0000000004670000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.962732138.0000000004670000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.960597354.00000000007A0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.960597354.00000000007A0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.960597354.00000000007A0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.962868450.0000000004800000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.962868450.0000000004800000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.962868450.0000000004800000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 5964 Parent PID: 6076

General

Start time:	18:51:10
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\TNT Documents.exe"
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6684 Parent PID: 5964

General

Start time:	18:51:11
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: explorer.exe PID: 3240 Parent PID: 5252

General

Start time:	18:51:47
Start date:	25/11/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	"C:\Windows\explorer.exe" /LOADSAVEDWINDOWS
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Disassembly

Code Analysis