JoeSandbox Cloud BASIC

ID: 513501
Sample Name: PO5594.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 09:25:44
Date: 02/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

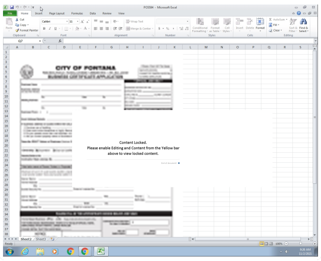
Windows Analysis Report PO5594.xlsx

Overview

General Information

Sample Name:	PO5594.xlsx
Analysis ID:	513501
MD5:	ae8569edde3fe5d.
SHA1:	fa19e7558492589.
SHA256:	eceeb9918530b8..
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



PO5594 - Microsoft Excel

CITY OF FONTANA

BUSINESS CERTIFICATE APPLICATION

Content Locked.
Please enable Editing and Content from the Yellow bar above to view locked content.

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

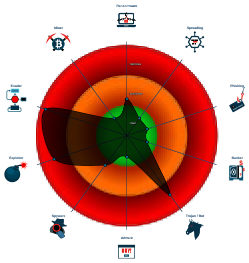
FormBook

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

Signatures

- Found malware configuration
- 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…
- Sample uses process hollowing tech…
- Uses netstat to query active network…
- Maps a DLL or memory area into an…
- Office equation editor starts process…
- Injects a PE file into a foreign proce…
- Sigma detected: Execution from Sus…
- Office equation editor drops PE file

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2124 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 2580 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
    - vbc.exe (PID: 2856 cmdline: 'C:\Users\Public\vbc.exe' MD5: 11CBFA99FB5EBE8C09674E79B9834D96)
        - vbc.exe (PID: 1868 cmdline: 'C:\Users\Public\vbc.exe' MD5: 11CBFA99FB5EBE8C09674E79B9834D96)
            - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
                - NETSTAT.EXE (PID: 2076 cmdline: C:\Windows\SysWOW64\NETSTAT.EXE MD5: 32297BB17E6EC700D0FC869F9ACAF561)
                    - cmd.exe (PID: 2036 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.passionfruitny.com/ddzw/"
  ],
  "decoy": [
    "azshalomcenter.com",
    "yumoo.design",
    "21pk.net",
    "zhauggim.xyz",
    "hoikhoinghiep.com",
    "1207rossmoyne.com",
    "izophoto.com",
    "spacex-live.net",
    "taskstudiox.com",
    "educationalsurprises.com",
    "5151vip16.com",
    "sarahannsartstudio.com",
    "indousmedicalscribing.com",
    "crossatlanticb.com",
    "codemnodum.com",
    "tvfret-america.online",
    "romualdoandrade.com",
    "creativeartsfilmacademy.club",
    "htsfrance.com",
    "bentonvilleartists.com",
    "reactivephysiorehab.com",
    "kencanatactical.com",
    "baycsolana.art",
    "komotoy.com",
    "metanetgateway.com",
    "daimondsofa.com",
    "cheese-box.online",
    "oeepa4a3bs.com",
    "consept-cafe.com",
    "thethomasgrouphomes.com",
    "marwatown.com",
    "daliborkamen.com",
    "taicholdingglobal.com",
    "palisadesstore.com",
    "adventuretravelsworld.com",
    "hamdykamal.net",
    "high-clicks3.com",
    "livebongdatv.com",
    "fiverrbetaa.xyz",
    "wardrobewish.com",
    "modsforcars.com",
    "schittstore.com",
    "toptanisimlik.com",
    "exteches.com",
    "kgkkristalljewels.com",
    "hpwdz.com",
    "talkaditown.com",
    "maininger.com",
    "preventgomohb.xyz",
    "juliamoranmartin.com",
    "flashpointyouth.com",
    "glenelg.store",
    "1courchevel.com",
    "snikido.com",
    "mikespotts.com",
    "memorylanecollections.com",
    "sportherd.com",
    "lesmariagesdesophie.com",
    "mammutphilippines.com",
    "shleppersmovingandstorage.com",
    "ervinowines.com",
    "kuwaitschoolsgame.com",
    "empiredigituseriness.com",
    "jyh8886.com"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000000.469999141.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000000.469999141.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000000.469999141.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	0x16ad9:$sqlite3step: 68 34 1C 7B E1 0x16bec:$sqlite3step: 68 34 1C 7B E1 0x16b08:$sqlite3text: 68 38 2A 90 C5 0x16c2d:$sqlite3text: 68 38 2A 90 C5 0x16b1b:$sqlite3blob: 68 53 D8 7F 8C 0x16c43:$sqlite3blob: 68 53 D8 7F 8C
00000005.00000002.507748389.00000000002F0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000002.507748389.00000000002F0000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Click to see the 31 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
5.0.vbc.exe.400000.5.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.0.vbc.exe.400000.5.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x7ba2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x138b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 0x133a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 0x139b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F 0x13b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 0x85ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 0x1261c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 0x9332:$sequence_7: 66 89 0C 02 5B 8B E5 5D 0x18da7:$sequence_8: 3C 54 74 04 3C 74 75 F4 0x19e4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.0.vbc.exe.400000.5.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	0x15cd9:$sqlite3step: 68 34 1C 7B E1 0x15dec:$sqlite3step: 68 34 1C 7B E1 0x15d08:$sqlite3text: 68 38 2A 90 C5 0x15e2d:$sqlite3text: 68 38 2A 90 C5 0x15d1b:$sqlite3blob: 68 53 D8 7F 8C 0x15e43:$sqlite3blob: 68 53 D8 7F 8C
5.2.vbc.exe.400000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.vbc.exe.400000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x7ba2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC 0x138b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 0x133a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 0x139b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F 0x13b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 0x85ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 0x1261c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 0x9332:$sequence_7: 66 89 0C 02 5B 8B E5 5D 0x18da7:$sequence_8: 3C 54 74 04 3C 74 75 F4 0x19e4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Click to see the 27 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

Machine Learning detection for dropped file

Exploits:

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

Networking:

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

Uses netstat to query active network connections and open ports

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

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
- Injects a PE file into a foreign processes
- 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

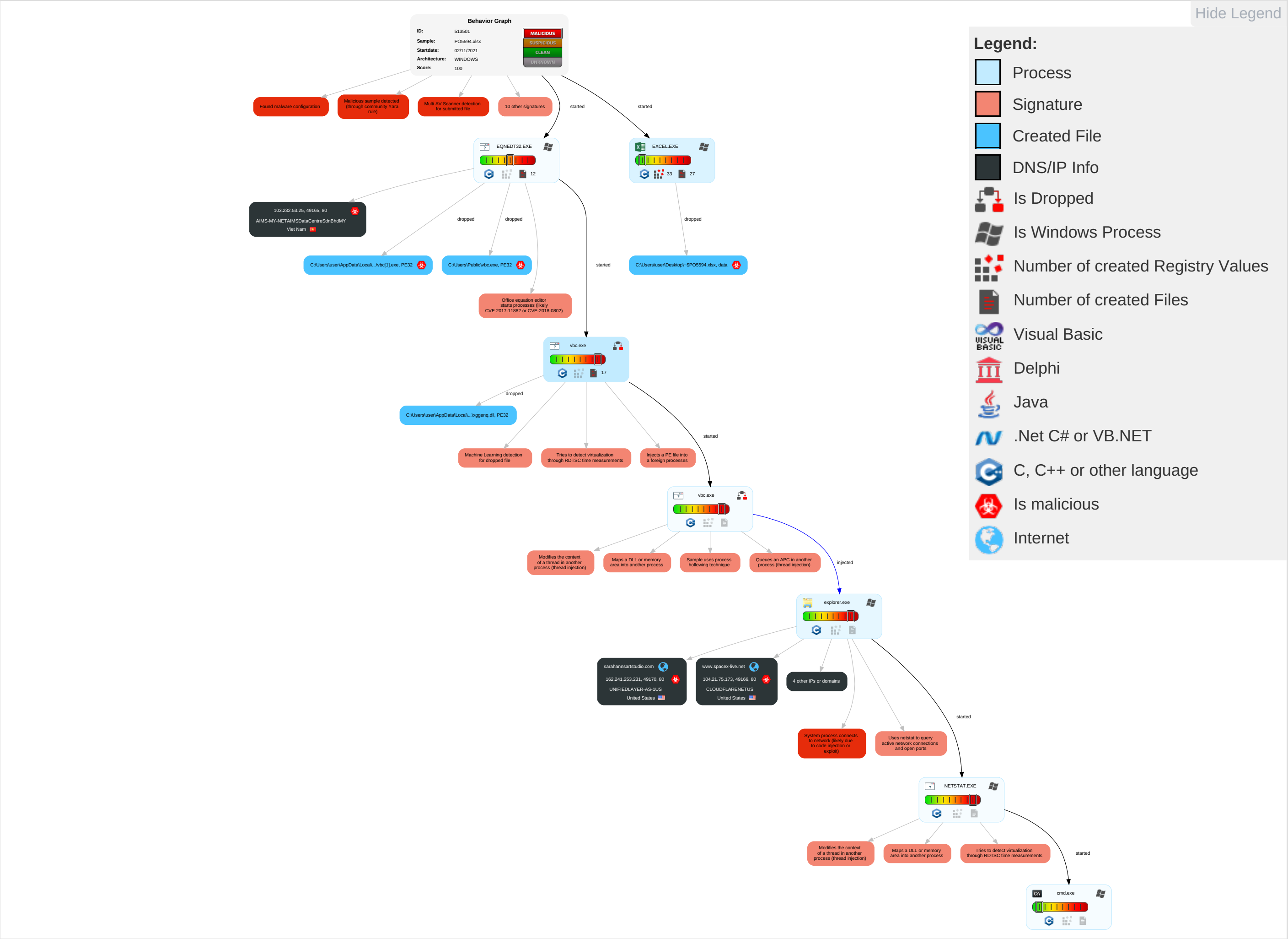
Remote Access Functionality:

- 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	Shared Modules 1	Path Interception	Process Injection 6 1 2	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 1 5 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Insec Netw Com
Default Accounts	Exploitation for Client Execution 1 3	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	Explo Redi Calls
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 6 1 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Explo Track Loca
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 1 2 2	SIM Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3	LSA Secrets	System Network Configuration Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mani Devic Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	System Network Connections Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamr Deni Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	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 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dowi Insec Proto

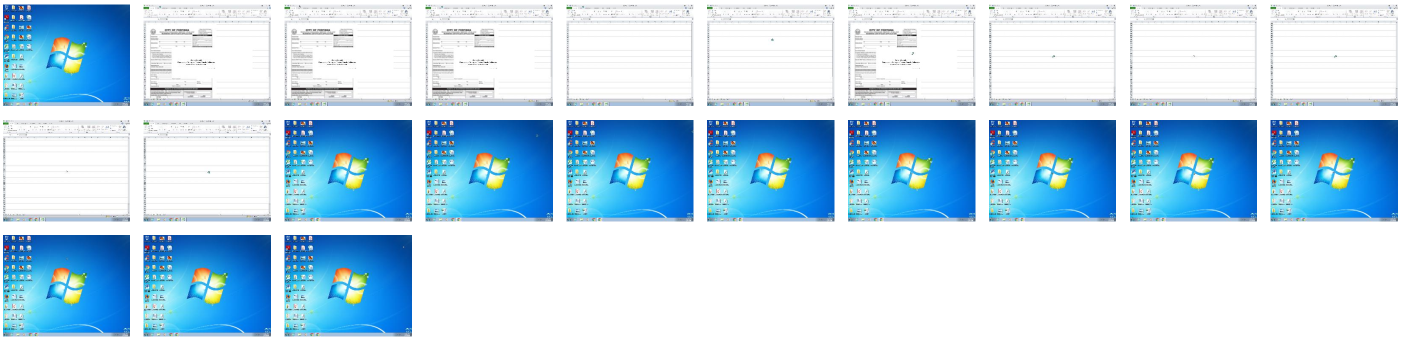
Behavior Graph

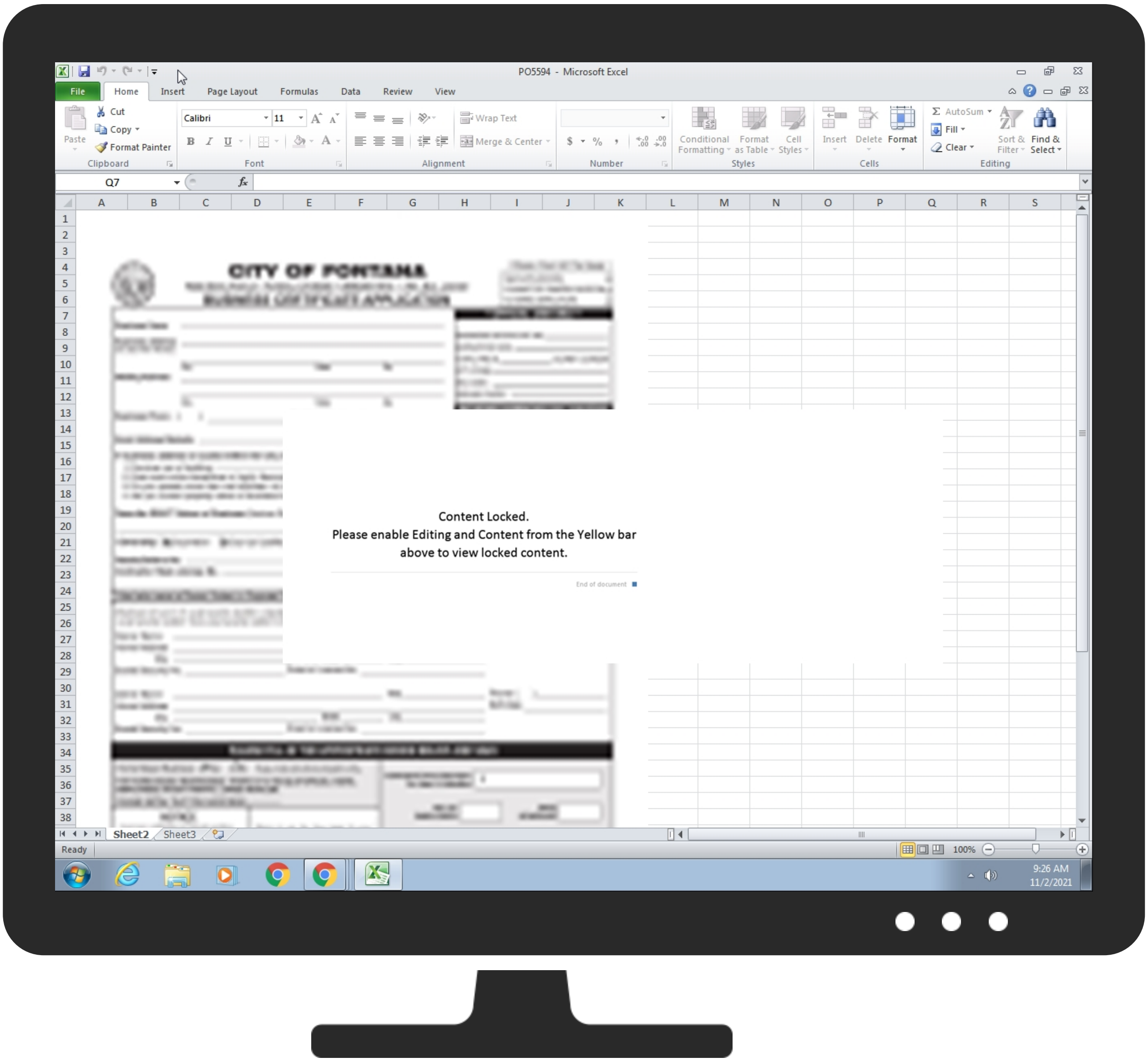

Hide Legend
Behavior Graph
ID: 513501
Sample: PO5594.xlsx
Startdate: 02/11/2021
Architecture: WINDOWS
Score: 100
MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN
Found malware configuration
Malicious sample detected (through community Yara rule)
Multi AV Scanner detection for submitted file
10 other signatures
started
started
EQNEDT32.EXE
12
EXCEL.EXE
33
27
103.232.53.25, 49165, 80
AIMS-MY-NETAIMSDataCentreSdnBhdMY
Viet Nam
dropped
dropped
dropped
started
C:\Users\user\AppData\Local\...\vbc[1].exe, PE32
C:\Users\Public\vbc.exe, PE32
C:\Users\user\Desktop\~$PO5594.xlsx, data
Office equation editor starts processes (likely CVE 2017-11882 or CVE-2018-0802)
vbc.exe
17
dropped
C:\Users\user\AppData\Local\...\xggenq.dll, PE32
started
Machine Learning detection for dropped file
Tries to detect virtualization through RDTSC time measurements
Injects a PE file into a foreign processes
vbc.exe
Modifies the context of a thread in another process (thread injection)
Maps a DLL or memory area into another process
Sample uses process hollowing technique
Queues an APC in another process (thread injection)
injected
explorer.exe
sarahannsartstudio.com
162.241.253.231, 49170, 80
UNIFIEDLAYER-AS-1US
United States
www.spacex-live.net
104.21.75.173, 49166, 80
CLOUDFLARENETUS
United States
4 other IPs or domains
System process connects to network (likely due to code injection or exploit)
Uses netstat to query active network connections and open ports
started
NETSTAT.EXE
Modifies the context of a thread in another process (thread injection)
Maps a DLL or memory area into another process
Tries to detect virtualization through RDTSC time measurements
started
cmd.exe
Legend:
Process
Signature
Created File
DNS/IP Info
Is Dropped
Is Windows Process
Number of created Registry Values
Number of created Files
Visual Basic
Delphi
Java
.Net C# or VB.NET
C, C++ or other language
Is malicious
Internet

Screenshots

Thumbnails

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





Content Locked.
Please enable Editing and Content from the Yellow bar above to view locked content.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PO5594.xlsx	32%	Virustotal		Browse
PO5594.xlsx	30%	ReversingLabs	Document-Office.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		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.vbc.exe.400000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.2.NETSTAT.EXE.4119a0.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
5.0.vbc.exe.400000.4.unpack	100%	Avira	TR/Patched.Ren.Gen2		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	TR/Crypt.ZPACK.Gen		Download File
4.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File

Source	Detection	Scanner	Label	Link	Download
5.0.vbc.exe.400000.1.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
5.0.vbc.exe.400000.0.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
5.0.vbc.exe.400000.3.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
5.0.vbc.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.2.vbc.exe.2f90000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.2.NETSTAT.EXE.27e796c.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
5.0.vbc.exe.400000.7.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.vbc.exe.400000.2.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
5.1.vbc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
sarahannsartstudio.com	3%	Virustotal		Browse

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://www.mozilla.com0	0%	URL Reputation	safe	
http://www.spacex-live.net/ddzw/?h2Mdq=Z+FzwJtUDkwgABdyd+p8UeqxtpX8YY+y3UFx7cJDGSHChxct3TL8QRd2MFxOEFehDmKc8w==&_x=gVp0dvG0DtZT6do0	0%	Avira URL Cloud	safe	
http://https://www.metanetgateway.com/ddzw/	0%	Avira URL Cloud	safe	
www.passionfruitny.com/ddzw/	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://www.schittstore.com/ddzw/?h2Mdq=eu2i37xABBm77RmOTVlK/UzsyDYSkffg03LYHul4MxZENkm7/tK6Jp9Y8VUWWe4q58P2rA==&_x=gVp0dvG0DtZT6do0	0%	Avira URL Cloud	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://https://www.metanetgateway.com/ddzw/?h2Mdq=CC4eYJ6GdM3g7jV/74DGeVNO7dTe5083KAYqQjLLOiGFZCFwrjOGC7P0J	0%	Avira URL Cloud	safe	
http://www.metanetgateway.com/ddzw/?h2Mdq=CC4eYJ6GdM3g7jV/74DGeVNO7dTe5083KAYqQjLLOiGFZCFwrjOGC7P0JmGnSxw4GGM5lA==&_x=gVp0dvG0DtZT6do0	0%	Avira URL Cloud	safe	
http://java.sun.com	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://103.232.53.25/8880/vbc.exe	0%	Avira URL Cloud	safe	
http://www.sarahannsartstudio.com/ddzw/?h2Mdq=iXrnxWa2MIQCLF3pcDg6+qoW1dWPNK8gD+C0AcHvSyjXkMlp/HpcZgrhMm+aOjdhifJKjg==&_x=gVp0dvG0DtZT6do0	0%	Avira URL Cloud	safe	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.spacex-live.net	104.21.75.173	true	true		unknown
www.metanetgateway.com	75.2.60.5	true	true		unknown
sarahannsartstudio.com	162.241.253.231	true	true	• 3%, Virustotal, Browse	unknown
schittstore.com	66.29.132.90	true	true		unknown
www.sarahannsartstudio.com	unknown	unknown	true		unknown
www.schittstore.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.spacex-live.net/ddzw/?h2Mdq=Z+FzwJtUDkwgABdyd+p8UeqxtpX8YY+y3UFx7cJDGSHChxct3TL8QRd2MFxOEFehDmKc8w==&_x=gVp0dvG0DtZT6do0	true	• Avira URL Cloud: safe	unknown
www.passionfruitny.com/ddzw/	true	• Avira URL Cloud: safe	low

Name	Malicious	Antivirus Detection	Reputation
http://www.schittstore.com/ddzw/?h2Mdq=eu2i37xABBm77RmOTVlK/UzsyDYSkffg03LYHul4MxZENkm7/tK6Jp9Y8VUWWe4q58P2rA==&_x=gVp0dvG0DtZT6do0	true	- Avira URL Cloud: safe	unknown
http://www.metanetgateway.com/ddzw/?h2Mdq=CC4eYJ6GdM3g7jV/74DGeVNO7dTe5083KAYqQjLLOiGFZCFwrjOGC7P0JmGnSxw4GGM5lA==&_x=gVp0dvG0DtZT6do0	true	- Avira URL Cloud: safe	unknown
http://103.232.53.25/8880/vbc.exe	true	- Avira URL Cloud: safe	unknown
http://www.sarahannsartstudio.com/ddzw/?h2Mdq=iXrnxWa2MIQCLF3pcDg6+qoW1dWPNK8gD+C0AcHvSyjXkMlp/HpcZgrhMm+aOjdhifJKjg==&_x=gVp0dvG0DtZT6do0	true	- Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.232.53.25	unknown	Viet Nam	🇻🇳	45668	AIMS-MY-NETAIMSDataCentreSdnBhdMY	true
66.29.132.90	schittstore.com	United States	🇺🇸	19538	ADVANTAGECOMUS	true
104.21.75.173	www.spacex-live.net	United States	🇺🇸	13335	CLOUDFLARENETUS	true
75.2.60.5	www.metanetgateway.com	United States	🇺🇸	16509	AMAZON-02US	true
162.241.253.231	sarahannsartstudio.com	United States	🇺🇸	46606	UNIFIEDLAYER-AS-1US	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	513501
Start date:	02.11.2021
Start time:	09:25:44
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO5594.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:	11
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@9/20@4/5
EGA Information:	Failed
HDC Information:	- Successful, ratio: 27.4% (good quality ratio 26.1%) - Quality average: 73.1% - Quality standard deviation: 28.8%
HCA Information:	- Successful, ratio: 86% - 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
09:26:37	API Interceptor	160x Sleep call for process: EQNEDT32.EXE modified
09:26:50	API Interceptor	35x Sleep call for process: vbc.exe modified
09:27:07	API Interceptor	214x Sleep call for process: NETSTAT.EXE modified
09:27:58	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.232.53.25	PO0945.xlsx	Get hash	malicious	Browse	- 103.232.53.25/9990/vbc.exe

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AIMS-MY-NETAIMSDataCentreSdnBhdMY	PO0945.xlsx	Get hash	malicious	Browse	- 103.232.53.25
	Confirmation Transfer Copy MT103-Ref-088091030101_PDF.exe	Get hash	malicious	Browse	- 103.232.55.66
	MVSEACON KOBE.xlsx	Get hash	malicious	Browse	- 103.232.53.184
	INVOICE56K.xlsx	Get hash	malicious	Browse	- 103.232.54.181
	INV564.xlsx	Get hash	malicious	Browse	- 103.232.54.181
	Confirmation Transfer Copy MT102-Ref-0001030101_PDF.exe	Get hash	malicious	Browse	- 103.232.55.66
	RECEIPT878.xlsx	Get hash	malicious	Browse	- 103.232.54.181
	MAERSK666.xlsx	Get hash	malicious	Browse	- 103.232.54.181
	Remittance copy.xlsx	Get hash	malicious	Browse	- 103.232.53.136
	MV MELINA.xlsx	Get hash	malicious	Browse	- 103.232.53.184
	Order_102121.xlsx	Get hash	malicious	Browse	- 103.232.53.136
	MMC Metal Corregir Cotizacin.xlsx	Get hash	malicious	Browse	- 103.232.53.42
	BM09 INV.PL.xlsx	Get hash	malicious	Browse	- 103.232.53.136
	lod4.xlsx	Get hash	malicious	Browse	- 103.232.53.136
	lod4.xlsx	Get hash	malicious	Browse	- 103.232.53.136
	lod2.xlsx	Get hash	malicious	Browse	- 103.232.53.136
	Payment_Order.xlsx	Get hash	malicious	Browse	- 103.232.53.136
	INVOICE827.xlsx	Get hash	malicious	Browse	- 103.232.54.181
	INVOICE707.xlsx	Get hash	malicious	Browse	- 103.232.54.181
	INVOICE44.xlsx	Get hash	malicious	Browse	- 103.232.54.181
ADVANTAGECOMUS	EQ034989.exe	Get hash	malicious	Browse	- 66.29.141.56
	Message.html	Get hash	malicious	Browse	- 66.29.132.29
	Message.html	Get hash	malicious	Browse	- 66.29.132.29
	RFQ#.exe	Get hash	malicious	Browse	- 66.29.137.46

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	lCFjxhAqu3.exe	Get hash	malicious	Browse	• 66.29.132.143
	dhlexcel9078.excel.exe	Get hash	malicious	Browse	• 66.29.151.197
	Proforma Invoices.exe	Get hash	malicious	Browse	• 66.29.130.249
	tgSQwVSEzE.exe	Get hash	malicious	Browse	• 66.29.130.249
	QUOTE N #U00b0 067.exe	Get hash	malicious	Browse	• 66.29.145.43
	PO08485.xlsx	Get hash	malicious	Browse	• 66.29.145.86
	3sO4kwopMH.exe	Get hash	malicious	Browse	• 66.29.130.249
	FzvFtf2XXK.exe	Get hash	malicious	Browse	• 66.29.130.249
	pKD3j672HL.exe	Get hash	malicious	Browse	• 66.29.130.249
	dec.exe	Get hash	malicious	Browse	• 66.29.141.211
	PkF9Fg2Tnc.exe	Get hash	malicious	Browse	• 66.29.142.214
	2WK7SGkGVZ.exe	Get hash	malicious	Browse	• 66.29.130.249
	jnnbbMX9Ch.exe	Get hash	malicious	Browse	• 66.29.130.249
	vbc.exe	Get hash	malicious	Browse	• 66.29.130.249
	PURCHASE ORDER 29kva.exe	Get hash	malicious	Browse	• 66.29.145.99
	CpUNO6WMEm.exe	Get hash	malicious	Browse	• 66.29.130.249

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):	292696
Entropy (8bit):	7.940580532253791
Encrypted:	false
SSDEEP:	6144:wBlL/cZwF4JmEVpM2MJhVRcGO+LTYKJhUVTj9qsYKGV77ECn:CeZUSpMHwf4YRqsWvn
MD5:	11CBFA99FB5EBE8C09674E79B9834D96
SHA1:	6E94C5EF59E7A989D93C799217FBF1803B3BB4A4
SHA-256:	B7F38916FF521E44E651031EE54E631805F13963BAAF6FF6E3CC1AA72F1D0A43
SHA-512:	8429269ED2A747CF11DB3972AFA4A7A0CD59B4EA61D6D189EB17B660A66DD2A7FDEB6CD4F4439044665069060477F856D588634B0CF01F5F67CD6A039FE00CD
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://103.232.53.25/8880/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...e:.V.................\...........0.......p....@...t...p..|...........................te xt....Z.......\.................. ..`.rdata.......p.......`..............@..@.data...8............r..............@....ndata.......P...........................rsrc................x..............@..@.. ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2962AA49.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2962AA49.png

Malicious:	false
Reputation:	moderate, very likely benign file
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\2DD5845C.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1295 x 471, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	68702
Entropy (8bit):	7.960564589117156
Encrypted:	false
SSDEEP:	1536:Hu2p9Cy+445sz12HnOFIr0Z7gK8mhVgSKe/6mLsw:O2p9w1HCIOTKEhQw
MD5:	9B8C6AB5CD2CC1A2622CC4BB10D745C0
SHA1:	E3C68E3F16AE0A3544720238440EDCE12DFC900E
SHA-256:	AA5A55A415946466C1D1468A6349169D03A0C157A228B4A6C1C85BFD95506FE0
SHA-512:	407F29E5F0C2F993051E4B0C81BF76899C2708A97B6DF4E84246D6A2034B6AFE40B696853742B7E38B7BBE7815FCCCC396A3764EE8B1E6CFB2F2EF399E8FC71
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG........IHDR.....................pHYs..........+......tIME......&...T....tEXtAuthor....H....tEXtDescription...!#....tEXtCopyright....:....tEXtCreation time.5.......tEXtSoftware.]p.:....t EXtDisclaimer.........tEXtWarning........tEXtSource.........tEXtComment........tEXtTitle....'.. .IDATx...y|T.?..l..3. .$.D..(v....Q.q.....W.[...Z..-.*Hlmm...4V..BU..V@,h.t.....}...cr.3.... ...B3s.....\|.}.G6j.t.Qv..-Q9...r\""""""""".H9...Y..*.v...........7........Q..^t{P..C..""""""""""".e..n@7B.{Q.S.HDDDDDDDD...........\bxHDDDDDDDDD.1<$"""""""""......d2Y@9`@c.v..8P...0`.. a|.....<... ..+...[""""""""""".....~..,........+.t..._..o.....8z.$ ..U.Mp".....Z8.a;.B..'...y..I^......e........,}.+.M..K...M...A.7.Z[[.E.....B...nF.:5..""""""""".(.....d.3*..E.=...[o...o.....n..._.{..-..M.3....px (.5..4lt..&....d.R!.......!.$''.n.....X,..__ar.d..0 .M#""""""""..S...T...Ai.8P^XX(..d.....u[.f...8........[`...q..9R../.....v.b.5.r`.[.A..a.....a6......S.o.h7...........g..v..+.~.oB.H..|..8...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3275C968.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 338 x 143, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	6364
Entropy (8bit):	7.935202367366306
Encrypted:	false
SSDEEP:	192:joXTTTt+cmcZjbF/z2sA9edfxFHTeDELxExDR:joXTTTEc5ZjR/zI9EfjTeDEGxDR
MD5:	A7E2241249BDCC0CE1FAAF9F4D5C32AF
SHA1:	3125EA93A379A846B0D414B42975AADB72290EB4
SHA-256:	EC022F14C178543347B5F2A31A0BFB8393C6F73C44F0C8B8D19042837D370794
SHA-512:	A5A49B2379DF51DF5164315029A74EE41A2D06377AA77D24A24D6ADAFD3721D1B24E5BCCAC72277BF273950905FD27322DBB42FEDA401CA41DD522D0AA3041 C
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG........IHDR...R...........S.....sRGB.........gAMA......a.....pHYs..........o.d...!tEXtCreation Time.2018:08:27 10:23:35Z......DIDATx^....M......3c0f0.2.9o.......-..r..:.V*.ty. .MEJ.^.$G.T.AJ.J.n.....0.`...B...g=....{..5.1...\|.g.z..Y.._...3k..y............@JD...)..KQ.........f.DD.1.....@JD...)..K..DD.1.....@JD...)..K..DD.1.....@JD...)..K..DD.....9.sdKv.\.R[...k...E ..3....ee.!..Wl...E&6.\.]..'K...x.O..%.EE..'...}..[c....?n..R...V..U5!.Rt...-xw*.....#..._....I....k.!":...H.....eKN.....9....{%......*7..6Y.."......P....."ybQ.....JJ`z..%..a.$<m.n'..[.f0~..r.........-.q... {.Mu3.yX...\...5.a.zNX.9..-.[......QU.r .qZ...&.{....$..`.Lu..]Z^'.].k|.z.3....H.../...k7.1>y.D..._x...........=.u.?ee.9.'.11:={.t]....)..k...F@P|f....9...K>...{...}...h9.b..h....w.....A~...u..j. 9..x..C=.JJ.h....K2.... .../I..=3C.6k.]...JD.....:tP.e...-+*...}..\.Yrss4...i.f..A7I...u.M....v.uY_.V|.].-Oo..........._.;@c....`.....|.R7>^...j*S...{...w.iV..UR..SJ.hy.W3...2Q@f......,.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\35BED6CA.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 130 x 176, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	19408
Entropy (8bit):	7.931403681362504
Encrypted:	false
SSDEEP:	384:6L3Vdo4yxL8FNgQ9jYtUO5Zn4tIlQ1Yes7D6PhbXngFfZdQTEfn4n6EVPBo6a:2exL8rgQ2tVF4GlQUuZXnYfTs6EJiL
MD5:	63ED10C9DF764CF12C64E6A9A2353D7D
SHA1:	608BE0D9462016EA4F05509704CE85F3DDC50E63
SHA-256:	4DAC3676FAA787C28DFA72B80FE542BF7BE86AAD31243F63E78386BC5F0746B3
SHA-512:	9C633C57445D67504E5C6FE4EA0CD84FFCFECFF19698590CA1C4467944CD69B7E7040551A0328F33175A1C698763A47757FD625DA7EF01A98CF6C585D439B4A
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\35BED6CA.png	
Preview:	.PNG........IHDR.............L.!... .IDATx..g.].y&X'...{;.t@F. .. .D*Q.eI..#[.5~lK3...z.3.gw...^.=;.FV..%..d..%R..E......F.ts<..X..f..F..5|..s..:Uu.W.U....!.9...A..u/...g.w......lx...pG..2.. x..w..!...w.pG..2..x..w..!.....m.a>.....R........x.IU[.A.....].Y.L..!....|AQ.h4....x..\6....|.i..]..Q..(...C..A..Z... (j.f4..u=..o.D.oj....y6......)I.......G.{zn.M,...?#..,...|....y....G.LOO..?.....7..- .>.._.m[.........q.O}..G....?....h4.=t..c...eY.........3g..|0...x...|..../F....o.._|...?.O..........c..x._..7vF..0.....B>.....}{..V....P(.....c.....4...s...K.K."c(.....}.0......._z...}..y<<.......<..^.7....k. r.W~..c._.....$J....:.w._~.........._..Wp.....q........G..vA.D.E......"...?...'....}nvv....^.^.42..f....Q(..$...`(vidd..8......y.Z{...L.~...k....z....@@0...Bk..?.r..7...9u...w.>w.C..j.n..a..V.?..?...e s#.G...l.&I..)..).J..>...+Mn.^.W.._....D...".}..k......8.N_.v..>.y.@0..,/.........>.a...........z.]../.r ..../3.....?.z..g.Z.....l0.L.S....._../.r

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3AC55E10.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	498420
Entropy (8bit):	0.6413453967611162
Encrypted:	false
SSDEEP:	384:bKXXwBkNWZ3cJuUvmWnTG+W4DH8ddxzsFfW3:AXwBkNWZ3cjvmWa+VDO
MD5:	253092ED7FC7A11EB7E73246CFCFF53D
SHA1:	B85995DB5C152CD0E2B9780C2AA0F75FC5A0C93E
SHA-256:	D5884EA5800BC2CAEA17513994955FBC6DC7040EBBBB5011EE96A44AC8511DEA
SHA-512:	2C838D963E9111A2919E008516D6AE1A03A24680C3C28856169A4DDD96684B7FDB0B43554F9C65063EC6A02D454FAF39E40C164292716798ED1CDDCEC53557F
Malicious:	false
Preview:	....l...............2...........m>..C... EMF........&..\K..hC..F...,... ...EMF+.@.................X...X...F...\...P...EMF+"@...........@..........$@..........0@.............? !@...........@...%...........%..................................R...p..............................@."C.a.l.i.b.r.i...\$.......f.\.@F.%...... ....RQQ^...\|.........h..$QQ^...|.. ...Id.\\|..... ....d.\.......................................%...X...%...7..................{$.................C.a.l.i.b.r.i.............X...\|......8.\........dv......%........... %...........%...........!..............................."...........%...........%...........%...........T...T.........................@.E.@....2.......L.......................P... ...6...F....F...F..EMF+*@..$..........?.......... .?.........@...........@..........*@..$..........?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\539060AD.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 130 x 176, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	14828
Entropy (8bit):	7.9434227607871355
Encrypted:	false
SSDEEP:	384:zIZYVvfv3ZOxvHe5EmlbliA2r1BMWWTXRRO/QX:Td3Z46xiXzW/kO
MD5:	58DD6AF7C438B638A88D107CC87009C7
SHA1:	F25E7F2F240DC924A7B48538164A5B3A54E91AC6
SHA-256:	9269180C35F7D393AB5B87FB7533C2AAA2F90315E22E72405E67A0CAC4BA453A
SHA-512:	C1A3543F221FE7C2B52C84F6A12607AF6DAEF60CCB1476D6D3E957A196E577220801194CABC18D6A9A8269004B732F60E1B227C789A9E95057F282A54DBFC80
Malicious:	false
Preview:	.PNG........IHDR.............L.!... .IDATx..gp\.y>~v...WTb... ...!.M.H...d.J..3.8.(.L&.lM.d.o..$..q.D.I.....k,J.b3%QD!.Bt,.........p.+.....x?`....{.9o..W.q.Y.gM.g=.5"dm.V..M...iX.. 6....g=.R(..N'.0&.I(..B2..\...\|.t......R.T.......J...Q.U....F.I..B.\...B.Z-....D")..,.J.....u..1.#....A.P.i..!...3.U1....RI..9....:..~..r..N.....Je,...l...(..CCC...v....a.l6KQ...ooo...d.fxx...k``...5. N.\.S.N...e2............b..7..8@.tgg.}..Ue7..e.G .`.J.d2)..B!M..r..T*Q.%..X.......{....,.q.\,.E".........z..*.abbB*...j.\.J.(.b.......\|>...........R....L&..X.eYV"..-.R)B.T*M&..pX*.j.Z..9..F. Z.6....b.\./%..~...).B<..T*.z..D"..(...\...d2YKKK...mm.T*..l.T*..I$.x<..J..q..*.J .X..O>...C.d2.JI...:...#....xkk.B.(....D .8..t:..o>...:vC%MNNj.ZHZ....`.T....,...A.....l$.q.\f.....eY..8.+.. ..`dd.b.X,.BH.T..4-..x.EV.|&.p.......O.P(.J.\>66.a.X,...><<....V.R.T*....d2.;v.....W.511.u.a....'..'...zkk.m.t:]__...ggg.o.............Y..z..a.....{..%.H..f...nw*..........'ND"...P(D"... .H. .|>/.Hd2....EQ.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\7E36B934.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 130 x 176, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	19408
Entropy (8bit):	7.931403681362504
Encrypted:	false
SSDEEP:	384:6L3Vdo4yxL8FNgQ9jYtUO5Zn4tIlQ1Yes7D6PhbXngFfZdQTEfn4n6EVPBo6a:2exL8rgQ2tVF4GlQUuZXnYfTs6EJiL
MD5:	63ED10C9DF764CF12C64E6A9A2353D7D
SHA1:	608BE0D9462016EA4F05509704CE85F3DDC50E63
SHA-256:	4DAC3676FAA787C28DFA72B80FE542BF7BE86AAD31243F63E78386BC5F0746B3
SHA-512:	9C633C57445D67504E5C6FE4EA0CD84FFCFECFF19698590CA1C4467944CD69B7E7040551A0328F33175A1C698763A47757FD625DA7EF01A98CF6C585D439B4A
Malicious:	false
Preview:	.PNG........IHDR.............L.!... .IDATx..g.].y&X'...{;.t@F. .. .D*Q.eI..#[.5~lK3...z.3.gw...^.=;.FV..%..d..%R..E......F.ts<..X..f..F..5|..s..:Uu.W.U....!.9...A..u/...g.w......lx...pG..2.. x..w..!...w.pG..2..x..w..!.....m.a>.....R........x.IU[.A.....].Y.L..!....|AQ.h4....x..\6....|.i..]..Q..(...C..A..Z... (j.f4..u=..o.D.oj....y6......)I.......G.{zn.M,...?#..,...|....y....G.LOO..?.....7..- .>.._.m[.........q.O}..G....?....h4.=t..c...eY.........3g..|0...x...|..../F....o.._|...?.O..........c..x._..7vF..0.....B>.....}{..V....P(.....c.....4...s...K.K."c(.....}.0......._z...}..y<<.......<..^.7....k. r.W~..c._.....$J....:.w._~.........._..Wp.....q........G..vA.D.E......"...?...'....}nvv....^.^.42..f....Q(..$...`(vidd..8......y.Z{...L.~...k....z....@@0...Bk..?.r..7...9u...w.>w.C..j.n..a..V.?..?...e s#.G...l.&I..)..).J..>...+Mn.^.W.._....D...".}..k......8.N_.v..>.y.@0..,/.........>.a...........z.]../.r ..../3.....?.z..g.Z.....l0.L.S....._../.r

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\96660C3F.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\96660C3F.png	
File Type:	PNG image data, 130 x 176, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	14828
Entropy (8bit):	7.9434227607871355
Encrypted:	false
SSDEEP:	384:zIZYVvfv3ZOxvHe5EmlbliA2r1BMWWTXRRO/QX:Td3Z46xiXzW/kO
MD5:	58DD6AF7C438B638A88D107CC87009C7
SHA1:	F25E7F2F240DC924A7B48538164A5B3A54E91AC6
SHA-256:	9269180C35F7D393AB5B87FB7533C2AAA2F90315E22E72405E67A0CAC4BA453A
SHA-512:	C1A3543F221FE7C2B52C84F6A12607AF6DAEF60CCB1476D6D3E957A196E577220801194CABC18D6A9A8269004B732F60E1B227C789A9E95057F282A54DBFC807
Malicious:	false
Preview:	.PNG........IHDR.............L.!... .IDATx..gp\.y>~v...WTb... ...!.M.H...d.J..3.8.(.L&.lM.d.o..$..q.D.I.....k,J.b3%QD!.Bt,.........p.+.....x?`....{.9o..W.q.Y.gM.g=.5"dm.V..M...iX..6....g=.R(..N'.0&.I(..B2..\...\|.t......R.T.......J...Q.U....F.I..B.\...B.Z-....D")..,.J.....u..1.#....A.P.i..!...3.U1....RI..9....:..~..r..N.....Je,...l...(..CCC...v....a.l6KQ...ooo...d.fxx...k``...5.N.\.S.N...e2............b..7..8@.tgg.}..Ue7..e.G .`.J.d2)..B!M..r..T*Q.%..X.......{...,.q.\,.E"........z..*.abbB*...j.\.J.(.b.......\|>...........R....L&..X.eYV"..-.R)B.T*M&..pX*.j.Z..9..F.Z.6....b.\./%..~...).B<..T*.z..D"..(...\...d2YKKK...mm.T*..l.T*..I$.x<..J..q..*.J .X..O>...C.d2.JI...:...#....xkk.B.(....D .8..t:..o>...:vC%MNNj.ZHZ....`.T....,...A.....l$.q.\f.....eY..8.+....`dd.b.X,.BH.T..4-..x.EV.|&.p.......O.P(.J.\>66.a.X,...><<....V.R.T*....d2.;v.....W.511.u.a....'..'...zkk.m.t:]__...ggg.o.............Y..z..a.....{..%.H..f...nw*..........'ND"...P(D"... .H..|>/.Hd2....EQ.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AFCBBB6.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1295 x 471, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	68702
Entropy (8bit):	7.960564589117156
Encrypted:	false
SSDEEP:	1536:Hu2p9Cy+445sz12HnOFIr0Z7gK8mhVgSKe/6mLsw:O2p9w1HCIOTKEhQw
MD5:	9B8C6AB5CD2CC1A2622CC4BB10D745C0
SHA1:	E3C68E3F16AE0A3544720238440EDCE12DFC900E
SHA-256:	AA5A55A415946466C1D1468A6349169D03A0C157A228B4A6C1C85BFD95506FE0
SHA-512:	407F29E5F0C2F993051E4B0C81BF76899C2708A97B6DF4E84246D6A2034B6AFE40B696853742B7E38B7BBE7815FCCCC396A3764EE8B1E6CFB2F2EF399E8FC715
Malicious:	false
Preview:	.PNG........IHDR.....................pHYs..........+......tIME......&...T....tEXtAuthor....H....tEXtDescription...!#....tEXtCopyright....:....tEXtCreation time.5.......tEXtSoftware.]p.:....tEXtDisclaimer.........tEXtWarning........tEXtSource.........tEXtComment........tEXtTitle....'.. .IDATx...y|T.?..l..3. .$.D..(v....Q.q.....W.[...Z..-.*Hlmm...4V..BU..V@,h.t.....}...cr.3.......B3s.....\|.}.G6j.t.Qv..-Q9...r\"""""""""".H9...Y..*.v...........7........Q..^t{P..C.."""""""""""".e..n@7B.{Q.S.HDDDDDDDD...........\bxHDDDDDDDDD.1<$""""""""""......d2Y@9`@c.v..8P...0`..a|.....<... ..+...[""""""""""".....~..,........+.t..._..o.....8z.$ ..U.Mp".....Z8.a;.B..'...y..I^......e........,}.+.M..K...M...A.7.Z[[.E.....B...nF.:5.."""""""""".(.....d.3*..E.=...[o...o.....n..._.{..-..M.3....px(.5..4lt..&....d.R!.......!.$''.n.....X,..__ar.d..0 .M#"""""""""..S...T...Ai.8P^XX(..d.....u[.f...8........[`...q..9R../.....v.b.5.r`.[.A..a.....a6......S.o.h7...........g..v..+.~.oB.H..|..8...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\BDFF6443.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\C46E2207.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C46E2207.png

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.).JI).".....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..&..%I.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Temp\nskF049.tmp\xggenq.dll

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (DLL) (native) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	103424
Entropy (8bit):	6.478883962622834
Encrypted:	false
SSDEEP:	1536:KyadpihizxoDXPNiYLe3ZLpdzYy19k3ncMlN7kOES9OO2nsWjcdIbUFaZVak:KyKiOLVnINSyOBIIbeaZVak
MD5:	E811908E17195BEA88661A6C3CB92B91
SHA1:	890857EF9EE4D3785086F3B86AB83AC8B913AEE9
SHA-256:	A9DF42DC541C9BAB258C914C002426C359B253D7425C5E6038E7384A1CF572FB
SHA-512:	5F5FA14FD98D699A37BF9F55E3D25F567F58179611C1DC1E56BEDE39F873CE731B33BCDC7C6D70C13D66DFB2130CF94D2412B9A295D4D79A138684FD1091D0
Malicious:	false
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$............~.J.~.J.~.J...J.~.J.,.J.~.J.,#J.~.J.,.J.~.J...K.~.J...K.~.J.~.J.~.J ...K.~.J...K.~.J...J.~.J...K.~.JRich.~.J........PE..L...I..a...........!..@..........................U..L...\U..O...................... ....O..@..text.............................. ..`.rdata...N.......P..................@..@.data....O...`...4...P..............@....rsrc..............................@..B.reloc........ ....@..B... ....

C:\Users\user\AppData\Local\Temp\w8ymj9mvxgy277qah473

Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	219333
Entropy (8bit):	**7.993174761144856**
Encrypted:	**true**
SSDEEP:	6144:WzcaN9fxkj0h27+aaZMK4sjGNATBmebit:Wzcu6O26f4sGjaq
MD5:	9F1DA5BF76CEE0067C0B852BC020ACC2
SHA1:	279BC1BAE6875A60E06039FFB146138DEAD7C6CF
SHA-256:	19057A959E5166348C03A91D7D147D124775A8A438E6B6E47288C5EF635BE16A
SHA-512:	362D19A989B5713BE9A5D953B5071A723C06B9AE6583276FDB91FA46C55A970084403B853389F1F8FBCB6DDDBA91908B2DBFD456BD79D8D6E18681A0D8E0386
Malicious:	false
Preview:	.U+.Y...f......uj.....iO.!.........*.....yT.....f.....2S|.....2...]..8.Gm.>...4.b.e.}........=.n. M.....7~9.-/..lt...pIa...'^.....1$........)s.b.......X..uR.."yGU..9......e..{....2....-..9.....d?...G\.3q....].. ......c}..K.....Mm...Q.=..?....<R.4...f.O.9...t...c...I..........*.....yT.....f.....2S|.....g&S.,gV>.....s.G...r.2m.iv(..:.Y......:C.....B.u.._....pIa.ct..P.*.....R(..rf,...I....k.;.)..~C..1.X...2Xva. &.&e..M.......A.....9.....d..."\....]........c}......^...m..~.Q.=..?....<f.4...fw..9%..t.....qZI.>........*.....yT.....f.....2S|.....g&S.,gV>.....s.G...r.2m.iv(..:.Y......:C.....B.u.._....pIa.ct..P.*.....R(..rf ,...I....k.;.)..~C..1.X...2Xv.....e..wf.....PU...9.....d..."\......]........c}......^...m..~.Q.=..?....<f.4...fw..9%..t.....qZI.>........*.....yT.....f.....2S|.....g&S.,gV>.....s.G...r.2m.iv(..:.Y......:C.....B .u.._....pIa.ct..P.*.....R(..rf,...I....k.;.)..~C..1.X...2Xv.....e..wf.....PU...9.....d..."\......]........c}

C:\Users\user\AppData\Local\Temp\~DF50F0E8E5645B9254.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:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34 FE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF5D47A23D2FA502C9.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:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34 FE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFF46076212F85A030.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:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34 FE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DFFBA49336F871D2DD.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	CDFV2 Encrypted
Category:	dropped
Size (bytes):	190424
Entropy (8bit):	7.96227380481848
Encrypted:	false
SSDEEP:	3072:fetf+Tozc7CM5/lSqtarCMAch5AQZBgZdq3n4AZeyxfIAkLTmjeZYHPIMedWZ6Pa:feqMc+M5d6rASAQfgYZeyxqLTmjeddWt
MD5:	AE8569EDDE3FE5D5E50F9669BBBA54B0
SHA1:	FA19E75584925894B781BCDB1DC53C6B024F7B08
SHA-256:	ECEEB9918530B8AB023A2465BACC9C2E572C7AAA7ADD05DF882E49C28FBE6E5B
SHA-512:	A5A37A10D622A7897A38F8FB9DC17EC91E94E08D650A3E988A45EBFF3B047FBD86AEB156461AF70874E8E2CCFBDE879505314AF342BB340CE7B07926A3D1B2 5
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\Desktop\~$PO5594.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:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58

C:\Users\user\Desktop\~$PO5594.xlsx

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, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	292696
Entropy (8bit):	7.940580532253791
Encrypted:	false
SSDEEP:	6144:wBlL/cZwF4JmEVpM2MJhVRcGO+LTYKJhUVTj9qsYKGV77ECn:CeZUSpMHwf4YRqsWvn
MD5:	11CBFA99FB5EBE8C09674E79B9834D96
SHA1:	6E94C5EF59E7A989D93C799217FBF1803B3BB4A4
SHA-256:	B7F38916FF521E44E651031EE54E631805F13963BAAF6FF6E3CC1AA72F1D0A43
SHA-512:	8429269ED2A747CF11DB3972AFA4A7A0CD59B4EA61D6D189EB17B660A66DD2A7FDEB6CD4F44390446650690604 77F856D588634B0CF01F5F67CD6A039FE00CD
Malicious:	**true**
Antivirus:	- Antivirus: Joe Sandbox ML, Detection: 100%
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...e:.V................\...........0.......p....@...t...p..|...........................text....Z.......\.................. ..`.rdata.......p.......`..............@..@.data...8............r..............@....ndata.......P...........................rsrc................x..............@..@...

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.96227380481848
TrID:	- Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	PO5594.xlsx
File size:	190424
MD5:	ae8569edde3fe5d5e50f9669bbba54b0
SHA1:	fa19e75584925894b781bcdb1dc53c6b024f7b08
SHA256:	eceeb9918530b8ab023a2465bacc9c2e572c7aaa7add05 df882e49c28fbe6e5b
SHA512:	a5a37a10d622a7897a38f8fb9dc17ec91e94e08d650a3e9 88a45ebff3b047fbd86aeb156461af70874e8e2ccfbde879 505314af342bb340ce7b07926a3d1b285
SSDEEP:	3072:fetf+Tozc7CM5/lSqtarCMAch5AQZBgZdq3n4AZeyxfIAkLTmjeZYHPIMedWZ6Pa:feqMc+M5d6rASAQfgYZeyxqLTmjeddWt
File Content Preview:	.......................>..

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 2, 2021 09:28:15.107445002 CET	192.168.2.22	8.8.8.8	0xc18c	Standard query (0)	www.spacex-live.net	A (IP address)	IN (0x0001)
Nov 2, 2021 09:28:25.225115061 CET	192.168.2.22	8.8.8.8	0xfc43	Standard query (0)	www.schittstore.com	A (IP address)	IN (0x0001)
Nov 2, 2021 09:28:30.676491022 CET	192.168.2.22	8.8.8.8	0x9c63	Standard query (0)	www.metanetgateway.com	A (IP address)	IN (0x0001)
Nov 2, 2021 09:28:36.070918083 CET	192.168.2.22	8.8.8.8	0x30e0	Standard query (0)	www.sarahannsartstudio.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 2, 2021 09:28:15.142863035 CET	8.8.8.8	192.168.2.22	0xc18c	No error (0)	www.spacex-live.net		104.21.75.173	A (IP address)	IN (0x0001)
Nov 2, 2021 09:28:15.142863035 CET	8.8.8.8	192.168.2.22	0xc18c	No error (0)	www.spacex-live.net		172.67.179.179	A (IP address)	IN (0x0001)
Nov 2, 2021 09:28:25.263832092 CET	8.8.8.8	192.168.2.22	0xfc43	No error (0)	www.schittstore.com	schittstore.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 09:28:25.263832092 CET	8.8.8.8	192.168.2.22	0xfc43	No error (0)	schittstore.com		66.29.132.90	A (IP address)	IN (0x0001)
Nov 2, 2021 09:28:30.724009991 CET	8.8.8.8	192.168.2.22	0x9c63	No error (0)	www.metanetgateway.com		75.2.60.5	A (IP address)	IN (0x0001)
Nov 2, 2021 09:28:36.195832014 CET	8.8.8.8	192.168.2.22	0x30e0	No error (0)	www.sarahannsartstudio.com	sarahannsartstudio.com		CNAME (Canonical name)	IN (0x0001)
Nov 2, 2021 09:28:36.195832014 CET	8.8.8.8	192.168.2.22	0x30e0	No error (0)	sarahannsartstudio.com		162.241.253.231	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 103.232.53.25
- www.spacex-live.net
- www.schittstore.com
- www.metanetgateway.com
- www.sarahannsartstudio.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	103.232.53.25	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Nov 2, 2021 09:26:55.926331043 CET	0	OUT	GET /8880/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: 103.232.53.25 Connection: Keep-Alive

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Nov 2, 2021 09:26:56.184113979 CET</td><td>1</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Tue, 02 Nov 2021 08:27:00 GMT
Server: Apache/2.4.49 (Win64) OpenSSL/1.1.1l PHP/7.4.24
Last-Modified: Tue, 02 Nov 2021 03:24:30 GMT
ETag: "47758-5cfc5d4e71e00"
Accept-Ranges: bytes
Content-Length: 292696
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 65 3a ff 56 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 5c 00 00 00 d6 01 00 00 04 00 00 fb 30 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 e0 02 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 18 74 00 00 a0 00 00 00 00 d0 02 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 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 eb 5a 00 00 00 10 00 00 00 5c 00 00 00 04 00 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 96 11 00 00 00 70 00 00 00 12 00 00 00 60 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 38 b0 01 00 00 90 00 00 00 06 00 00 00 72 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 50 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 d0 02 00 00 0a 00 00 00 78 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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@QFRichQFPELe:V\0p@tp|.textZ\ `.rdatap`@@.data8r@.ndataP.rsrcx@@</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	104.21.75.173	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 2, 2021 09:28:15.177232027 CET	315	OUT	GET /ddzw/?h2Mdq=Z+FzwJtUDkwgABdyd+p8UeqxtpX8YY+y3UFx7cJDGSHChxct3TL8QRd2MFxOEFehDmKc8w==&_x=gVp0dvG0DtZT6do0 HTTP/1.1 Host: www.spacex-live.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 2, 2021 09:28:15.206080914 CET	316	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 02 Nov 2021 08:28:15 GMT Transfer-Encoding: chunked Connection: close Cache-Control: max-age=3600 Expires: Tue, 02 Nov 2021 09:28:15 GMT Location: https://www.spacex-live.net/ddzw/?h2Mdq=Z+FzwJtUDkwgABdyd+p8UeqxtpX8YY+y3UFx7cJDGSHChxct3TL8QRd2MFxOEFehDmKc8w==&_x=gVp0dvG0DtZT6do0 Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=Or3FV13v2reNYN%2BWp%2F8vpijU8YUbETOgTka3tg7j%2FeZQv8MrFazDzgubmUsk0Z%2BUmvmnRtuyBlKbzhU3UmYTTucW83rZgvHdwXFjE%2F967z36ZLASYwl%2FRekDeZWqQJOXG1LZaPdx"}],"group":"cf-nel","max_age":604800} NEL: {"success_fraction":0,"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 6a7bfd02eaeb4ee6-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49168	66.29.132.90	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 2, 2021 09:28:25.442976952 CET	316	OUT	GET /ddzw/?h2Mdq=eu2i37xABBm77RmOTVlK/UzsyDYSkffg03LYHul4MxZENkm7/tK6Jp9Y8VUWWe4q58P2rA==&_x=gVp0dvG0DtZT6do0 HTTP/1.1 Host: www.schittstore.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 2, 2021 09:28:25.625227928 CET	318	IN	HTTP/1.1 301 Moved Permanently keep-alive: timeout=5, max=100 content-type: text/html content-length: 707 date: Tue, 02 Nov 2021 08:28:25 GMT server: LiteSpeed location: https://www.schittstore.com/ddzw/?h2Mdq=eu2i37xABBm77RmOTVlK/UzsyDYSkffg03LYHul4MxZENkm7/tK6Jp9Y8VUWWe4q58P2rA==&_x=gVp0dvG0DtZT6do0 x-turbo-charged-by: LiteSpeed connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 31 30 30 25 22 3e 0a 3c 68 65 61 64 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 73 68 72 69 6e 6b 2d 74 6f 2d 66 69 74 3d 6e 6f 22 20 2f 3e 0a 3c 74 69 74 6c 65 3e 20 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 20 73 74 79 6c 65 3d 22 63 6f 6c 6f 72 3a 20 23 34 34 34 3b 20 6d 61 72 67 69 6e 3a 30 3b 66 6f 6e 74 3a 20 6e 6f 72 6d 61 6c 20 31 34 70 78 2f 32 30 70 78 20 41 72 69 61 6c 2c 20 48 65 6c 76 65 74 69 63 61 2c 20 73 61 6e 73 2d 73 65 72 69 66 3b 20 68 65 69 67 68 74 3a 31 30 30 25 3b 20 62 61 63 6b 67 72 6f 75 6e 64 2d 63 6f 6c 6f 72 3a 20 23 66 66 66 3b 22 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 68 65 69 67 68 74 3a 61 75 74 6f 3b 20 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 3b 20 22 3e 20 20 20 20 20 3c 64 69 76 20 73 74 79 6c 65 3d 22 74 65 78 74 2d 61 6c 69 67 6e 3a 20 63 65 6e 74 65 72 3b 20 77 69 64 74 68 3a 38 30 30 70 78 3b 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 2d 34 30 30 70 78 3b 20 70 6f 73 69 74 69 6f 6e 3a 61 62 73 6f 6c 75 74 65 3b 20 74 6f 70 3a 20 33 30 25 3b 20 6c 65 66 74 3a 35 30 25 3b 22 3e 0a 20 20 20 20 20 20 20 20 3c 68 31 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 3a 30 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 31 35 30 70 78 3b 20 6c 69 6e 65 2d 68 65 69 67 68 74 3a 31 35 30 70 78 3b 20 66 6f 6e 74 2d 77 65 69 67 68 74 3a 62 6f 6c 64 3b 22 3e 33 30 31 3c 2f 68 31 3e 0a 3c 68 32 20 73 74 79 6c 65 3d 22 6d 61 72 67 69 6e 2d 74 6f 70 3a 32 30 70 78 3b 66 6f 6e 74 2d 73 69 7a 65 3a 20 33 30 70 78 3b 22 3e 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 0d 0a 3c 2f 68 32 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 62 65 65 6e 20 70 65 72 6d 61 6e 65 6e 74 6c 79 20 6d 6f 76 65 64 2e 3c 2f 70 3e 0a 3c 2f 64 69 76 3e 3c 2f 64 69 76 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html style="height:100%"><head><meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" /><title> 301 Moved Permanently</title></head><body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;"><div style="height:auto; min-height:100%; "> <div style="text-align: center; width:800px; margin-left: -400px; position:absolute; top: 30%; left:50%;"> <h1 style="margin:0; font-size:150px; line-height:150px; font-weight:bold;">301</h1><h2 style="margin-top:20px;font-size: 30px;">Moved Permanently</h2><p>The document has been permanently moved.</p></div></div></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49169	75.2.60.5	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 2, 2021 09:28:30.750937939 CET	318	OUT	GET /ddzw/?h2Mdq=CC4eYJ6GdM3g7jV/74DGeVNO7dTe5083KAYqQjLLOiGFZCFwrjOGC7P0JmGnSxw4GGM5lA==&_x=gVp0dvG0DtZT6do0 HTTP/1.1 Host: www.metanetgateway.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 2, 2021 09:28:31.052886963 CET	319	IN	HTTP/1.1 301 Moved Permanently access-control-allow-headers: Origin, X-Requested-With, Content-Type, Accept access-control-allow-methods: * access-control-allow-origin: * cache-control: public, max-age=0, must-revalidate content-length: 52 content-type: text/plain date: Tue, 02 Nov 2021 04:27:09 GMT age: 14481 location: https://www.metanetgateway.com/ddzw/?h2Mdq=CC4eYJ6GdM3g7jV/74DGeVNO7dTe5083KAYqQjLLOiGFZCFwrjOGC7P0JmGnSxw4GGM5lA==&_x=gVp0dvG0DtZT6do0 x-nf-request-id: 01FKFW76VGRSKD54DKFQGMATP0 server: Netlify Data Raw: 52 65 64 69 72 65 63 74 69 6e 67 20 74 6f 20 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6d 65 74 61 6e 65 74 67 61 74 65 77 61 79 2e 63 6f 6d 2f 64 64 7a 77 2f 0a Data Ascii: Redirecting to https://www.metanetgateway.com/ddzw/

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49170	162.241.253.231	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 2, 2021 09:28:36.335340977 CET	320	OUT	GET /ddzw/?h2Mdq=iXrnxWa2MIQCLF3pcDg6+qoW1dWPNK8gD+C0AcHvSyjXkMlp/HpcZgrhMm+aOjdhifJKjg==&_x=gVp0dvG0DtZT6do0 HTTP/1.1 Host: www.sarahannsartstudio.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 2, 2021 09:28:38.020910978 CET	321	IN	HTTP/1.1 301 Moved Permanently Date: Tue, 02 Nov 2021 08:28:37 GMT Server: nginx/1.19.10 Content-Type: text/html; charset=UTF-8 Content-Length: 0 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: http://sarahannsartstudio.com/ddzw/?h2Mdq=iXrnxWa2MIQCLF3pcDg6+qoW1dWPNK8gD+C0AcHvSyjXkMlp/HpcZgrhMm+aOjdhifJKjg==&_x=gVp0dvG0DtZT6do0 host-header: c2hhcmVkLmJsdWVob3N0LmNvbQ== X-Endurance-Cache-Level: 0 X-nginx-cache: WordPress X-Server-Cache: true X-Proxy-Cache: MISS

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2124 Parent PID: 596

General

Start time:	09:26:16
Start date:	02/11/2021
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:	0x13f790000
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: 2580 Parent PID: 596

General

Start time:	09:26:37
Start date:	02/11/2021
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: 2856 Parent PID: 2580

General

Start time:	09:26:45
Start date:	02/11/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	292696 bytes
MD5 hash:	11CBFA99FB5EBE8C09674E79B9834D96
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: 00000004.00000002.476798938.0000000002F90000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.476798938.0000000002F90000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.476798938.0000000002F90000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: vbc.exe PID: 1868 Parent PID: 2856

General

Start time:	09:26:46
Start date:	02/11/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	292696 bytes
MD5 hash:	11CBFA99FB5EBE8C09674E79B9834D96
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: 00000005.00000000.469999141.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.469999141.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.469999141.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.507748389.00000000002F0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.507748389.00000000002F0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.507748389.00000000002F0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000001.472000936.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000001.472000936.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000001.472000936.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.469326544.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.469326544.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.469326544.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.507790702.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.507790702.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.507790702.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.507885297.0000000000700000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.507885297.0000000000700000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.507885297.0000000000700000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1764 Parent PID: 1868

General

Start time:	09:26:51
Start date:	02/11/2021
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: 00000006.00000000.493026638.0000000009725000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.493026638.0000000009725000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.493026638.0000000009725000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.499945438.0000000009725000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.499945438.0000000009725000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.499945438.0000000009725000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: NETSTAT.EXE PID: 2076 Parent PID: 1764

General

Start time:	09:27:04
Start date:	02/11/2021
Path:	C:\Windows\SysWOW64\NETSTAT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\NETSTAT.EXE
Imagebase:	0xd30000
File size:	27136 bytes
MD5 hash:	32297BB17E6EC700D0FC869F9ACAF561
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: 00000007.00000002.666335831.00000000003A0000.00000004.00000001.sdmp, Author: Joe Security - Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.666335831.00000000003A0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com - Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.666335831.00000000003A0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group - Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.666274023.0000000000240000.00000040.00020000.sdmp, Author: Joe Security - Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.666274023.0000000000240000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com - Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.666274023.0000000000240000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group - Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.666207492.0000000000080000.00000040.00020000.sdmp, Author: Joe Security - Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.666207492.0000000000080000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com - Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.666207492.0000000000080000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2036 Parent PID: 2076

General

Start time:	09:27:07
Start date:	02/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x4ab30000
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

Joe Sandbox Cloud Basic 34.0.0 Boulder Opal