ID: 345208
Sample Name: TRA-St-0015-O01.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 20:33:47
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

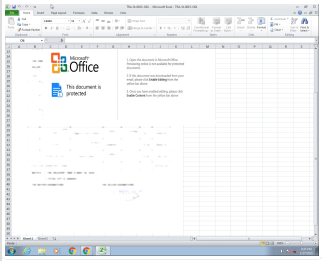
Analysis Report TRA-St-0015-O01.xlsx

Overview

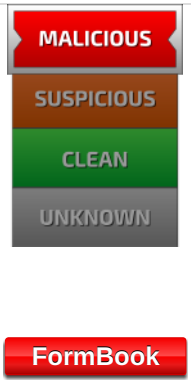
General Information

Sample Name:	TRA-St-0015-O01.xlsx
Analysis ID:	345208
MD5:	63c2af36e2ec6b0..
SHA1:	d1d834ca00c053..
SHA256:	129cd5a1fca6d3f..
Tags:	VelvetSweatshop xlsx

Most interesting Screenshot:



Detection



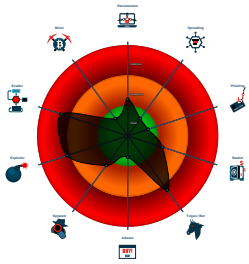
FormBook

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

Signatures

- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: File Dropped By EQ…
- Sigma detected: Scheduled temp file…
- 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…
- Sigma detected: Executables Starte…
- Sigma detected: Execution in Non-E…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 1100 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2556 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2720 cmdline: 'C:\Users\Public\vbc.exe' MD5: C7B2B0FA4A71FE33536148C2584DA7DB)
    - schtasks.exe (PID: 2920 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\XaHKwnPuj' /XML 'C:\Users\user\AppData\Local\Temp\tmp2222.tmp' MD5: 97E0EC3D6D99E8CC2B17EF2D3760E8FC)
    - vbc.exe (PID: 2928 cmdline: C:\Users\Public\vbc.exe MD5: C7B2B0FA4A71FE33536148C2584DA7DB)
    - vbc.exe (PID: 2476 cmdline: C:\Users\Public\vbc.exe MD5: C7B2B0FA4A71FE33536148C2584DA7DB)
    - vbc.exe (PID: 2472 cmdline: C:\Users\Public\vbc.exe MD5: C7B2B0FA4A71FE33536148C2584DA7DB)
    - vbc.exe (PID: 2456 cmdline: C:\Users\Public\vbc.exe MD5: C7B2B0FA4A71FE33536148C2584DA7DB)
    - vbc.exe (PID: 2884 cmdline: C:\Users\Public\vbc.exe MD5: C7B2B0FA4A71FE33536148C2584DA7DB)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.2169610523.0000000012381000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000002.2169610523.0000000012381000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x2c6660:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x2c68da:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x2d23fd:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x2d1ee9:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x2d24ff:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x2d2677:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x2c72f2:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x2d1164:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x2c7feb:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x2d809f:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x2d90a2:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000004.00000002.2169610523.0000000012381000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x2d5181:$sqlite3step: 68 34 1C 7B E1 • 0x2d5294:$sqlite3step: 68 34 1C 7B E1 • 0x2d51b0:$sqlite3text: 68 38 2A 90 C5 • 0x2d52d5:$sqlite3text: 68 38 2A 90 C5 • 0x2d51c3:$sqlite3blob: 68 53 D8 7F 8C • 0x2d52eb:$sqlite3blob: 68 53 D8 7F 8C
00000004.00000002.2169219241.00000000023DE000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Process Memory Space: vbc.exe PID: 2720	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: File Dropped By EQNEDT32EXE

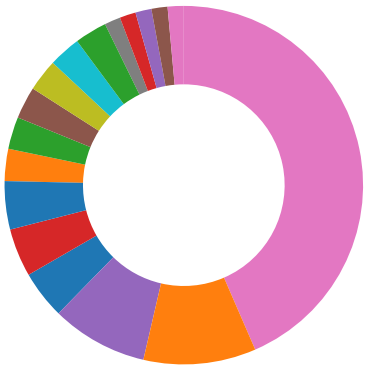
Sigma detected: Scheduled temp file as task from temp location

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:

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

Exploits:

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

Compliance:

Uses new MSVCR Dlls

Uses secure TLS version for HTTPS connections

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

Uses schtasks.exe or at.exe to add and modify task schedules

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:

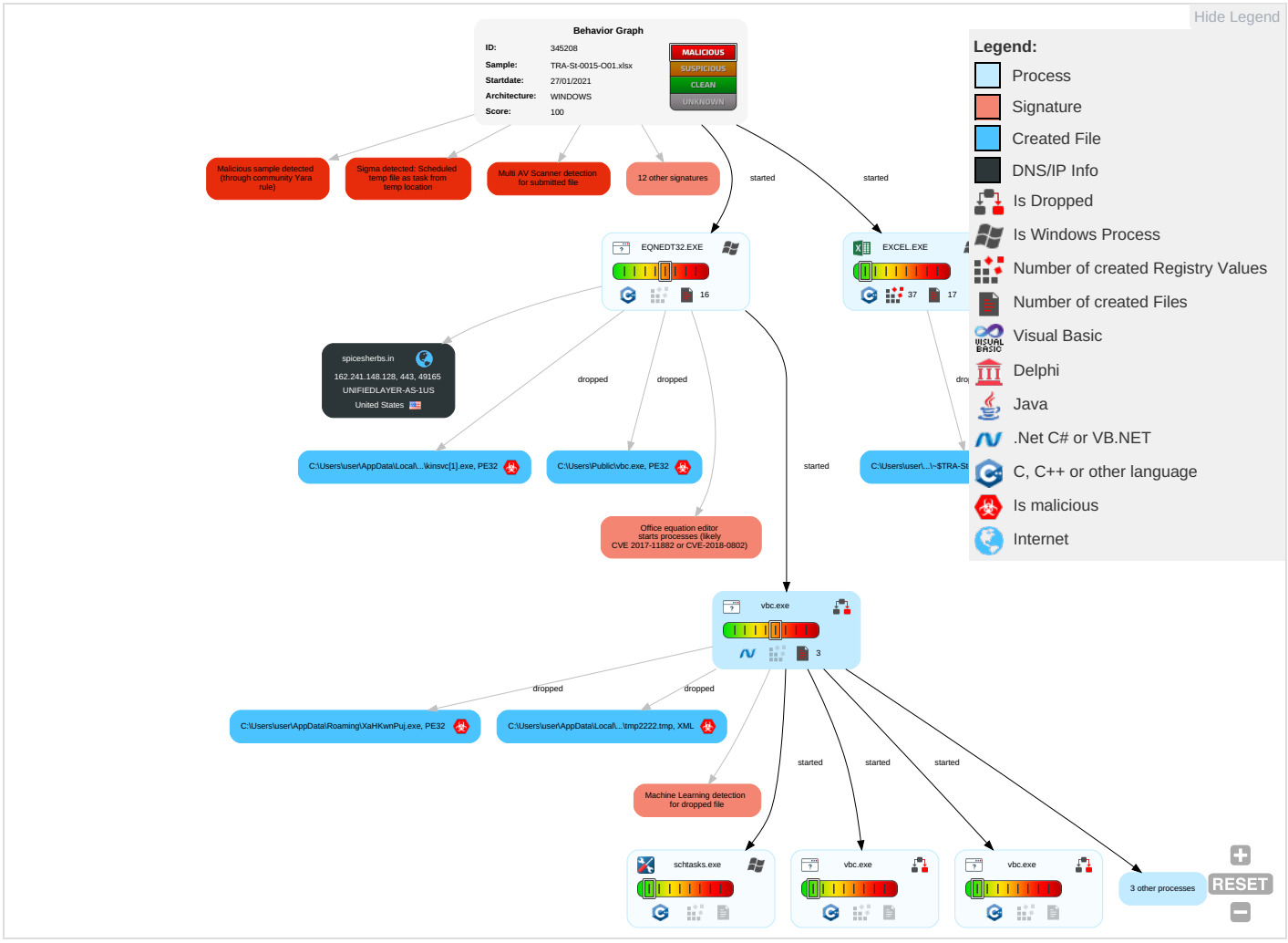
Yara detected FormBook

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	Command and Scripting Interpreter 1	Scheduled Task/Job 1	Process Injection 1 1	Masquerading 1 1 1	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesdrop Insecure Network Communica
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 3	LSASS Memory	Security Software Discovery 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 3	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	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1 1	LSA Secrets	Remote System 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	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming o Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poi

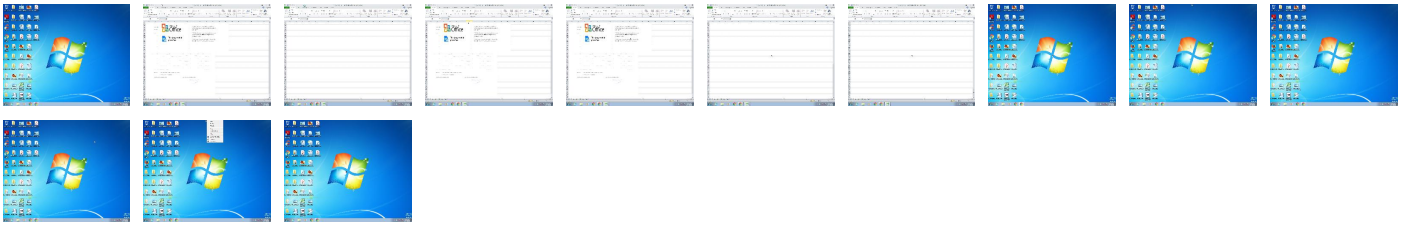
Behavior Graph

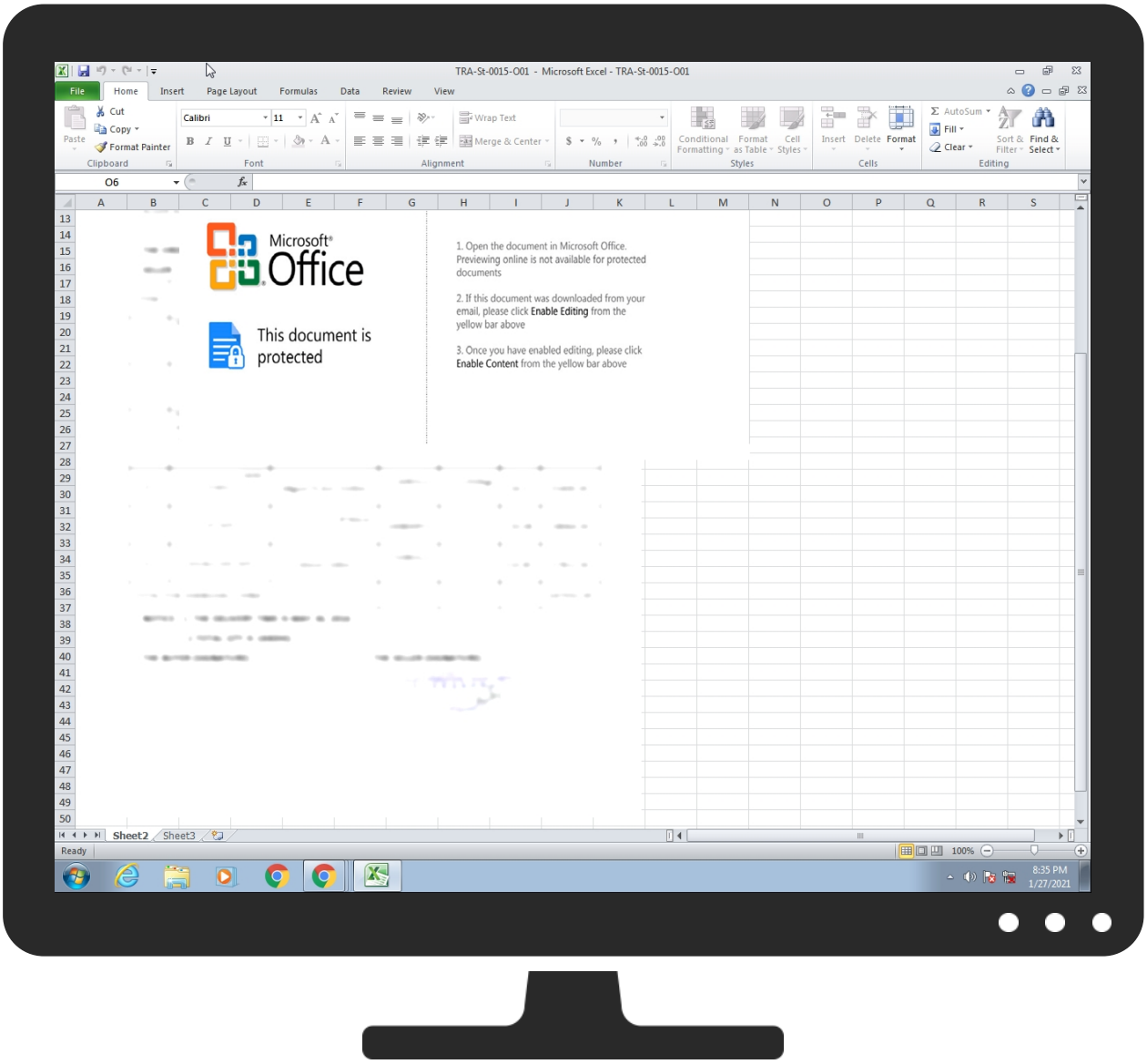


Screenshots

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
TRA-St-0015-O01.xlsx	32%	Virustotal		Browse
TRA-St-0015-O01.xlsx	23%	ReversingLabs	Document-Office.Trojan.Heuristic	

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\kinsvc[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\XaHKwnPuj.exe	100%	Joe Sandbox ML		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
spicesherbs.in	162.241.148.128	true	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.%s.comPA	vbc.exe, 00000004.00000002.217 0919142.000000001BA40000.00000 002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http:// schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous .	vbc.exe, 00000004.00000002.217 0919142.000000001BA40000.00000 002.00000001.sdmp	false		high
http://www.day.com/dam/1.0	BADF7393.emf.0.dr	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	vbc.exe, 00000004.00000002.216 9176262.0000000002371000.00000 004.00000001.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.241.148.128	unknown	United States		46606	UNIFIEDLAYER-AS-1US	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	345208
Start date:	27.01.2021
Start time:	20:33:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TRA-St-0015-O01.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:	12
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@16/14@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 5.7% (good quality ratio 3.3%) • Quality average: 34.8% • Quality standard deviation: 33.3%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 192.35.177.64, 72.247.178.11, 72.247.178.49 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, audownload.windowsupdate.nsatc.net, apps.digsigtrust.com, ctldl.windowsupdate.com, a767.dscg3.akamai.net, apps.identrust.com, au-bg-shim.trafficmanager.net • 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
20:35:06	API Interceptor	60x Sleep call for process: EQNEDT32.EXE modified
20:35:11	API Interceptor	48x Sleep call for process: vbc.exe modified
20:35:13	API Interceptor	1x Sleep call for process: schtasks.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
162.241.148.128	SWIFT (MTC 103) 89.xlsx	Get hash	malicious	Browse	• cassiagumrefined.com/js/file/TH98/86HTe.exe

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	Order confirmation 64236000000025 26.01.2021.exe	Get hash	malicious	Browse	• 192.254.186.135
	printouts of outstanding as of Jan-27-2021.xlsm	Get hash	malicious	Browse	• 192.185.131.49
	98.doc	Get hash	malicious	Browse	• 192.185.52.115
	0113 INV_PAK.xlsx	Get hash	malicious	Browse	• 192.185.35.76
	Purchase Order.xlsx	Get hash	malicious	Browse	• 50.87.169.249
	quote20210126.exe.exe	Get hash	malicious	Browse	• 70.40.220.182
	Informacion.doc	Get hash	malicious	Browse	• 162.241.224.176
	xl2Ml2iNJe.exe	Get hash	malicious	Browse	• 162.241.217.108
	file.doc	Get hash	malicious	Browse	• 192.185.52.115
	Remittance Advice 117301.xlsx	Get hash	malicious	Browse	• 162.214.76.195
	vA0mtZ7JzJ.exe	Get hash	malicious	Browse	• 162.241.60.214
	INGNhYonmgtGZ9Updf.exe	Get hash	malicious	Browse	• 74.220.199.9
	Dridex-01-a99e.xlsm	Get hash	malicious	Browse	• 198.57.200.100
	Inv_1480.xls	Get hash	malicious	Browse	• 192.185.217.211
	Mensaje-22-012021.doc	Get hash	malicious	Browse	• 162.241.253.129
	INV5949.xls	Get hash	malicious	Browse	• 192.232.216.109
	DOCUMENTS_RECEIVED.html	Get hash	malicious	Browse	• 192.185.112.211
	INV 5047.xls	Get hash	malicious	Browse	• 192.185.217.211
	FP4554867134UQ.doc	Get hash	malicious	Browse	• 192.232.250.227
	MENSAJE.doc	Get hash	malicious	Browse	• 192.185.52.115

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
7dcce5b76c8b17472d024758970a406b	Final_Notification.docx	Get hash	malicious	Browse	• 162.241.148.128
	documenting.doc	Get hash	malicious	Browse	• 162.241.148.128
	SecuriteInfo.com.Heur.3279.xlsm	Get hash	malicious	Browse	• 162.241.148.128
	Rolled Alloys Possible Infection.docx	Get hash	malicious	Browse	• 162.241.148.128
	Statement of Account as of Jan_27 2021.xlsm	Get hash	malicious	Browse	• 162.241.148.128
	printouts of outstanding as of Jan-27-2021.xlsm	Get hash	malicious	Browse	• 162.241.148.128
	printouts of outstanding as of Jan_27_2021.xlsm	Get hash	malicious	Browse	• 162.241.148.128

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	FACTUUR-INV00012.xlsx	Get hash	malicious	Browse	• 162.241.148.128
	0007334.xlsx	Get hash	malicious	Browse	• 162.241.148.128
	Purchase Order.xlsx	Get hash	malicious	Browse	• 162.241.148.128
	SecuriteInfo.com.Heur.30497.xls	Get hash	malicious	Browse	• 162.241.148.128
	case (2553).xls	Get hash	malicious	Browse	• 162.241.148.128
	case (1057).xls	Get hash	malicious	Browse	• 162.241.148.128
	case (4335).xls	Get hash	malicious	Browse	• 162.241.148.128
	case (1522).xls	Get hash	malicious	Browse	• 162.241.148.128
	case (4374).xls	Get hash	malicious	Browse	• 162.241.148.128
	case (166).xls	Get hash	malicious	Browse	• 162.241.148.128
	PAYMENT.xlsx	Get hash	malicious	Browse	• 162.241.148.128
	case (547).xls	Get hash	malicious	Browse	• 162.241.148.128
	Dridex-06-bc1b.xlsm	Get hash	malicious	Browse	• 162.241.148.128

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8efIqigYDff:RN7MlanAQwEIztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n-.....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..lr.....I.I6/..d.].xIX<...&U...GD..Mn.y&.[<(tk.....%B.b;/..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....I.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a.,...E5X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep...xI@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/I\.cDB0.'.Y...r.[.....vM...o.=....zK..r..I..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	893
Entropy (8bit):	7.366016576663508
Encrypted:	false
SSDEEP:	24:hBntmDvKUQQDvKUr7C5fpqp8gPvXHmXvponXux:3ntmD5QQD5XC5RqHHXmXvp++x
MD5:	D4AE187B4574036C2D76B6DF8A8C1A30
SHA1:	B06F409FA14BAB33CBAF4A37811B8740B624D9E5
SHA-256:	A2CE3A0FA7D2A833D1801E01EC48E35B70D84F3467CC9F8FAB370386E13879C7
SHA-512:	1F44A360E8BB8ADA22BC5BFE001F1BABB4E72005A46BC2A94C33C4BD149FF256CCE6F35D65CA4F7FC2A5B9E15494155449830D2809C8CF218D0B9196EC646BC

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Malicious:	false
Reputation:	high, very likely benign file
Preview:	0..y..*.H.....j0..f...1.0...*.H.....N0..J0..2.....D....'..09...@k0...*.H.....0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30...000930211219Z..210930 140115Z0?1$0"..U....Digital Signature Trust Co.1.0...U....DST Root CA X30.."0...*.H.....0.....P..W..be.....,k0.[...}.@.....3vI*.?II..N..>H.e...!.e.*.2....w..{.....s.z..2..~ ..0....*8.y.1.P..e.Qc...a.Ka..Rk...K.(.H.....>.... .[.*....p....%.tr.{j.4.0...h.{T....Z...=d.....Ap..r.&.8U9C....\@.....%.....:..n.>..\..<.i....*.)W..=....]......B0@0...U.....0....0...U..... ....0...U.....{,q...K.u...`...0...*.H.....,...\...(f7:...?K.... ]..YD.>.>..K.t.....t..~.....K. D....}..j.....N..:.pI.....:^H...X._..Z.....Y..n.....f3.Y[...sG.+..7H..VK....r2...D.SrmC.&H.Rg. X..gvqx...V..9$1....Z0G..P.....dc`.....}...=2.e..|.Wv..(9..e...w.j..w.....)...55.1.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	328
Entropy (8bit):	3.0765536003145497
Encrypted:	false
SSDEEP:	6:kKekHbqoN+SkQlPlEGYRMY9z+4KlDA3RUeKlF+adAlf:mku3kPlE99SNxAhUeo+aKt
MD5:	DA24412AA96F1A51D7A1C7F0E63901F0
SHA1:	13B1483CE43D630CCA5F460AB270DA7F764512D9
SHA-256:	613A697AB25376DAA6A23A4F82928456CF95820090B32CB17BAA6C98179DEC8E
SHA-512:	8F8F20E9A916384433A6A439A08286AA0F09D0EDF3542CC56DD0B27D75358EA45D43EC7E213588DEB5760F8CFAFCBFD93C62988096C5A25DCAE73D849DB1E3A
Malicious:	false
Reputation:	low
Preview:	p..... ....._!O./...(..... .....&.....h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s .t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.e.b.b.a.e.1.d.7.e.a.d.6.1.:.0."...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\E0F5C59F9FA661F6F4C50B87FEF3A15A	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	252
Entropy (8bit):	3.0042074090694686
Encrypted:	false
SSDEEP:	3:kkFklNoKmEvfllXlE/QhzllPlzRkwWBARLNDU+ZMlKlBkvclcMlVHblB1UAYpFit:kKsmERliBAIdQZV7eAYLit
MD5:	DDA8BE33A50FC45ACBADDE1E16982CF8
SHA1:	BD92A8AEDC28D46640624F4410CDCE3872D4277A
SHA-256:	B4E9CBCAA6B854ADD8D0A0038237F380E2419948DD0C4BF8C4E5F9376AEF6F17
SHA-512:	C71DBD91B99A57B771DF7387961752CC8CCC267AF405FE6B295B8834D54DC6A53D6344DD472D56736E152F0634C66F01EF33FA848867D79D62694207EE8035D4
Malicious:	false
Reputation:	low
Preview:	p..... ....`....a../...(..... .....u.....(.....}...h.t.t.p.:././.a.p.p.s...i.d.e.n.t.r.u.s.t...c.o.m./.r.o.o.t.s./.d.s.t.r.o.o.t.c.a.x.3...p.7.c...".3.7.d.-.5.9.e.7.6 .b.3.c.6.4.b.c.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\kinsvc[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):	508928
Entropy (8bit):	7.7654598154070165
Encrypted:	false
SSDEEP:	12288:S1LhRC+HyykFZ/6/dn3Vsy167F8E6tLvM89GrxD4G:S1/3SXFZ/ad3VRQ8Ltr9Gdp
MD5:	C7B2B0FA4A71FE33536148C2584DA7DB
SHA1:	D449E0DC0D24447634C61987CF0907FB72CF93A4
SHA-256:	DB8923F36B12AC2D21DE6B241E3AC228170456F7DB87DC38552E89F9A4E8903A
SHA-512:	EA5BC49B81DC9FC57A47BC4384C1A56C6157D02AC9F53655DA65A96138D5CFA1244B82562D4B7844E89762154CC1C14896CDEB945F832A9436516F96DFC5639
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://https://spicesherbs.in/herbs/kinsvc/kinsvc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....=.`.....".."...P..... .....@.. ..... ..@.....P...O.....`..... ....H.....text..... ....`.rsrc...`.....@..@.reloc..... .....@..B.....H.....|.....@....7.....0.....(....(.....(.....o....*.....(.....(!.....("....(#.....($....*N..(....o....(%....*&..(&....*.s'.....s(.....s).....s*.....s+.....*....0.....~....o,....+..*.0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*&..(1....*...0..<.....~.....(2.....,!r...p.....(3...o4...s5.....~.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\284D8619.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\BADF7393.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):	2.898645806967479
Encrypted:	false
SSDEEP:	3072:S34UL0tS6WB0JOqFVY5QcARI/McGdAT9kRLFdtSyUu50yknG/qc+x:84UcLe0JOqQQZR8MDdATCR3tS+jqcC
MD5:	02BE9DEC93BBAE0645D69572E9563911
SHA1:	DDBA1220AA092E00FFAB90155D796D735E93E627
SHA-256:	A9955A402E6FC0BBE4CA2D34DA0BADA39DC9239F3F9FE6F4A71BA6A9EC230B40
SHA-512:	A9963FAD341517EE356156EFAEEC4C3100A3682E8D293A530BB0EF1601D5FB5500593BA9EA29898B72B04B565F3A6EC7FFAD973DBBD070B60239859D2E15C9D 9
Malicious:	false
Reputation:	low
Preview:	....l.....S.....@...#.. EMF.....(.....\K..hC..F...... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....I...c...%.....%.....R...p.....@."C.a.l.i.b.r.i.....N.T..... .....t.....N.T..... ....yQQ..... .....zQQ.....O.....X...%...7.....{ .@.....C.a.l.i.b.r.....X.....8....2JQ.....t...t...{HQ.....dv.. ....%.....%.....%.....!.....I...c..."....%.....%.....%.....T...T.....@.E.@T.....L.....I...c...P... ...6...F...$.....EMF+*@..$..... .....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CEC07078.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 90", baseline, precision 8, 700x990, frames 3
Category:	dropped
Size (bytes):	48770
Entropy (8bit):	7.801842363879827
Encrypted:	false
SSDEEP:	768:uLgWImQ6AMqTeyjskbJeYnriZvApugsiKi7iszQ2rvBZzmFz3/soBqZhsglgDQPT:uLgY4MqTeywVYr+0ugbDTzQ27A3UXsgf
MD5:	AA7A56E6A97FFA9390DA10A2EC0C5805
SHA1:	200A6D7ED9F485DD5A7B9D79B596DE3ECEBD834A
SHA-256:	56B1EDECC9A282A9FAAFD95D4D9844608B1AE5CCC8731F34F8B30B3825734974
SHA-512:	A532FE4C52FED46919003A96B882AE6F7C70A3197AA57BD1E6E917F766729F7C9C1261C36F082FBE891852D083EDB2B5A34B0A325B7C1D96D6E58B0BED6C578
Malicious:	false
Preview:	......JFIF.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C.....C..... ....."....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..R..(...(...(.....3Fh.....(....P.E.P.Gj(...(....Q@.%-...(.....P.QKE.%.....;.R.@.E-...(.....P.QKE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'j^.....(...(...(....w...3Fh....E.....4w...h.%.....E./J)(.....Z)(.....Z)(....

C:\Users\user\AppData\Local\Temp\CabA5C2.tmp	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	Microsoft Cabinet archive data, 59134 bytes, 1 file
Category:	dropped
Size (bytes):	59134
Entropy (8bit):	**7.995450161616763**
Encrypted:	**true**

C:\Users\user\AppData\Local\Temp\CabA5C2.tmp	
SSDEEP:	1536:R695NkJMM0/7laXXHAQHQaYfwlmz8eflqigYDff:RN7MlanAQwElztTk
MD5:	E92176B0889CC1BB97114BEB2F3C1728
SHA1:	AD1459D390EC23AB1C3DA73FF2FBEC7FA3A7F443
SHA-256:	58A4F38BA43F115BA3F465C311EAAF67F43D92E580F7F153DE3AB605FC9900F3
SHA-512:	CD2267BA2F08D2F87538F5B4F8D3032638542AC3476863A35F0DF491EB3A84458CE36C06E8C1BD84219F5297B6F386748E817945A406082FA8E77244EC229D8F
Malicious:	false
Preview:	MSCF.....,.....I.....T.....R.. .authroot.stl.ym&7.5..CK..8T....c_.d...:.(.....].M$[v.4.).E.$7*I.....e..Y..Rq...3.n..u.....\|..=H....&..1.1..f.L..>e.6....F8.X.b.1$,.a...n-.....D..a....[.....i,+.+..<.b._#...G..U.....n..21*pa..>.32..Y..j...;Ay.....n/R... ._.+..<...Am.t.<. ..V..y`.yO..e@../...<#..#.....dju*..B.....8..H'..lr.....I.I6/..d.].xIX<...&U...GD..Mn.y&.[<(tk.....%B.b;./..`.#h....C.P...B..8d.F...D.k..... 0..w...@(.. @K....?.)ce.....\.\.....I.....Q.Qd..+...@.X..##3..M.d..n6.....p1..)...x0V...ZK.{...{.=#h.v.).....b...*..[...L..*c..a..,...E5X..i.d..w.....#o*+.....X.P...k...V.$...X.r.e....9E.x..=\...Km.....B...Ep...xl@@c1.....p?...d.{EYN.K.X>D3..Z..q.] .Mq.....L.n}.....+/l\.cDB0.'.Y...r.[.....vM...o.=....zK..r..I..>B....U..3....Z...ZjS...wZ.M...IW;..e.L...zC.wBtQ..&.Z.Fv+..G9.8..!..\T:K`.....m.....9T.u..3h.....{...d[...@...Q.?..p.e.t[.%7.....^.....s.

C:\Users\user\AppData\Local\Temp\TarA5C3.tmp	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	data
Category:	dropped
Size (bytes):	152788
Entropy (8bit):	6.316654432555028
Encrypted:	false
SSDEEP:	1536:WIA6c7RbAh/E9nF2hspNuc8odv+1//FnzAYtYyjCQxSMnl3xlUwg:WAmfF3pNuc7v+ltjCQSMnnSx
MD5:	64FEDADE4387A8B92C120B21EC61E394
SHA1:	15A2673209A41CCA2BC3ADE90537FE676010A962
SHA-256:	BB899286BE1709A14630DC5ED80B588FDD872DB361678D3105B0ACE0D1EA6745
SHA-512:	655458CB108034E46BCE5C4A68977DCBF77E20F4985DC46F127ECBDE09D6364FE308F3D70295BA305667A027AD12C952B7A32391EFE4BD5400AF2F4D0D83087
Malicious:	false
Preview:	0..T...*.H.....T.0..T....1.0...`.H.e.....0..D...+....7.....D.0..D.0...+....7.....R19%..2101150042 37Z0...+.....0..D.0..*.....`...@.,..0..0.r1...0...+....7..~1.....D...0...+....7..i1...0...+....7<..0 ..+....7...1.....@N...%.=.,..0$..+....7...1.....`@V'..%..*..S.Y.00..+....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0..,.....[./..uIv..%1...0...+....7..h1.....6.M...0...+....7..~1.....0...+....7...1...0...+.....0 ..+....7...1...O..V.....b0$..+....7...1...>.)....s,.=$.~R.'..00. .+....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+....7..h1.....o&...0...+....7..i1...0...+....7<..0 ..+....7...1...lo...^....[...J@0$..+....7...1...J\u".F....9.N...`...00..+....7..b1". ...@.....G..d..m..$.....X...}0B..+....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Local\Temp\tmp2222.tmp	
Process:	C:\Users\Public\vbc.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1621
Entropy (8bit):	5.1546643449463865
Encrypted:	false
SSDEEP:	24:2dH4+SEqCZ7ClNMFi/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBxtn:cbhZ7ClNQi/rydbz9l3YODOLNdq3R
MD5:	2F157857CAC56F3C7E44E7262FD6EAAD
SHA1:	022DCAA46EEEFD345D9BD8DF1870FD0C916E828B
SHA-256:	92991267A638A487B7117A3EBC7F732AD8C253A77149680D45E1289C5144AAD0
SHA-512:	C603FF5AA514DD00881C8CEE9AA8A7A369342844638138F9338900192E9D3ABBA2958E478E95BA7CD21E70F6F7223E4F128629F5212FFE1A43D35171F39E8784
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>user-PC\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>user-PC\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>user-PC\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true</StartWhenAvailable>

C:\Users\user\AppData\Roaming\XaHKwnPuj.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	508928
Entropy (8bit):	7.7654598154070165
Encrypted:	false
SSDEEP:	12288:S1LhRC+HyykFZ/6/dn3Vsy167F8E6tLvM89GrxD4G:S1/3SXFZ/ad3VRQ8Ltr9Gdp
MD5:	C7B2B0FA4A71FE33536148C2584DA7DB
SHA1:	D449E0DC0D24447634C61987CF0907FB72CF93A4
SHA-256:	DB8923F36B12AC2D21DE6B241E3AC228170456F7DB87DC38552E89F9A4E8903A
SHA-512:	EA5BC49B81DC9FC57A47BC4384C1A56C6157D02AC9F53655DA65A96138D5CFA1244B82562D4B7844E89762154CC1C14896CDEB945F832A9436516F96DFC5639
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%

C:\Users\user\AppData\Roaming\XaHKwnPuj.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....=.`.....".."...P..... .....@.. ..... ..... ..@.....P...O.....`..... ....H.....text..... ....`.rsrc...`.....@..@.reloc..... .....@..B.....H.....\|.....@....7.....0.....(....(.....(.....o....*.....(.....(!.....("....(#.....($....*N..(....o....(%....*&.. (&....*.s'.....s(.....s).....s*.....s+.....*....0.....~....o,....+..*.0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*&..(1....*...0..<.....~..... (2.....,!r...p.....(3...o4...s5.....~.....

C:\Users\user\Desktop\~$TRA-St-0015-O01.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**
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:	modified
Size (bytes):	508928
Entropy (8bit):	7.7654598154070165
Encrypted:	false
SSDEEP:	12288:S1LhRC+HyykFZ/6/dn3Vsy167F8E6tLvM89GrxD4G:S1/3SXFZ/ad3VRQ8Ltr9Gdp
MD5:	C7B2B0FA4A71FE33536148C2584DA7DB
SHA1:	D449E0DC0D24447634C61987CF0907FB72CF93A4
SHA-256:	DB8923F36B12AC2D21DE6B241E3AC228170456F7DB87DC38552E89F9A4E8903A
SHA-512:	EA5BC49B81DC9FC57A47BC4384C1A56C6157D02AC9F53655DA65A96138D5CFA1244B82562D4B7844E89762154CC1C14896CDEB945F832A9436516F96DFC5639
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....=.`.....".."...P..... .....@.. ..... ..... ..@.....P...O.....`..... ....H.....text..... ....`.rsrc...`.....@..@.reloc..... .....@..B.....H.....\|.....@....7.....0.....(....(.....(.....o....*.....(.....(!.....("....(#.....($....*N..(....o....(%....*&.. (&....*.s'.....s(.....s).....s*.....s+.....*....0.....~....o,....+..*.0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*&..(1....*...0..<.....~..... (2.....,!r...p.....(3...o4...s5.....~.....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.9944183504926105
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	TRA-St-0015-O01.xlsx
File size:	907776
MD5:	63c2af36e2ec6b0c464889473ba19048
SHA1:	d1d834ca00c0538a448e64e10231a5c78c09838d
SHA256:	129cd5a1fca6d3febd900de6cbecb9e30e22a19d7b2aeda41ee3c1eac54981ba
SHA512:	557108c60fedb061cded9fb1b1c82bc4e5ef6dd338476d90e134d52a6c05832b03028e537139b61f371a8b4ae05d47d3f09ac23a213b9cb3e19e826a6b3fc38e
SSDEEP:	24576:yG4DPNX84Ad4lsmboKda75Cy6pRxLUpvEFwn:yG8PZ84pyZh0yiCsFA
File Content Preview:	.....>.....~.....z.....|.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General	
Document Type:	OLE
Number of OLE Files:	1

OLE File "TRA-St-0015-O01.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 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: 896520

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	896520
Entropy:	7.99976973003
Base64 Encoded:	True
Data ASCII:	. . . . . + o .] . . . @ . . . . g s J . . j . . . . ^ 6 . . . . . A > . ' . . . w . p . V = , ; J . _ B e F . . . . . F . . Z . . . . . F . . Z . . . . . F . . Z . . . . . F . . Z . . . . . F . . Z . . . . . F . . Z . . . . . F . . Z . . . . . F . . Z . . . . . F . . Z . . . . . F . . Z . . . . . F . . Z . . . . . F . . Z . . . . .
Data Raw:	f3 ad 0d 00 00 00 00 00 f0 1d 2b 6f d0 5d d0 0d f9 40 84 af d3 80 20 67 73 4a f2 ad 6a c5 a0 cd c9 5e 36 8d f6 be c0 bc 03 f0 e8 18 05 41 3e bb 27 da f3 eb 77 bc 70 ca 56 3d 2c 3b 4a dc 5f 42 65 46 b4 a2 0f 92 ba d3 05 04 0b 18 88 d8 80 e1 02 d5 af 0b 46 07 ec 5a 05 04 0b 18 88 d8 80 e1 02 d5 af 0b 46 07 ec 5a 05 04 0b 18 88 d8 80 e1 02 d5 af 0b 46 07 ec 5a 05 04 0b 18 88 d8 80 e1

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

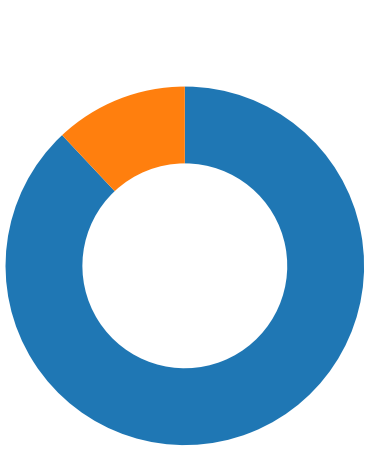
General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.55845197116
Base64 Encoded:	False
Data ASCII:	. . . . $ . . . . . $ . . . . . f . . . . . M . i . c . r . o . s . o . f . t . . E . n . h . . n . c . e . d . . R . S . A . . a . n . d . . A . E . S . . C . r . y . p . t . o . g . r . a . p . h . i . c . . P . r . o . v . i . d . e . r . . . . . [q . n $ . . . > . . o . . . . . G . . [. . , n % C . . h & . . . . . > . I I { S J . ' . . . . . K / . . # M . . . . .
Data Raw:	04 00 02 00 24 00 00 00 8c 00 00 00 24 00 00 00 00 00 00 00 0e 66 00 00 04 80 00 00 80 00 00 00 18 00 00 00 00 00 00 00 00 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 45 00 6e 00 68 00 61 00 6e 00 63 00 65 00 64 00 20 00 52 00 53 00 41 00 20 00 61 00 6e 00 64 00 20 00 41 00 45 00 53 00 20 00 43 00 72 00 79 00 70 00 74 00 6f 00 67 00 72 00 61 00 70 00 68 00

Network Behavior

Network Port Distribution

Total Packets: 50

- 53 (DNS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 20:35:07.590151072 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:07.748012066 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:07.748229027 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:07.757462025 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:07.915226936 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:07.921597958 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:07.921638966 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:07.921669960 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:07.921843052 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:07.967900038 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:08.129703045 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:08.129851103 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:09.671431065 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:09.834105968 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:09.834187984 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:09.834243059 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:09.834299088 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:09.834338903 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:09.834352970 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:09.834389925 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:09.834424019 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:09.834462881 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:09.834484100 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:09.834501028 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:09.834537983 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:09.834567070 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:09.834592104 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:09.834647894 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:09.834705114 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:09.834719896 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:09.834908962 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:09.836659908 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:09.994482040 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:09.994538069 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:09.994570971 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:09.994600058 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:09.994640112 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:09.994677067 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:09.994714975 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:09.994751930 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:09.994790077 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:09.994796991 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:09.994831085 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:09.994837046 CET	443	49165	162.241.148.128	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 20:35:09.994867086 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:09.994879961 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:09.994899035 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:09.994913101 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:09.994927883 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:09.994945049 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:09.994977951 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:09.994988918 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:09.995068073 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:09.995132923 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:09.995172977 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:09.995274067 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:09.995351076 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:09.995373011 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:09.995441914 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:09.995445967 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:09.995482922 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:09.995507956 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:09.995521069 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:09.995533943 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:09.995563984 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:10.001457930 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:10.153412104 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:10.153491020 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:10.153531075 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:10.153568029 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:10.153606892 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:10.153614044 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:10.153634071 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:10.153656960 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:10.153666019 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:10.153709888 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:10.153717041 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:10.153757095 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:10.153793097 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:10.153795004 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:10.153820992 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:10.153834105 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:10.153846025 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:10.153871059 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:10.153908968 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:10.153934002 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:10.153949022 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:10.153960943 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:10.153990030 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:10.153995991 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:10.154040098 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:10.154056072 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:10.154078007 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:10.154088974 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:10.154115915 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:10.154134035 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:10.154155016 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:10.154192924 CET	443	49165	162.241.148.128	192.168.2.22
Jan 27, 2021 20:35:10.154217005 CET	49165	443	192.168.2.22	162.241.148.128
Jan 27, 2021 20:35:10.154231071 CET	443	49165	162.241.148.128	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 20:35:07.327306032 CET	52197	53	192.168.2.22	8.8.8.8
Jan 27, 2021 20:35:07.516894102 CET	53	52197	8.8.8.8	192.168.2.22
Jan 27, 2021 20:35:07.517139912 CET	52197	53	192.168.2.22	8.8.8.8
Jan 27, 2021 20:35:07.573364019 CET	53	52197	8.8.8.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 20:35:08.400657892 CET	53099	53	192.168.2.22	8.8.8.8
Jan 27, 2021 20:35:08.448559046 CET	53	53099	8.8.8.8	192.168.2.22
Jan 27, 2021 20:35:08.454209089 CET	52838	53	192.168.2.22	8.8.8.8
Jan 27, 2021 20:35:08.502331018 CET	53	52838	8.8.8.8	192.168.2.22
Jan 27, 2021 20:35:08.989140034 CET	61200	53	192.168.2.22	8.8.8.8
Jan 27, 2021 20:35:09.045689106 CET	53	61200	8.8.8.8	192.168.2.22
Jan 27, 2021 20:35:09.051862001 CET	49548	53	192.168.2.22	8.8.8.8
Jan 27, 2021 20:35:09.110131025 CET	53	49548	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 20:35:07.327306032 CET	192.168.2.22	8.8.8.8	0x1168	Standard query (0)	spicesherbs.in	A (IP address)	IN (0x0001)
Jan 27, 2021 20:35:07.517139912 CET	192.168.2.22	8.8.8.8	0x1168	Standard query (0)	spicesherbs.in	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 20:35:07.516894102 CET	8.8.8.8	192.168.2.22	0x1168	No error (0)	spicesherbs.in		162.241.148.128	A (IP address)	IN (0x0001)
Jan 27, 2021 20:35:07.573364019 CET	8.8.8.8	192.168.2.22	0x1168	No error (0)	spicesherbs.in		162.241.148.128	A (IP address)	IN (0x0001)

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Jan 27, 2021 20:35:07.921669960 CET	162.241.148.128	443	192.168.2.22	49165	CN=webmail.spicesherbs.in CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sun Dec 20 14:59:03 CET 2020 Wed Oct 07 21:21:40 CEST 2020	Sat Mar 20 14:59:03 CET 2021 Wed Sep 29 21:21:40 CEST 2021	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19,0-10-11-13-23-65281,23-24,0	7dcce5b76c8b17472d024758970a406b
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		

Code Manipulations

Statistics

Behavior

- EXCEL.EXE
- EQNEDT32.EXE
- vbc.exe
- schtasks.exe
- vbc.exe
- vbc.exe
- vbc.exe
- vbc.exe
- vbc.exe

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1100 Parent PID: 584

General

Start time:	20:34:46
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:	0x13fba0000
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\~$TRA-St-0015-O01.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	13FDEF526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$TRA-St-0015-O01.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13FDEF591	WriteFile
C:\Users\user\Desktop\~$TRA-St-0015-O01.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	13FDEF526	WriteFile
C:\Users\user\Desktop\~$TRA-St-0015-O01.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	13FDEF591	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	7c6	binary	37 63 36 00 4C 04 00 00 02 00 00 00 00 00 00 00 56 00 00 00 01 00 00 00 2A 00 00 00 20 00 00 00 74 00 72 00 61 00 2D 00 73 00 74 00 2D 00 30 00 30 00 31 00 35 00 2D 00 6F 00 30 00 31 00 2E 00 78 00 6C 00 73 00 78 00 00 00 74 00 72 00 61 00 2D 00 73 00 74 00 2D 00 30 00 30 00 31 00 35 00 2D 00 6F 00 30 00 31 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: 2556 Parent PID: 584

General

Start time:	20:35:06
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	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: 2720 Parent PID: 2556

General

Start time:	20:35:10
Start date:	27/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0xbf0000
File size:	508928 bytes
MD5 hash:	C7B2B0FA4A71FE33536148C2584DA7DB
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: 00000004.00000002.2169610523.0000000012381000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.2169610523.0000000012381000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.2169610523.0000000012381000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.2169219241.00000000023DE000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\XaHKwnPuj.exe	read data or list directory | read attributes | delete | synchronize | generic write	device | sparse file	sequential only | non directory file	success or wait	1	7FEE997835A	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp2222.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	7FEE92A06C8	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2222.tmp	success or wait	1	7FEE92A0850	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\XaHKwnPuj.exe	0	65536	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 a4 3d 11 60 00 00 00 00 00 00 00 00 e0 00 22 00 0b 01 50 00 00 b8 07 00 00 0a 00 00 00 00 00 00 a2 d6 07 00 00 20 00 00 00 e0 07 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 20 08 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	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....PE..L....=.`..... "...P..... ....@.. ....@.....	success or wait	8	7FEE997835A	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2222.tmp	unknown	1621	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>user-PC\user</Author>.. </RegistrationInfo>..	success or wait	1	7FEE929A5B4	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FEEA30AEED	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FEEA30AEED	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\f89061884b75dab0e3967d7221e5290d\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FEEA39F29F	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FEEA30BA45	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.V9921e851#\85a40a6654f0aac2a2c52d1deb4d3f17\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	7FEEA39F29F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\60b77585c8aa9cfd1b30a64092c81041\System.ni.dll.aux	unknown	620	success or wait	1	7FEEA39F29F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\d1da4b8a843ec63bb8be25f8202bedc1\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FEEA39F29F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Windows.Forms\37004ddc6f466d807c52ca3b7f9f9827\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	7FEEA39F29F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\43de4a177616225e9b6262468e1c3b53\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	7FEEA39F29F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Runt73a1fc9d#\51c132146f0baa62b3cc1cc827581d0f\System.Runtime.Remoting.ni.dll.aux	unknown	1276	success or wait	1	7FEEA39F29F	ReadFile

Analysis Process: schtasks.exe PID: 2920 Parent PID: 2720

General

Start time:	20:35:13
Start date:	27/01/2021
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\XaHKwnPuj' /XML 'C:\Users\user\AppData\Local\Temp\tmp2222.tmp'
Imagebase:	0xffa90000
File size:	285696 bytes
MD5 hash:	97E0EC3D6D99E8CC2B17EF2D3760E8FC
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2222.tmp	unknown	2	success or wait	1	FFA9DB8E	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2222.tmp	unknown	1622	success or wait	1	FFA9DC8C	ReadFile

Analysis Process: vbc.exe PID: 2928 Parent PID: 2720

General

Start time:	20:35:13
Start date:	27/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0xbf0000
File size:	508928 bytes
MD5 hash:	C7B2B0FA4A71FE33536148C2584DA7DB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vbc.exe PID: 2476 Parent PID: 2720

General

Start time:	20:35:14
Start date:	27/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0xbf0000
File size:	508928 bytes
MD5 hash:	C7B2B0FA4A71FE33536148C2584DA7DB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vbc.exe PID: 2472 Parent PID: 2720

General

Start time:	20:35:14
Start date:	27/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0xbf0000
File size:	508928 bytes

MD5 hash:	C7B2B0FA4A71FE33536148C2584DA7DB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vbc.exe PID: 2456 Parent PID: 2720

General

Start time:	20:35:15
Start date:	27/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0xbf0000
File size:	508928 bytes
MD5 hash:	C7B2B0FA4A71FE33536148C2584DA7DB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: vbc.exe PID: 2884 Parent PID: 2720

General

Start time:	20:35:15
Start date:	27/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0xbf0000
File size:	508928 bytes
MD5 hash:	C7B2B0FA4A71FE33536148C2584DA7DB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis