ID: 532859
Sample Name: TNT Documents.exe
Cookbook: default.jbs
Time: 18:56:46
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

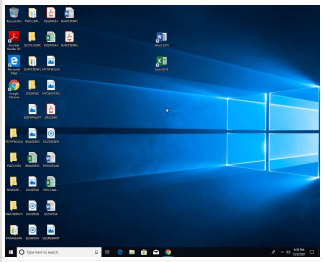
Windows Analysis Report TNT Documents.exe

Overview

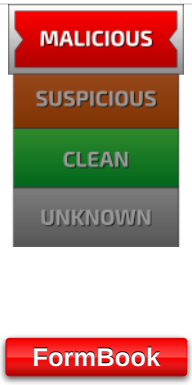
General Information

Sample Name:	TNT Documents.exe
Analysis ID:	532859
MD5:	f943d9ee7955904.
SHA1:	7dca5c03f55ab6c..
SHA256:	2c26343342361e..
Tags:	exe Formbook TNT
Infos:	

Most interesting Screenshot:



Detection

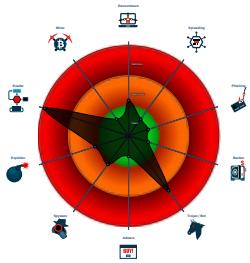


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- System process connects to networ…
- Antivirus detection for URL or domain
- 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: 4548 cmdline: "C:\Users\user\Desktop\TNT Documents.exe" MD5: F943D9EE79559042BFFF9B4E55270CFA)
  - TNT Documents.exe (PID: 6384 cmdline: {path} MD5: F943D9EE79559042BFFF9B4E55270CFA)
  - TNT Documents.exe (PID: 6400 cmdline: {path} MD5: F943D9EE79559042BFFF9B4E55270CFA)
    - explorer.exe (PID: 3292 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - mstsc.exe (PID: 6268 cmdline: C:\Windows\SysWOW64\mstsc.exe MD5: 2412003BE253A515C620CE4890F3D8F3)
        - cmd.exe (PID: 1148 cmdline: /c del "C:\Users\user\Desktop\TNT Documents.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 4484 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **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
0000000B.00000000.349024537.000000000F905000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000B.00000000.349024537.000000000F905000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x46c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x41b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x47c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000B.00000000.349024537.000000000F905000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x6ae9:$sqlite3step: 68 34 1C 7B E1 • 0x6bfc:$sqlite3step: 68 34 1C 7B E1 • 0x6b18:$sqlite3text: 68 38 2A 90 C5 • 0x6c3d:$sqlite3text: 68 38 2A 90 C5 • 0x6b2b:$sqlite3blob: 68 53 D8 7F 8C • 0x6c53:$sqlite3blob: 68 53 D8 7F 8C
0000000B.00000000.331135577.000000000F905000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000B.00000000.331135577.000000000F905000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x46c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x41b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x47c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 29 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.TNT Documents.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
7.2.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
7.2.TNT Documents.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15ce9:$sqlite3step: 68 34 1C 7B E1 • 0x15dfc:$sqlite3step: 68 34 1C 7B E1 • 0x15d18:$sqlite3text: 68 38 2A 90 C5 • 0x15e3d:$sqlite3text: 68 38 2A 90 C5 • 0x15d2b:$sqlite3blob: 68 53 D8 7F 8C • 0x15e53:$sqlite3blob: 68 53 D8 7F 8C
7.0.TNT Documents.exe.400000.8.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
7.0.TNT Documents.exe.400000.8.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$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
Click to see the 16 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Yara detected FormBook
- Antivirus detection for URL or domain
- Machine Learning detection for sample

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- System process connects to network (likely due to code injection or exploit)
- 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
- .NET source code contains very large strings

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:

- System process connects to network (likely due to code injection or exploit)
- 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

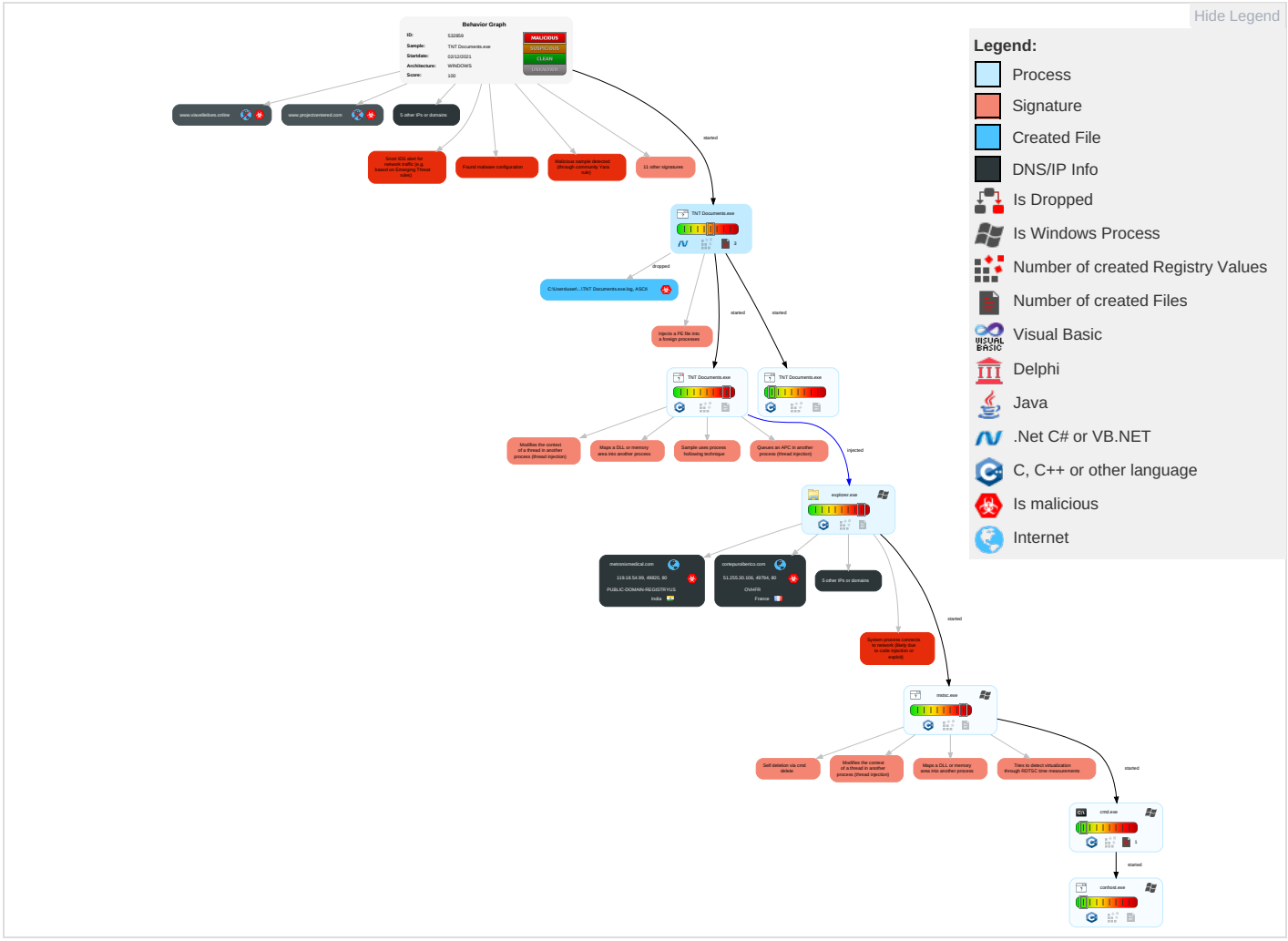
Remote Access Functionality:

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 6 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 6 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Owner/User Discovery	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-F Access Poir
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Timestomp 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	File Deletion 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellu Base Statio

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
TNT Documents.exe	47%	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
7.2.TNT Documents.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.0.TNT Documents.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.0.TNT Documents.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.0.TNT Documents.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
coached.info	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comI.TTF	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.sajatypeworks.comus4	0%	Avira URL Cloud	safe	
http://www.coached.info/how6/?iN9tFB=ViiEyPWfYSojbIItq3CvR44gsAi5K3j61FSCtvXBJNhPIgkqJAzuFuyRGTnTAJ9C7DX1GVbTZg==&4h=7n_DRJGxnRd	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnar	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn9	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/soft	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.founder.c	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.founder.com.cn/cnG	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://fontfabrik.comx	0%	Avira URL Cloud	safe	
http://www.metronixmedical.com/how6/?iN9tFB=eO7AK5UTSuqTcoXAE4JKPt5tOBv6nnmPk0M2G0ISpIO4jWwGwHlgDwMnGXB5SfKol3UegXCZpg==&4h=7n_DRJGxnRd	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/slnt	0%	Avira URL Cloud	safe	
http://www.urwpp.de2	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.fontbureau.comF(	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cna	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/(	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.coma	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.founder.com.cn/cnaX	0%	Avira URL Cloud	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.com=	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcomo?	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/M	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/F	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fonts.comX	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/.comp	0%	Avira URL Cloud	safe	
http://www.tiro.comU	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.specialtyplastics.online/how6/?iN9tFB=xCGPRvAkK+xY+IPwAFenqNjQ2EZcc1A/OJpQ1mtXoxRJ135kHr2e9wYqnwHz38WooRcfQb4d5g==&4h=7n_DRJGxnRd	100%	Avira URL Cloud	malware	
http://www.urwpp.der	0%	Avira URL Cloud	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.zhongyicts.com.cno.	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.tiro.comic	0%	URL Reputation	safe	
http://www.fontbureau.comitud	0%	URL Reputation	safe	
http://www.cortepuroiberico.com/how6/?iN9tFB=6MRiWtHRwAFwDvhVcJAGZD0p4fLcIEcyVDy1Zth0WcmsI64tqWfeZe6Y2j9BcQs7bzR6A9198A==&4h=7n_DRJGxnRd	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
metronixmedical.com	119.18.54.99	true	true		unknown
www.functionalsoft.com	74.208.236.210	true	false		unknown
coached.info	34.102.136.180	true	false	• 0%, Virustotal, Browse	unknown
cortepuroiberico.com	51.255.30.106	true	true		unknown
www.specialtyplastics.online	209.17.116.163	true	true		unknown
projectcentered.com	158.69.116.156	true	true		unknown
www.pirosconsulting.com	unknown	unknown	true		unknown
www.metronixmedical.com	unknown	unknown	true		unknown
www.pentagonpublishers.com	unknown	unknown	true		unknown
www.floridanratraining.com	unknown	unknown	true		unknown
www.viavelleiloes.online	unknown	unknown	true		unknown
www.cortepuroiberico.com	unknown	unknown	true		unknown
www.coached.info	unknown	unknown	true		unknown
www.projectcentered.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.coached.info/how6/?iN9tFB=ViiEyPWfYSojbIItq3CvR44gsAi5K3j61FSCtvXBJNhPIgkqJAzuFuyRGTnTAJ9C7DX1GVbTZg==&4h=7n_DRJGxnRd	false	• Avira URL Cloud: safe	unknown
www.floridanratraining.com/how6/	true	• Avira URL Cloud: safe	low
http://www.metronixmedical.com/how6/?iN9tFB=eO7AK5UTSuqTcoXAE4JKPt5tOBv6nnmPk0M2G0ISpIO4jWwGwHlgDwMnGXB5SfKol3UegXCZpg==&4h=7n_DRJGxnRd	true	• Avira URL Cloud: safe	unknown
http://www.specialtyplastics.online/how6/?iN9tFB=xCGPRvAkK+xY+IPwAFenqNjQ2EZcc1A/OJpQ1mtXoxRJ135kHr2e9wYqnwHz38WooRcfQb4d5g==&4h=7n_DRJGxnRd	true	• Avira URL Cloud: malware	unknown
http://www.cortepuroiberico.com/how6/?iN9tFB=6MRiWtHRwAFwDvhVcJAGZD0p4fLcIEcyVDy1Zth0WcmsI64tqWfeZe6Y2j9BcQs7bzR6A9198A==&4h=7n_DRJGxnRd	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
119.18.54.99	metronixmedical.com	India		394695	PUBLIC-DOMAIN-REGISTRYUS	true
34.102.136.180	coached.info	United States		15169	GOOGLEUS	false
51.255.30.106	cortepuroiberico.com	France		16276	OVHFR	true
209.17.116.163	www.specialtyplastics.online	United States		55002	DEFENSE-NETUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532859
Start date:	02.12.2021
Start time:	18:56:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 53s
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:	28
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@9/1@10/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 8.7% (good quality ratio 7.7%) • Quality average: 72.4% • Quality standard deviation: 32.8%
HCA Information:	• Successful, ratio: 96% • 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
18:57:58	API Interceptor	1x Sleep call for process: TNT Documents.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
209.17.116.163	RFQ - SST#2021111503.exe	Get hash	malicious	Browse	• www.eduka do.online/teni/?1bSD 0d6p=0pqFA ulx9peJBQa LHhi2O539G rRUe9Dg5qn QgkcE3vGHf 3Q1HjrP1jP /RDvSqSrk2 xiP&jJB=9r9x5R
	yVvATSvedsfMg0l.exe	Get hash	malicious	Browse	• www.ichel brousset.c om/czh8/?h 0DX=irrd3y uyc1GImfAB ledh2a+c4k F1IqLY7IOB v/DJSDLKV1 P8G+/4s2D0 JrIDDvMvFj LtzXE2ZQ== &UpZ=4hzll

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DZqb1YCMJknskFE.exe	Get hash	malicious	Browse	• www.alvarezdelugo.store/9mj8/?b61TGp=UkZThqrRocv5vk1faiVRq9+iiPL+c1gbqU90ov2hL2y42KpkYKZbBF4nZ16GjYtZO51IlqH2Lg==&2dXl=-Zt00jOpTfntw
	DHL Documents.exe	Get hash	malicious	Browse	• www.specialtyplastics.online/how6/?l2Jl=xCGPRvAkK+xY+IPwAFenqNjQ2EZcc1A/OJpQ1mtXoxRJ135kHr2e9wYqnzra08qQhypJ&Tf5pq=W6zlk8Rp
	Dhl_AWB5032675620,pdf.exe	Get hash	malicious	Browse	• www.durston.store/b62n/?t64PStG=z6Vsvg8A5NXyXPPhKMZIBHml/L7mqqirp/PWrU0BeLpkyNyDM5h+f+EgtIJL2Tixlbzc&Sp=4hX0vf
	vbc.exe	Get hash	malicious	Browse	• www.applebroog.industries/fqiq/?2d=0RH9gkF6jVnFZMBLg5arrRt8ci9oBvnO845D4NtwM1wnd4qumJjOU8GaWcQJQdSDPFjg&KBZh8h=9rFxIRS8frv8A02
	TT_SWIFT_Export Order_noref S10SMG00318021.exe	Get hash	malicious	Browse	• www.aarondecker.online/46uq/?j0=SFN8Rxuh3&3fQ0Khi=IBlQMs5j29CKqlv3/eZQ6Z47udTwmev2lX+bwOiN2E8lumQwhRgtDV6FzU7U1t+cHC/Y
	Nuevo Pedido.exe	Get hash	malicious	Browse	• www.downingmunroe.online/udeh/?2dYxhfjx=XsaaYVs5B+09RIkVBuB9uz7A4nUjKuiPTgX8t5JQ0XDGnKq9QQr8GjRKS5XBt9MDEtTg&s6AD=5jltOBY8-rN
	Payment Advice.doc	Get hash	malicious	Browse	• www.nihonkoryu.site/cy88/?JpCxc=UdPBVTbj1CZF+opyLZ3z0qAaJaL/JpkwFii79QX209xtQVaMtZARr5G5+pIvOlE0oIFN3g==&9rl=-Z8xBfo8a6

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	68886.xlsx	Get hash	malicious	Browse	• www.visco ent.online/scb0/?bXi=L8pgukv0AuVDNAdjNh2AJGutMHnCfg3bCrFlNw+YyifAdhr3mrIeLuq3PR+hiDkJiRhf3g==&PB=hxoT
	PO_No.202201EYL-01_ABW.exe	Get hash	malicious	Browse	• www.aaron decker.onl ine/46uq/?j6Al=IBlQMs5j29CKqlv3/eZQ6Z47udTwmev2IX+bwOiN2E8lumQwhRgtDV6FzXbE6MukZnWf&4hqTJ=PpNtRPgx0VJ
	rfq.exe	Get hash	malicious	Browse	• www.elois eball.onli ne/s2qi/?MhBd9XLx=CJ4ega8we8rDK2oOyDtNp6AuRxR37H0DfWv6L4ABKIpafKqiPSieQwyYu/RVEHddVBRA&SR=d0DLMt
	New Order.xlsx	Get hash	malicious	Browse	• www.visco ent.online/scb0/?NN6=L8pgukv0AuVDNAdjNh2AJGutMHnCfg3bCrFlNw+YyifAdhr3mrIeLuq3PR+hiDkJiRhf3g==&lFND1Z=6lPhL
	PO202104-114 - APQ Comercial Apoquindo,pdf.exe	Get hash	malicious	Browse	• www.durst on.store/b62n/?ChJte=z6Vsvg8A5NXyXPPhKMZIBHml/L7mqqirp/PWrU0BeLpkyNyDM5h+f+EgtIJhpjSxhZ7c&d6A=SJExlzkP
	As5zvmxhPo.exe	Get hash	malicious	Browse	• www.scbco mmunity.pa rtners/xgmi/?SzrxP8lx=ibySZgQScShq1lS4qM2nT1qHIBOXZbGjkidZCxDm/G3nGy75y5MD+ijFjtG1ArxxbKo6&tTbDp=7nf8x
	SWIFT-MLSB-11,546.doc	Get hash	malicious	Browse	• www.howel lenterpris es.biz/cy88/?0deDKH=f2Jd-DLxZJsXUZ&cjXL1rR=fkUWIEJ3aTmqc1Hb/8mQzV6AtAV96QXeCAvCSnvV4vLU/JJ/qpHHTJ9bGgGB5MvhUhf5fg==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SHIPMENT ARRIVAL NOTICE - ORIGINAL DOCUMENTS__pdf.exe	Get hash	malicious	Browse	• www.gzsz.online/ubw4/?cR-H=RPx2ZUkBCpbabyLVYaiQALpYpcukYHUKRCHGI7PR5DR61tf9OEQgp5XPT5XPjlBrfWaDsOZcvg==&G4=q6PdCh7
	Quote request.exe	Get hash	malicious	Browse	• www.eloiseball.online/s2qi/?lZwxYz=y6AldH-&TJELpfLP=CJ4ega8we8rDK2oOyDtNp6AuRxR37H0DfWv6L4ABKIpafKqiPSieQwyYu/RVEHddVBRA
	scan_21000076119_pdf.exe	Get hash	malicious	Browse	• www.edukado.online/teni/?3fx8BFd=0pqFAulx9peJBQaLHhi2O539GrRUe9Dg5qnQgkcE3vGHf3Q1HjrP1jP/RAPo6DLcsWDI&A6U89=j2JXRdWhjhk8k
	NEW ORDER 2021.exe	Get hash	malicious	Browse	• www.metalworkingadditives.online/b2c0/?N0=tQ9OUq/fzxn+R82X6GTzZlmpGIW84sc0d5YJpv42KDMZxUSBkatd7Ys79Ad1zpKElTcI&o48=QhiPALAplp

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.specialtyplastics.online	DHL Documents.exe	Get hash	malicious	Browse	• 209.17.116.163

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	Dhl Document.exe	Get hash	malicious	Browse	• 208.91.199.224
	DHL Waybill receipt.exe	Get hash	malicious	Browse	• 208.91.199.223
	Shipping Document BL Copy.exe	Get hash	malicious	Browse	• 103.195.185.115
	DHL SHIPMENT NOTIFICATION 284748395PD.exe	Get hash	malicious	Browse	• 208.91.199.223
	SHIPPING DOCUMENT & PL.exe	Get hash	malicious	Browse	• 103.195.185.115
	Swift MT103 pdf.exe	Get hash	malicious	Browse	• 208.91.199.225
	Scan096355.exe	Get hash	malicious	Browse	• 208.91.199.225
	yYa94CeATF8h2NA.exe	Get hash	malicious	Browse	• 208.91.199.223
	part-1500645108.xlsb	Get hash	malicious	Browse	• 103.76.231.42
	part-1500645108.xlsb	Get hash	malicious	Browse	• 103.76.231.42
	item-40567503.xlsb	Get hash	malicious	Browse	• 162.215.254.201
	item-40567503.xlsb	Get hash	malicious	Browse	• 162.215.254.201
	PG4636 - Confirmed .xls.exe	Get hash	malicious	Browse	• 208.91.198.143
	item-107262298.xlsb	Get hash	malicious	Browse	• 162.215.254.201

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	item-107262298.xlsb	Get hash	malicious	Browse	• 162.215.254.201
	item-1202816963.xlsb	Get hash	malicious	Browse	• 162.215.254.201
	item-1202816963.xlsb	Get hash	malicious	Browse	• 162.215.254.201
	DHL Receipt.html	Get hash	malicious	Browse	• 199.79.62.126
	BOQ.exe	Get hash	malicious	Browse	• 208.91.199.223
	RFQ-Spares and tools.exe	Get hash	malicious	Browse	• 208.91.198.143
OVHFR	ClaimCopy-1848214335-12022021.xlsb	Get hash	malicious	Browse	• 158.69.133.78
	ClaimCopy-1848214335-12022021.xlsb	Get hash	malicious	Browse	• 158.69.133.78
	ClaimCopy-539408676-12022021.xlsb	Get hash	malicious	Browse	• 158.69.133.78
	ClaimCopy-539408676-12022021.xlsb	Get hash	malicious	Browse	• 158.69.133.78
	ClaimCopy-539408676-12022021.xlsb	Get hash	malicious	Browse	• 158.69.133.78
	reg.exe	Get hash	malicious	Browse	• 213.186.33.5
	REQUEST FOR SPECIFICATION.exe	Get hash	malicious	Browse	• 213.251.158.218
	ETgVKIYRW5.dll	Get hash	malicious	Browse	• 149.56.106.83
	cMVyW1SDZz.dll	Get hash	malicious	Browse	• 149.56.106.83
	ETgVKIYRW5.dll	Get hash	malicious	Browse	• 149.56.106.83
	cMVyW1SDZz.dll	Get hash	malicious	Browse	• 149.56.106.83
	2iJBYBel22.dll	Get hash	malicious	Browse	• 149.56.106.83
	2iJBYBel22.dll	Get hash	malicious	Browse	• 149.56.106.83
	Tender SN980018277 & SN9901827 Signed Copy.exe	Get hash	malicious	Browse	• 51.161.104.181
	Invoice.exe	Get hash	malicious	Browse	• 54.38.220.85
	AegEywmjUJ.exe	Get hash	malicious	Browse	• 51.79.99.124
	P.O SPECIFICATION.xlsx	Get hash	malicious	Browse	• 51.79.99.124
	DC-330NC.xlsx	Get hash	malicious	Browse	• 51.79.99.124
	FILE_915494026923219.xlsm	Get hash	malicious	Browse	• 158.69.222.101
	UioA2E9DBG.dll	Get hash	malicious	Browse	• 158.69.222.101

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):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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..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):	7.5483150102950916
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	TNT Documents.exe
File size:	503808
MD5:	f943d9ee79559042bfff9b4e55270cfa
SHA1:	7dca5c03f55ab6cbebd6bb3a8203d5c1d7516567
SHA256:	2c26343342361efe4ada7dd077f832792eb77f184ec9a6c5b8c3a8ad35dd5aaa
SHA512:	c9d6bffff768eb7ff3853eeec196e21286a7d5be040c1b1dc4882cc106fd61d6d33ce24444eb77452fef33310a8d202a7568a4cf6db9c4e9b824b6d54b91cf09
SSDEEP:	12288:dIzgxqzpbqi/RAu/jlYQpYRKz7OoDxI7pIHL0i:dew2Zqi/B/Jb+IX9I7pIr0
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...I.9.....P..... .....@.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x47c5be
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xA539E86C [Sat Nov 3 17:54:52 2057 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	0x7a5c4	0x7a600	False	0.809814702503	data	7.56105630003	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x7e000	0x5ac	0x600	False	0.421223958333	data	4.10451869633	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x80000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/02/21-18:59:22.638450	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49794	80	192.168.2.7	51.255.30.106
12/02/21-18:59:22.638450	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49794	80	192.168.2.7	51.255.30.106
12/02/21-18:59:22.638450	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49794	80	192.168.2.7	51.255.30.106
12/02/21-18:59:43.047578	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49820	80	192.168.2.7	119.18.54.99
12/02/21-18:59:43.047578	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49820	80	192.168.2.7	119.18.54.99
12/02/21-18:59:43.047578	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49820	80	192.168.2.7	119.18.54.99
12/02/21-18:59:48.300111	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49822	80	192.168.2.7	34.102.136.180
12/02/21-18:59:48.300111	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49822	80	192.168.2.7	34.102.136.180
12/02/21-18:59:48.300111	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49822	80	192.168.2.7	34.102.136.180
12/02/21-18:59:48.478607	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49822	34.102.136.180	192.168.2.7
12/02/21-18:59:59.432108	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49827	80	192.168.2.7	158.69.116.156
12/02/21-18:59:59.432108	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49827	80	192.168.2.7	158.69.116.156
12/02/21-18:59:59.432108	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49827	80	192.168.2.7	158.69.116.156

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 18:59:22.561023951 CET	192.168.2.7	8.8.8.8	0xb8d4	Standard query (0)	www.cortepuroiberico.com	A (IP address)	IN (0x0001)
Dec 2, 2021 18:59:27.700095892 CET	192.168.2.7	8.8.8.8	0x47d2	Standard query (0)	www.specialtyplastics.online	A (IP address)	IN (0x0001)
Dec 2, 2021 18:59:42.128535032 CET	192.168.2.7	8.8.8.8	0xdbef	Standard query (0)	www.metronixmedical.com	A (IP address)	IN (0x0001)
Dec 2, 2021 18:59:48.248903990 CET	192.168.2.7	8.8.8.8	0xbbe2	Standard query (0)	www.coached.info	A (IP address)	IN (0x0001)
Dec 2, 2021 18:59:53.948990107 CET	192.168.2.7	8.8.8.8	0x4020	Standard query (0)	www.pentagonpublishers.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 18:59:58.996303082 CET	192.168.2.7	8.8.8.8	0xe702	Standard query (0)	www.projectcentered.com	A (IP address)	IN (0x0001)
Dec 2, 2021 19:00:09.559422970 CET	192.168.2.7	8.8.8.8	0x47eb	Standard query (0)	www.functionalsoft.com	A (IP address)	IN (0x0001)
Dec 2, 2021 19:00:14.876486063 CET	192.168.2.7	8.8.8.8	0xaa06	Standard query (0)	www.viavelleiloes.online	A (IP address)	IN (0x0001)
Dec 2, 2021 19:00:19.954091072 CET	192.168.2.7	8.8.8.8	0x8197	Standard query (0)	www.pirosconsulting.com	A (IP address)	IN (0x0001)
Dec 2, 2021 19:00:25.002089977 CET	192.168.2.7	8.8.8.8	0xe1bb	Standard query (0)	www.floridanratraining.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 18:59:22.592832088 CET	8.8.8.8	192.168.2.7	0xb8d4	No error (0)	www.cortepuroiberico.com	cortepuroiberico.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 18:59:22.592832088 CET	8.8.8.8	192.168.2.7	0xb8d4	No error (0)	cortepuroiberico.com		51.255.30.106	A (IP address)	IN (0x0001)
Dec 2, 2021 18:59:27.823506117 CET	8.8.8.8	192.168.2.7	0x47d2	No error (0)	www.specialtyplastics.online		209.17.116.163	A (IP address)	IN (0x0001)
Dec 2, 2021 18:59:42.871825933 CET	8.8.8.8	192.168.2.7	0xdbef	No error (0)	www.metronixmedical.com	metronixmedical.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 18:59:42.871825933 CET	8.8.8.8	192.168.2.7	0xdbef	No error (0)	metronixmedical.com		119.18.54.99	A (IP address)	IN (0x0001)
Dec 2, 2021 18:59:48.279051065 CET	8.8.8.8	192.168.2.7	0xbbe2	No error (0)	www.coached.info	coached.info		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 18:59:48.279051065 CET	8.8.8.8	192.168.2.7	0xbbe2	No error (0)	coached.info		34.102.136.180	A (IP address)	IN (0x0001)
Dec 2, 2021 18:59:53.979896069 CET	8.8.8.8	192.168.2.7	0x4020	Name error (3)	www.pentagonpublishers.com	none	none	A (IP address)	IN (0x0001)
Dec 2, 2021 18:59:59.324498892 CET	8.8.8.8	192.168.2.7	0xe702	No error (0)	www.projectcentered.com	projectcentered.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 18:59:59.324498892 CET	8.8.8.8	192.168.2.7	0xe702	No error (0)	projectcentered.com		158.69.116.156	A (IP address)	IN (0x0001)
Dec 2, 2021 19:00:09.585350990 CET	8.8.8.8	192.168.2.7	0x47eb	No error (0)	www.functionalsoft.com		74.208.236.210	A (IP address)	IN (0x0001)
Dec 2, 2021 19:00:14.937154055 CET	8.8.8.8	192.168.2.7	0xaa06	Server failure (2)	www.viavelleiloes.online	none	none	A (IP address)	IN (0x0001)
Dec 2, 2021 19:00:19.995712042 CET	8.8.8.8	192.168.2.7	0x8197	Name error (3)	www.pirosconsulting.com	none	none	A (IP address)	IN (0x0001)
Dec 2, 2021 19:00:25.555591106 CET	8.8.8.8	192.168.2.7	0xe1bb	Server failure (2)	www.floridanratraining.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.cortepuroiberico.com
- www.specialtyplastics.online
- www.metronixmedical.com
- www.coached.info

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.7	49794	51.255.30.106	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 18:59:22.638449907 CET	14538	OUT	GET /how6/?iN9tFB=6MRiWtHRwAFwDvhVcJAGZD0p4fLcIEcyVDy1Zth0WcmsI64tqWfeZe6Y2j9BcQs7bzR6A9198A==&4h=7n_DRJGxnRd HTTP/1.1 Host: www.cortepuroiberico.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Dec 2, 2021 18:59:22.687228918 CET	14538	IN	HTTP/1.1 502 Bad Gateway Server: nginx Date: Thu, 02 Dec 2021 17:59:22 GMT Content-Type: text/html Content-Length: 150 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 35 30 32 20 42 61 64 20 47 61 74 65 77 61 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 35 30 32 20 42 61 64 20 47 61 74 65 77 61 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>502 Bad Gateway</title></head><body> 502 Bad Gateway <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.7	49815	209.17.116.163	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 18:59:36.959983110 CET	14601	OUT	GET /how6/?iN9tFB=xCGPRvAkK+xY+IPwAFenqNjQ2EZcc1A/OJpQ1mtXoxRJ135kHr2e9wYqnwHz38WooRcfQb4d5g==&4h=7n_DRJGxnRd HTTP/1.1 Host: www.specialtyplastics.online Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Dec 2, 2021 18:59:37.078370094 CET	14601	IN	HTTP/1.1 400 Bad Request Server: openresty/1.19.9.1 Date: Thu, 02 Dec 2021 17:59:37 GMT Content-Type: text/html Content-Length: 163 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6f 70 65 6e 72 65 73 74 79 2f 31 2e 31 39 2e 39 2e 31 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>400 Bad Request</title></head><body> 400 Bad Request <hr> openresty/1.19.9.1 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.7	49820	119.18.54.99	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 18:59:43.047578096 CET	14603	OUT	GET /how6/?iN9tFB=eO7AK5UTSuqTcoXAE4JKPt5tOBv6nnmPk0M2G0ISpIO4jWwGwHlgDwMnGXB5SfKol3UegXCZpg==&4h=7n_DRJGxnRd HTTP/1.1 Host: www.metronixmedical.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 18:59:43.231224060 CET	14603	IN	HTTP/1.1 302 Found Date: Thu, 02 Dec 2021 17:59:43 GMT Server: Apache Location: https://metronixmedical.com/how6/?iN9tFB=eO7AK5UTSuqTcoXAE4JKPt5tOBv6nnmPk0M2G0ISpIO4jWwGwHlgDwMnGXB5SfKol3UegXCZpg==&4h=7n_DRJGxnRd Content-Length: 320 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 6d 65 74 72 6f 6e 69 78 6d 65 64 69 63 61 6c 2e 63 6f 6d 2f 68 6f 77 36 2f 3f 69 4e 39 74 46 42 3d 65 4f 37 41 4b 35 55 54 53 75 71 54 63 6f 58 41 45 34 4a 4b 50 74 35 74 4f 42 76 36 6e 6e 6d 50 6b 30 4d 32 47 30 49 53 70 49 4f 34 6a 57 77 47 77 48 6c 67 44 77 4d 6e 47 58 42 35 53 66 4b 6f 6c 33 55 65 67 58 43 5a 70 67 3d 3d 26 61 6d 70 3b 34 68 3d 37 6e 5f 44 52 4a 47 78 6e 52 64 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head><body> Found The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.7	49822	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 18:59:48.300111055 CET	14611	OUT	GET /how6/?iN9tFB=ViiEyPWfYSojbIItq3CvR44gsAi5K3j61FSCtvXBJNhPIgkqJAzuFuyRGTnTAJ9C7DX1GVbTZg==&4h=7n_DRJGxnRd HTTP/1.1 Host: www.coached.info Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Dec 2, 2021 18:59:48.478606939 CET	14611	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 02 Dec 2021 17:59:48 GMT Content-Type: text/html Content-Length: 275 ETag: "61a4f026-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: TNT Documents.exe PID: 4548 Parent PID: 5372

General

Start time:	18:57:47
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\TNT Documents.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\TNT Documents.exe"
Imagebase:	0x70000
File size:	503808 bytes
MD5 hash:	F943D9EE79559042BFFF9B4E55270CFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.297323666.0000000003389000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.297323666.0000000003389000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.297323666.0000000003389000.00000004.00000001.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: 6384 Parent PID: 4548

General

Start time:	18:57:59
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\TNT Documents.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x130000
File size:	503808 bytes
MD5 hash:	F943D9EE79559042BFFF9B4E55270CFA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: TNT Documents.exe PID: 6400 Parent PID: 4548

General

Start time:	18:58:01
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\TNT Documents.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xaa0000

File size:	503808 bytes
MD5 hash:	F943D9EE79559042BFFF9B4E55270CFA
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: 00000007.00000002.361357634.00000000014F0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.361357634.00000000014F0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.361357634.00000000014F0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.361164513.00000000010D0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.361164513.00000000010D0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.361164513.00000000010D0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.290851774.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.290851774.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.290851774.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.289769088.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.289769088.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.289769088.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.360525017.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.360525017.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.360525017.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3292 Parent PID: 6400

General

Start time:	18:58:07
Start date:	02/12/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff662bf0000
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: 0000000B.00000000.349024537.000000000F905000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000000.349024537.000000000F905000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000000.349024537.000000000F905000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000000.331135577.000000000F905000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000000.331135577.000000000F905000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000000.331135577.000000000F905000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: mstsc.exe PID: 6268 Parent PID: 3292

General

Start time:	18:58:34
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\mstsc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\mstsc.exe
Imagebase:	0xec0000
File size:	3444224 bytes
MD5 hash:	2412003BE253A515C620CE4890F3D8F3
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: 00000011.00000002.524379332.0000000003A30000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000002.524379332.0000000003A30000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000002.524379332.0000000003A30000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000002.523498302.0000000003310000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000002.523498302.0000000003310000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000002.523498302.0000000003310000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000002.524461205.0000000003A60000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000002.524461205.0000000003A60000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000002.524461205.0000000003A60000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 1148 Parent PID: 6268

General

Start time:	18:58:39
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\TNT Documents.exe"
Imagebase:	0x870000
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: 4484 Parent PID: 1148

General

Start time:	18:58:41
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff673460000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis