ID: 383898
Sample Name: invoice.exe
Cookbook: default.jbs
Time: 12:02:34
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

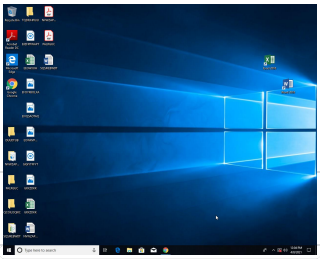
Analysis Report invoice.exe

Overview

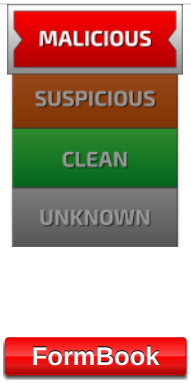
General Information

Sample Name:	invoice.exe
Analysis ID:	383898
MD5:	492017e064cab9..
SHA1:	a3addbdea8245b..
SHA256:	524306af2db603c.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

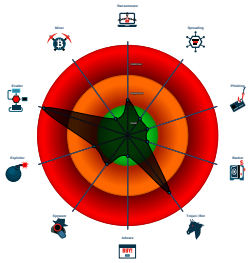


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…

Classification



Startup

- **System is w10x64**
- invoice.exe (PID: 1972 cmdline: 'C:\Users\user\Desktop\invoice.exe' MD5: 492017E064CAB97DD8EA27ABD3E5CFCA)
  - invoice.exe (PID: 480 cmdline: C:\Users\user\Desktop\invoice.exe MD5: 492017E064CAB97DD8EA27ABD3E5CFCA)
    - explorer.exe (PID: 3472 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - wscript.exe (PID: 5064 cmdline: C:\Windows\SysWOW64\wscript.exe MD5: 7075DD7B9BE8807FCA93ACD86F724884)
        - cmd.exe (PID: 6164 cmdline: /c del 'C:\Users\user\Desktop\invoice.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6196 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.sookepointcargo.com/e3rs/"
  ],
  "decoy": [
    "mcni360clientapp.com",
    "dateyourlovelive.club",
    "amongugadu.com",
    "jarruslogistics.com",
    "jeejwbvf.icu",
    "amnil-wecu.xyz",
    "armaccountingbs.com",
    "revistadedisseny.com",
    "aqiyi.club",
    "cuchdblackboard.com",
    "hancement.info",
    "humanizantes.com",
    "slingshotct.com",
    "degen.fund",
    "onemindtransformed.com",
    "theunlearningjourney.com",
    "zmid.xyz",
    "profirma-nachfolge.com",
    "curiget.xyz",
    "officinadellapappa.com",
    "leverage.community",
    "improvetechprocess.com",
    "legacyadmin.support",
    "quantumwater.info",
    "gsinghproperties.com",
    "gigbager.com",
    "menpeeinthesink.com",
    "ultimate.icu",
    "hotelmaktub.com",
    "arizonagridiron.com",
    "rvsmiami.com",
    "allzodiac.com",
    "knoxvilleoutdoorkitchens.com",
    "gunungbatufrozen.com",
    "keystone-sd.com",
    "positiveagenda-consulting.com",
    "harshdeepfashion.com",
    "imetmymurdereronline.com",
    "thesnackculture.com",
    "carolinapropertiessolution.com",
    "prfectskin.com",
    "okaog.com",
    "highdeserthealthinsurance.com",
    "ovelgonne.com",
    "tgcmaine.com",
    "jinlan.online",
    "airportlimo4u.com",
    "serendipity-collective.com",
    "bibeiw.com",
    "unagelo.com",
    "pageonefourplay.info",
    "apmrfgpu.icu",
    "cognitiveautomationtool.com",
    "applelucycooking.com",
    "can-march.xyz",
    "modernmarvelrealtors.com",
    "panasianetwork.net",
    "flowhcf.com",
    "earwaxsux.com",
    "konakia.net",
    "bges301.com",
    "rosuba.com",
    "hedgetheory.com",
    "myyearwithoutjews.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.490575290.0000000002AE0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.490575290.0000000002AE0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000009.00000002.490575290.0000000002AE0000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166c9:$sqlite3step: 68 34 1C 7B E1 • 0x167dc:$sqlite3step: 68 34 1C 7B E1 • 0x166f8:$sqlite3text: 68 38 2A 90 C5 • 0x1681d:$sqlite3text: 68 38 2A 90 C5 • 0x1670b:$sqlite3blob: 68 53 D8 7F 8C • 0x16833:$sqlite3blob: 68 53 D8 7F 8C
00000003.00000002.287914993.0000000001AE0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000003.00000002.287914993.0000000001AE0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

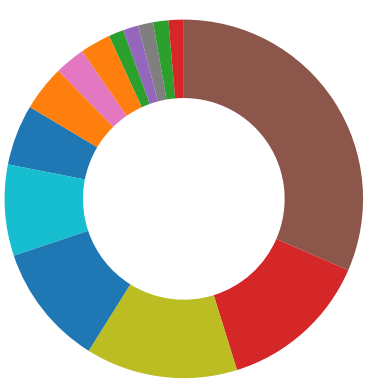
Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.invoice.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.invoice.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18997:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.2.invoice.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158c9:$sqlite3step: 68 34 1C 7B E1 • 0x159dc:$sqlite3step: 68 34 1C 7B E1 • 0x158f8:$sqlite3text: 68 38 2A 90 C5 • 0x15a1d:$sqlite3text: 68 38 2A 90 C5 • 0x1590b:$sqlite3blob: 68 53 D8 7F 8C • 0x15a33:$sqlite3blob: 68 53 D8 7F 8C
3.2.invoice.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.invoice.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- 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

Yara detected FormBook

Machine Learning detection for sample

Networking:

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

C2 URLs / IPs found in malware configuration

Performs DNS queries to domains with low reputation

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

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)

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

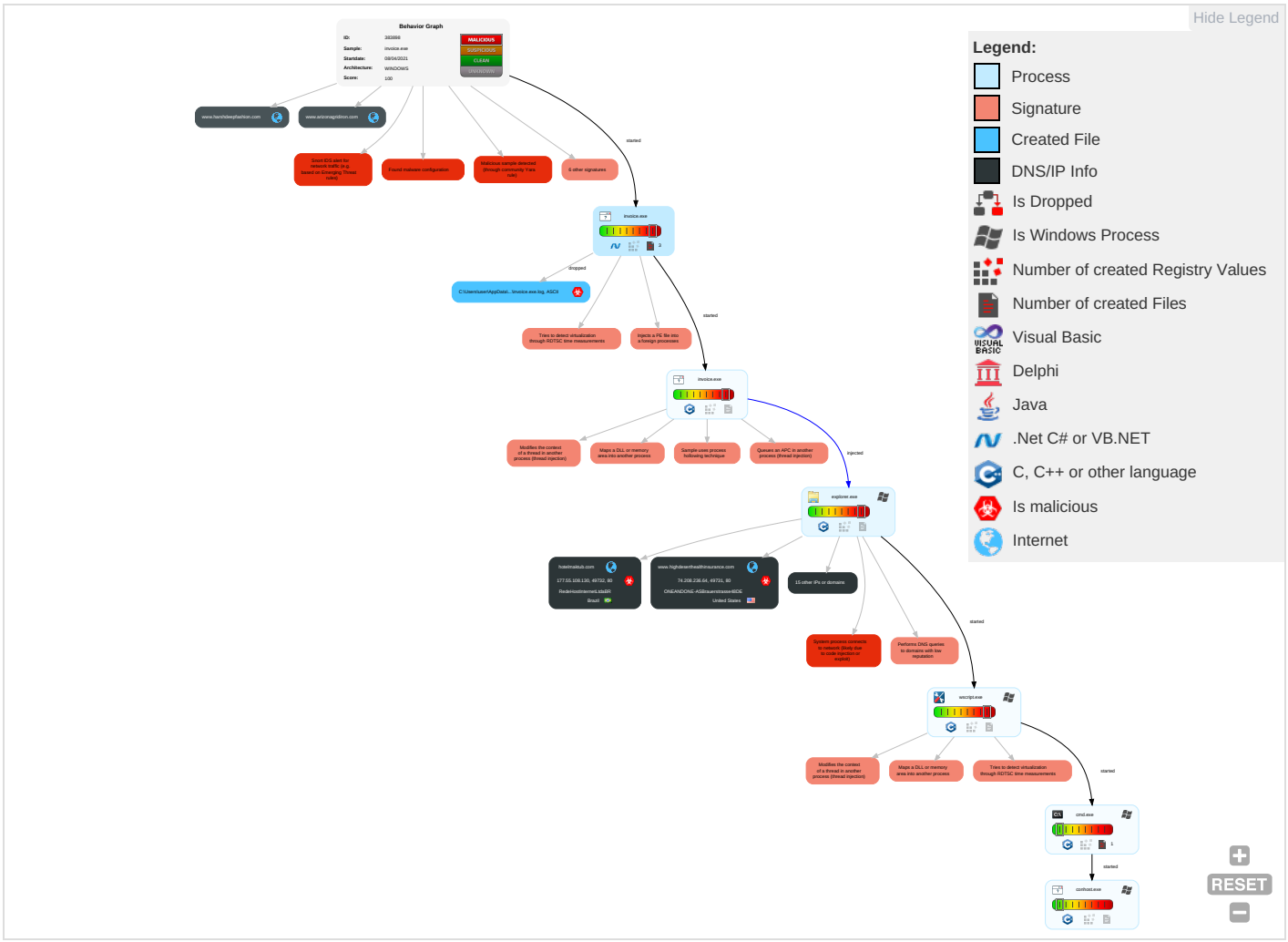
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phor Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 6 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

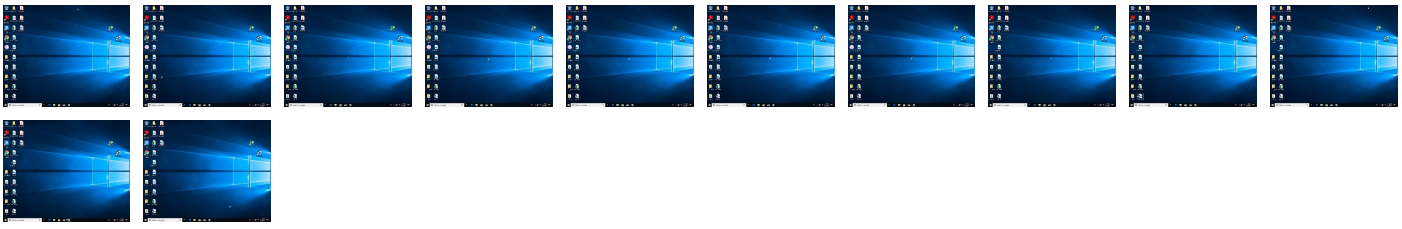
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
invoice.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.invoice.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
legacyadmin.support	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	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.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://https://www.legacyadmin.support/e3rs/?w0G=0yUiwx1wLvxUfzb5kCZXOl2J	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.knoxvilleoutdoorkitchens.com/?fp=acjVxO24ruBE1bSnAJOOFeZ9d2%2Bill3hWebcMHeneryqde34aljK8g	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.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	
www.sookepointcargo.com/e3rs/	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.highdeserthealthinsurance.com	74.208.236.64	true	true		unknown
armaccountingbs.com	2.57.90.16	true	true		unknown
legacyadmin.support	192.0.78.24	true	true	• 0%, Virustotal, Browse	unknown
www.harshdeepfashion.com	216.239.34.21	true	false		unknown
www.jinlan.online.s.strikinglydns.com	35.156.117.131	true	true		unknown
hotelmaktub.com	177.55.108.130	true	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.arizonagridiron.com	23.27.42.72	true	false		unknown
flowhcf.com	184.168.131.241	true	true		unknown
www.knoxvilleoutdoorkitchens.com	208.91.197.91	true	true		unknown
www.dateyourlovelive.club	unknown	unknown	true		unknown
www.legacyadmin.support	unknown	unknown	true		unknown
www.gunungbatufrozen.com	unknown	unknown	true		unknown
www.hotelmaktub.com	unknown	unknown	true		unknown
www.flowhcf.com	unknown	unknown	true		unknown
www.sookepointcargo.com	unknown	unknown	true		unknown
www.jinlan.online	unknown	unknown	true		unknown
www.armaccountingbs.com	unknown	unknown	true		unknown
www.zmid.xyz	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.sookepointcargo.com/e3rs/	true	• Avira URL Cloud: safe	low

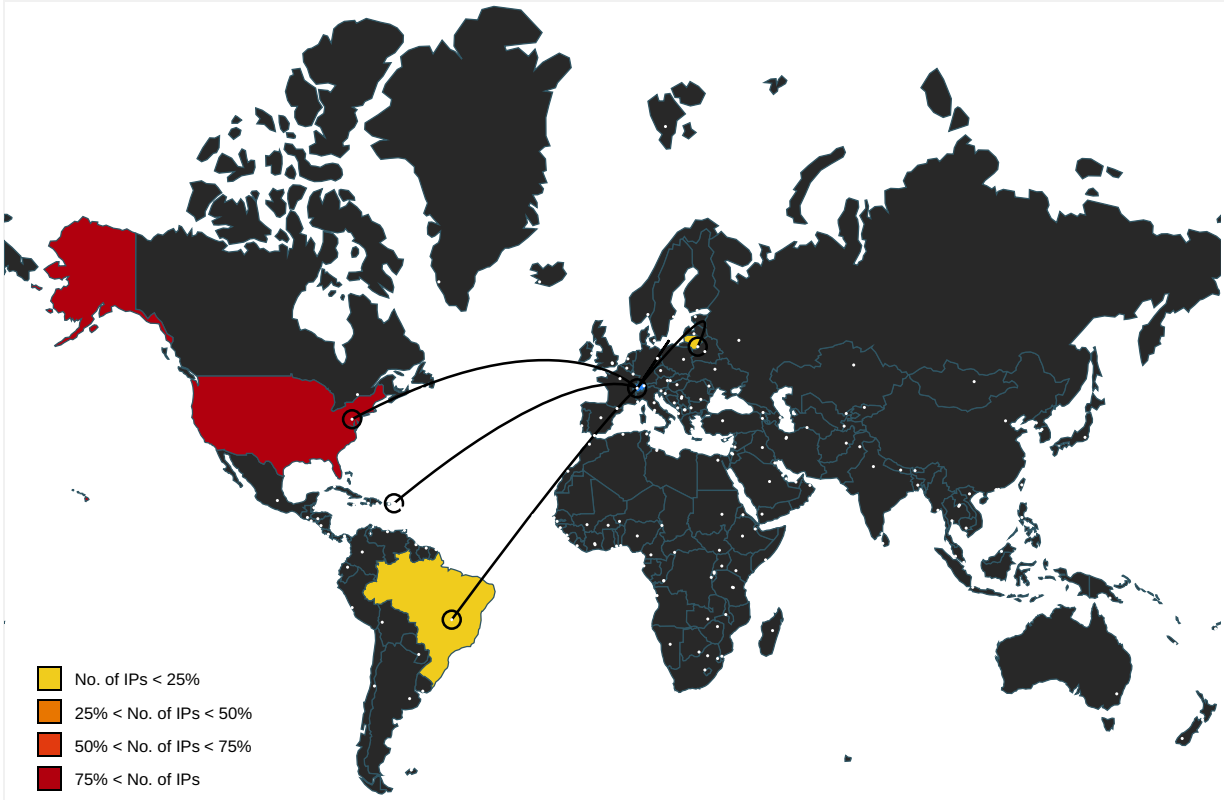
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	invoice.exe, 00000000.00000002.251392987.0000000006E22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.272462034.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	invoice.exe, 00000000.00000002.251392987.0000000006E22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.272462034.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	invoice.exe, 00000000.00000002.251392987.0000000006E22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.272462034.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	invoice.exe, 00000000.00000002.251392987.0000000006E22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.272462034.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	invoice.exe, 00000000.00000002.251392987.0000000006E22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.272462034.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	invoice.exe, 00000000.00000002.251392987.0000000006E22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.272462034.000000000BC30000.00000002.00000001.sdmp	false		high
http://https://dist.nuget.org/win-x86-commandline/latest/nuget.exe	invoice.exe	false		high
http://https://github.com/d-haxton/HaxtonBot/archive/master.zip	invoice.exe	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name4	invoice.exe, 00000000.00000002.245256874.0000000002EBE000.00000004.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000004.00000000.272462034.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000004.00000000.272462034.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	invoice.exe, 00000000.00000002.251392987.0000000006E22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.272462034.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	invoice.exe, 00000000.00000002.245201549.0000000002EB3000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.coml	invoice.exe, 00000000.00000002.251392987.0000000006E22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.272462034.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	invoice.exe, 00000000.00000002.251392987.0000000006E22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.272462034.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	invoice.exe, 00000000.00000002.251392987.0000000006E22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.272462034.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	invoice.exe, 00000000.00000002.251392987.0000000006E22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.272462034.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	invoice.exe, 00000000.00000002.251392987.0000000006E22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.272462034.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.legacyadmin.support/e3rs/?w0G=0yUiwx1wLvxUfzb5kCZXOl2J	wscript.exe, 00000009.00000002.494442857.0000000004CF2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	invoice.exe, 00000000.00000002.251392987.0000000006E22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.272462034.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	invoice.exe, 00000000.00000002.251392987.0000000006E22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.272462034.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	invoice.exe, 00000000.00000002.251392987.0000000006E22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.272462034.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	invoice.exe, 00000000.00000002.251392987.0000000006E22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.272462034.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.knoxvilleoutdoorkitchens.com/?fp=acjVxO24ruBE1bSnAJOOFeZ9d2%2Bill3hWebcMHeneryqde34aljK8g	wscript.exe, 00000009.00000002.494442857.0000000004CF2000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	invoice.exe, 00000000.00000002.251392987.0000000006E22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.272462034.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	invoice.exe, 00000000.00000002.251392987.0000000006E22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.272462034.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	invoice.exe, 00000000.00000002.251392987.0000000006E22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.272462034.000000000BC30000.00000002.00000001.sdmp	false		high
http://https://github.com/Spegeli/Pokemon-Go-Rocket-API/archive/master.zip	invoice.exe	false		high
http://www.fonts.com	invoice.exe, 00000000.00000002.251392987.0000000006E22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.272462034.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	invoice.exe, 00000000.00000002.251392987.0000000006E22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.272462034.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deDPlease	invoice.exe, 00000000.00000002.251392987.0000000006E22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.272462034.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	invoice.exe, 00000000.00000002.251392987.0000000006E22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.272462034.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	invoice.exe, 00000000.00000002.245256874.0000000002EBE000.00000004.00000001.sdmp, invoice.exe, 00000000.00000002.245138274.0000000002EA1000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	invoice.exe, 00000000.00000002.251392987.0000000006E22000.00000004.00000001.sdmp, explorer.exe, 00000004.00000000.272462034.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.0.78.24	legacyadmin.support	United States		2635	AUTOMATTICUS	true
35.156.117.131	www.jinlan.online.s.strikinglydns.com	United States		16509	AMAZON-02US	true
208.91.197.91	www.knoxvilleoutdoorkitchens.com	Virgin Islands (BRITISH)		40034	CONFLUENCE-NETWORK-INCVG	true
74.208.236.64	www.highdesertthealthinsurance.com	United States		8560	ONEANDONE-ASBrauerstrasse48DE	true
184.168.131.241	flowhcf.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
2.57.90.16	armaccountingbs.com	Lithuania		47583	AS-HOSTINGERLT	true
177.55.108.130	hotelmaktub.com	Brazil		53057	RedeHostInternetLtdaBR	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383898
Start date:	08.04.2021
Start time:	12:02:34
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	invoice.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:	27
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@7/1@15/8
EGA Information:	Failed
HDC Information:	• Successful, ratio: 16.7% (good quality ratio 14.8%) • Quality average: 69.4% • Quality standard deviation: 33.4%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 93.184.220.29, 20.82.210.154, 52.255.188.83, 104.43.193.48, 23.54.113.53, 104.43.139.144, 95.100.54.203, 13.107.5.88, 13.107.42.23, 20.50.102.62, 172.217.168.19, 23.10.249.26, 23.10.249.43, 20.54.26.129 • Excluded domains from analysis (whitelisted): ghs.google.com, cs9.wac.phicdn.net, arc.msn.com.nsatc.net, client-office365-tas.msedge.net, ocos-office365-s2s.msedge.net, config.edge.skype.com.trafficmanager.net, store-images.s-microsoft.com-c.edgekey.net, e-0009.e-msedge.net, config-edge-skype.l-0014.l-msedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, l-0014.config.skype.com, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, config.edge.skype.com, www.bing.com, fs.microsoft.com, afdo-tas-offload.trafficmanager.net, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, ocos-office365-s2s-msedge-net.e-0009.e-msedge.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, l-0014.l-msedge.net • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:03:30	API Interceptor	1x Sleep call for process: invoice.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.0.78.24	o2KKHvtb3c.exe	Get hash	malicious	Browse	• www.translations.tools/nsag/?GTgP=1Yx90tXdezyuV8sDZLNplGUVoptWSuBjE4/oeiBfqPIPAmaYyomwKJS6i2A6lUxe1bSuh3UNpg==&5jr=UlSpj

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO#41000055885.exe	Get hash	malicious	Browse	• www.billpollakwritingandediting.com/s2oc/?GzrL=WBjT_rUpa&8pDp00Hp=iEnqtY0VDkZROpxH3svCV1z4vh0RNvDxHQ/1OCo0cqhO00C//BGB8blyEE+Kz7q/Bf/i
	swift_76567643.exe	Get hash	malicious	Browse	• www.robztech.com/m8es/?CVJ=t8DGnXKWWWU8raNxivnbQjw3Z37WBEdYjZZIAloy7atrUUbC+CA3ztV2uFkjRRfw03U+&oX9=Txo8ntB0WBsp
	PDF NEW P.OJerhWEMSj4RnE4Z.exe	Get hash	malicious	Browse	• www.ichaugames.com/edbs/?LZ9p=YgPC843WNdMasmCWk8z83XX/O5HllNmlhNkRKlPYh5DfpYamg+RMipCIUjeKta/lrbmo&MnZ=GXLpz
	Swift.exe	Get hash	malicious	Browse	• www.pranatarot.com/edbs/?M6AII=DP8A5Ne5M9xGBq1tjWprXkQLMPcjoeoXNStDN+ay4cQr/vSv+J0F/9nmPhuRTLw7c/6NIAJFgw==&T8RH=9rqdJ4wpALk
	TNUiVpymgH.exe	Get hash	malicious	Browse	• www.longdoggy.net/vu9b/?yhRdNvKX=NeJ6fTW54FiVLomARoXtZYU3dCbrOkLIBtzKWj45EW4cSvDsCl/Ad3ky2rZHNP/pygFH&Sj=CTFH
	Swift Advise.exe	Get hash	malicious	Browse	• www.billpollakwritingandediting.com/s2oc/?Hlnxrrv=iEnqtY0VDkZROpxH3svCV1z4vh0RNvDxHQ/1OCo0cqhO00C//BGB8blyEE+gsLa/Fd3i&N48xBX=5jrXZXrHL6gpNHc
	vfe1GoeC5F.exe	Get hash	malicious	Browse	• www.emmajanetracy.com/iu4d/?wTPHg6=ZliXVxFXgH&F8Sl=JOOHHYcCVAiumnatH9FSz+DjDh0K1BlAW5euFZ4O/VfuOjdNwQJji3cnAkLnRBXIBtcN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	New Purchase Order GH934782GHY489330.exe	Get hash	malicious	Browse	• www.texasgirlcooks.com/n8ih/?FRd4X8=LwVPcdZXggMsOEqjpBC1UWbJi/W0BJRKlKtnOmrCDSW2VJzQcSCcpwg+xjq2DIU/ljr6&v8yH=ZPGXSpGP_
	enlu5xSNKV.exe	Get hash	malicious	Browse	• www.mels.ink/jzvu/?T48h3FW=iJYv1UkuT0Zpi+IGsxHty87S2Dat4Pv7Wp3PPo6PPkk3ttxekOlDn9vNvymr9ZuQ7HO4&GPGXR=rVgD9v10QRyTEj
	KL9fcbfrMB.exe	Get hash	malicious	Browse	• www.micheldrake.com/p2io/?TT=FjUh3Tu&idCtDnlP=d2NgnqRSaE399kDepSeXKrGILlrAeXd0mpr9jEILXnCNsbPLuX7uZtRN+ZZx/uILlcnE
	Bs04AQyK2o.exe	Get hash	malicious	Browse	• www.blake-skinner.com/cyna/?GzuD=PDCWDhm1FORq+rZomwaGxMfk5udIXQ8UnpXBsbRxRfrc3sHkOqGAjqDUEuQ1Be52SJ1X&AnB=O0DXDNwPE
	DXeJI2nlOG.exe	Get hash	malicious	Browse	• www.longdoggy.net/vu9b/?jPg8q=NeJ6fTW54FiVLomARoXtZYU3dCbrOkLIBtzKWj45EW4cSvDsCI/Ad3ky2o1XR+jS1VsWAWCG5Q==&nbEHs=jFNtdTXxm
	Rz9fvf4OTb.exe	Get hash	malicious	Browse	• www.oklahomacfs.com/gts/?YB0x2ft8=PA67ZkolMfBFCI4mOjQDIsof7zDtaA6aTfME7PP0+Fx0ghZxyy52dimMDrUfoPufFN5g&Vr=LhnLH8Hph
	Doc.exe	Get hash	malicious	Browse	• www.summit-fall.com/q8be/?Wrg=4hnHMfUXP&jDHtm=PvpSyhwaK0EPkwK3lIaPMDnFk8sqPd4QRGTJe178Ccz19CG/ZacuMU3Q8hVSYAMnSG3u

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	order samples 056-062 _pdf.exe	Get hash	malicious	Browse	• www.talesontwowheels.com/nu8e/?7ntLT=BUO3cM6bBv9ZuCKW4ifJ+Pyw8zjobdDvL9OFzJCTcSEVCDIw9t8JRYv77i9NgmLL6sLM&v4Xpf=oBZl2rip
	yxQWzvifFe.exe	Get hash	malicious	Browse	• www.espressoandhoney.com/gts/?8p=2dRTAnw8b&uDHXm=EzY5lfbdKr94xDCu9UGw63kyV4asBdh+DU/WNzhiAESrVolwAii5R+YbRgqBWfyCYIrF
	PO_210316.exe.exe	Get hash	malicious	Browse	• www.duncantraining.com/ntg/?tXUp=YP7DfZXHo&p0D=pJ3E5H0AXs3SyFTGH0EJGGbFjKRwNMwKWWcsy0pCeIK4FiOVM3d0QBCPOWB+ULVSbRXF
	NEW ORDER QUOTATION.xlsx	Get hash	malicious	Browse	• www.earth-emily.com/4qdc/?qDKt=Wph7KmT0uL3Cs02FLA1oy52G3sDFb69Rya6X81f4dYa3z5cXpdxP3Vix0KXZYCXkaGKP+A==&BFQLa6=QL08lznxCVnXyzKP
	OPSzlwylj5.exe	Get hash	malicious	Browse	• www.leadeligey.com/bw82/?Rxo=vUh86D2kaUcvG8cSXUIE+TYOTfOFz6ihzRiGvCHG7B+/lKZzNCz3xlSTvPJyBkyGX6Ae&MJBx=FdCx5LDXHnmh2JEP
208.91.197.91	TazxfJHRhq.exe	Get hash	malicious	Browse	• www.jamessicilia.com/evpn/?JDK8ix=fhrZBjxaI0WDrOMMLB9i/eTcrXrQxugx+jgojm7BAd6fBe64JiOWliSCzfUjPirJzJCm&w4=jFNp36Ihu
	8sxgohtHjM.exe	Get hash	malicious	Browse	• www.newmandu.com/vu9b/?0pn=gvDMKnL2DiygUqkLOW8equ0SBtiZsQsp9RF77GdE0oWtaZL2dcC9ipMcSo2LbyxlKRwH&uZQL2=D48x

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PRC-20-518 ORIGINAL.xlsx	Get hash	malicious	Browse	• www.chitrakaah.com/g050/?MBN0yn=gh6gYfQCrnQBnQvKqXR1BBdq6l0/ia6nXcyoJzz4U03ljs0U8DV8qCnN3+fv2J4IGdTu1A==&2dht=XHE0Qdm
	ORIGINAL SHIPPING DOCUMENTSPDF.exe	Get hash	malicious	Browse	• www.rajeshpaul.com/qqeq/?D8IxB=7nSpJtUpafTIT6&eb=my9HLCyGyTUI7ijeZNMt9rsHqU3anFReddNHkecDwv0iZCMXfCC6FueMusiXp9GGW0pUqn5axA==
	PO#7689.zip.exe	Get hash	malicious	Browse	• www.greenlightsmokables.com/md5/?Jzu4_4C=zHBqlneB+dU0jWTqKpl7P0UhTg+HlH4MpY8JEipF1WP+CJ4l7o5pEqU4RJVuKm5urAdq&NrThfj=D48x
	products order pdf.exe	Get hash	malicious	Browse	• www.tudeladirecto.com/nt8e/?wTX=EFNpsN9xNb-Dd&n4p=d5sTnujAaLwCHAV7Hkod4AGONRw1Ceya8p7QHyuAjU2hemaQC5CnvhOz2MROTqxwdpcV
	7Q5Er1TObp.exe	Get hash	malicious	Browse	• www.newmandu.com/vu9b/?FTjl4F=gvDMKnL2DiygUqkLOW8equ0SBtiZsQsp9RF77GdE0oWtaZL2dcC9ipMcSo2LbyxlKRwH&vRDtx=khL0M89p_R8hBZa
	New Purchase Order.exe	Get hash	malicious	Browse	• www.fairview.global/noi6/?Ktklc=djQtGmR2ozp5r2jxyahjtN1TJLTs4NvNMxVFhpbWlLclFF8JTFJQ/pXyn76jfICi7GGZ&lzul=z8o4n2BhWV
	Bombermania.exe	Get hash	malicious	Browse	• live.interballs.com/reporting_server/
	Bombermania.exe	Get hash	malicious	Browse	• live.interballs.com/reporting_server/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	2021_03_16.exe	Get hash	malicious	Browse	• www.ltc-gold.com/2bg/?lnud=/i/Ib+Dffob7lMQ5ivcx1VEzEzf2K5SYmZpCl/xPFCYFxY/A/vBZb7BF8LsLTj5bzBQKXYQmxg==&1bm=3fedQNQ0wlQl0H
	orii11.exe	Get hash	malicious	Browse	• www.fotoincasa.com/mdi/?8pp=r1iONhcrP0pbpGclQVhVGgc+Q37F54QKHkqxX6oGe/sLqU52wzsf7IojbzpCHshmMIC4&sZCx=1bYdfPf8ef5pjPm
	bnb.exe	Get hash	malicious	Browse	• www.fotoincasa.com/mdi/?Jh=r1iONhcrP0pbpGclQVhVGgc+Q37F54QKHkqxX6oGe/sLqU52wzsf7IojbzpoYcRmIKK4&njl0d=Rzuls4
	Purchase Order.exe	Get hash	malicious	Browse	• www.fairview.global/noi6/?rXOp32I=djQtGmR2ozp5r2jxyahjtN1TJLTs4NvNMxVFhpbWlLclFF8JTFJQ/pXyn76JA4yi/EOZ&Bd4Dh=CX6p
	PO_98276300.exe	Get hash	malicious	Browse	• www.ojavedа.com/ame8/?8p=TUdynzXewDV4R6hcP/TtpIkDjP+ZRmt16Hw3snKWLRaKzibVm3POi5J75QFaIAfkEyg3&Cb=hN98bjZH
	DHL_receipt.exe	Get hash	malicious	Browse	• www.greenlightsmokable.com/s8gq/?GVTl=CdTDr&CtxLR=GcXO2IQJXedQXP0VXXtwOzFelwMaLaizNNb08pvp0e1v1F0rbo8J5l47qDnDSsA31Tvl
	QUOTATION00187612.exe	Get hash	malicious	Browse	• www.gamingmag.online/nsk/?5juH1Lw=DnZ6smjvmKtwuwAXRixl0xHJiuXjV7QbSQXcUxw83NwxPjQzvt78aHwZY7I20FYugkDr&kxl0dL=nDH8a8R86Pb8o

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	AWB-INVOICE_PDF.exe	Get hash	malicious	Browse	• www.pathwaysnorman.com/idir/?jFNhC=QcfpPsZsTQkbfi9dIqkstDiu8gpji7zGKQT9CcYXB17rdgdInICGKPMkjk7u0mNGiAFDxGC1Zg==&PlHT0=_6g89p5H3xehg
	DHL Document. PDF.exe	Get hash	malicious	Browse	• www.xpressteamironing.com/d8ak/?Szr0s4=GfmXTYq2Yn2AckQWwnE6BBibtFv31Qjt2UWEfiHUUpW9PpEAUCSsafVf838QtlI0BZoH7o+vNw==&QL3=uTyTqJdh5XE07
	INV.xlsx	Get hash	malicious	Browse	• www.h-v-biz.com/c8so/?cf=hsMrMOU/4wmWTnQK7BegBqlrTsujOywA7VbOIqdg4Ej/UmxkJ2Rbh4V4PlD+e7xk19hcsA==&nH4xu=erRXJfgPJ

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CONFLUENCE-NETWORK-INCVG	TazxfJHRhq.exe	Get hash	malicious	Browse	• 208.91.197.91
	8sxgohtHjM.exe	Get hash	malicious	Browse	• 208.91.197.91
	PO7321.exe	Get hash	malicious	Browse	• 208.91.197.39
	PRC-20-518 ORIGINAL.xlsx	Get hash	malicious	Browse	• 208.91.197.39
	Lista e porosive te blerjes.exe	Get hash	malicious	Browse	• 209.99.64.33
	BL836477488575.exe	Get hash	malicious	Browse	• 204.11.56.48
	BL84995005038483.exe	Get hash	malicious	Browse	• 204.11.56.48
	DHL Shipping Documents.exe	Get hash	malicious	Browse	• 208.91.197.27
	Formbook.exe	Get hash	malicious	Browse	• 204.11.56.48
	ORIGINAL SHIPPING DOCUMENTSPDF.exe	Get hash	malicious	Browse	• 208.91.197.91
	PDF NEW P.OJerhWEMSj4RnE4Z.exe	Get hash	malicious	Browse	• 208.91.197.27
	bank details.exe	Get hash	malicious	Browse	• 208.91.197.27
	PO#7689.zip.exe	Get hash	malicious	Browse	• 208.91.197.91
	ORDER_PDF.exe	Get hash	malicious	Browse	• 209.99.64.18
	deIt7iuD1y.exe	Get hash	malicious	Browse	• 204.11.56.48
	Bista_094924,ppdf.exe	Get hash	malicious	Browse	• 208.91.197.27
	PO_RFQ007899_PDF.exe	Get hash	malicious	Browse	• 209.99.64.55
	PaymentInvoice.exe	Get hash	malicious	Browse	• 208.91.197.39
	products order pdf.exe	Get hash	malicious	Browse	• 208.91.197.91
	ZGNbR8E726.exe	Get hash	malicious	Browse	• 204.11.56.48
AUTOMATTICUS	0BAdCQQVtP.exe	Get hash	malicious	Browse	• 192.0.78.175
	vbc.exe	Get hash	malicious	Browse	• 192.0.78.25
	o2KKHvtb3c.exe	Get hash	malicious	Browse	• 192.0.78.24
	PO#41000055885.exe	Get hash	malicious	Browse	• 192.0.78.24
	BL836477488575.exe	Get hash	malicious	Browse	• 192.0.78.194
	FARASIS.xlsx	Get hash	malicious	Browse	• 192.0.79.33
	FARASIS.xlsx	Get hash	malicious	Browse	• 192.0.79.32
	RFQ-V-SAM-0321D056-DOC.exe	Get hash	malicious	Browse	• 192.0.78.25

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	swift_76567643.exe	Get hash	malicious	Browse	• 192.0.78.24
	PDF NEW P.OJerhWEMSj4RnE4Z.exe	Get hash	malicious	Browse	• 192.0.78.24
	yQh96Jd6TZ.exe	Get hash	malicious	Browse	• 192.0.78.25
	Swift.exe	Get hash	malicious	Browse	• 192.0.78.24
	TNUiVpymgH.exe	Get hash	malicious	Browse	• 192.0.78.24
	g0g865fQ2S.exe	Get hash	malicious	Browse	• 192.0.78.25
	Original Invoice-COAU7230734290.xlsx	Get hash	malicious	Browse	• 192.0.78.25
	TSPO0001978-xlxs.exe	Get hash	malicious	Browse	• 192.0.78.231
	Swift Advise.exe	Get hash	malicious	Browse	• 192.0.78.24
	RMwfvA9kZy.exe	Get hash	malicious	Browse	• 192.0.78.25
	vfe1GoeC5F.exe	Get hash	malicious	Browse	• 192.0.78.24
	New Purchase Order GH934782GHY489330.exe	Get hash	malicious	Browse	• 192.0.78.24
AMAZON-02US	Calt7BoW2a.exe	Get hash	malicious	Browse	• 3.14.206.30
	0BAdCQQVtP.exe	Get hash	malicious	Browse	• 52.40.12.112
	TazxfJHRhq.exe	Get hash	malicious	Browse	• 52.216.152.43
	1wOdXavtlE.exe	Get hash	malicious	Browse	• 52.216.179.59
	hvEop8Y70Y.exe	Get hash	malicious	Browse	• 15.165.26.252
	8sxgohtHjM.exe	Get hash	malicious	Browse	• 3.13.255.157
	eQLPRPErea.exe	Get hash	malicious	Browse	• 13.248.216.40
	vbc.exe	Get hash	malicious	Browse	• 3.13.255.157
	o2KKHvtb3c.exe	Get hash	malicious	Browse	• 18.218.104.192
	Order Inquiry.exe	Get hash	malicious	Browse	• 3.14.206.30
	6IGbftBsBg.exe	Get hash	malicious	Browse	• 104.192.141.1
	nicoleta.fagaras-DHL_TRACKING_1394942.html	Get hash	malicious	Browse	• 52.218.213.96
	PaymentAdvice.exe	Get hash	malicious	Browse	• 3.14.206.30
	ikoAlmKWvI.exe	Get hash	malicious	Browse	• 104.192.141.1
	BL01345678053567.exe	Get hash	malicious	Browse	• 3.14.206.30
	AL JUNEIDI LIST.xlsx	Get hash	malicious	Browse	• 65.0.168.152
	DYANAMIC Inquiry.xlsx	Get hash	malicious	Browse	• 65.0.168.152
	Statement of Account.xlsx	Get hash	malicious	Browse	• 15.165.26.252
	Shipping Documents.xlsx	Get hash	malicious	Browse	• 52.217.8.51
	bmws51TeIm.exe	Get hash	malicious	Browse	• 3.141.177.1

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\invoice.exe.log	
Process:	C:\Users\user\Desktop\invoice.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\invoice.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.214342330666735
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	invoice.exe
File size:	894464
MD5:	492017e064cab97dd8ea27abd3e5cfca
SHA1:	a3addbdea8245b2e16c6ef551755b9d0e66e8e2b
SHA256:	524306af2db603c7db95227603c3014b67c27cfb2f88d12de2a599ece24575e2
SHA512:	66d5180a58dfaf4f1971480090197115c76af46e46098e6b33ec2d6f30d63b40e45f13f29e41b7b19cb8dc3a0dd24c1846fb45009c6f10c5419d30fcf6208a13
SSDEEP:	12288:/eGIIK2eESBAcIRUpDrV5F4pO9q7d36dQc8fZVa0RdYrLST8BHVlnwC5IKUaE+:/e5IV6AVUF5Ipb/cmES4VlnFl/
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....n`.....P..^...F.....~|... .....@.. .....@.....

File Icon

Icon Hash:	e8d4ae708e8ec461

Static PE Info

General

Entrypoint:	0x4a7c7e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x606EACE1 [Thu Apr 8 07:12:33 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa7c2c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa8000	0x3422c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xde000	0xc	.reloc
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	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa5c84	0xa5e00	False	0.789592360588	data	7.55515603565	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa8000	0x3422c	0x34400	False	0.389877392344	data	5.76163363059	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0xde000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xa8220	0x521e	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xad450	0x6f5a	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xb43bc	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xc4bf4	0x94a8	data		
RT_ICON	0xce0ac	0x5488	data		
RT_ICON	0xd3544	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 15794175, next used block 4294902528		
RT_ICON	0xd777c	0x25a8	data		
RT_ICON	0xd9d34	0x10a8	data		
RT_ICON	0xdadec	0x988	data		
RT_ICON	0xdb784	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xdbbfc	0x92	data		
RT_VERSION	0xdbca0	0x38a	data		
RT_MANIFEST	0xdc03c	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2016 Computer City
Assembly Version	1.12.0.2
InternalName	CharTypeInfo.exe
FileVersion	1.12.0.2
CompanyName	Computer City
LegalTrademarks	
Comments	
ProductName	UnmanagedAccessor
ProductVersion	1.12.0.2
FileDescription	UnmanagedAccessor
OriginalFilename	CharTypeInfo.exe

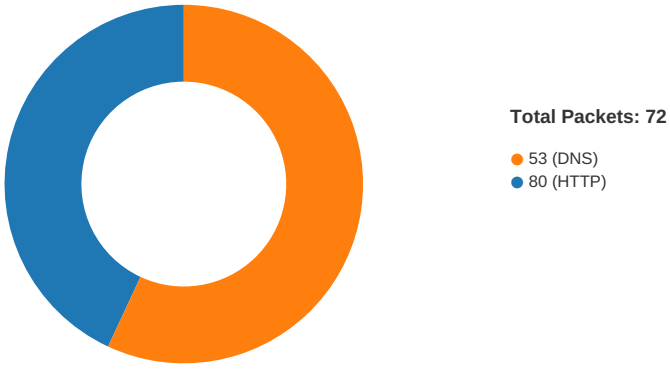
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/08/21-12:04:21.809030	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49717	80	192.168.2.5	184.168.131.241
04/08/21-12:04:21.809030	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49717	80	192.168.2.5	184.168.131.241
04/08/21-12:04:21.809030	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49717	80	192.168.2.5	184.168.131.241
04/08/21-12:04:59.252139	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49725	80	192.168.2.5	208.91.197.91
04/08/21-12:04:59.252139	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49725	80	192.168.2.5	208.91.197.91
04/08/21-12:04:59.252139	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49725	80	192.168.2.5	208.91.197.91

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/08/21-12:05:07.034640	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.5	8.8.8.8
04/08/21-12:05:08.358998	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.5	8.8.8.8
04/08/21-12:05:18.088414	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49732	80	192.168.2.5	177.55.108.130
04/08/21-12:05:18.088414	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49732	80	192.168.2.5	177.55.108.130
04/08/21-12:05:18.088414	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49732	80	192.168.2.5	177.55.108.130

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:04:21.632926941 CEST	49717	80	192.168.2.5	184.168.131.241
Apr 8, 2021 12:04:21.808682919 CEST	80	49717	184.168.131.241	192.168.2.5
Apr 8, 2021 12:04:21.808800936 CEST	49717	80	192.168.2.5	184.168.131.241
Apr 8, 2021 12:04:21.809030056 CEST	49717	80	192.168.2.5	184.168.131.241
Apr 8, 2021 12:04:21.984464884 CEST	80	49717	184.168.131.241	192.168.2.5
Apr 8, 2021 12:04:22.028017998 CEST	80	49717	184.168.131.241	192.168.2.5
Apr 8, 2021 12:04:22.028047085 CEST	80	49717	184.168.131.241	192.168.2.5
Apr 8, 2021 12:04:22.028240919 CEST	49717	80	192.168.2.5	184.168.131.241
Apr 8, 2021 12:04:22.028343916 CEST	49717	80	192.168.2.5	184.168.131.241
Apr 8, 2021 12:04:22.203593016 CEST	80	49717	184.168.131.241	192.168.2.5
Apr 8, 2021 12:04:32.389282942 CEST	49718	80	192.168.2.5	35.156.117.131
Apr 8, 2021 12:04:32.407913923 CEST	80	49718	35.156.117.131	192.168.2.5
Apr 8, 2021 12:04:32.408046007 CEST	49718	80	192.168.2.5	35.156.117.131
Apr 8, 2021 12:04:32.408296108 CEST	49718	80	192.168.2.5	35.156.117.131
Apr 8, 2021 12:04:32.426136971 CEST	80	49718	35.156.117.131	192.168.2.5
Apr 8, 2021 12:04:32.428894997 CEST	80	49718	35.156.117.131	192.168.2.5
Apr 8, 2021 12:04:32.429075003 CEST	49718	80	192.168.2.5	35.156.117.131
Apr 8, 2021 12:04:32.429214954 CEST	49718	80	192.168.2.5	35.156.117.131
Apr 8, 2021 12:04:32.447406054 CEST	80	49718	35.156.117.131	192.168.2.5
Apr 8, 2021 12:04:37.530929089 CEST	49719	80	192.168.2.5	2.57.90.16
Apr 8, 2021 12:04:37.571005106 CEST	80	49719	2.57.90.16	192.168.2.5
Apr 8, 2021 12:04:37.571151972 CEST	49719	80	192.168.2.5	2.57.90.16
Apr 8, 2021 12:04:37.571713924 CEST	49719	80	192.168.2.5	2.57.90.16
Apr 8, 2021 12:04:37.611814976 CEST	80	49719	2.57.90.16	192.168.2.5
Apr 8, 2021 12:04:37.611836910 CEST	80	49719	2.57.90.16	192.168.2.5
Apr 8, 2021 12:04:37.611850023 CEST	80	49719	2.57.90.16	192.168.2.5
Apr 8, 2021 12:04:37.612085104 CEST	49719	80	192.168.2.5	2.57.90.16
Apr 8, 2021 12:04:37.612297058 CEST	49719	80	192.168.2.5	2.57.90.16
Apr 8, 2021 12:04:37.652245045 CEST	80	49719	2.57.90.16	192.168.2.5
Apr 8, 2021 12:04:59.106825113 CEST	49725	80	192.168.2.5	208.91.197.91
Apr 8, 2021 12:04:59.251840115 CEST	80	49725	208.91.197.91	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:04:59.251971006 CEST	49725	80	192.168.2.5	208.91.197.91
Apr 8, 2021 12:04:59.252139091 CEST	49725	80	192.168.2.5	208.91.197.91
Apr 8, 2021 12:04:59.397062063 CEST	80	49725	208.91.197.91	192.168.2.5
Apr 8, 2021 12:04:59.498363972 CEST	80	49725	208.91.197.91	192.168.2.5
Apr 8, 2021 12:04:59.498404980 CEST	80	49725	208.91.197.91	192.168.2.5
Apr 8, 2021 12:04:59.498425007 CEST	80	49725	208.91.197.91	192.168.2.5
Apr 8, 2021 12:04:59.498682022 CEST	49725	80	192.168.2.5	208.91.197.91
Apr 8, 2021 12:04:59.498739004 CEST	49725	80	192.168.2.5	208.91.197.91
Apr 8, 2021 12:04:59.531753063 CEST	80	49725	208.91.197.91	192.168.2.5
Apr 8, 2021 12:04:59.531820059 CEST	49725	80	192.168.2.5	208.91.197.91
Apr 8, 2021 12:04:59.644556999 CEST	80	49725	208.91.197.91	192.168.2.5
Apr 8, 2021 12:05:11.767712116 CEST	49731	80	192.168.2.5	74.208.236.64
Apr 8, 2021 12:05:11.899678946 CEST	80	49731	74.208.236.64	192.168.2.5
Apr 8, 2021 12:05:11.899977922 CEST	49731	80	192.168.2.5	74.208.236.64
Apr 8, 2021 12:05:11.900079012 CEST	49731	80	192.168.2.5	74.208.236.64
Apr 8, 2021 12:05:12.031223059 CEST	80	49731	74.208.236.64	192.168.2.5
Apr 8, 2021 12:05:12.034537077 CEST	80	49731	74.208.236.64	192.168.2.5
Apr 8, 2021 12:05:12.034565926 CEST	80	49731	74.208.236.64	192.168.2.5
Apr 8, 2021 12:05:12.034796953 CEST	49731	80	192.168.2.5	74.208.236.64
Apr 8, 2021 12:05:12.034859896 CEST	49731	80	192.168.2.5	74.208.236.64
Apr 8, 2021 12:05:12.165515900 CEST	80	49731	74.208.236.64	192.168.2.5
Apr 8, 2021 12:05:17.881434917 CEST	49732	80	192.168.2.5	177.55.108.130
Apr 8, 2021 12:05:18.087061882 CEST	80	49732	177.55.108.130	192.168.2.5
Apr 8, 2021 12:05:18.087527037 CEST	49732	80	192.168.2.5	177.55.108.130
Apr 8, 2021 12:05:18.088413954 CEST	49732	80	192.168.2.5	177.55.108.130
Apr 8, 2021 12:05:18.291481972 CEST	80	49732	177.55.108.130	192.168.2.5
Apr 8, 2021 12:05:18.292332888 CEST	80	49732	177.55.108.130	192.168.2.5
Apr 8, 2021 12:05:18.292355061 CEST	80	49732	177.55.108.130	192.168.2.5
Apr 8, 2021 12:05:18.292543888 CEST	49732	80	192.168.2.5	177.55.108.130
Apr 8, 2021 12:05:18.292608976 CEST	49732	80	192.168.2.5	177.55.108.130
Apr 8, 2021 12:05:18.495742083 CEST	80	49732	177.55.108.130	192.168.2.5
Apr 8, 2021 12:05:23.338290930 CEST	49734	80	192.168.2.5	192.0.78.24
Apr 8, 2021 12:05:23.354049921 CEST	80	49734	192.0.78.24	192.168.2.5
Apr 8, 2021 12:05:23.354183912 CEST	49734	80	192.168.2.5	192.0.78.24
Apr 8, 2021 12:05:23.354604006 CEST	49734	80	192.168.2.5	192.0.78.24
Apr 8, 2021 12:05:23.370249987 CEST	80	49734	192.0.78.24	192.168.2.5
Apr 8, 2021 12:05:23.483477116 CEST	80	49734	192.0.78.24	192.168.2.5
Apr 8, 2021 12:05:23.483500957 CEST	80	49734	192.0.78.24	192.168.2.5
Apr 8, 2021 12:05:23.483649969 CEST	49734	80	192.168.2.5	192.0.78.24
Apr 8, 2021 12:05:23.483750105 CEST	49734	80	192.168.2.5	192.0.78.24
Apr 8, 2021 12:05:23.499483109 CEST	80	49734	192.0.78.24	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:03:15.073683977 CEST	52212	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:03:15.107563019 CEST	53	52212	8.8.8.8	192.168.2.5
Apr 8, 2021 12:03:15.243592978 CEST	54302	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:03:15.256288052 CEST	53	54302	8.8.8.8	192.168.2.5
Apr 8, 2021 12:03:15.258438110 CEST	53784	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:03:15.270612955 CEST	53	53784	8.8.8.8	192.168.2.5
Apr 8, 2021 12:03:15.706372976 CEST	65307	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:03:15.719813108 CEST	53	65307	8.8.8.8	192.168.2.5
Apr 8, 2021 12:03:15.722573042 CEST	64344	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:03:15.736054897 CEST	53	64344	8.8.8.8	192.168.2.5
Apr 8, 2021 12:03:16.338979006 CEST	62060	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:03:16.351699114 CEST	53	62060	8.8.8.8	192.168.2.5
Apr 8, 2021 12:03:18.154172897 CEST	61805	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:03:18.167529106 CEST	53	61805	8.8.8.8	192.168.2.5
Apr 8, 2021 12:03:18.795605898 CEST	54795	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:03:18.808784962 CEST	53	54795	8.8.8.8	192.168.2.5
Apr 8, 2021 12:03:19.236841917 CEST	49557	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:03:19.254936934 CEST	53	49557	8.8.8.8	192.168.2.5
Apr 8, 2021 12:03:19.832006931 CEST	61733	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 12:03:19.844795942 CEST	53	61733	8.8.8.8	192.168.2.5
Apr 8, 2021 12:03:20.705095053 CEST	65447	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:03:20.717613935 CEST	53	65447	8.8.8.8	192.168.2.5
Apr 8, 2021 12:03:21.448858023 CEST	52441	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:03:21.461405039 CEST	53	52441	8.8.8.8	192.168.2.5
Apr 8, 2021 12:03:22.880736113 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:03:22.893364906 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 8, 2021 12:03:25.878978014 CEST	59596	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:03:25.891555071 CEST	53	59596	8.8.8.8	192.168.2.5
Apr 8, 2021 12:03:26.643290043 CEST	65296	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:03:26.656200886 CEST	53	65296	8.8.8.8	192.168.2.5
Apr 8, 2021 12:03:27.609880924 CEST	63183	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:03:27.623181105 CEST	53	63183	8.8.8.8	192.168.2.5
Apr 8, 2021 12:03:44.317714930 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:03:44.336030960 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 8, 2021 12:03:49.234772921 CEST	59736	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:03:49.239942074 CEST	51058	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:03:49.240032911 CEST	52636	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:03:49.247836113 CEST	53	59736	8.8.8.8	192.168.2.5
Apr 8, 2021 12:03:49.251970053 CEST	53	51058	8.8.8.8	192.168.2.5
Apr 8, 2021 12:03:49.253436089 CEST	53	52636	8.8.8.8	192.168.2.5
Apr 8, 2021 12:04:08.718833923 CEST	56969	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:04:08.732348919 CEST	53	56969	8.8.8.8	192.168.2.5
Apr 8, 2021 12:04:21.582397938 CEST	55161	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:04:21.624262094 CEST	53	55161	8.8.8.8	192.168.2.5
Apr 8, 2021 12:04:32.059622049 CEST	54757	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:04:32.387444973 CEST	53	54757	8.8.8.8	192.168.2.5
Apr 8, 2021 12:04:37.486022949 CEST	49992	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:04:37.528493881 CEST	53	49992	8.8.8.8	192.168.2.5
Apr 8, 2021 12:04:42.619398117 CEST	60075	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:04:42.979065895 CEST	53	60075	8.8.8.8	192.168.2.5
Apr 8, 2021 12:04:48.228594065 CEST	55016	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:04:48.836759090 CEST	53	55016	8.8.8.8	192.168.2.5
Apr 8, 2021 12:04:51.358530045 CEST	64345	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:04:51.371253967 CEST	53	64345	8.8.8.8	192.168.2.5
Apr 8, 2021 12:04:53.898787022 CEST	57128	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:04:53.926758051 CEST	53	57128	8.8.8.8	192.168.2.5
Apr 8, 2021 12:04:58.948373079 CEST	54791	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:04:59.105505943 CEST	53	54791	8.8.8.8	192.168.2.5
Apr 8, 2021 12:05:03.749087095 CEST	50463	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:05:03.768049955 CEST	53	50463	8.8.8.8	192.168.2.5
Apr 8, 2021 12:05:04.512552977 CEST	50394	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:05:05.506127119 CEST	50394	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:05:06.521694899 CEST	50394	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:05:06.674634933 CEST	53	50394	8.8.8.8	192.168.2.5
Apr 8, 2021 12:05:07.034513950 CEST	53	50394	8.8.8.8	192.168.2.5
Apr 8, 2021 12:05:08.358870983 CEST	53	50394	8.8.8.8	192.168.2.5
Apr 8, 2021 12:05:11.724265099 CEST	58530	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:05:11.765930891 CEST	53	58530	8.8.8.8	192.168.2.5
Apr 8, 2021 12:05:17.043440104 CEST	53813	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:05:17.880172968 CEST	53	53813	8.8.8.8	192.168.2.5
Apr 8, 2021 12:05:18.316375971 CEST	63732	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:05:18.349823952 CEST	53	63732	8.8.8.8	192.168.2.5
Apr 8, 2021 12:05:23.309679031 CEST	57344	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:05:23.336853981 CEST	53	57344	8.8.8.8	192.168.2.5
Apr 8, 2021 12:05:27.472863913 CEST	54450	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:05:27.485549927 CEST	53	54450	8.8.8.8	192.168.2.5
Apr 8, 2021 12:05:28.296029091 CEST	59261	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:05:28.329763889 CEST	53	59261	8.8.8.8	192.168.2.5
Apr 8, 2021 12:05:28.497765064 CEST	57151	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:05:28.774436951 CEST	53	57151	8.8.8.8	192.168.2.5
Apr 8, 2021 12:05:34.462431908 CEST	59413	53	192.168.2.5	8.8.8.8
Apr 8, 2021 12:05:34.527434111 CEST	53	59413	8.8.8.8	192.168.2.5

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Apr 8, 2021 12:05:07.034640074 CEST	192.168.2.5	8.8.8.8	cffd	(Port unreachable)	Destination Unreachable
Apr 8, 2021 12:05:08.358998060 CEST	192.168.2.5	8.8.8.8	cffd	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 12:04:21.582397938 CEST	192.168.2.5	8.8.8.8	0x3722	Standard query (0)	www.flowhcf.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:04:32.059622049 CEST	192.168.2.5	8.8.8.8	0x5ca1	Standard query (0)	www.jinlan.online	A (IP address)	IN (0x0001)
Apr 8, 2021 12:04:37.486022949 CEST	192.168.2.5	8.8.8.8	0xc2f0	Standard query (0)	www.armaccountingbs.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:04:42.619398117 CEST	192.168.2.5	8.8.8.8	0xe949	Standard query (0)	www.zmid.xyz	A (IP address)	IN (0x0001)
Apr 8, 2021 12:04:48.228594065 CEST	192.168.2.5	8.8.8.8	0x6c76	Standard query (0)	www.sookepointcargo.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:04:53.898787022 CEST	192.168.2.5	8.8.8.8	0x6c6d	Standard query (0)	www.dateyourlovelive.club	A (IP address)	IN (0x0001)
Apr 8, 2021 12:04:58.948373079 CEST	192.168.2.5	8.8.8.8	0x5abb	Standard query (0)	www.knoxvilleoutdoorkitchens.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:05:04.512552977 CEST	192.168.2.5	8.8.8.8	0x2ea	Standard query (0)	www.gunungbatufrozen.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:05:05.506127119 CEST	192.168.2.5	8.8.8.8	0x2ea	Standard query (0)	www.gunungbatufrozen.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:05:06.521694899 CEST	192.168.2.5	8.8.8.8	0x2ea	Standard query (0)	www.gunungbatufrozen.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:05:11.724265099 CEST	192.168.2.5	8.8.8.8	0x9951	Standard query (0)	www.highdeserthealthinsurance.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:05:17.043440104 CEST	192.168.2.5	8.8.8.8	0x52bd	Standard query (0)	www.hotelmaktub.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:05:23.309679031 CEST	192.168.2.5	8.8.8.8	0x2d71	Standard query (0)	www.legacyadmin.support	A (IP address)	IN (0x0001)
Apr 8, 2021 12:05:28.497765064 CEST	192.168.2.5	8.8.8.8	0x9df1	Standard query (0)	www.arizonagridiron.com	A (IP address)	IN (0x0001)
Apr 8, 2021 12:05:34.462431908 CEST	192.168.2.5	8.8.8.8	0x8974	Standard query (0)	www.harshdeepfashion.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 12:04:21.624262094 CEST	8.8.8.8	192.168.2.5	0x3722	No error (0)	www.flowhcf.com	flowhcf.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:04:21.624262094 CEST	8.8.8.8	192.168.2.5	0x3722	No error (0)	flowhcf.com		184.168.131.241	A (IP address)	IN (0x0001)
Apr 8, 2021 12:04:32.387444973 CEST	8.8.8.8	192.168.2.5	0x5ca1	No error (0)	www.jinlan.online	www.jinlan.online.s.strikinglydns.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:04:32.387444973 CEST	8.8.8.8	192.168.2.5	0x5ca1	No error (0)	www.jinlan.online.s.strikinglydns.com		35.156.117.131	A (IP address)	IN (0x0001)
Apr 8, 2021 12:04:32.387444973 CEST	8.8.8.8	192.168.2.5	0x5ca1	No error (0)	www.jinlan.online.s.strikinglydns.com		18.157.120.97	A (IP address)	IN (0x0001)
Apr 8, 2021 12:04:37.528493881 CEST	8.8.8.8	192.168.2.5	0xc2f0	No error (0)	www.armaccountingbs.com	armaccountingbs.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:04:37.528493881 CEST	8.8.8.8	192.168.2.5	0xc2f0	No error (0)	armaccountingbs.com		2.57.90.16	A (IP address)	IN (0x0001)
Apr 8, 2021 12:04:42.979065895 CEST	8.8.8.8	192.168.2.5	0xe949	No error (0)	www.zmid.xyz	ghs.google.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:04:48.836759090 CEST	8.8.8.8	192.168.2.5	0x6c76	Server failure (2)	www.sookepointcargo.com	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 12:04:53.926758051 CEST	8.8.8.8	192.168.2.5	0x6c6d	Name error (3)	www.dateyourlovelive.club	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 12:04:59.105505943 CEST	8.8.8.8	192.168.2.5	0x5abb	No error (0)	www.knoxvilleoutdoorkitchens.com		208.91.197.91	A (IP address)	IN (0x0001)
Apr 8, 2021 12:05:06.674634933 CEST	8.8.8.8	192.168.2.5	0x2ea	Server failure (2)	www.gunungbatufrozen.com	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 12:05:07.034513950 CEST	8.8.8.8	192.168.2.5	0x2ea	Server failure (2)	www.gunungbatufrozen.com	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 12:05:08.358870983 CEST	8.8.8.8	192.168.2.5	0x2ea	Server failure (2)	www.gunungbatufrozen.com	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 12:05:11.765930891 CEST	8.8.8.8	192.168.2.5	0x9951	No error (0)	www.highdeserthealthinsurance.com		74.208.236.64	A (IP address)	IN (0x0001)
Apr 8, 2021 12:05:17.880172968 CEST	8.8.8.8	192.168.2.5	0x52bd	No error (0)	www.hotelmaktub.com	hotelmaktub.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:05:17.880172968 CEST	8.8.8.8	192.168.2.5	0x52bd	No error (0)	hotelmaktub.com		177.55.108.130	A (IP address)	IN (0x0001)
Apr 8, 2021 12:05:17.880172968 CEST	8.8.8.8	192.168.2.5	0x52bd	No error (0)	hotelmaktub.com		187.84.225.36	A (IP address)	IN (0x0001)
Apr 8, 2021 12:05:23.336853981 CEST	8.8.8.8	192.168.2.5	0x2d71	No error (0)	www.legacyadmin.support	legacyadmin.support		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 12:05:23.336853981 CEST	8.8.8.8	192.168.2.5	0x2d71	No error (0)	legacyadmin.support		192.0.78.24	A (IP address)	IN (0x0001)
Apr 8, 2021 12:05:23.336853981 CEST	8.8.8.8	192.168.2.5	0x2d71	No error (0)	legacyadmin.support		192.0.78.25	A (IP address)	IN (0x0001)
Apr 8, 2021 12:05:28.774436951 CEST	8.8.8.8	192.168.2.5	0x9df1	No error (0)	www.arizonagridiron.com		23.27.42.72	A (IP address)	IN (0x0001)
Apr 8, 2021 12:05:34.527434111 CEST	8.8.8.8	192.168.2.5	0x8974	No error (0)	www.harshdeepfashion.com		216.239.34.21	A (IP address)	IN (0x0001)
Apr 8, 2021 12:05:34.527434111 CEST	8.8.8.8	192.168.2.5	0x8974	No error (0)	www.harshdeepfashion.com		216.239.36.21	A (IP address)	IN (0x0001)
Apr 8, 2021 12:05:34.527434111 CEST	8.8.8.8	192.168.2.5	0x8974	No error (0)	www.harshdeepfashion.com		216.239.38.21	A (IP address)	IN (0x0001)
Apr 8, 2021 12:05:34.527434111 CEST	8.8.8.8	192.168.2.5	0x8974	No error (0)	www.harshdeepfashion.com		216.239.32.21	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.flowhcf.com
- www.jinlan.online
- www.armaccountingbs.com
- www.knoxvilleoutdoorkitchens.com
- www.highdeserthealthinsurance.com
- www.hotelmaktub.com
- www.legacyadmin.support

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49717	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:04:21.809030056 CEST	1544	OUT	GET /e3rs/?uFQl=XP7HMT_8&w0G=7EcTScmBGLYmOphx6WmAanuMW8SmjCZcy1cTUFzuZxTbodjrouz1iofcKvfRvNdFU6cO HTTP/1.1 Host: www.flowhcf.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:04:22.028017998 CEST	1545	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.16.1 Date: Thu, 08 Apr 2021 10:04:21 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: http://www.flowhcf.org/e3rs/?uFQl=XP7HMT_8&w0G=7EcTScmBGLYmOphx6WmAanuMW8SmjCZcy1cTUFzuZxTbodjrouz1iofcKvfRvNdFU6cO Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49718	35.156.117.131	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:04:32.408296108 CEST	1545	OUT	GET /e3rs/?uFQl=XP7HMT_8&w0G=0ZKu2HAGzvZQR/qsYgBhCWXzZU+pty94akjoW6oXtCN964+Lsvy2TlnFlM7SmRuoaV8X HTTP/1.1 Host: www.jinlan.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49719	2.57.90.16	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:04:37.571713924 CEST	1546	OUT	GET /e3rs/?w0G=UjY/ETYDec4qhoizf7RP+uVqhCLoGuhip7tAF9t9xQZdbBeLWBLuGPY37yNXVCM5GTyP&uFQl=XP7HMT_8 HTTP/1.1 Host: www.armaccountingbs.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:04:37.611836910 CEST	1547	IN	HTTP/1.1 404 Not Found Server: nginx/1.16.1 Date: Thu, 08 Apr 2021 10:04:37 GMT Content-Type: text/html Content-Length: 153 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 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 36 2e 31 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>404 Not Found</title></head><body> 404 Not Found <hr> nginx/1.16.1 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49725	208.91.197.91	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:04:59.252139091 CEST	1646	OUT	GET /e3rs/?w0G=3w4QHVrJOCimt90ZTeKXMe7ZrYb4bnkzv7QZzufjPqhFBPGQ1SrJ/wFsHy6lqdqQBlr0&uFQl=XP7HMT_8 HTTP/1.1 Host: www.knoxvilleoutdoorkitchens.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:04:59.498363972 CEST	1648	IN	HTTP/1.1 200 OK Date: Thu, 08 Apr 2021 10:04:59 GMT Server: Apache Set-Cookie: vsid=926vr3654218993933208; expires=Tue, 07-Apr-2026 10:04:59 GMT; Max-Age=157680000; path=/; domain=www.knoxvilleoutdoorkitchens.com; HttpOnly X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKX74ixpzVyXbJprcLfbH4psP4+L2entqri0lzh6pkA aXLPIcclv6DQBeJJjGFWrBIF6QMyFwXT5CCRyjS2penECAwEAAQ==_jc9joRJOg7xepppfUjhgNUfaQZzFQ8rnfCxQ RWJh90VSrWOsDLcYcPwxAW8oD+eV6/1Kf7dQa9exp2BXhMPJvQ== Content-Length: 2723 Keep-Alive: timeout=5, max=123 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 3c 21 2d 2d 0d 0a 09 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 6b 6e 6f 78 76 69 6c 6c 65 6f 75 74 64 6f 6f 72 6b 69 74 63 68 65 6e 73 2e 63 6f 6d 2f 3f 66 70 3d 61 63 6a 56 78 4f 32 34 72 75 42 45 31 62 53 6e 41 4a 4f 4f 46 65 5a 39 64 32 25 32 42 69 6c 6c 33 68 57 65 62 63 4d 48 65 6e 65 72 79 71 64 65 33 34 61 6c 6a 4b 38 67 37 4c 35 63 4d 48 67 6f 32 59 35 30 72 51 71 4f 4b 63 69 4e 72 36 6c 72 62 63 68 6b 44 7a 6e 6f 48 59 53 61 65 71 35 25 32 46 69 45 62 56 51 4f 76 6c 53 51 33 4b 70 6a 37 4f 50 63 49 38 55 41 4f 48 65 6b 6b 71 7a 33 51 48 31 76 4b 4d 73 59 7a 64 71 54 57 6c 52 66 65 52 6e 66 70 71 73 44 25 32 42 76 4c 30 6d 25 32 42 68 61 69 44 77 73 6f 75 42 4e 57 41 7a 64 50 25 32 46 59 68 51 58 49 76 38 5a 55 76 4a 42 6c 56 59 51 6e 72 44 79 6d 44 26 70 72 76 74 6f 66 3d 78 4a 34 43 74 5a 31 34 4e 72 4b 72 77 73 6c 52 31 64 58 4d 4b 38 30 63 72 58 6a 57 46 37 73 4b 68 6b 62 5a 34 47 4e 39 42 78 45 25 33 44 26 70 6f 72 75 3d 4e 62 56 72 69 6b 79 69 73 34 61 7a 25 32 42 74 62 53 74 51 45 64 44 75 69 32 32 5a 52 46 78 63 36 71 56 71 59 62 6b 49 36 4f 4c 54 30 38 64 6a 54 4a 39 71 79 31 66 72 58 55 39 53 56 4d 66 39 39 4b 4c 42 39 67 6f 34 6c 30 72 46 38 41 74 25 32 42 69 41 42 71 25 32 46 6a 64 43 64 51 4a 64 70 30 70 62 6f 30 4b 34 47 75 78 45 4c 55 65 79 6f 53 35 77 75 64 4a 44 6b 50 44 66 33 4a 70 59 66 32 41 43 61 47 78 36 4b 31 51 5a 64 51 31 38 34 46 25 32 42 35 4c 69 46 61 30 6d 63 78 52 55 76 72 47 59 4a 37 78 42 59 57 79 7a 42 51 25 32 46 65 79 79 37 77 25 32 46 32 33 77 4f 54 4b 75 42 66 7a 45 46 77 61 37 34 56 75 57 30 53 70 63 36 59 43 6f 4d 49 36 45 4e 72 44 6b 77 67 55 33 68 67 25 33 44 25 33 44 26 63 69 66 72 3d 31 26 77 30 47 3d 33 77 34 51 48 56 72 4a 4f 43 69 6d 74 39 30 5a 54 65 4b 58 4d 65 37 5a 72 59 62 34 62 6e 6b 7a 76 37 51 5a 7a 75 66 6a 50 71 68 46 42 50 47 51 31 53 72 4a 25 32 46 77 46 73 48 79 36 6c 71 64 71 51 42 6c 72 30 26 75 46 51 6c 3d 58 50 37 48 4d 54 5f 38 22 3b 0d 0a 09 2f 2a 0d 0a 2d 2d 3e 0d 0a 3c 68 74 6d 6c 20 64 61 74 61 2d 61 64 62 6c 6f 63 6b 6b 65 79 3d 22 4d 46 77 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 42 42 51 41 44 53 77 41 77 53 41 4a 42 41 4b 58 37 34 69 78 70 7a 56 79 58 62 4a 70 72 63 4c 66 62 48 34 70 73 50 Data Ascii: ...top.location="http://www.knoxvilleoutdoorkitchens.com/?fp=acjVxO24ruBE1bSnAJOOFeZ9d2%2Bill3hWeb cMHeneryqde34aljK8g7L5cMHgo2Y50rQqOKciNr6lrbchkDznoHYSaeq5%2FiEbVQOvlSQ3Kpj7OPcI8UAOHekkqz 3QH1vKMsYzdqTWlRfeRnfpqsD%2BvL0m%2BhaiDwsouBNWAzdP%2FYhQXIv8ZUvJBlVYQnrDymD&prvtof=xJ4CtZ1 4NrKrwslR1dXMK80crXjWF7sKhkbZ4GN9BxE%3D&poru=NbVrikyis4az%2BtbStQEdDui22ZRFxc6qVqYbkI6OLT0 8djTJ9qy1frXU9SVMf99KLB9go4l0rF8At%2BiABq%2FjdCdQJdp0pbo0K4GuxELUeyoS5wudJDkPDf3JpYf2ACaGx 6K1QZdQ184F%2B5LiFa0mcxRUvrGYJ7xBYWyzBQ%2Feyy7w%2F23wOTKuBfzEFwa74VuW0Spc6YCoMI6 ENrDkwgU3hg%3D%3D&cifr=1&w0G=3w4QHVrJOCimt90ZTeKXMe7ZrYb4bnkzv7QZzufjPqhFBPGQ1SrJ%2FwFsHy6 lqdqQBlr0&uFQl=XP7HMT_8";/*--><html data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKX74 ixpzVyXbJprcLfbH4psP

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49731	74.208.236.64	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:05:11.900079012 CEST	5238	OUT	GET /e3rs/?w0G=7ZSYqSAb20IhJodkc2ZZv2+VQiffweVGAnhTkqT9MP7KQ1W755ixlatoWnihL/C2wZs0&uFQl=X P7HMT_8 HTTP/1.1 Host: www.highdeserthealthinsurance.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:05:12.034537077 CEST	5238	IN	HTTP/1.1 302 Found Content-Type: text/html Content-Length: 0 Connection: close Date: Thu, 08 Apr 2021 10:05:11 GMT Server: Apache/2.4.10 (Debian) Cache-Control: no-cache Location: http://raygemme.com/e3rs/?w0G=7ZSYqSAb20IhJodkc2ZZv2+VQiffweVGAnhTkqT9MP7KQ1W755ixlatoWnih L/C2wZs0&uFQl=XP7HMT_8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49732	177.55.108.130	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:05:18.088413954 CEST	5243	OUT	GET /e3rs/?uFQl=XP7HMT_8&w0G=Ok77fVcdVMfliR4pMXON/NN29f2Jfu2AMoU186FmLUOu6U92Y3SpeQqKBhzvm DYI2dCa HTTP/1.1 Host: www.hotelmaktub.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:05:18.292332888 CEST	5243	IN	HTTP/1.1 404 Not Found Date: Thu, 08 Apr 2021 10:05:18 GMT Server: Apache/2.4.20 (Unix) OpenSSL/1.0.1e-fips Content-Length: 203 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 34 30 34 20 4e 6f 74 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 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 65 33 72 73 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 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>404 Not Found</title></head><body> Not Found The requested URL /e3rs/ was not found on this server. </body></html>

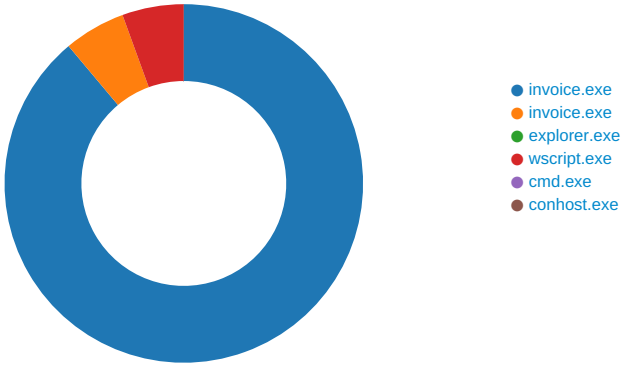
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.5	49734	192.0.78.24	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 12:05:23.354604006 CEST	5273	OUT	GET /e3rs/?w0G=0yUiwx1wLvxUfzb5kCZXOl2J+dvoSMZhdpoUDtYYFWxv9npQwlOrxt3zkZH4aLHtWZT3&uFQl=XP7HMT_8 HTTP/1.1 Host: www.legacyadmin.support Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 12:05:23.483477116 CEST	5273	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Thu, 08 Apr 2021 10:05:23 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.legacyadmin.support/e3rs/?w0G=0yUiwx1wLvxUfzb5kCZXOl2J+dvoSMZhdpoUDtYYFWxv9npQwlOrxt3zkZH4aLHtWZT3&uFQl=XP7HMT_8 X-ac: 3.mxp _dca 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 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 </body></html>

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: invoice.exe PID: 1972 Parent PID: 5628

General

Start time:	12:03:22
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\invoice.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\invoice.exe'
Imagebase:	0x800000
File size:	894464 bytes
MD5 hash:	492017E064CAB97DD8EA27ABD3E5CFCA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.245201549.0000000002EB3000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.246170025.0000000003EAC000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.246170025.0000000003EAC000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.246170025.0000000003EAC000.00000004.00000001.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	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCCCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DCCCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\invoice.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DFDC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\invoice.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6DFDC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DCA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DC003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DC003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DCA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB11B4F	ReadFile

Analysis Process: invoice.exe PID: 480 Parent PID: 1972

General

Start time:	12:03:31
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\invoice.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\invoice.exe
Imagebase:	0xd70000
File size:	894464 bytes
MD5 hash:	492017E064CAB97DD8EA27ABD3E5CFCA
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: 00000003.00000002.287914993.0000000001AE0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.287914993.0000000001AE0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.287914993.0000000001AE0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.286861103.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.286861103.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.286861103.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.287952464.0000000001B10000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.287952464.0000000001B10000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.287952464.0000000001B10000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	4182C7	NtReadFile

Analysis Process: explorer.exe PID: 3472 Parent PID: 480

General

Start time:	12:03:33
Start date:	08/04/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wscript.exe PID: 5064 Parent PID: 3472

General

Start time:	12:03:49

Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wscript.exe
Imagebase:	0xe0000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
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: 00000009.00000002.490575290.0000000002AE0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.490575290.0000000002AE0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.490575290.0000000002AE0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.490405309.00000000026A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.490405309.00000000026A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.490405309.00000000026A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.488897398.00000000021B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.488897398.00000000021B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.488897398.00000000021B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	21C82C7	NtReadFile

Analysis Process: cmd.exe PID: 6164 Parent PID: 5064

General

Start time:	12:03:54
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\invoice.exe'
Imagebase:	0x1c0000
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: 6196 Parent PID: 6164

General

Start time:	12:03:55
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis